Univerzita Pardubice

Fakulta elektrotechniky a informatiky

Analýza zabezpečení podnikových sítí s protokolem IEEE 802.1X

Bc. Martin Bubeník

Diplomová práce

2018

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2017/2018**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Martin Bubeník**
Osobní číslo:	**I14243**
Studijní program:	**N2646 Informační technologie**
Studijní obor:	**Informační technologie**
Název tématu:	**Analýza zabezpečení podnikových sítí s protokolem IEEE 802.1X**
Zadávající katedra:	**Katedra softwarových technologií**

Zásady pro vypracování:

Cílem práce je analyzovat zabezpečení komunikace v podnikových sítích LAN s důrazem na analýzu používaných zabezpečených a nezabezpečených protokolů standardu 802.1X. V teoretické části autor představí principy zabezpečení podnikových sítí a podrobně představí principy a použitelnost standardu 802.1X v podnikovém prostředí. V praktické části pak autor analyzuje možnosti využití existujících nástrojů orientujících se na analýzu používaných protokolů 802.1X metodou aktivní enumerace a pasivního odposlechu. Definujte metodiku hodnocení zabezpečení sítí. Tuto metodiku aplikujte na reálné zkušební sítě. Pokud bude zjištěno využívání nezabezpečených nebo nedostatečně zabezpečených protokolů poukáže na jejich nedostatky v souladu s pravidly etického hackingu a bude provedena sada bezpečnostních testů. Na základě analýzy komunikace v LAN síti bude automaticky vygenerován protokol zaměřený na úroveň bezpečnosti provozované sítě.

Rozsah grafických prací:

Rozsah pracovní zprávy: **60**

Forma zpracování diplomové práce: **tištěná**

Seznam odborné literatury:

GEIER, James T.: Implementing 802.1X security solutions by wired and wireless networks. Indianapolis, Wiley, 2008, xxiii, ISBN 9780470168608.
MC CABE, James D.: Network analysis, architecture and design. 3rd ed. Boston: Elsevier/Morgan Kaufmann Publishers, 2007, xx, Morgan Kaufmann series in Networking.

Vedoucí diplomové práce: **doc. Ing. Tomáš Brandejský, Dr.**
Katedra softwarových technologií

Datum zadání diplomové práce: **30. října 2017**

Termín odevzdání diplomové práce: **18. května 2018**

Ing. Zdeněk Němec, Ph.D.
děkan

L.S.

prof. Ing. Antonín Kavička, Ph.D.
vedoucí katedry

V Pardubicích dne 15. listopadu 2017

Prohlašuji:

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

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

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 17. května 2018

Bc. Martin Bubeník

Poděkování

Rád bych poděkoval vedoucímu mé diplomové práce doc. Ing. Tomáši Brandejskému, Dr. za vedení a odbornou pomoc při řešení této práce.

ANOTACE

Tato diplomová práce se zabývá analýzou zabezpečení komunikace v podnikových sítí LAN s důrazem na analýzu používaných zabezpečených a nezabezpečených protokolů standardu 802.1X. Práce se věnuje principům zabezpečení podnikových sítí od jednoduchého statického způsobu zabezpečení pomocí sdíleného klíče až po pokročilé metody autentizačního protokolu EAP využívaných v podnikových sítích se zaměřením na jejich bezpečnost a rizika, vyplývající z jejich použití. V praktické části se zabývá metodikou hodnocení zabezpečení sítí, definuje vlastní metodiku. Tato metodika je základem pro vznik architektury testů pro bezpečnostní audit podnikových sítí, která je v praktické části využita při penetračním testování.

KLÍČOVÁ SLOVA

Bezpečnost sítí, bezpečnostní audit, penetrační testování, 802.1X, RADIUS, EAP

TITLE

Security analysis of corporate networks based on the IEEE 802.1X protocol

ANNOTATION

This master's thesis deals with the analysis of communication security in corporate LANs with an emphasis on the analysis of used secure and unsecured 802.1X protocols. The work deals with the principles of enterprise network security from simple static security using a shared key to advanced EAP authentication methods which are used in corporate networks, with focus on their security and the risks resulting from their use. In the practical part I deal with methodology of evaluation of network security and define my own methodology. This methodology is the basis for development of the test architecture for corporate network security audits, which is afterwards used for penetration testing in the practical part.

KEYWORDS

Network security, security audit, penetration testing, 802.1X, RADIUS, EAP

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Bezpečnost počítačových sítí je ve světě informačních technologií poslední dobou velmi často skloňovaným tématem. Pojem bezpečnost počítačových sítí pak v sobě skrývá 2 aspekty, na které musíme nahlížet: zabezpečení dat a dosažení provozuschopnosti všech systémů bez omezení. V prostředí velkých firem a institucí jsou pak tyto aspekty naprosto klíčové. Omezená funkčnost, či dokonce nedostupnost systémů může mít v kritických odvětvích nedozírné následky, kdy mohou být v ohrožení i lidské životy (např. ve zdravotnictví, dopravě). Ve firemní sféře pak nedostupnost systémů a dat znamená vysoké ztráty za ušlé zisky, neboť fungování společností je v dnešní době na tyto systémy doslova odkázáno.

S pokročilými technologiemi dochází také k masivnímu rozšiřování rychlých WLAN sítí ve standardu *IEEE 802.11ac*[17]. Díky jejich propustnosti, možnosti obsluhy velkého množství klientů a nejmodernějším WLAN standardům dokáží konkurovat metalickým LAN sítím o kapacitách gigabitových propustností. Velkému rozšíření a oblibě rychlých WLAN sítí ve značné míře napomáhá současný koncept BYOD („Bring Your Own Device“)[16] neboli využití vlastních zařízení (notebooky, tablety, smartphony a další) ve firemním prostředí. Nezávislá společnost provádějící analýzu trhu předpokládá v následujích 3 letech rapidní nárůst počtu WLAN přístupových bodů, umožňujících přenos dat s využitím nejmodernějšího standardu WLAN *IEEE 802.11ac*.

S rozvojem WLAN bezdrátových sítí je třeba mnohem více klást důraz na jejich zabezpečení. Vůči metalickým (drátovým) LAN sítím mohou mít dosah i mimo prostory společnosti a potenciálním útočníkem může být jakýkoliv náhodný kolemjdoucí. Motiv pro úspěšný útok pak může mít za cíl vyřazení interních systémů z provozu, únik firemních dat či aktuálně velmi závažná hrozba pod označením Ransomware[1].

Uveďme 2 příklady velkých úniků dat: rok 2013, maloobchodní řetězec Target v USA a únik dat osobních údajů o desítkách milionů zákazníků včetně 40 milionů čísel platebních karet. Únik podobného rozsahu postihl i v roce 2011 společnost Sony a jejich zákazníky.

O důležitosti dostatečného zabezpečení nejen citlivých osobních údajů, s nimiž firmy mohou nakládat, hovoří i aktuální směrnice evropské unie GDPR. Směrnice vstoupí

[1]Malware, jež zašifruje data na infikovaném počítači s požadavkem na zaplacení výkupného pro jejich dešifrování

v platnost v roce 2018 a striktně omezuje nakládání s osobními údaji pod hrozbou velmi vysokých pokut při jejím porušení.

WLAN sítě procházely z pohledu zabezpečení vývojem a zabezpečení, jež bylo využíváno při jejich zrodu, již dnes není dostatečné. Přesto se stále ve společnostech najdou sítě, které tímto zabezpečením disponují a vystavují se tak riziku napadení. Toto téma je proto stále vnímáno jako velmi aktuální a vzhledem k masivnímu rozvoji bezdrátových sítí v podnikových sítích LAN je i téma této diplomové práce zaměřeno na podnikové sítě postavené zejména na bezdrátových sítích WLAN.

Cíl práce

Cílem této diplomové práce je analýza zabezpečení podnikových sítí LAN s důrazem na analýzu používaných zabezpečených a nezabezpečených protokolů standardu 802.1X. Popisuje jednotlivé autentizační metody EAP z pohledu jejich bezpečnosti, poukazuje na zranitelná místa a poskytuje doporučení, jakým způsobem míru zranitelnosti snížit či úplně odstranit. V praktické části se zabývá metodikou hodnocení zabezpečení sítí a definuje vlastní metodiku, jak správně provést analýzu zabezpečení podnikové sítě s protokolem IEEE 802.1X se zaměřením na potenciální kritická, zranitelná místa metodou aktivní enumerace a pasivního odposlechu. Tato metodika je základem pro vznik architektury testů pro bezpečnostní audit podnikových sítí, která je v praktické části využita při penetračním testování nad referenční síťovou infrastrukturou simulující podnikovou síť. Výstupem bezpečnostního auditu je automaticky generovaný HTML report, zaměřený na úroveň bezpečnosti provozované sítě.

Kapitola 1 popisuje základní principy fungování bezdrátových sítí WiFi a jejich vývoj v čase z pohledu jednotlivých standardů. S vývojem standardů pro bezdrátové sítě docházelo i ke zlepšování zabezpečovacích mechanismů těchto sítí. Součástí této kapitoly je tak teoretický rozbor dostupných bezpečnostních mechanismů s poukázáním na jejich zranitelná místa. V kapitole 2 se na tyto zranitelnosti podíváme podrobněji po technicko-praktické stránce a poukážeme na způsoby, jakými je možné tyto zranitelnosti v praxi využít. Kapitola 3 se věnuje technikám zabývajícími se bezpečnostními audity a penetračním testováním. Jsou zde uvedeny způsoby, jakými je možné bezpečnostní audit provést, typy prováděných testů z pohledu způsobu provedení či znalosti o testovaném systému a popsány základním způsobem veřejně dostupné metodiky pro bezpečnostní

audit. V rámci praktické části práce je na závěr kapitoly vytvořena vlastní metodika zabývající se konkrétně auditem bezdrátových sítí s ověřováním pomocí 802.1X. Kapitola 4 navazuje na definovanou vlastní metodiku, analyzuje požadavky z ní vycházející a možnosti využití existujících nástrojů v připravované architektuře testů pro audit podnikových sítí založených na standardu 802.1X. Výsledkem analýzy vhodných nástrojů jsme pro klíčovou část architektury testů, detekci použité EAP metody, zvolili volně dostupný nástroj EAPeak, který jsme implementačně rozšířili o automaticky generovaný HTML report. Správné navržení metodiky a architektury je prakticky ověřeno v kapitole 5, která se zabývá auditem referenční podnikové sítě.

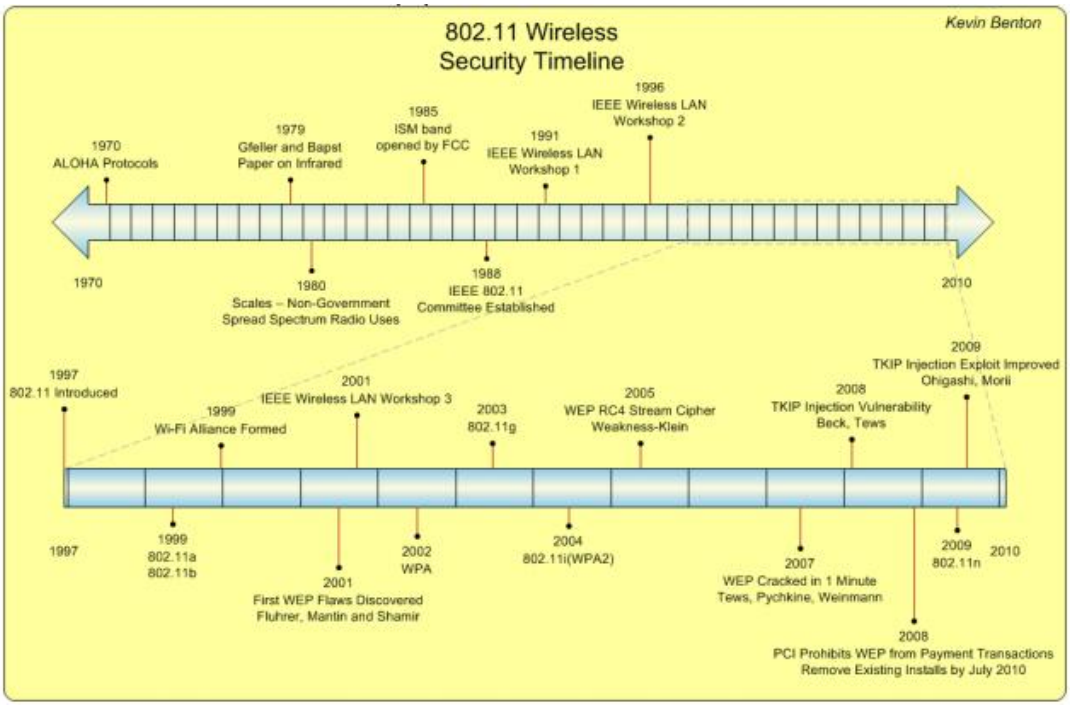
1 ZABEZPEČENÍ KOMUNIKACE S VYUŽITÍM IEEE 802.1X

Vývoj a úroveň zabezpečení WLAN bezdrátových sítí prošlo od jeho počátku po současnost velkou proměnou. Jak jsme již zmínili v úvodu, šíření signálu bezdrátových sítí nelze ohraničit pouze na určený prostor a musíme řešit jejich zabezpečení. Původní standard pro bezdrátové sítě WLAN 802.11 z roku 1997 již obsahoval první typ zabezpečení WEP (Wired Equivalent Privacy). Tento typ kryptografického algoritmu nevydržel neohrožen dlouho, již v roce 2001 byl Kalifornskou univerzitní skupinou představen dokument o nedostatcích tohoto algoritmu v použití šifrovací sady RC4 a následně byl oznámen první úspěšný útok na algoritmus WEP. Organizace IEEE, zodpovědná za standard 802.11, tak v roce 2002 představila v rámci připravovaného nového standardu 802.11i (draft) nový typ zabezpečení. Vzhledem k potřebě rychlé reakce na již děravý WEP vznikal nový algoritmus s předpokladem využití současného hardware pro bezdrátový přenos. Velmi rychle tak vznikl nový typ zabezpečení zvaný WPA (Wi-Fi Protected Access) využívající algoritmus TKIP (Temporal Key Integrity Protocol). Standard 802.11i byl ratifikován v roce 2004 s podporou zabezpečení nazvaným WPA2. Oproti původnímu předchůdci WPA využívá jiný algoritmus AES (Advanced Encryption Standard), který je do dnešní doby považován za bezpečný a doporučený pro využití v menších podnikových sítích WLAN bez vybudované infrastruktury umožňující nasazení 802.1X. Pro podnikové zabezpečení s podporou 802.1X je v kombinaci s RADIUS autentifikačním serverem jedinou bezpečnou autentizační metodou. Průběh vývoje jednotlivých algoritmů ilustruje obrázek 1 převzatý z [4].

1.1 Standard IEEE 802.11

Standard IEEE 802.11 je základem pro definici bezdrátového přenosu dat v sítích WLAN. Definuje způsob přenosu po fyzické a linkové (spojové) vrstvě 7-vrstvého síťového modelu a formu zabezpečení bezdrátových sítí. Skupina IEEE (Institute of Electrical and Electronics Engineers)[2] definovala první verzi standardu v roce 1997 v přenosovém pásmu 2,4GHz s rozprostřeným spektrem a maximální přenosovou rychlostí 2Mbit/s. Tento standard se tak stal původním standardem pro vznik nových standardů označovaných jako 802.1X

[2]https://www.ieee.org/



Obrázek 1: Vývoj jednotlivých algoritmů pro zabezpečení WLAN sítí [4]

(kde písmeno x označuje písmeno z abecedy pro pojmenování standardu). IEEE 802.11 řeší základní problém v přístupu ke sdílenému médiu (protokol CSMA/CA), který je nástupcem protokolu ALOHA, respektivě Slotted ALOHA. V drátových (metalických) LAN sítích je využíván přístup CSMA/CD [4].

Vzhledem k nízkým kapacitám byl v roce 1999 uvolněn standard **802.11b**, který umožňoval přenosové rychlosti až 11Mbit/s ve stejném přenosovém pásmu (2,4GHz). V tentýž rok byl následně IEEE doplněn standard **802.11a** umožňující přenos v pásmu 5GHz rychlostí až 54Mbit/s. Výhodou nového 5GHz pásma bylo větší množství nepřekrývajících se kanálů (8 oproti 3 v pásmu 2,4GHz). V rozšířenějším pásmu 2,4GHz pak v roce 2003 přišel očekávaný nástupce standardu 802.11b, **802.11g** s přenosovou rychlostí 54Mbit/s, v Evropě hojně využívaný a zpětně kompatibilní s 802.11b. Aktuálně nejvíc využívaný standard **802.11n** je uveden v roce 2009 a zavádí novou technologii MIMO (Multiple-Input, Multiple-output)[12], která dokáže zvýšit přenosovou kapacitu až na 600Mbit/s (teoretických) díky kombinaci více antén v rámci jednoho přístupového bodu. Norma udává možnost využití až 8 antén, v praxi se však zatím využívají většinou 3–4. Standard kombinuje možnost využití v obou pásmech, 2,4 i 5GHz.

Aktuálně posledním vydaným standardem, který je již masivně implementován v zařízeních, je **802.11ac**. Vychází z 802.11n, změny zahrnují možnost nastavení širších kanálů (80 nebo 160 MHz versus 40 MHz) v pásmu 5 GHz, více prostorových toků (až osm proti čtyřem), modulace vyššího řádu (až 256-QAM vs. 64-QAM) a přidání systému MIMO pro více uživatelů (MU-MIMO). Umožňují tak teoretický datový tok 1300Mbit/s při 80 MHz kanálech v pásmu 5GHz.

Následující tabulka uvádí základní přehled standardů pro bezdrátové sítě[3]:

Standard	**Vydán**	**Pásmo [GHz]**	**Max. rychlost [Mbit/s]**	**Fyz. vrstva**
IEEE 802.11	1997	2,4	2	DSSS a FHSS
IEEE 802.11a	1999	5	54	OFDM
IEEE 802.11b	1999	2,4	11	DSSS
IEEE 802.11g	2003	2,4	54	OFDM
IEEE 802.11n	2009	2,4 nebo 5	600	MIMO OFDM
IEEE 802.11ac	2013	2,4 a 5	866	MIMO OFDM

Tabulka 1: Přehled jednotlivých standardů IEEE 802.1X

1.2 Řízení přístupu k síti

Klíčovým tématem při budování WLAN sítí je otázka zabezpečení přístupu pouze pro autorizované uživatele, případně autorizované zařízení. K dispozici máme několik přístupů, které v této kapitole rozebereme, včetně přiblížení výhod a nevýhod jednotlivých řešení.

1.2.1 MAC adresa

Přístup k síti, který je řízený prostřednictvím jednotlivých přístupových bodů (access pointů). Každé bezdrátové zařízení je jednoznačně identifikovatelné prostřednictvím MAC adresy, která je při tomto způsobu řízení přístupu kontrolována vůči seznamu povolených adres uloženým na daném přístupovém bodě. Výhodou tohoto řešení je jednoduchost nasazení, nevýhodou je značná decentralizovanost (seznam povolených MAC adres uložený na každém přístupovém bodě). Detailněji je tato metoda popsána v kapitole 1.3.

1.2.2 Sdílený klíč

Pro přístup k síti je potřeba znát „tajný klíč“, který s využitím šifrovacích algoritmů WEP, WPA či WPA2 umožní přístup k síti. Výhodou řešení je snadné nastavení, při kompromitaci klíče je ale nutné sdělit nový klíč všem uživatelům, kteří jej musí znovu nastavit ve svých zařízeních. Nelze řídit přístup po jednotlivých uživatelích, resp. skupinách uživatelů. Více o těchto bezpečnostních mechanismech je rozebráno v kapitolách 1.4 a 1.5.

1.2.3 Certifikát, přístupové údaje

Tento přístup se využívá primárně ve firemních sítích s využitím protokolu 802.1X. Každý uživatel má svůj certifikát nebo přístupové údaje (kombinace uživatelského jména a hesla), které jsou centrálně spravovány v databázi (např. MySQL, LDAP, Active Directory apod.) a uživatel je získá při nástupu do zaměstnání. Výhodou tohoto řešení je jeho centralizace a propojení v rámci jedné uživatelovy identity napříč všemi podnikovými systémy. Jedním krokem pak administrátor může tento účet zablokovat (ať již z důvodu kompromitace či ukončení pracovního poměru) a uživatel přístup do sítě ztratí. Detailněji se tímto způsobem řízení přístupu k síti zabývá kapitola 1.6.

1.3 Skrývání SSID a filtrace MAC adres

První a nejjednodušší způsob, jak zabezpečit ochranu bezdrátové sítě je pomocí skrytí SSID a filtrováním MAC adres. SSID (Service Set Identifier) označuje pojmenování bezdrátové sítě a v konfiguraci přístupového bodu lze potlačit vysílání názvu této sítě. Ta se pak chová jako skrytá síť, není veřejně viditelná při skenování dostupných bezdrátových sítí. Předpokladem je, že se potenciální útočník nebude snažit útočit na síť, o které neví. Nevýhodou tohoto způsobu řešení je pak nutnost znát přesný název sítě, což může být pro běžné uživatele značný problém. Zároveň je nutné na klientských zařízeních ručně nastavit „profil“ pro připojení k dané síti.

MAC adresa (Media Access Control) je unikátní označení každého bezdrátového zařízení v rámci celého světa. Skládá se z 6 dvojic kombinací čísel a písmen oddělených zpravidla dvojtečkou či pomlčkou. V rámci MAC adresy první 3 dvojice označují výrobce bezdrátového zařízení, další 3 pak jeho identifikaci.

Přístup k bezdrátové síti řídí samotný bezdrátový přístupový bod, který při pokusu o asociaci (připojení) klienta k síti ověří přítomnost jeho MAC adresy v seznamu povolených adres a pokud najde shodu, připojení povolí.

Výhodou tohoto přístupu je jeho jednoduchost při zavádění i využívání, často jej upřednostňují lokální poskytovatelé přístupu do sítě Internet (ISP provideři). Nevýhodou tohoto systému je nutnost mít na každém přístupovém bodu (access pointu) vedený seznam povolených zařízení (MAC address list). Při vyšším počtu přístupových bodů je pak správa celého systému značně neefektivní.

Další stinnou stránkou tohoto přístupu je i možnost klonování MAC adres na bezdrátových zařízeních, což umožní „schovat“ pod jednu povolenou MAC adresu více zařízení a lze tak získat přístup k síti pro několik zařízení. Pokud je navíc bezdrátová síť nešifrovaná, lze MAC adresu jednoduše odposlechnout z komunikace, např. prostřednictvím volně dostupného software Wireshark[3].

Tento přístup lze kombinovat s přístupy uvedenými dále, např. s využitím zabezpečení WPA2 (kapitola 1.5.2), čímž získáme možnost vícefaktorového přístupu k síti.

Problematika skrývání SSID a filtrování MAC adres včetně výhod a nevýhod tohoto způsobu nasazení je rozebírána v kapitole 2.1.

1.4 WEP

Standard WEP (Wired Equivalent Privacy) je prvním z protokolů, který měl zabezpečit komunikaci v rámci WLAN. WEP byl součástí první verze standardu 802.11 z roku 1997 a jak již z názvu vyplývá, měl poskytovat obdobné zabezpečení bezdrátových sítí jako drátových. Ve standardu byl uveden jako nepovinný, tj. nemusel být výrobci implementován. Šifrování probíhá na druhé (linkové–spojové) vrstvě síťového modelu ISO/OSI, jež je definována ve standardu 802.11 za pomoci proudové šifry RC4 (Rivest Cipher 4).

V roce 2002 však IEEE představila návrh nového standardu 802.11i, který přichází s novým typem šifrování WPA, jenž následně zůstal jedinou variantou, jak vyřešit problémy se zranitelností WEP. V roce 2004 byl standard 802.11i ratifikován s novým, vylepšeným typem WPA2, jenž je brán jako zabezpečený dodnes. Popsán v kapitole 1.5.2.

Vzhledem k základním nedostatkům v prvopočátku celého návrhu šifrování u WEP, které vedly záhy k jeho prolomení a neodstranění příčiny (a dnes je již tento typ šifrování

[3] `http://www.wireshark.org`

dávno překonaný), jej zde uvádíme pouze pro doplnění a nebudeme se jím detailněji v této práci dále zabývat.

1.5 WPA Personal

Při vývoji nového typu zabezpečení bezdrátových sítí již bylo uvažováno nad využitím ve velkých bezdrátových sítích, typické nasazení několik desítek přístupových bodů ve velkých korporacích. V těchto případech není autentizace za pomoci sdíleného klíče vhodná, při návrhu standardu WPA tak již vznikla implementace ověřování pomocí protokolu 802.1X. Metoda pro bezdrátové sítě využívající k autentizaci sdílený klíč byla nazvána „WPA Personal“, sítě využívající ověřování pomocí 802.1X pak „WPA enterprise“, kterému je věnována samostatná kapitola 1.6.

1.5.1 WPA

WPA (Wi-Fi Protected Access) je nový standard zabývající se zabezpečením bezdrátových sítí se snahou nahradit mechanismus WEP, který byl krátce po svém uvedení prohlášen za zneužitelný. Sdružení výrobců WiFi Alliance ve snaze najít rychlé řešení nového způsobu zabezpečení přišlo v roce 2002 s mechanismem WPA, který byl součástí připravovaného standardu 802.11i(draft). Při vývoji WPA bylo zohledňováno několik aspektů:

- dopředná kompatibilita s paralelně vznikajícím standardem WPA2, jenž byl v roce 2004 ratifikován a vydán jako součást 802.11i;
- zpětná kompatibilita s mechanismem WEP (s využitím původního hardwaru s pouhým přehráním firmware);
- nahrazení zneužitelných částí implementace WEPu novými, bezpečnějšími.

WPA tak měl být pouze dočasným řešením, než bude plně připraven WPA2 a bude ratifikován standard 802.11i. Nicméně povinností výrobců zařízení bylo od roku 2003 již mít implementovanou podporu mechanismu WPA pro svá zařízení jako alternativu k zneužitelnému mechanismu WEP.

Základní slabinou mechanismu WEP bylo použití stejného sdíleného klíče všemi zařízeními. WPA využívá protokol TKIP (Temporal Key Integrity Protocol), který s každým zařízením

využívá sadu hiearchických klíčů, které se v rámci komunikace dynamicky mění. Sdílený klíč je tak použit pouze jednou při inicializaci spojení, nedochází k jeho opakování. Pro ověření integrity dat je implementován protokol MIC (Message Integrity Check) generující 64 bitový kontrolní součet. V případě, že MIC detekuje v rámci jedné minuty 2 chybné rámce, je klientské zařízení znovu asociováno k přístupovému bodu–dojde k vytvoření nových klíčů. Algoritmus WPA taktéž odolá proti útokům typu Replay[4]. Každému rámci je přiřazeno sekvenční číslo, které je s každým rámcem inkrementováno. Pokud je přijat rámec, jehož sekvenční číslo je menší než aktuální, je tento rámec zahozen.

Vzhledem k potřebě zpětné kompatibility s původním zabezpečením WEP a použitím na stejném hardware, využívá WPA stejnou proudovou šifru RC4 se 128 bitovým klíčem a 48 bitovým inicializačním vektorem. Velikost inicializačního vektoru se oproti WEP šifrování zdvojnásobila, čímž byl vyřešen problém s opakováním sekvencí. Obrázek 2 ilustruje způsob šifrování a dešifrování dat u WPA (převzato z [4]).

Autentizace

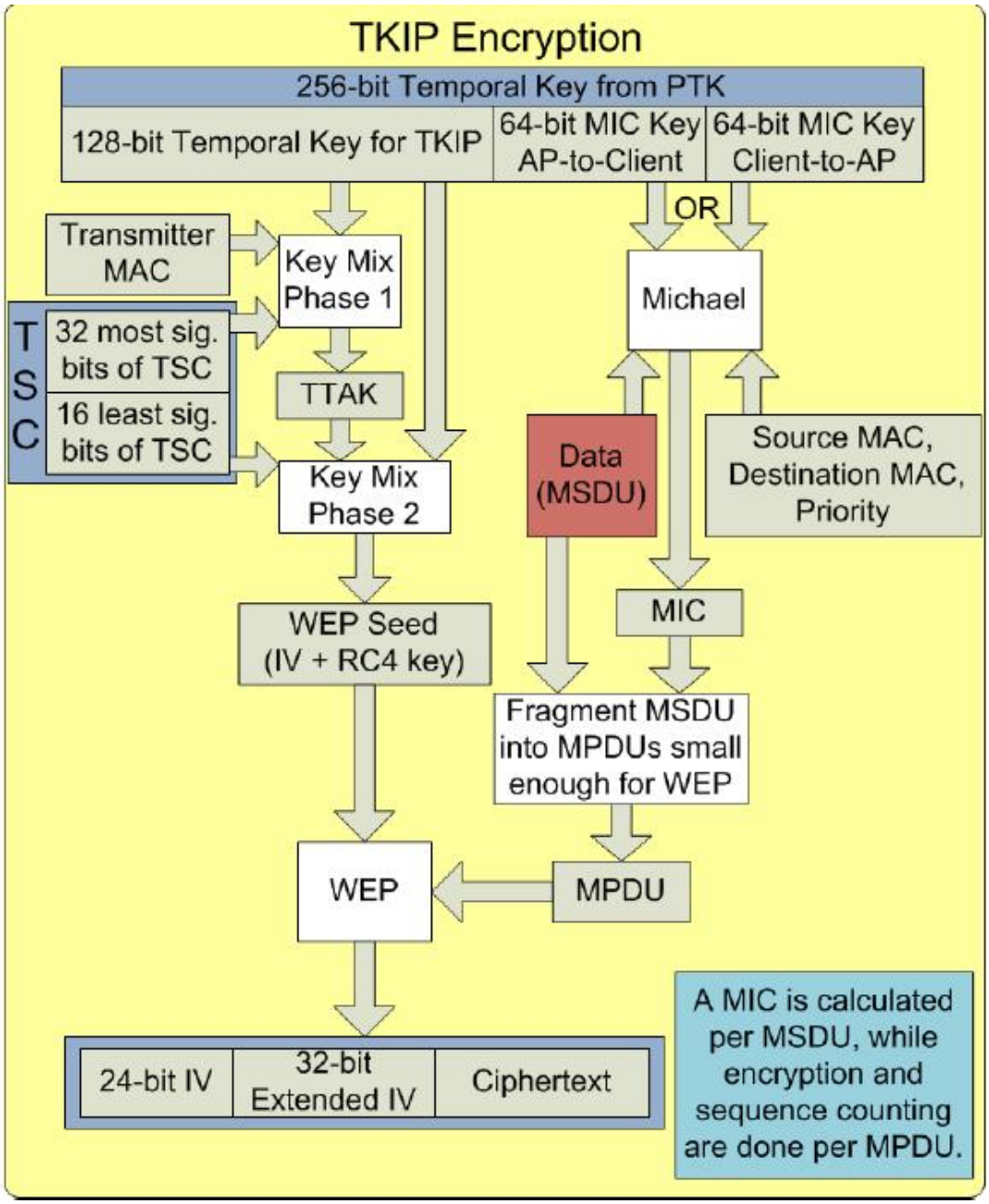
Autentizace u WPA je prováděna prostřednictvím sdíleného klíče PSK (Pre-Shared key), často označováno jako WPA-PSK. Tento klíč musí být uložen na každém zařízení, které se chce do dané sítě připojit, a zároveň na příslušném přístupovém bodě. Je využit pouze pro autentizaci, následně je s každým klientem vyměňována sada hiearchických klíčů dynamicky měněných. Pokud je sdílený klíč shodný s klíčem uloženým v přístupovém bodě, dojde k úspěšné autentizaci a asociaci zařízení. Rozdíl oproti WEP klíči je v jeho délce, která byla navýšena na 256 bitů. Do zařízení se obvykle nezadává přímo, namísto něj se zadává heslo (passphase) velikosti 8–63 znaků, které se na klíč konvertuje vztahem:

$$PMK = PBKDF2(HMAC - SHA1, passphrase, ssid, 4096, 256)$$

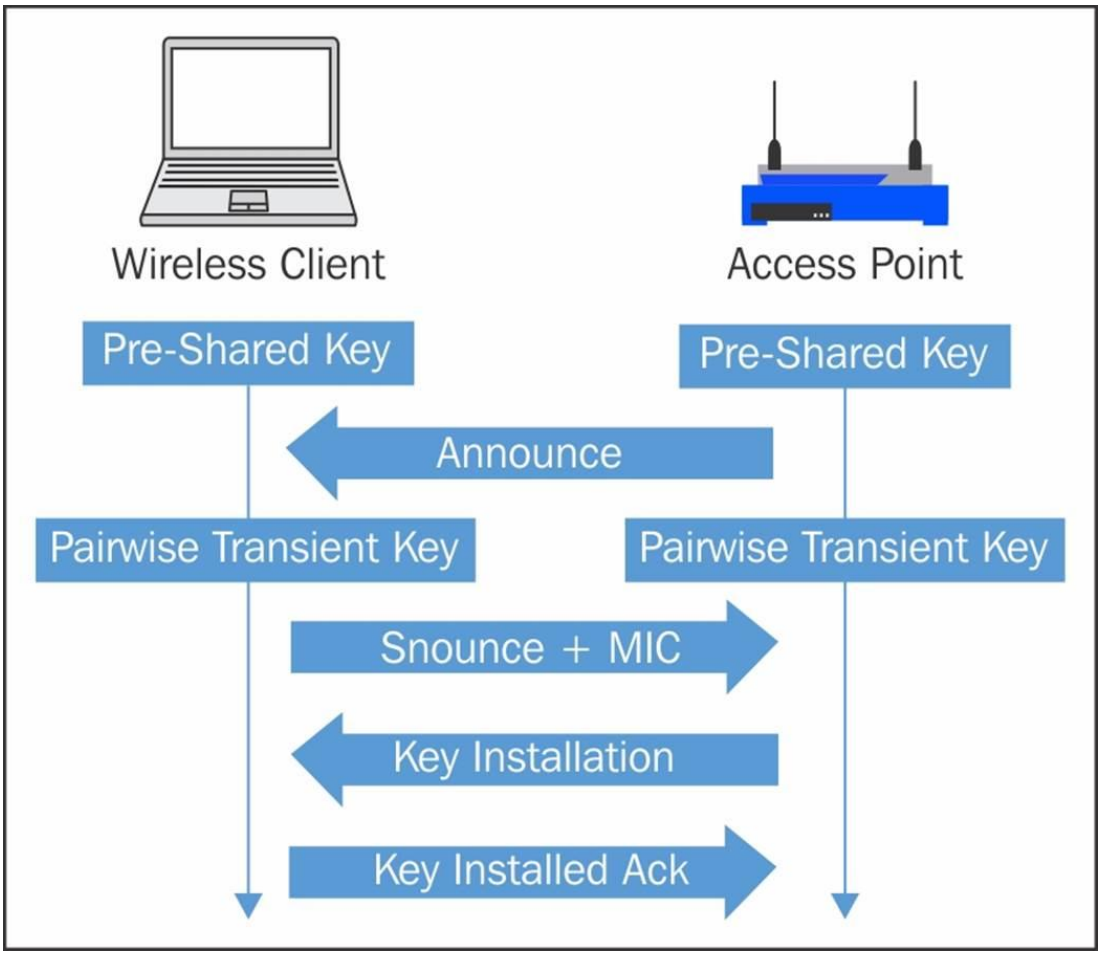
Detailní popis jednotlivých parametrů je nad rámec této práce, vysvětlení lze nalézt v publikaci [23].

Obrázek 3 ilustruje autentizaci zařízení přes Pre-Shared key (sdílený klíč) WPA. Převzato z [2].

[4]útok, který se snaží využít jeden a ten samý rámec několikrát pro získání více IV, a tím zvýšit šanci na větší a rychlejší možnost, jak dopočítat tajný klíč



Obrázek 2: Šifrování a dešifrování dat pomocí WPA a algoritmu TKIP [4]



Obrázek 3: Autentizace zařízení WPA klíčem provedená pomocí 4 kroků (handshake) [2]

Shrnutí mechanismu WPA

Ačkoliv šifrovací mechanismus WPA se snažil nedostatky svého předchůdce (WEP) odstranit, vznikal ve zrychleném procesu a implementuje v sobě stále základní bloky mechanismu WEP. Díky tomu byl vyvíjen s možným omezením a byl tvořen pro svou dobu. Tato doba již dávno pominula a je doporučeno tento mechanismus nahradit novějším WPA2, který vznikal na „čistém stole“. Vzhledem k tomu, že mechanismus WPA2 je standardizován od roku 2004, již všechna zařízení tento standard mají implementovaný a není tak důvod zůstávat u staršího WPA (až na případné extrémně výjimečné případy).

1.5.2 WPA2

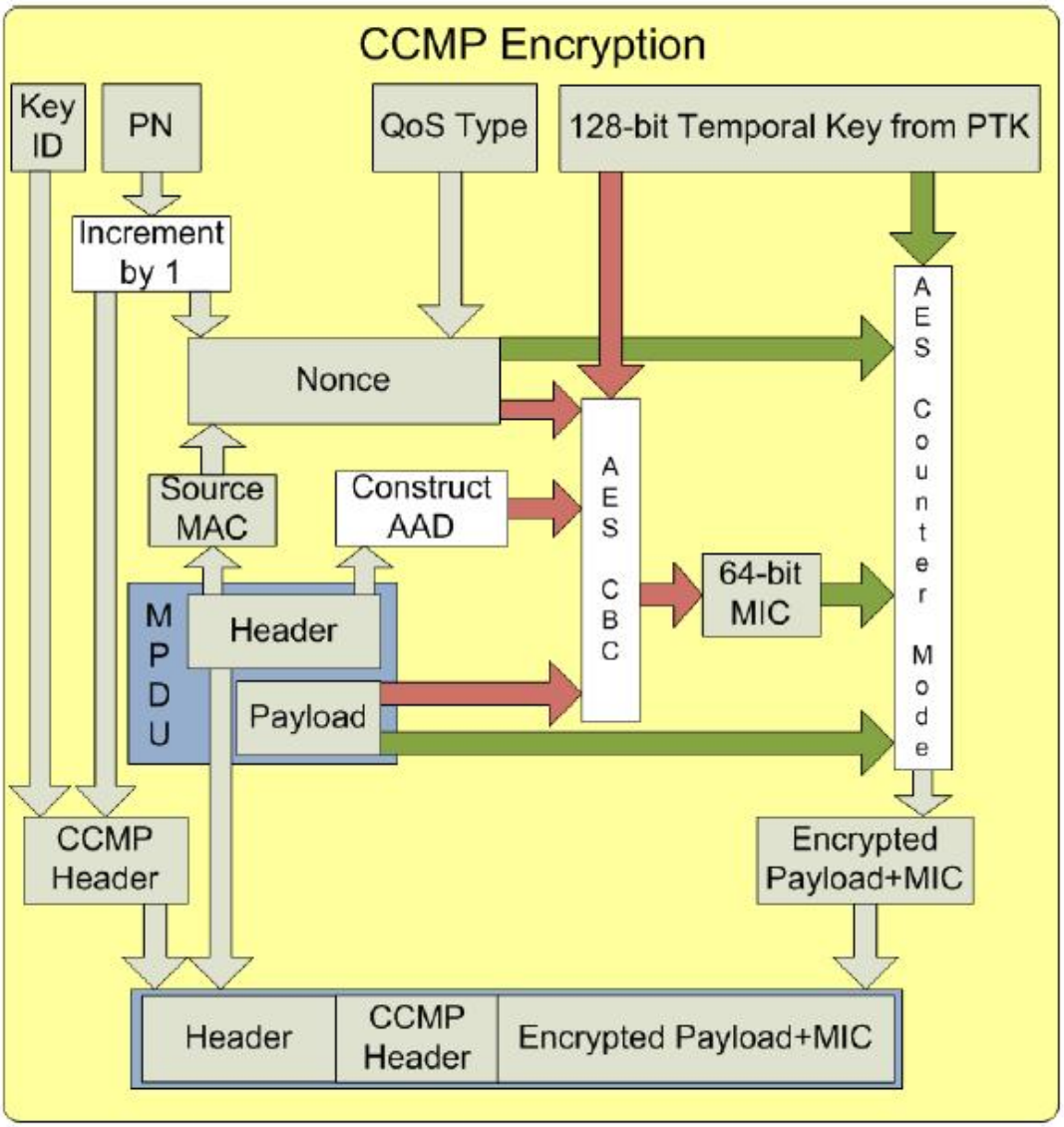
WPA2 je nástupcem mechanismu WPA, který plně implementuje standard 802.11i ratifikovaný v roce 2004. Na rozdíl od svého předchůdce WPA byl tento mechanismus vyvinut „na zelené louce“ a nevychází z žádného předchůdce. Vývojáři tak nebyli omezeni jak po technické, tak časové stránce. Vývoj probíhal paralelně s WPA a neobsahuje již žádné vazby na mechanisnus WEP.

WPA2 využívá nový protokol CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol), jehož základem je šifrovací mechanismus AES (Advanced Encryption Standard) se 128 bitovým klíčem. Integrita přenášených dat je kontrolována protokolem MIC a generováním 64-bitového kontrolního součtu, který je navíc přenášen šifrovaně. Tento mechanismus je dnes považován za důvěryhodný a odbourává všechny nedostatky předchozích metod WEP, WPA-TKIP. Vzhledem k novému šifrovacímu mechanismu AES není WPA2 zpětně kompatibilní a bylo nutné vyvinout nový hardware, který si s AES umí poradit.

Obrázek 4 ilustruje způsob šifrování a dešifrování dat u WPA2 (převzato z [4]).

Autentizace

Autentizace se u WPA2 provádí prostřednictvím sdíleného klíče PSK (Pre-Shared key) stejným způsobem jako u WPA. Pro tento klíč platí, že musí být uložen na každém zařízení, které se chce do dané sítě připojit, a zároveň na příslušném přístupovém bodě. Pokud je sdílený klíč shodný s klíčem uloženým v přístupovém bodě, dojde k úspěšné autentizaci a



Obrázek 4: Šifrování a dešifrování dat pomocí WPA2 a algoritmu AES [4]

asociaci zařízení. Rozdíl oproti WPA klíči je v jeho délce, která byla navýšena až na 256 bitů (varianty 128, 192 nebo 256 bitů). U WPA2 je však navíc ještě definovaná předběžná autentizace (pre-authentication), která umožňuje autentizovat se vůči přístupovému bodu, který ještě nemá v dosahu. Autentizace je vyslána prostřednictvím přístupového bodu, na němž je aktuálně autentizován. Tohoto mechanismu se využívá při roamingu mezi WLAN.

Dva roky po ratifikaci tohoto standardu vyšlo nařízení, které vynucuje implementaci WPA2 na všech zařízeních vyrobených od března 2006. V dnešní době tak již můžeme považovat přítomnost WPA2 ve všech přístupových bodech, včetně segmentu malých WiFi přístupových bodů. Zároveň je umožněno využívat režim WPA2 v tzv. mixed módu, který nám umožňuje připojit klientská zařízení, jež WPA2 neumí, a autentizovat je nad WPA. Podpora pro běžné operační systémy vyšla bezprostředně po rozšíření WPA2, není tedy důvod mechanismus nevyužívat.

Shrnutí mechanismu WPA2

Při návrhu mechanismu WPA2 se inženýři poučili z předešlých zranitelností a dnes je považovaný za jediný bezpečný. Splňuje tak všechny nároky na zabezpečení bezdrátových sítí–důvěrnost, integritu. Vždy je však nutné volit sdílené klíče dostatečně složité (ideálně kombinace běžných znaků, čísel, speciálních znaků v dostatečné délce), aby bylo šifrování účinné.

1.6 Podnikové zabezpečení–WPA enterprise

Řízení přístupu do rozsáhlých bezdrátových sítí prostřednictvím sdíleného klíče je z pohledu zabezpečení, správy a údržby celé sítě značně nevhodné. Sdílený klíč je tajná informace, která je uložená na každém přístupovém bodu a je společná pro všechny uživatele. Nabízí se tak riziko kompromitace této tajné informace některým ze zaměstnanců a zabezpečení bezdrátové sítě může být narušeno. Navíc řízení přístupu sdíleným klíčem snižuje možnost granurálního řízení přístupu k síti jednotlivým zaměstnancům. Uveďme jeden příklad za všechny: zaměstnanci sdělíme přístupový klíč do sítě, protože to jeho pracovní nasazení vyžaduje. Se zaměstnancem následně ukončíme pracovní poměr a v této chvíli pro odebrání přístupu do sítě bychom museli na všech přístupových bodech změnit sdílený klíč, ten

distribuovat ostatním zaměstnancům a tento postup opakovat při každé změně na pozici. Reálně vidíme, že tato cesta rozhodně není ideální.

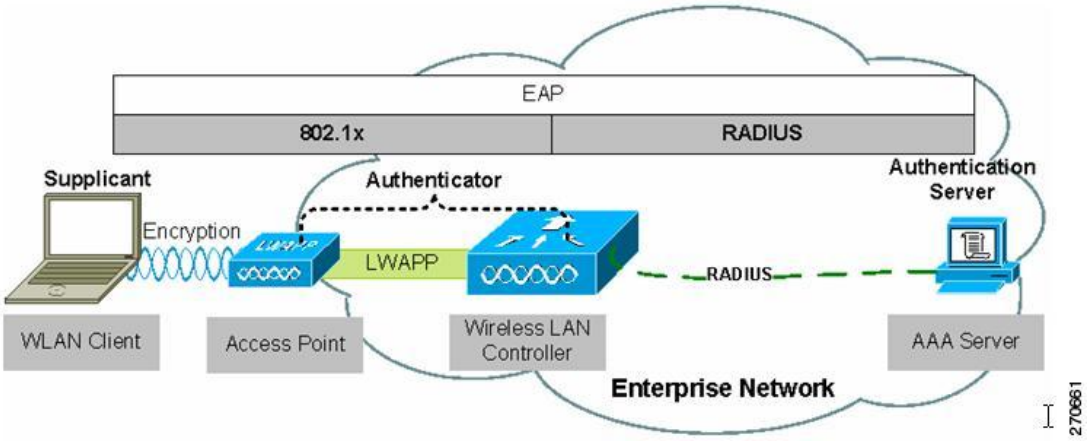
Řešením této modelové situace je autentizovat každého uživatele zvlášť prostřednictvím certifikátu nebo kombinací přítupového jména a hesla. V ideálním případě přímo integrováním do centrální databáze identit (např. databáze MySQL, adresářová služba LDAP, Active Directory, apod.). Zakázáním konkrétní identity pak znemožníme přístup i do příslušné bezdrátové sítě jedním kliknutím. Tento způsob nasazení autentizace je ve velké míře nasazován ve firemním prostředí, kde je velká míra fluktulace lidí a celý systém umožňuje pohodlnou správu a audit.

Pro tyto účely byl vyvinut protokol 802.1X, který se zabývá ověřováním identity uživatele a řízením přístupu k síti. Původně byl tento protokol napsán pro přístup k metalickým a optickým sítím LAN, v rámci velkého rozmachu bezdrátových sítí byl implementován i pro tyto sítě.

V této kapitole bude standard 802.1X popsán od komponent, ze kterých se skládá, po jednotlivé autentizační metody, jež prošly taktéž vývojem a ne všechny jsou zcela bezpečné. Na tyto nedostatky poukážeme. Oporou při psaní této kapitoly byla publikace [9].

Architektura IEEE 802.1X se skládá z následujících 3 částí, viz. obrázek 5 [8]:

- **Klient** v některých literaturách označovaný jako suplikant. Jedná se o klientské bezdrátové zařízení (notebook, telefon, tablet aj.), které chce získat přístup k bezdrátové síti. Podmínkou je podpora protokolu 802.1X na straně klientského zařízení.
- **Autentizátor** je aktivní síťový prvek (switch, bezdrátový přístupový bod) s podporou protokolu 802.1X. Tvoří prostředníka mezi klientským zařízením a autentizačním serverem. Prvek se chová jako firewall, dokud není klient autentizován, neumožní mu přístup do sítě. Pro komunikaci využívá protokol RADIUS, který bude detailněji popsán v kapitole 1.6.1.
- **Autentizační server** ověřuje identitu uživatele, kterou přeposlal autentizátor. Typicky se jedná o centrální adresářovou službu společnosti spravující identity uživatelů v rámci všech systémů–např. LDAP, Active Directory aj. Jakmile identitu uživatele ověří, odešle autentizátoru informaci o zamítnutí či povolení připojení do sítě. V případě využití RADIUS protokolu je autentizační server nazýván RADIUS serverem. Existuje mnoho implementací RADIUS serverů, uveďme alespoň nejrozšířenější.



Obrázek 5: Architektura 802.1X [8]

V komerční sféře můžeme jmenovat implementaci Network Policy Server–Server NPS z dílny společnosti Microsoft, v opensource Freeradius na platformě Linux.

1.6.1 RADIUS

Protokol RADIUS (Remote Access Dial In Users Service) je komunikační protokol mezi autentizátorem (aktivním síťovým prvkem) a autentizačním serverem (může být označován jako NAS–Network access server). Úlohou RADIUS serveru je kromě autentizace síťových prvků také jejich autorizace k síťovým službám a účtování (accounting). Díky tomu se můžeme často setkat s označením AAA protokol (Authentication, Authorization and Accounting).

Protokol RADIUS byl původně vyvinut společností Livingston Enterprises a později byl uznán jako standard IEEE pod RFC 2865 a 2866. Pro svou komunikaci využívá protokolu UDP (nespojovaný protokol transportní vrstvy) a porty 1812 pro autentizaci a 1813 pro účtování (accounting). V současné době existuje několik implementací RADIUS serveru v komerční i open-source podobě, základem typické implementace je možnost dohledávat uživatele v textových souborech, LDAP serverech či různých databází (MySQL, PostgreSQl, MS SQL apod.).

RADIUS je jako autentizační protokol běžně používán v IEEE 802.1x bezpečnostním standardu (často používán v metalických sítích poskytovatelů ISP). I když nebyl RADIUS původně vytvořen pro autentizační metody v bezdrátových sítích, vylepšuje WEP zabezpečení ve spojení s ostatními bezpečnostními metodami jako EAP-PEAP (budou rozebrány

v kapitole 1.6.2). RADIUS je rozšiřitelný a většina výrobců zařízení a software používají vlastní RADIUS implementace včetně vlastních portů, na kterých běží komunikace (např. Cisco a jeho RADIUS implementace TACACS). Alternativou k protokolu RADIUS je protokol DIAMETER. Oproti RADIUSu využívá pro komunikaci transportní vrstvu TCP namísto UDP u RADIUSU.

RADIUS server zpracovává požadavek ve 2 krocích–autentizace a autorizace. Ověřením zkontroluje identitu uživatele, tedy porovná údaje ve své databázi se zaslanými údaji. Po úspěšné autentizaci dojde k autorizaci, která rozhoduje, jaké služby budou uživateli zpřístupněny. Princip komunikace je založen na dvojici atribut-hodnota (AVP–Attribute Value Pairs), například jako pár „username“ a „Martin“.

Autentizace, autorizace, účtování

Autentizace je proces ověření totožnosti uživatele, jeho oprávněnosti připojit se k dané síti. Udělením oprávnění k připojení však nemusí nutně znamenat dostupnost všech síťových služeb. Autentizace je provedena předáním identity. Autentizaci můžeme dělit do 3 kategorií [5]:

- autentizace **znalostí**–svou identitu žadatel prokáže znalostí (např. znalostí správné kombinace uživatelského jména a hesla nebo PINu);
- autentizace **žadatelem**–žadatel dokazuje svou identitu pomocí svých vlastností, které lze prověřit (např. snímek oční zornice, otisk prstu, hlas);
- autentizace **předmětem**–identita je prokázána na základě předmětu, který žadatel vlastní (např. USB dongle, id průkaz, platební karta apod.).

Autorizace znamená udělení specifického typu služby uživateli, kterou požaduje, na základě jeho autentizace. Autorizace může být založena na omezeních, například omezení na určité hodiny v rámci dne, nebo omezení na fyzickou polohu, nebo omezení vícenásobného přihlášení jednoho uživatele. Autorizace určuje povahu služby, která je poskytnuta uživateli. Mezi typy služeb například patří: filtrování IP adres, přidělení adresy, přidělení cesty, šifrování, atd.

Účtování znamená sledování využívání síťových služeb uživateli. Tyto informace mohou být použity pro správu, plánování, účtování nebo další účely. Účtování v reálném čase je doručeno současně s využíváním zdrojů. Dávkové účtování ukládá informace o účtech,

dokud není později doručena. Běžně se sbírají informace o identitě uživatele, povaze dodaných služeb a časy počátků a konců dodaných služeb.

Při autentizaci klienta jsou využívány následující zprávy:

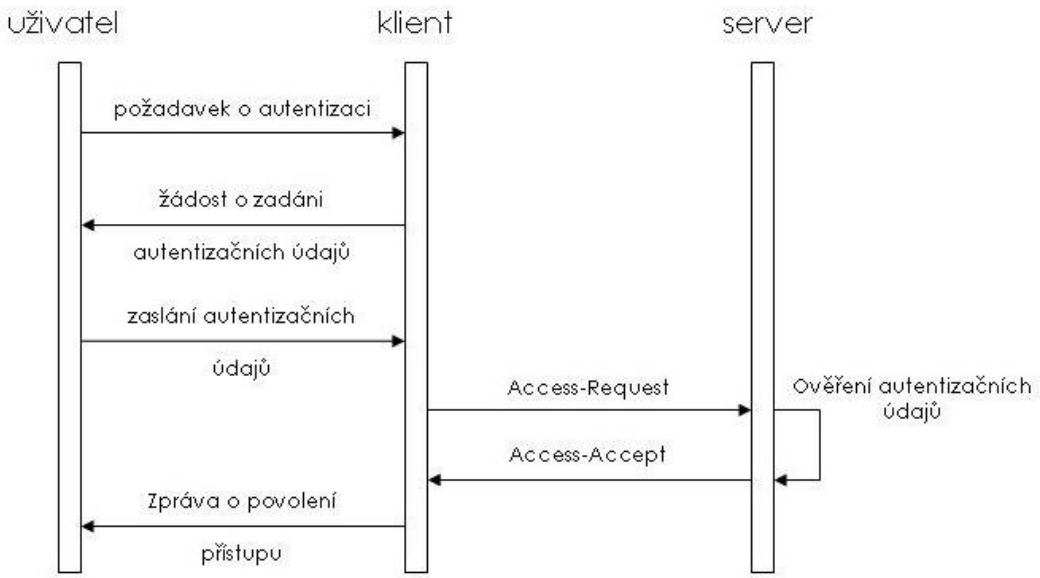
- **Access Request:** Autentizátor posílá RADIUS serveru požadavek na autentifikaci klienta obsahující uživatelské jméno, heslo a případně další údaje jako jsou IP adresa autentizátoru, číslo portu či MTU. Přenos hesla mezi RADIUS serverem a autentizátorem je zabezpečen pomocí „tajné informace“, která je sdílena mezi oběma entitami.
- **Access Reject:** RADIUS server vyhodnotil přístup jako zamítnutý, příčinou mohou být špatné přihlašovací údaje nebo klient nemá do sítě přístup (vyhodnocení autorizačním pravidlem).
- **Access Challenge:** RADIUS server si touto zprávou žádá dodatečné údaje o klientovi.
- **Access Accept:** RADIUS server vyhodnotil přístup jako povolený, klient má přístup umožněn. Zároveň mohou být k této zprávě připojeny informace potřebné pro připojení klienta do sítě (IP konfigurace).

Průběh komunikace přes RADIUS protokol je znázorněna na obrázku 6 (povolení přístupu) a 7 (zamezení přístupu). Ilustrace komunikace byly převzaty z [11] bez úprav, pojmem „uživatel“ je v textu myšleno klientské zařízení připojující se k bezdrátové síti, „klient“ je autentizátor a „server“ reprezentuje autentizační server (RADIUS).

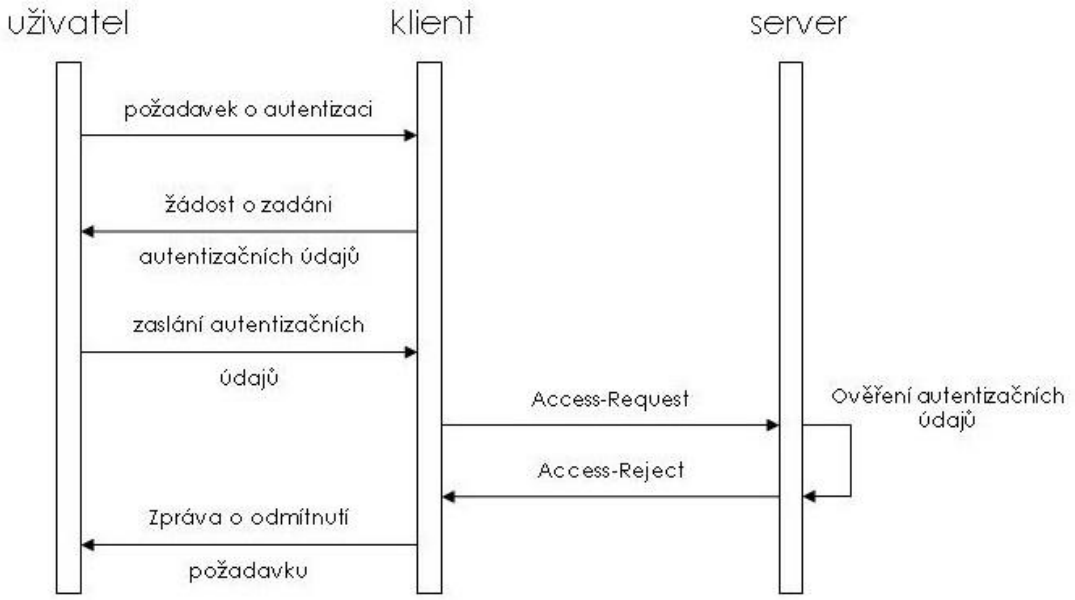
Struktura RADIUS paketu

Data mezi autentizátorem a autentizačním serverem jsou posílána prostřednictvím RADIUS paketů [19]. Struktura paketu je složena z několika atributů, které budou níže popsány:

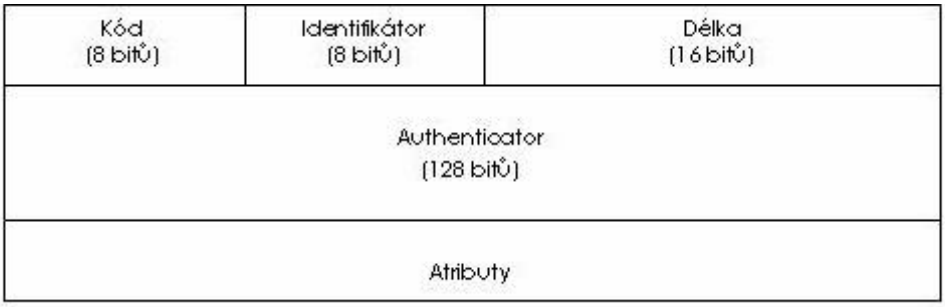
- **Kód** (8 bitů) identifikuje typ RADIUS paketu. V případě přijetí paketu s neplatnou hodnotou je tento paket zahozen. Kód může nabývat hodnot *Access-Request*, *Access-Accept*, *Access-Reject*, *Accounting-Request*, *Accounting-Response*, *Access-Challenge*.
- **Identifikátor** (8 bitů) pomáhá při správném párování odpovídajících požadavků a odpovědí.
- **Délka** (16 bitů) určuje velikost RADIUS paketu obsahující pole kód, identifikátor, délku, authenticator a atributy. Jestliže je paket menší než je určeno v poli délka, může



Obrázek 6: Povolení přístupu klienta přes RADIUS protokol [11]



Obrázek 7: Zamezení přístupu klienta přes RADIUS protokol [11]



Obrázek 8: Struktura RADIUS paketu

to znamenat chybu a paket může být zahozen. Minimální délka je 20B, maximální délka je 4096B. Viz. obrázek 8.

- **Authenticator** (128 bitů) hodnota atributu je využívána při autentizaci odpovědi z RADIUS serveru a při šifrování přenášeného hesla.
- **Atributy** nesou specifické autentizační, autorizační, informační a konfigurační detaily pro požadavky a odpovědi. Konec seznamu atributů je určen délkou RADIUS paketu. Hodnoty atributů lze vyčíst v [19].

1.6.2 EAP, EAPoL

Protokol EAP (Extensible Authentication Protocol) je základem standardu 802.1X. Původně je definován v RFC dokumentu 3748[5] nahrazující RFC 2284[6]. Poslední aktualizace protokolu EAP se pak objevila v RFC 5247[7]. Často je označován jako autentizační framework, jelikož dokáže zapouzdřit jakoukoliv autentizační metodu, která správně implementuje formát zasílaných zpráv. EAP je definován na druhé vrstvě síťového modelu ISO/OSI a jak již plyne z architektury 802.1X (obrázek 5), úkolem protokolu EAP je komunikace mezi klientským zařízením, které se chce do sítě připojit, autentizátorem a autentizačním serverem, kde je zapouzdřena do RADIUS protokolu. EAP umožňuje snadnou práci s identitou (kombinace uživatelského jména a hesla), tokeny i klientskými certifikáty. Nezajišťuje ověřování jako takové, ale transportní mechanismus pro ověřovací systémy.

[5] `https://tools.ietf.org/html/rfc3748`
[6] `https://tools.ietf.org/html/rfc2284`
[7] `https://tools.ietf.org/html/rfc5247`

Komunikace mezi klientským zařízením a autentizátorem při procesu připojování do sítě využívající autentizaci 802.1X je popsána sledem následujích zpráv:

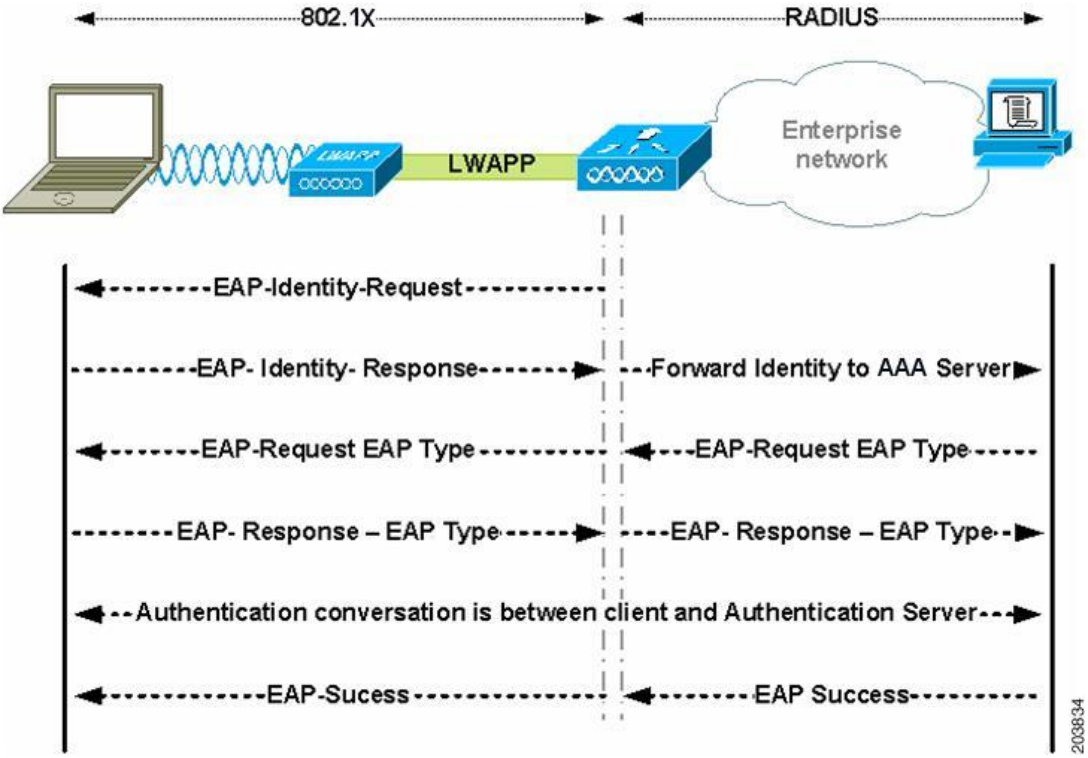
1. **EAPOL-Start:** Klientské zařízení se chce připojit do sítě, vyšle požadavek na připojení.
2. **EAP-Request-Identity:** Autentizátor odpoví a žádá klienta o předložení identity.
3. **EAP-Response-Identity:** Klient zasílá svou identitu (uživatelské jméno a heslo, certifikát apod.).
4. **EAP-Request-Method:** Autentizátor přepošle klientovi informace o zvolené EAP metodě, v závislosti na této metodě může zpráva obsahovat challenge řetězec.
5. **EAP-Response-Method:** Klient potvrdí použití dané metody a případně předloží challenge řetězec.
6. *Volitelné v závislosti na metodě:* Probíhá výměna a kontrola certifikátů.
7. **EAP-Success:** V případě úspěšného a validního ověření je klient autentizován a je mu povolen přístup autentizátorem do sítě, jinak EAP-Failure.
8. **EAPOL-Key:** V případě nastaveného šifrování v síti (WEP nebo WPA) proběhne výměna a generování klíčů.

Komunikaci a pořadí zasílání zpráv u EAP protokolu ilustruje obrázek 9 [8].

Jak jsme již zmínili v úvodu kapitoly 1.6.2, protokol EAP pouze zapouzdřuje jednotlivé metody, které fakticky řeší proces autentizace. V průběhu vývoje vzniklo těchto metod kolem 40 typů, ne všechny se ale začlenily do praxe a byly implementovány ve všech hlavních operačních systémech. Seznam všech typů metod je přiložen v příloze 5.6.2. Uveďme tedy ty majoritní, s nimiž se dnes můžeme setkat a nezůstaly pouze vymyšlené v teoretické rovině:

- **EAP-MD5**
- **EAP-PEAP**
- **EAP-LEAP**
- **EAP-TLS**

Výše vyjmenovanými metodami se detailně zabývají kapitoly 1.6.3 až 1.6.7.

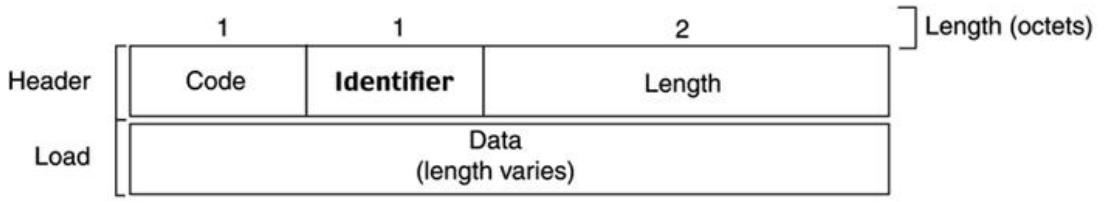


Obrázek 9: Komunikace zasíláním zpráv u EAP [8]

Struktura EAP paketu

Data mezi klientem, autentizátorem a autentizačním serverem jsou posílána prostřednictvím EAP paketů [1]. Struktura paketu je složena z několika atributů, které budou níže popsány:

- **Kód** (8 bitů) identifikuje typ EAP paketu. V případě přijetí paketu s neplatnou hodnotou je tento paket zahozen. Kód může nabývat hodnot *Request (1)*, *Response (2)*, *Success (3)*, *Failure (4)*.
- **Identifikátor** (8 bitů) pomáhá při správném párování odpovídajících požadavků a odpovědí.
- **Délka** (16 bitů) určuje velikost EAP paketu.
- **Data** nesou specifické autentizační, autorizační, informační a konfigurační detaily pro požadavky a odpovědi. Hodnoty atributů lze vyčíst v [1].



Obrázek 10: Struktura EAP paketu

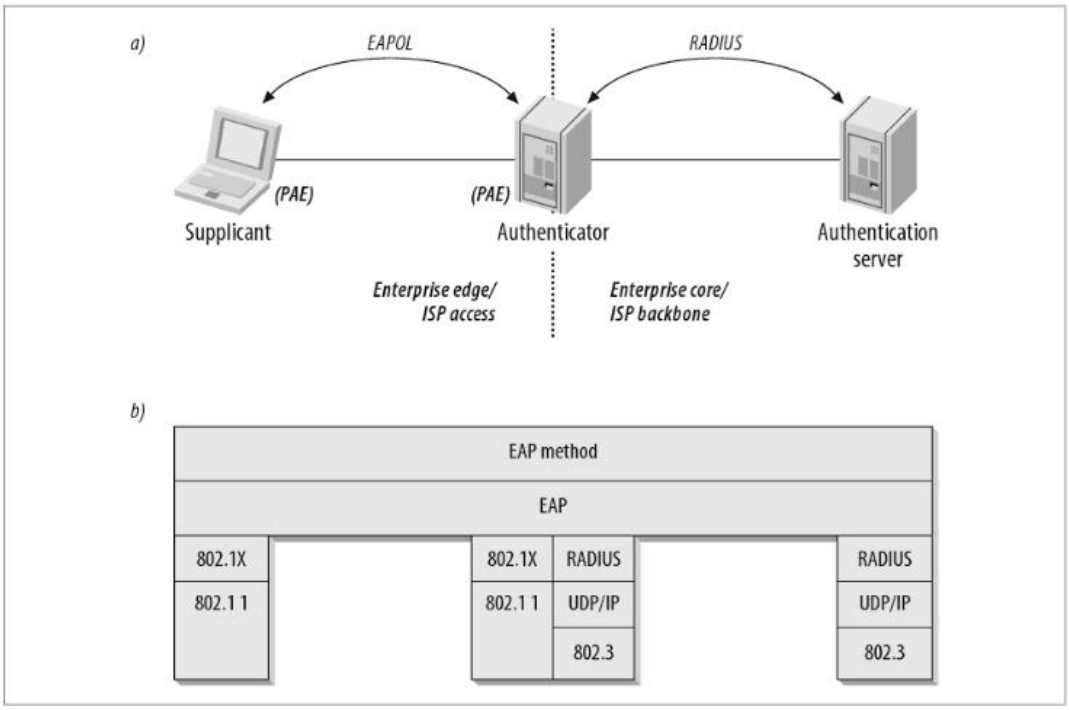
EAPoL

Vzhledem k tomu, že protokol EAP není zprostředkující protokol, ale pouze definuje formát zasílaných zpráv, bylo nutné řešit jeho zapouzdření pro přenos přes síť. Vznikl tak protokol EAPoL (EAP over LAN), který nejprve definoval přenos přes metalické sítě LAN (IEEE 802.3 ethernet) a později byl upraven pro přenos v bezdrátových sítích IEEE 802.11 WiFi. Na rozdíl od EAP paketů prochází EAPoL pakety pouze mezi klientským zařízením a autentizátorem. Jsou definovány následující typy EAPoL paketů:

- **EAP-Packet:** typ 0, zapouzdřuje EAP paket;
- **EAPOL-Start:** typ 1, značí zahájení komunikace ze strany klienta a dává autentizátoru najevo, že chce být autentifikován;
- **EAPOL-Logoff:** typ 2, klient dává autentizátoru na vědomí, že chce být odpojen od sítě. Autentizátor na základě toho nastaví zpět port do neautorizovaného stavu a čeká na autentizaci dalšího klienta;
- **EAPOL-Key:** typ 3, pokud využívá bezdrátová síť šifrování dat pomocí WEP či WPA(2), slouží tento paket k předání klíčů mezi klientem a autentizátorem;
- **EAPOL-Encapsulated-ASF-Alert:** paket sloužící pro rozesílání upozornění, např. SNMP trap přes neautorizované porty.

Komunikační protokoly v rámci standardu 802.1X–shrnutí

V kapitolách 1.6.1 a 1.6.2 jsme popsali jednotlivé protokoly, které mechanismus 802.1X využívá. Jádrem celého ověřovacího mechanismu je protokol RADIUS, který můžeme označit jako „backend“ nebo výkonnou část ověřovacího mechanismu. Komunikaci s klientskými zařízeními (nazvěme ji „frontend“ nebo funkční část) pak zaštiťuje protokol EAP následně



Obrázek 11: Využití jednotlivých protokolů u 802.1X autentizace [14]

zapouzdřený do protokolu RADIUS. Shrnutí zapouzdření a využití jednotlivých protokolů mezi klientem, autentizátorem a autentizačním serverem znázorňuje obrázek 11 [14].

Roaming a 802.1X

V rozsáhlých WiFi sítích je pro dobré pokrytí bezdrátovým signálem nutné využití několika přístupových bodů, které signál rovnoměrně distribují. Vzhledem k tomu, že si klientská zařízení vždy hledají přístupový bod s nejlepší úrovní signálu, může docházet k plynulému přechodu připojených klientů mezi jednotlivými přístupovými body. Toto chování se v bezdrátových sítích nazývá roaming. Podpora pro roaming musí být implementována přímo v každém přístupovém bodě a zároveň se s tímto požadavkem muselo počítat při úpravě standardu 802.1X pro využití v bezdrátových sítí.

Roaming tak vyžaduje:

- snadný přechod z bezdrátového připojení k drátovému a naopak;
- přechod z jednoho přístupového bodu s nízkou úrovní signálu k jinému přístupovému bodu s lepším pokrytím.

V procesu přechodu mezi jednotlivými přístupovými body tak dochází k deasociaci a reasociaci k novému přístupovému bodu. V případě nasazení autentizace přes standard 802.1X by to tak znamenalo velkou latenci a odpadnutí připojení k síti po značně dlouhou dobu (30 sekund a více). Technika pojmenovaná jako „Session resumption“ redukuje čas potřebný pro znovupřipojení k síti při autentizaci přes 802.1X. Tato technika je podporována metodami EAP-TLS, EAP-FAST a EAP-PEAP.

1.6.3 EAP-MD5

Metoda EAP-MD5 je jedna z nejjednodušších metod poskytující ověření identity (umí ověřovat pouze na základě uživatelského jména a hesla). Je definována v RFC 3748[8] a jejím základem je přenos hesla ve formě MD5 hashe (Message-Digest algoritmus). Uživatelské jméno je přenášeno v otevřené podobě. A právě způsob přenosu hesla formou MD5 hashe jí nabízí pouze minimální zabezpečení. MD5 hash je náchylný na útok hrubou silou a slovníkový útok. Metoda EAP-MD5 navíc podporuje pouze jednosměrnou autentizaci klienta vůči serveru, autenticita serveru ale již ověřena není. Je tu tak prostor pro útok typu Man-in-Middle. Zároveň metoda nepodporuje výměnu dynamických klíčů (WEP, WPA) v rámci komunikace mezi klientem a přístupovým bodem. Lze použít pouze statické klíče WEP, které neposkytují dostatečné zabezpečení, viz. předchozí kapitola o WEP 1.4 a WPA 1.5. Obecně ji tak nelze z výše popsaných důvodů považovat za bezpečnou a její podpora ze strany vývojářů moderních operačních systémů tak již není. Uveďme jeden příklad za všechny–nejrozšířenější operační systém Windows již ve své verzi Vista z roku 2007 tento protokol přestal podporovat[9].

Průběh autentizace prostřednictvím metody EAP-MD5:

- Autentizátor zašle klientovi výzvu pro zadání identity (EAP-Request-Identity).
- Klient odpoví zprávou EAP-Response-Identity obsahující uživatelské jméno.
- Autentizátor pošle klientovi MD5 Challenge, náhodně vygenerovaný řetězec (EAP-MD5-Challenge).
- V případě, že klient nechce použít metodu EAP-MD5, pošle autentizátoru zprávu Legacy-Nak, jež obsahuje typ metody, kterou by rád využil.

[8] `https://tools.ietf.org/html/rfc3748`

[9] `http://support.microsoft.com/kb/922574`

- Klient vytvoří MD5 response řetězec, který získá aplikováním hashovací funkce MD5 nad konkatenací identifikačního čísla MD5 challenge rámce, hesla a MD5 challenge řetězce.
- V případě úspěšné autentizace RADIUS serverem je klient úspěšně autentizován (EAP-Success); v opačném případě přijde EAP-Failure a přístup do sítě zůstane zakázán.

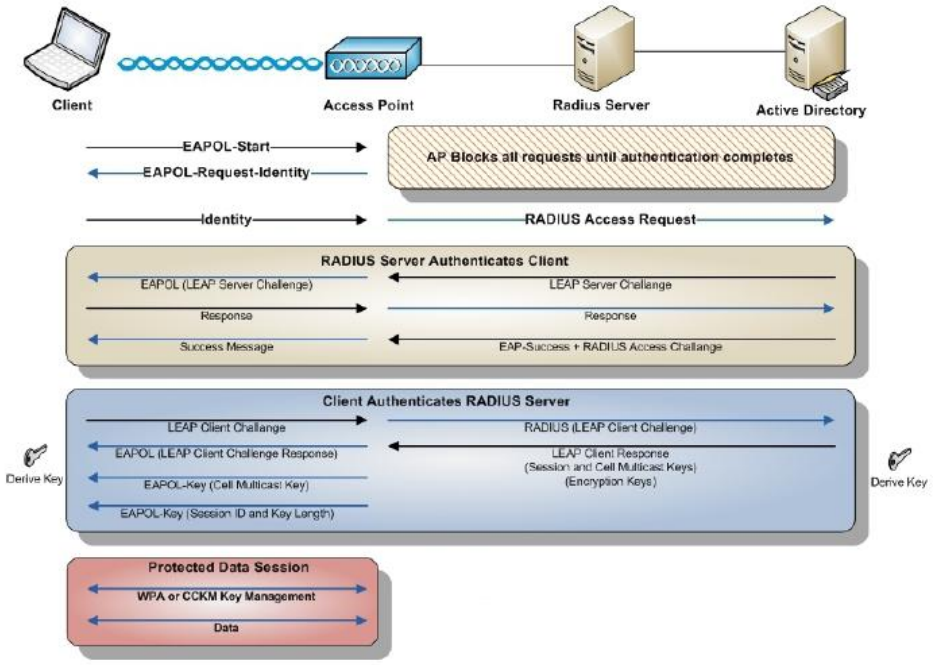
V kapitole 2.2.1 jsou detailněji popsány možnosti, jak lze u metody EAP-MD5 zneužít její zranitelnosti a odhalit tak přístupové údaje uživatele.

1.6.4 EAP-LEAP

Autentizační metoda EAP-LEAP (Lightweight Extensible Authentication Protocol) je proprietární řešení od společnosti Cisco. Byla vydána v roce 2000 jako dočasné řešení před ratifikací standardu 802.11i. Jak již název napovídá, snahou bylo vytvořit odlehčenou verzi metody se snadnou použitelností. S metodou EAP-MD5 má společnou jednu vlastnost– autentizace probíhá na základě uživatelského jména a hesla. I když uživatelské jméno je stále přenášeno v čitelné podobě se zprávou EAP-Response-Identity. Na rozdíl od metody EAP-MD5, kde je využíván CHAP (Challenge-Handshake Authentication Protocol) pro autentizaci klienta, vůči serveru využívá LEAP modernizovaný MS-CHAPv1 publikovaný v roce 1998 v RFC 2433[10]. Jedná se o první verzi vydanou pod hlavičkou společnosti Microsoft. I když tato verze ověřování podporovala pouze ověření klienta vůči serveru a neumožňovala ověření autenticity serveru (obousměrná autentizace), byla tato funkcionalita společností Cisco pro metodu LEAP doimplementována. Vzhledem k proprietárnímu řešení nebyl ale způsob, jakým to bylo provedeno, zveřejněn. Díky vzájemné autentizaci je tak metoda LEAP odolná proti útoku Man-in-the-Middle. LEAP navíc oproti metodě EAP-MD5 podporuje dynamickou výměnu šifrovacích klíčů mezi klientem a autentizátorem–klíče jsou měněny při každé autentizaci.

Achillovou patou metody LEAP je stále způsob, jakým je posíláno heslo pro ověření. Stejně jako u metody EAP-MD5 je posíláno nezabezpečeně prostřednictvím challenge a challenge-response řetězce. Při znalosti generování těchto řetězců lze slovníkovým útokem heslo odhalit. Detailněji se problematikou zabývá kapitola 2.2.2. V roce 2004 pak byl zveřejněn exploid ASLEAP využívající tuto zranitelnost [25]. Metodu LEAP tak nelze

[10] `https://tools.ietf.org/html/rfc2433`



Obrázek 12: Autentizace prostřednictvím metody EAP-LEAP [6]

považovat za bezpečnou a společnost Cisco doporučuje přejít na novější metodu EAP-FAST, která byla uveřejněna v roce 2007 jako oficiální nástupce metody EAP-LEAP, nebo alespoň využívat dostatečně silná hesla, v případně nutné potřeby zůstat u metody EAP-LEAP.

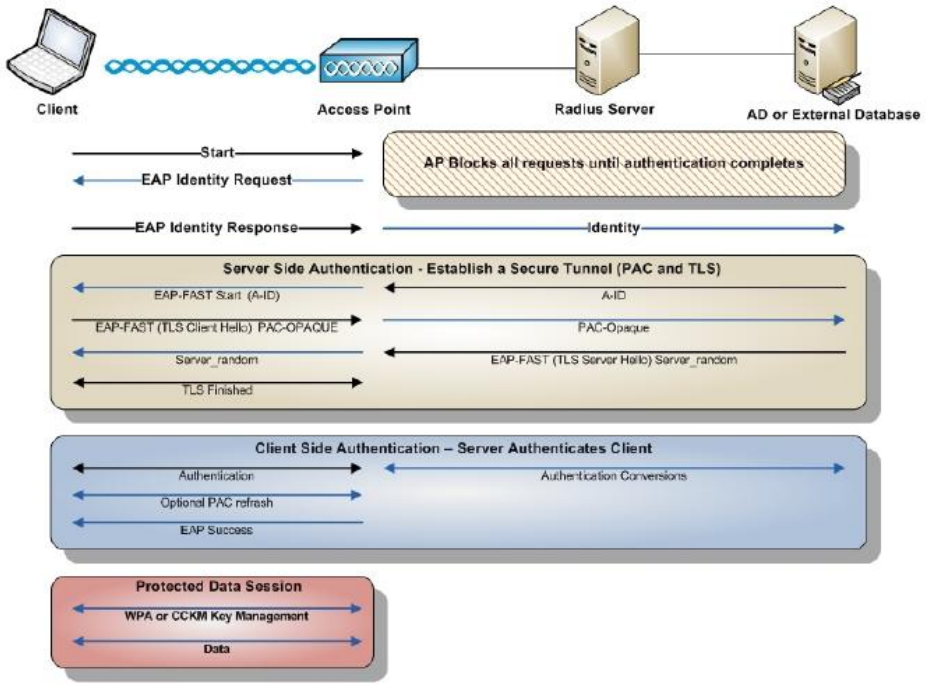
Proprietárnost řešení metody EAP-LEAP měla za následek i absenci nativní podpory v operačních systémech Windows. Pro použití tak musela být podpora doinstalována prostřednictvím softwaru třetí strany.

Proces autentizace metodou EAP-LEAP ilustruje obrázek 12 [6].

1.6.5 EAP-FAST

Metoda pro ověřování EAP-FAST (Flexible Authentication via Secure Tunneling) byla vyvinuta jako proprietární společností Cisco a oficiálně označena jako nástupce zneužitelné metody EAP-LEAP. V roce 2007 však byla tato metoda ratifikována IETF v rámci RFC 4851[11]. Při návrhu nové metody byl brán v potaz důraz na zapouzdření celé EAP komunikace do zabezpečeného tunelu (Transport Level Security–TLS tunel) bez nutnosti použití certifikátů. Oproti své předchůdkyni je metoda EAP-FAST v procesu autentizace rozdělena

[11] `http://tools.ietf.org/html/rfc4851`



Obrázek 13: Autentizace prostřednictvím metody EAP-FAST [6]

na 2, resp. 3 části (nultá část je nepovinná, bude rozebráno dále). V první části dojde k sestavení přímého PtP (point-to-point) spojení mezi klientem a autentizačním (RADIUS) serverem bez účasti autentizátoru. Vytvoření tunelu je založeno na tzn. unikátním klíči (PAC–Protected Access Credentials), který je unikátní pro každého uživatele a vytvořen přímo na RADIUS serveru [7]. Distribuce PAC klíče ke klientovi je prováděna pomocí nulté fáze, tzv. PAC provisioning. Nicméně je možné distribuci PAC klíče řešit i manuálně a nultou fázi nevyužívat.

Jakmile je zabezpečený tunel mezi klientem a RADIUS serverem sestaven (úspěšné dokončení fáze 1), přichází na řadu fáze 2, a to autentizace uživatele. Ta probíhá přes zabezpečený TLS tunel s využitím metody MS-CHAPv2 umožňující vzájemnou autentizaci. Proces autentizace metodou EAP-FAST ilustruje obrázek 13 [6]. Jednotlivé fáze metody EAP-FAST jsou znázorněny přehledně v následující tabulce:

Metoda EAP-FAST je tak díky TLS tunelu odolná vůči útokům typu Man-in-Middle, vzhledem k zabezpečenému přenosu hesel i slovníkový útok není možný. Zranitelnost metody EAP-FAST může nastat při nastaveném automatickém PAC provisioningu (automatické distribuce PAc klíče na klienty). Útočník může získat PAC klíč a na základě něho kompromitovat přihlašovací údaje uživatele. Tato zranitelnost se dá odstranit manuální

Fáze	Funkce	Vyžaduje
0	Přenos PAC klíče	Přenos pomocí Diffie-Hellman protokolu
1	Vytvoření tunelu	Potřeba PAC klíče (jedinečný pro každého uživatele)
2	Autentizace uživatele	Autentizace uživatele jménem a heslem

Tabulka 2: Přehled jednotlivých fází metody EAP-FAST

distribucí PAC klíče nebo využitím serverových certifikátů pro nultou fázi distribuce PAC klíčů (volitelně). Podpora EAP-FAST není v OS Windows nativní, je potřeba doinstalovat jako modul. V OS Linux a Apple OS je podpora zajištěna (u MacOS X od verze 10.4.8).

1.6.6 EAP-PEAP

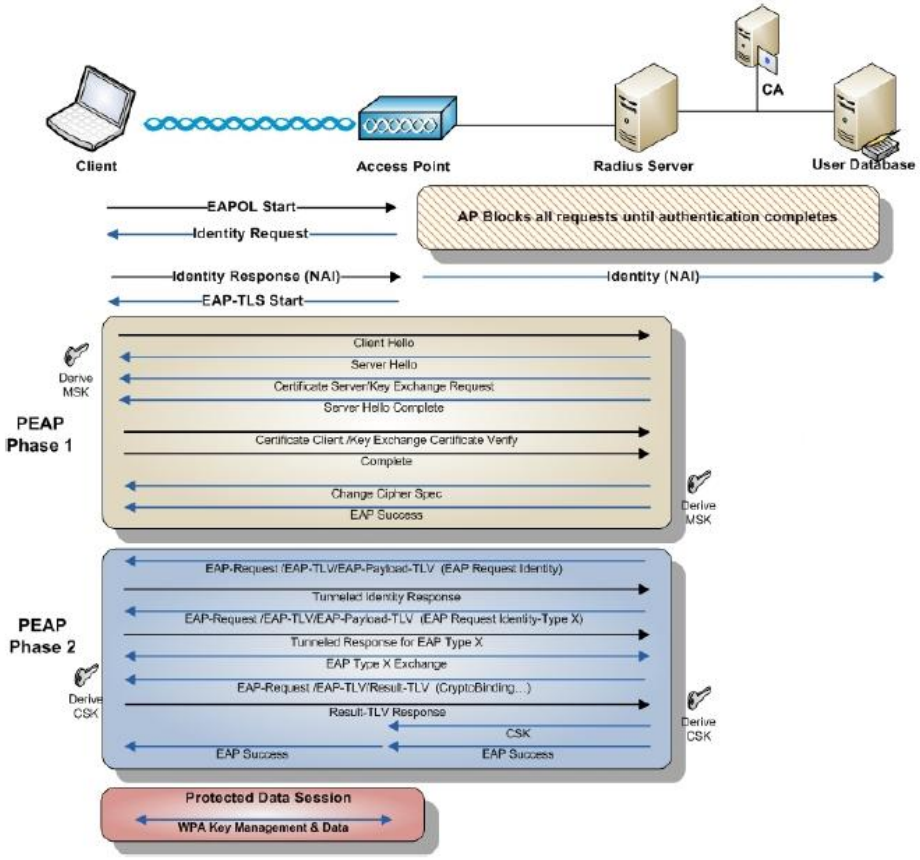
Metoda EAP-PEAP (Protected Extensible Authentication Protocol) byla vyvinuta v roce 2002 společnostmi Cisco Systems, Microsoft a RSA Security. Jak již z názvu vyplývá, její snahou bylo odstranění všech rizik, kterými metody popsané v kapitolách 1.6.3 až 1.6.5 trpěly. Zároveň byl kladen důraz na jednoduchost implementace a nasazení se snahou o co nejvyšší rozšiřitelnost. Framework EAP při svém návrhu předpokládal nasazení v rámci zabezpečených kanálů (jak fyzických, tak komunikačních). Metoda EAP-PEAP tento předpoklad splňuje, zapouzdřuje EAP do šifrovaného Transport Layer Security (TLS) tunelu.

EAP-PEAP pro sestavení TLS šifrovaného tunelu vyžaduje pouze certifikát na straně serveru, na klientské straně není vyžadováno žádné specifické nastavení, nahraný klíč, apod. To snižuje náročnost na implementaci, nasazení a správu zároveň ve srovnání s předchozími metodami. EAP-PEAP podporuje dynamickou výměnu klíčů, vzájemnou autentizaci a je ve své podstatě implementovaný ve všech rozšířených OS. Ve Windows se poprvé objevil u Windows XP.

Významným rozdílem metody EAP-PEAP od ostatních je fakt, že specifikuje pouze řetězení EAP mechanismů, ale ne žádné konkrétní metody pro autentizaci. EAP-PEAP tak řeší pouze vnější zabezpečení, vnitřní je již na jednotlivých mechanismech. Nejrozšířenějšími mechanismy pro autentizaci jsou metody:

- **EAP-PEAPv0(EAP-MSCHAPv2)**
- **EAP-PEAPv1(EAP-GTC)**

Proces autentizace metodou EAP-PEAP ilustruje obrázek 14 [6].



Obrázek 14: Autentizace prostřednictvím metody EAP-PEAP [6]

EAP-PEAPv0(EAP-MSCHAPv2)

PEAPv0 je specifikován v IETF draftu[12] vydaným společností Microsoft v roce 2002. Pro autentizaci je využita metoda MS-CHAPv2 (tedy Challenge Handshake Authentication Protocol version 2), která umožňuje dvoufázovou autentizaci, ověření klienta vůči serveru a autenticitu serveru. Důležitou podmínkou použití metody je správné nasazení sady kořenových certifikátů na straně klientského zařízení, aby mohlo dojít k validnímu ověření certifikátu, kterým se server prokazuje (obrana proti útoku typu Man-in-Middle).

S metodou EAP-TLS je PEAPv0/EAP-MSCHAPv2 dnes celosvětově nejrozšířenější metodou pro ověřování. Je implementována většinou výrobců klientských a serverových prvků, což umožňuje relativně snadné nasazení v síti.

EAP-PEAPv1(EAP-GTC)

PEAPv1 je specifikován v IETF draftu[13] a [14] vydaným společností Cisco. Metoda měla zajišťovat interoperabilitu s existujícími autentizačními systémy s tokenovými kartami a adresáři prostřednictvím šifrovaného kanálu. I když se společnost Microsoft podíla na vývoji této metody, nikdy ji oficiálně nepodporovala, což znamenalo její absenci v rámci OS Windows. Cílem společnosti Cisco bylo vyvinout metodu, jež bude druhou variantou k metodě EAP-MSCHAPv2. Primárně však ale Cisco stále prosazovalo svou metodu EAP-FAST, k masivnímu rozšíření tak nikdy nedošlo.

1.6.7 EAP-TLS

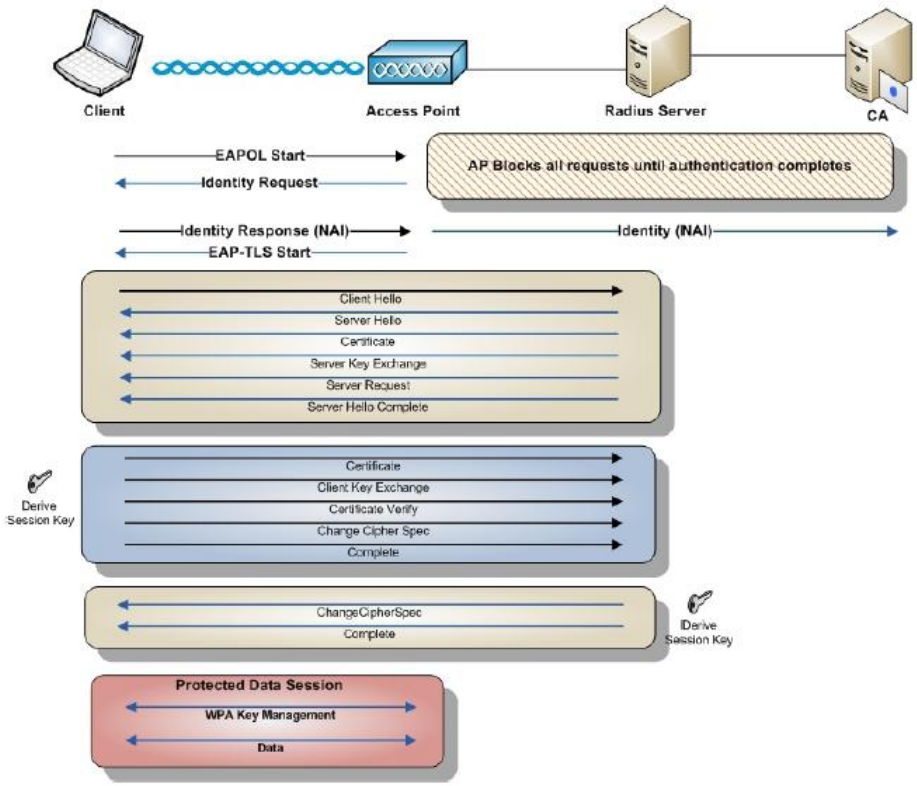
Metoda EAP-TLS (EAP-Transport Layer Security) je specifikována v RFC 5216[15] (v době psaní této práce (červenec 2017) poslední RFC zabývající se touto metodou), byla první metodou plně certifikovanou WiFi Aliancí pro použití v bezdrátových sítích využívající šifrované TLS spojení mezi klientem a RADIUS serverem. Díky tomu se i do značné míry stala podporovanou napříč všemi výrobci hardware. Implementace metody EAP-TLS je založena na vzájemné autentizaci klienta a RADIUS serveru prostřednictvím X.509 certifikátů. Ověření pomocí certifikátů je v této metodě povinné a nahrazuje

[12] `https://tools.ietf.org/html/draft-kamath-pppext-peapv0-00`

[13] `https://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-00`

[14] `https://tools.ietf.org/html/draft-josefsson-pppext-eap-tls-eap-05`

[15] `https://tools.ietf.org/html/rfc5216`



Obrázek 15: Autentizace prostřednictvím metody EAP-TLS [6]

ověření uživatelským jménem a heslem. To značí ve velké míře dodatečné náklady na vybudování infrastruktury pro vlastní certifikační autoritu, distribuci kořenových certifikátů a bezpochyby i náklady po stránce finanční (zakoupení certifikátů podepsaných veřejnou certifikační autoritou). Serverový certifikát je uložen přímo u autentizačního serveru, na straně klienta pak může být uložen v souborovém systému, registru nebo na čipové kartě (tokenu). Přes vyšší náklady se jedná o ověřovací metodu s velice vysokým stupněm bezpečnosti. S metodou EAP-PEAP popsanou v kapitole 1.6.6 tvoří nejvíce využívané metody pro ověřování. Odolnost vůči útokům typu Man-in-the-Middle či poskytování dynamické obnovy šifrovacích klíčů je již samozřejmostí, včetně podpory napříč všemi OS.

Proces autentizace metodou EAP-TLS ilustruje obrázek 15 [6].

1.6.8 Shrnutí

V kapitole 1.6 jsme popsali jednotlivé části protokolu 802.1X zabývající se autentizací, autorizací a účtováním. Popsali jsme základní a zároveň nejrozšířenější metody v rámci autentizačního frameworku EAP a poukázali na jejich zranitelnosti. Vyjmenované metody

nejsou výčtem všech, které byly vyvinuty, většinou ale zůstaly pouze na papíře a k jejich masivnímu nasazení nedošlo. Pro ilustraci a doplnění alespoň některé zajímavé vyjmenujme: EAP-TTLS, EAP-IKEv2, EAP-SIM, EAP-POTP, EAP-PSK, EAP-PWD a další.

2 SLABINY BEZPEČNOSTNÍCH MECHANISMŮ

V kapitole 1 jsme v teoretické rovině rozebrali možnosti zabezpečení bezdrátových sítí založených standardu 802.11. Z části jsme odkryli bezpečnostní rizika a zranitelnosti vyplývající z nasazení jednotlivých metod pro zabezpečení sítě, případně vyplývající z nasazení v rámci nesprávné konfigurace. Rozebrali jsme metody založené na jednoduchých principech zabezpečení, které ale neposkytují dostatečnou úroveň zabezpečení především pro firemní využití.

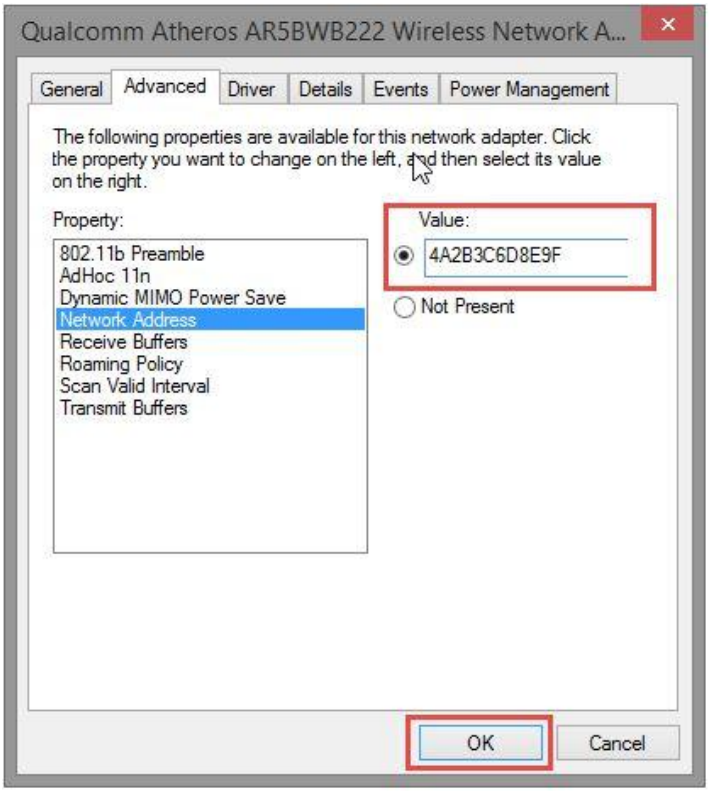
V této části detailněji rozebereme jednotlivé mechanismy z technicko–praktického pohledu se zaměřením na metody, které jsou založeny na standardu 802.1X a vhodné pro podnikové využití. Základní ověřovací mechanismy (WEP, WPA) byly rozebrány v kapitole 1.4 a 1.5 a nebudeme se jimi tedy více zabývat.

Metody ověřování dostupné ve standardu 802.1X prošly určitým evolučním procesem a až při jejich nasazování do reálného prostředí byly objeveny jejich nedostatky vyplývající z jejich principu návrhu, nevhodného nasazení (špatné konfiguraci) či nedodržení základních pravidel pro bezpečnost („best practices“). Na tyto nedostatky či zranitelnosti budeme v této kapitole poukazovat, rozebírat je po technické stránce a poskytovat doporučení pro zmírnění potencionálních nedostatků a snížení míry napadnutelnosti dané zranitelnosti metody.

2.1 Skrývání SSID a filtrace MAC adres

Přístup na základě MAC adresy

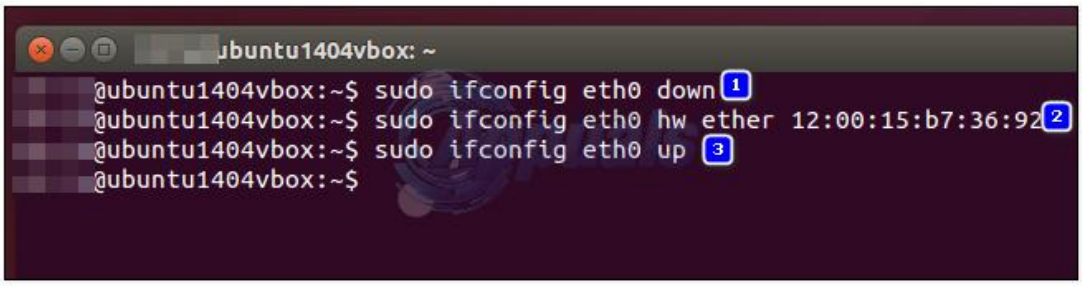
Většina přístupových bodů dokáže přes svou administraci řídit přístup bezdrátových klientů na základě MAC adresy (unikátní adresa každého bezdrátového adaptéru v rámci celého světa). Problém je v tom, že MAC adresu lze u bezdrátového adaptéru pomocí softwarových prostředků změnit na jakoukoliv jinou. V OS Windows lze na většině adaptérů změnit přímo v ovladači karty (viz. obrázek 16) nebo případně v registrech, v OS Linux přímo v konzoli s patřičnými oprávněními (viz. obrázek 17). Změnou MAC adresy tak



Obrázek 16: Změna MAC adresy adaptéru pod OS Windows

máme „otevřené dveře“ do sítě a můžeme se k danému přístupovému bodu připojit (za předpokladu absence další úrovně zabezpečení). MAC adresa je v bezdrátových sítích přenášena v čitelné podobě, pro její odchycení tak neexistuje žádná překážka. Postupujeme následovně:

1. Přepneme režim WiFi bezdrátového adaptéru v počítači do pasivního režimu. Pro tyto účely je vhodnější využití PC s OS Linux.



Obrázek 17: Změna MAC adresy adaptéru pod OS Linux

2. V pasivním režimu je možné odposlouchávat síťový provoz a získat tak seznam MAC adres. Pro tento účel můžeme využít nástroje `airdump-ng` z balíku aircrack-ng[16].
3. Ze seznamu zjištěných MAC adres klientů si libovolnou z nich nastavíme.
4. Pokud v bezdrátové síti není nastaveno žádné šifrování, autentizace a asociace k daném AP se zdaří.

V této fázi jsme již připojeni do dané bezdrátové sítě a můžeme použít další prostředky pro např. DoS útok na přístupový bod, slovníkový útok na konzoli (webové rozhraní) přístupového bodu (pokud je nastavené výchozí heslo z výroby, máme vyhráno). Vzhledem k tomu, že jsme použili pro asociaci s daným přístupovým bodem MAC adresu jiného zařízení, může docházet ke kolizím s původním adaptérem. Pokud však získáme přístup do konfigurace daného přístupového bodu, nic nám nebrání přidat do seznamu povolených MAC adres další (klidně i zfalšovanou).

Skrývání SSID

Skrývání SSID (pojmenované dané bezdrátové sítě) umožňuje dnes každý přístupový bod. Částečně to může být jedna z forem ochrany před útokem na danou síť (předpokládáme, že útočník nebude útočit na síť, o které neví, že existuje). Pokud však je k dané síti připojen alespoň jeden klient, je možné prostřednictvím přepnutí bezdrátového adaptéru do pasivního režimu název bezdrátové sítě se skrytým SSID odhalit v relativně krátké době. Podmínkou je však alespoň jeden klient připojený do dané sítě. V opačném případě zůstává SSID nezjistitelné. Při nastavení režimu skrytého SSID dojde k zablokování posílání *Beacon* rámců v rámci kterých je SSID vysíláno, nicméně v rámcích *Probe request* a *Probe response* při připojování uživatelů k síti je název SSID posílán stále. Při pasivním režimu tak stačí tyto rámce odchytit a máme SSID odhaleno.

Doporučení na závěr

Skrývání SSID a přístup na základě MAC adresy již v návrhu bezdrátových sítí nebyly brány jako prostředky pro zabezpečení proti neoprávněnému přístupu. V praxi jsou dost často využívány poskytovateli internetové konektivity (ISP provideři), kde jejich primárním účelem není ochrana přenášených dat po síti (tu přebírají protokoly na transportní či

[16] `https://www.aircrack-ng.org`

aplikační vrstvě ISO/OSI modelu). Určitým doporučením může být nastavení administrativního rozhraní přístupového bodu do jiné VLAN[17] a ochránit jej tak před útoky typu DoS[18] apod. Obecně však tyto metodiky nelze považovat za ochranné mechanismy před neautorizovaným zcizením dat.

2.2 Podnikové zabezpečení–WPA enterprise

V kapitole 1.6 jsme popsali základ architektury 802.1X, která byla navržena nejen pro ověřování uživatelů v podnikových sítí. Rozebrali jsme po teoretické stránce jednotlivé ověřovací metody a naznačili jejich zranitelnosti. Na tyto zranitelnosti se v této části podíváme podrobněji, ukážeme, jak je možné tyto zranitelnosti potlačit nebo alespoň zmenšit riziko jejich zneužití.

2.2.1 EAP-MD5

Původní návrh standardu 802.1X byl uzpůsoben pro využití v metalických sítích, kde je riziko odposlechu proti bezdrátovým sítím minimální. Z tohoto aspektu vyplýval i návrh některých ověřovacích metod–nebyl kladen důraz na možnost odposlechu. Metoda EAP-MD5 je jednou z nich. Mezi klientem, přístupovým bodem (autentizátorem) a autentizačním serverem není vytvořen zabezpečený tunel, EAP zprávy jsou tak posílány v otevřeném tvaru. To velice zjednodušuje práci potenciálnímu útočníkovi v případě pasivního odposlechu.

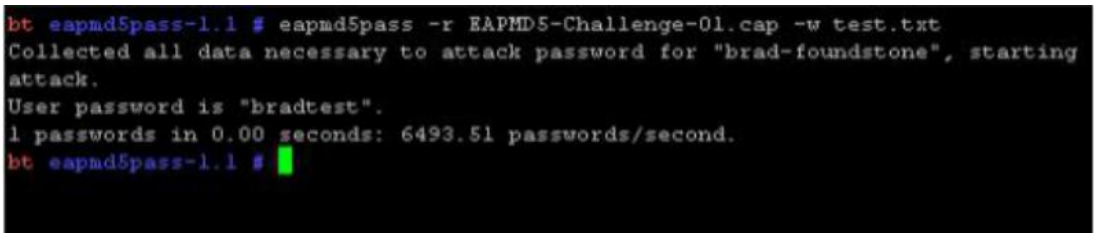
Jak jsme zmínili výše, EAP zprávy jsou posílány v otevřené, nezabezpečené podobě. Z toho vyplývá fakt, že je uživatelské jméno při autentizaci snadno odchytitelné a útočník má první část přihlašovacích údajů. Přístupové heslo je posíláno v podobě hashe vytvořeného metodou MD5. Z principu vytváření hashů MD5 sice nemůžeme hash zpět dekódovat na text, můžeme ale využít útoku hrubou silou a s pomocí slovníku porovnávat, zdali nedojde ke shodě. V dnešní době výkonného hardware tak můžeme mít velmi brzy výsledek.

V rámci etického hackingu můžeme využít nástroje `eapmd5pass` z linuxové distribuce Kali Linux[19]. Pro využití tohoto nástroje budeme potřebovat počítač s WiFi kartou, která

[17] Virtual Local Area Network

[18] Denial of Service

[19] Linuxová distribuce zaměřená na penetrační testování a etický hacking; `https://www.kali.org/`



Obrázek 18: Slovníkový útok na EAP-MD5

umožňuje přepnutí do pasivního režimu pro odposlech, a nástroj Wireshark[20] umožňující zachytávání komunikace do pcap souborů. Ten následně pošleme na vstup nástroje `eapmd5pass` společně s textovým souborem (slovníkem). `Eapmd5pass` najde v zachycené komunikaci rámce typu *Challenge-Response* a hrubou silou se pokusí najít odpovídající řetězec ze slovníku. Popis komunikace při autentizaci jsme rozebírali v kapitole 1.6.3.

Tento způsob odhalování hesel má jednu nevýhodu, odchytává pouze komunikaci klientů, kteří se aktuálně připojují do bezdrátové sítě. Přístupové údaje lze ale získat od klientů, kteří jsou již k přístupovému bodu asociováni. Při tomto principu využijeme možnosti zaslat klientům deautentizační rámec (simulujeme stav, jako by jej poslal samotný přístupový bod–jedná se o podvrh) a pokud má klient nastavené automatické připojování k dané síti, pokusí se znovu o autentizaci. Na tento typ komunikace útočník čeká, odchytí ji a s pomocí výše uvedené utility `eapmd5pass` může znovu zkoušet prolomení hesla stejným způsobem.

Ukázka slovníkového útoku je na obrázku 18.

Doporučení na závěr

Metoda EAP-MD5 nepodporuje dynamickou výměnu klíčů WEP ani WPA, umožňuje pouze statický WEP klíč. Na nedostatky tohoto způsobu šifrování autor poukázal v kapitole 1.4. Z tohoto důvodu není tato metoda dnes výrazně rozšířena a není doporučováno její využití. Pokud z technických či jiných důvodů musíme využívat metodu EAP-MD5 pro ověřování, je na zvážení správce dané sítě, zdali nevyužít metodu EAP-TTLS a uvnitř této metody využít EAP-MD5. EAP komunikace je v této metodě přenášena zabezpečeným tunelem a možnost odposlechu je minimalizována. Samozřejmostí je používání dostatečně silných hesel.

[20] `https://www.wireshark.org/`

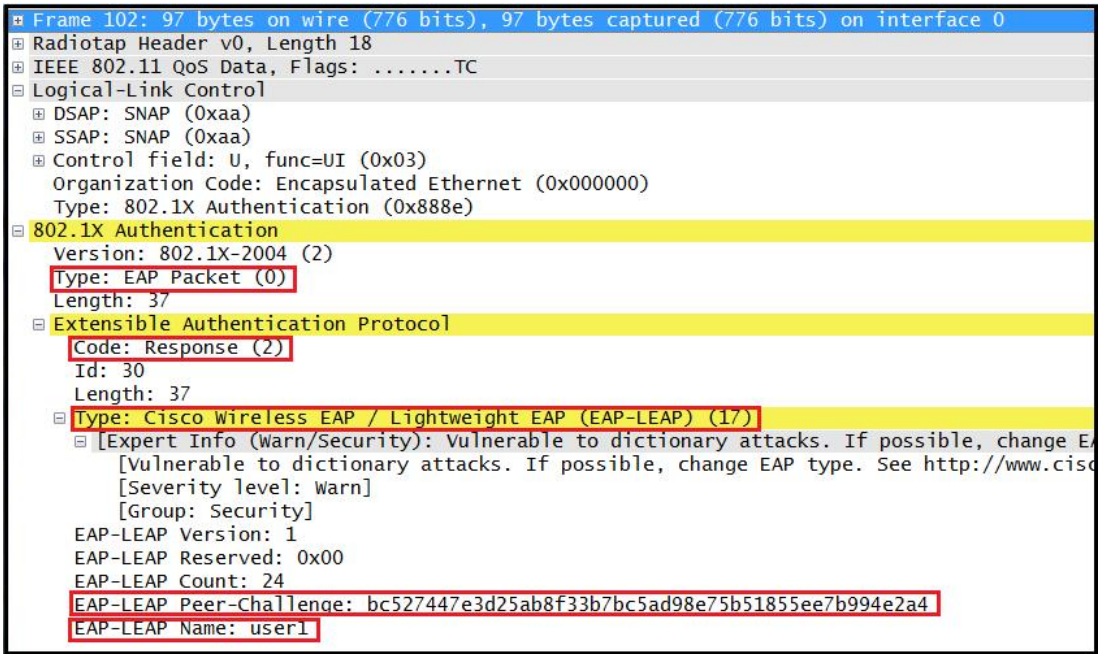
2.2.2 EAP-LEAP

Metoda EAP-LEAP vznikala v době, kdy byl dotvářen standard 802.11i a jedinou formou zabezpečení bezdrátových síti byl WEP (zatím považovaný za bezpečný). V době jejího vzniku bylo snahou vytvořit odlehčenou verzi metody se snadnou implementací. To se částečně povedlo, EAP-LEAP je již odolná proti útokům typu Man-in-Middle, podporuje dynamickou výměnu klíčů WEP/WPA, umožňuje dvoufázovou autentizaci.

Autentizace v rámci metody LEAP funguje na principu *Challenge-Response* a je založená na autentizačním algoritmu společnosti Microsoft MS-CHAPv1. I když se už jedná o vylepšenou verzi oproti algoritmu použitým v EAP-MD5, stále v této metodě spočívá zranitelnost v podobě prolomení hesla slovníkovým útokem. Navíc uživatelská jména jsou přenášena v čitelné podobě stejně jako v případě metody EAP-MD5. Princip mechanismu MS-CHAPv1 [24]:

1. Autentizátor zašle klientovi 8B dlouhý challenge řetězec.
2. Klient vytvoří 16B dlouhý MD4 hash hesla (NT hash) pro vygenerování 3 DES klíčů:
   - NT1–NT7
   - NT8–NT14
   - NT15–NT16 +\0\0\0\0\0
3. Poté se každý z klíčů použije k zašifrování challenge řetězce, každý 8B dlouhý.
4. Je provedena konkatenace všech 3 řetězců, čímž vznikne 24B dlouhý řetězec zaslaný klientem jako odpověď challenge-response autentizátoru.
5. Na základě tohoto řetězce autentizátor rozhodne, zda-li bude klient autentizován.

Klíčovým problémem je slabá úroveň posledního klíče DES. Posledních 5 nul se objevuje v každém řetězci *challenge/response*, což snižuje velikost řetězce na 16 bitů. Útok hrubou silou na algoritmus DES je tak při výkonu dnešního HW otázkou několika vteřin (klíč této velikosti dává pouze 65 536 možností). To nám pomáhá počítat dva z osmi bajtů hashe MD4, zbývá tedy 6B. Následně potřebujeme převést připravený slovník s hesly na slovník obsahující pouze NT hashe těchto hesel. Vyfiltrujeme NT hashe končící dvěma znaky, jen jsme zajistili v předchozí fázi. Posledním krokem je provedení klasického slovníkového útoku s použitím hesel ze slovníku, jejichž NT hash končí zjištěnými 2 znaky. Dojde-li ke shodě, je na základě NT hashe vyhledán v původním slovníku–zjištěné heslo uživatele.



Obrázek 19: Odchycení rámců metody EAP-LEAP nástrojem Wireshark

Proces získání hesla pomocí slovníkového útoku (shrnutí):

1. Převedení připraveného slovníku na slovník obsahující NT hashe těchto hesel[21].
2. Odchycení komunikace stejným způsobem jako u metody EAP-MD5.
3. Získání rámců challenge/response ze zachycené komunikace, zjištění uživatelského jména.
4. Získání posledních 2 bitů z NT hashe.
5. Provedení slovníkového útoku.

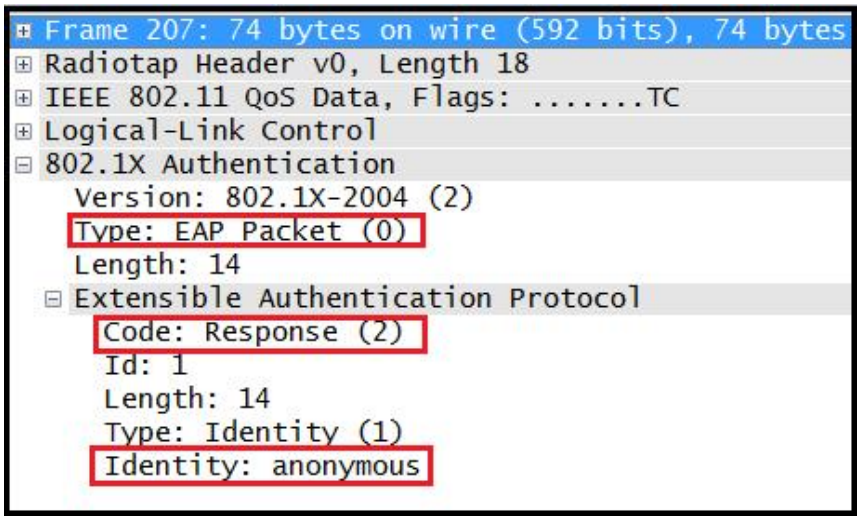
První úspěšný pokus prolomení metody EAP-LEAP publikoval Joshua Wright pomocí utility `asleap`[22] v roce 2004. Vstupem této utility je pcap soubor s odchycenou komunikací a odkaz na slovník. Ukázka odchycené komunikace mezi klientem a autentizátorem je na obrázku 19 pomocí softwaru Wireshark.

Doporučení na závěr

Metoda EAP-LEAP je již dnes považována za zastaralou a její nasazení se nedoporučuje. Společnost Cisco vyvinula novou metodu EAP-FAST (zabývá se jí kapitola 1.6.5), která metodu EAP-LEAP nahrazuje. Díky proprietárnímu řešení nebyla nikdy EAP-LEAP nijak

[21] NT hashe jsou založeny na MD4 hashovací funkci

[22] `http://asleap.sourceforge.net/README`



Obrázek 20: Odchycení rámců metody EAP-FAST nástrojem Wireshark–skrytí identity

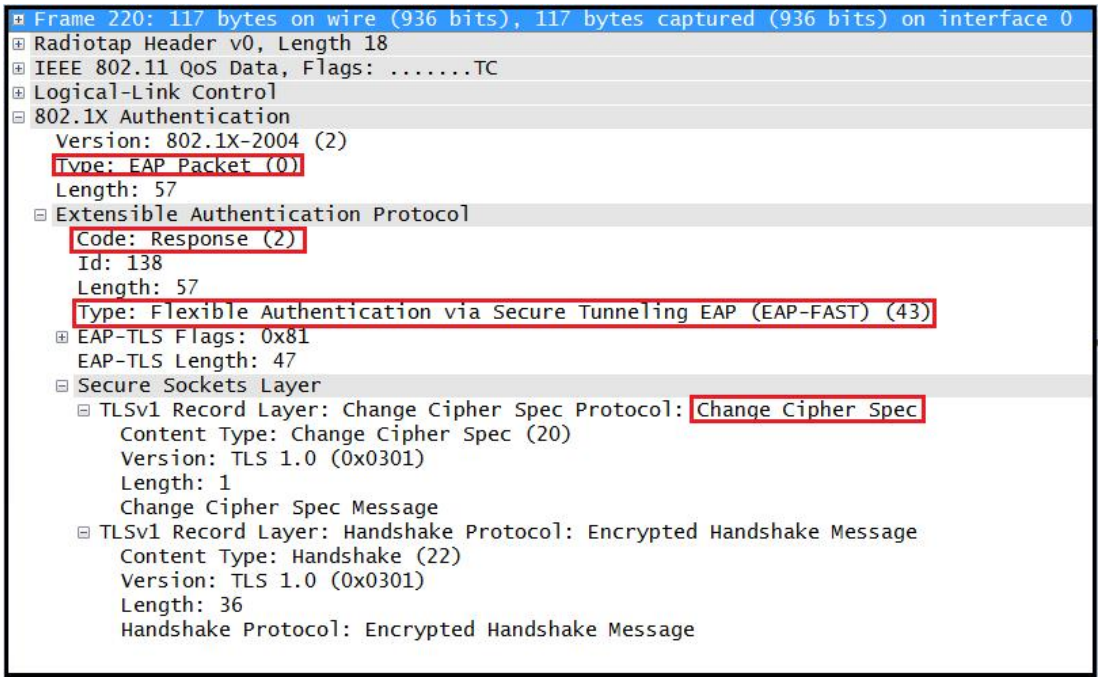
značně rozšířena, podpora chyběla v běžně využívaných operačních systémech. V extrémním případě při nutnosti využívat EAP-LEAP je potřeba používat silná komplexní hesla, která jsou méně náchylná na slovníkový útok.

2.2.3 EAP-FAST

Metoda EAP-FAST byla vyvinuta jako proprietární společností Cisco, následně však byla vydána v rámci RFC 4851. EAP-FAST oproti předchozím metodám již využívá pro přenos EAP rámců šifrovaný TLS tunel, který je dnes považovaný za bezpečný. Díky zabezpečenému tunelu tak již nelze provést odchycení uživatelského jména. Při ustavování TLS tunelu je použita identita *Anonymous* (viz. obrázek 20) a následně po úspěšném ustavení TLS posílána v zabezpečené podobě 21.

Vytvoření tunelu je založeno na tzn. unikátním klíči (PAC–Protected Access Credentials), který je unikátní pro každého uživatele a vytvořen přímo na RADIUS serveru [7]. Distribuce PAC klíče ke klientovi je prováděna pomocí nulté fáze, tzv. PAC provisioningu. K této fázi dochází pouze při prvotním nasazení metody, při expiraci PAC klíče nebo přidání nového klienta. Distribuce klíče může být provedena i manuálně, např. stažením z úložiště, přenesením po metalické síti apod. Manuální způsob nevyužívá fázi 0 (viz. tabulka 2) a uchovává metodu EAP-FAST bezpečnou.

Zneužití metody může nastat při PAC provisioningu, tedy při automatické distribuci PAC klíče. Existují 2 varianty automatické distribuce klíče:



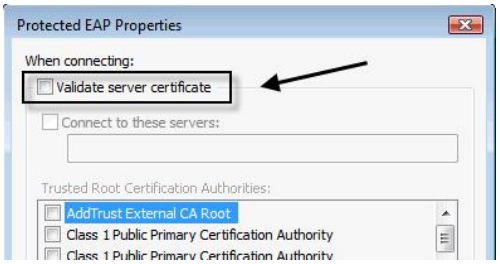
Obrázek 21: Odchycení rámců metody EAP-FAST nástrojem Wireshark

- Authenticated–využití serverového certifikátu, s ověřením;
- Anonymous–využití anonymního Diffie–Hellman tunelu, bez ověření.

Při *Authenticated* metodě dochází klientem k ověřování certifikátu a případný podvrh je klient schopen poznat. K této metodě je však potřeba mít na serveru nasazený důvěryhodný certifikát. Tento typ nasazení je ale složitější na nasazení a navíc serverový certifikát není u metody EAP-FAST povinný, pouze volitelný. Často se tak pro PAC provisioning využívá druhá metoda, *Anonymous*. Tato metoda serverový certifikát nevyžaduje, v první fázi je využit anonymní Diffie–Hellman tunel. V tomto režimu nelze ověřit autenticitu RADIUS serveru a díky tomu je metoda náchylná na útok typu RADIUS impersonation. Využití této zranitelnosti je však možné pouze ve specifické fázi 0, při PAC provisioningu. Úspěšným provedením útoku může útočník odchytit autentizaci pomocí MS-CHAPv2 a pokusit se o slovníkový útok pro zjištění hesla.

Doporučení na závěr

Nasazení metody EAP-FAST s automatickou distribucí PAC klíčů (PAC provisioning) je doporučeno s využitím v režimu Authenticated, tj. s ověřením identity serveru prostřednictvím certifikátu. Pořízení kvalifikovaného a důvěryhodného certifikátu je dnes již záležitost



Obrázek 22: Vypnutí ověření certifikátu RADIUS serveru v OS Windows

dostupná pro každou firmu, případně lze využít interní certifikační autority, které všichni klienti důvěřují. Tento způsob nasazení omezuje možnost napadnutí metody a řadí ji mezi bezpečné.

2.2.4 EAP-PEAP

Metoda EAP-PEAP je dnes nejvíce zastoupena při implementaci ověřování pomocí standardu 802.1X. Protože EAP-PEAP řeší pouze zapouzdření EAP komunikace do zabezpečeného TLS tunelu, jsou definovány metody, které zajišťují faktické ověření. Mezi nejpoužívanější metodu patří EAP-PEAPv0(EAP-MSCHAPv2). Budeme-li mluvit o metodě EAP-PEAP v rámci textu dále, budeme uvažovat právě tento způsob ověřování identity uživatele.

Jak již bylo zmíněno, EAP-PEAP oproti metodám EAP-MD5 a EAP-LEAP využívá na počátku ustavení TLS tunelu mezi klientem a autentizačním serverem. Tento způsob zabezpečení je dnes považovaný za bezpečný. Navíc metoda EAP-PEAP využívá možnosti anonymizace uživatelského jména při prvním handshaku v rámci sestavování TLS (obrázek 20). Správné uživatelské jméno je pak přeneseno přes zabezpečený tunel při ověřování metodou MS-CHAPv2. Metoda podporuje dvoufázové ověřování, autenticita serveru je klientem ověřována prostřednictvím certifikátu–jeho implementace u EAP-PEAP je na straně serveru povinná.

Možnost zneužití u metody EAP-PEAP však nastává na straně klienta. Funkce pro ověřování certifikátu serveru není povinná a lze vypnout (obrázek 22). Útok, který tuto zranitelnost využívá, nazýváme RADIUS impersonation.

RADIUS impersonation

V situaci, kdy není klient nastaven tak, aby ověřoval identitu RADIUS serveru (resp. jeho certifikát), stává se klient náchylný na útok RADIUS impersonation, který této zranitelnosti využívá. V rámci konfigurace klienta může být certifikát ověřován, resp. neověřován způsoby:

- **Bez ověření**–Autenticita RADIUS serveru není ověřována vůbec. Klient se tak na povolení autentizace RADIUS serverem pokusí autentizovat, aniž by ověřil, zdali může protistraně důvěřovat.
- **Částečné ověření**–nejedná se o žádný terminus technicus, pouze vlastní označení ověření, kdy je sice ověřen certifikát, neproběhne ale ověření certifikátu vůči žádné důvěryhodné certifikační autoritě. Pokud klient označí certifikát jako důvěryhodný, začne proces autentizace.
- **Úplné ověření**–klient ověřuje certifikát vůči certifikační autoritě, která certifikát vydala. V tomto případě je nutné mít na klientovi správně nasazenou hiearchii veřejných, resp. interních certifikačních autorit, aby k ověření mohlo dojít.

Samotné chování útoku typu RADIUS impersonation je podobné útoku *RogueAP*[23]. Útočník nemusí být nijak zvlášť vybaven, k útoku postačí notebook s anténami dostatečného zisku pro velký dosah a potřebný software. Pro simulaci tohoto útoku byla vyvinuta upravená verze RADIUS serveru pojmenovaná jako FreeRADIUS–WPE[24]. Tato verze je modifikována tak, aby automaticky povolila ověřování (AP) ze všech privátních rozsahů adres, automaticky přijímala jakýkoliv typ EAP rámců, automaticky přijímala pověření uživatele a automaticky přihlašovala výzvy a reakce MS-CHAPv2 [18]. Útok je pak proveden následovně:

1. Útočník vytvoří přístupový bod se stejným názvem (SSID) bezdrátové sítě jako má síť, kterou má v plánu napadnout. Řešení lze připravit prostřednictvím jakéhokoliv notebooku s WiFi kartou. Patřičným softwarem je možné vytvořit přístupový bod s daným SSID. Aby „donutil“ klienty připojovat se k jeho podvrženému přístupovému bodu, musí docílit lepšího pokrytí signálem než původní přístupový bod.
2. Pro ošálení co nejvíce klientů (hlavně těch již připojených) je možné těmto klientům poslat deautentizační rámec. Pokud má klient nastaveno automatické připojování

[23] `http://www.rogueap.com`

[24] `http://www.willhackforsushi.com/?page_id=37`

k dané WiFi síti, pokusí se znovu o připojení. V této fázi najde útočníkův přístupový bod s lepším pokrytím a upravený RADIUS server může začít sbírat potřebné rámce.

3. Klient zahájí proces vytváření TLS tunelu, nemá-li povolenou kontrolu certifikátu serveru, případně neprovádí-li kontrolu důsledně (viz. body uvedené výše), je TLS tunel ustaven a klient se může autentizovat k podvrženému RADIUS serveru. Útočník má přístup ke komunikaci v rámci TLS tunelu a může odposlechnout rámce typu *Challenge-Response*.
4. Metoda MS-CHAPv2 přes své vylepšení oproti předchůdcům je stále náchylná na útok hrubou silou [20]. Útočník se tak může pokusit tímto způsobem získat hesla uživatelů.

Doporučení na závěr

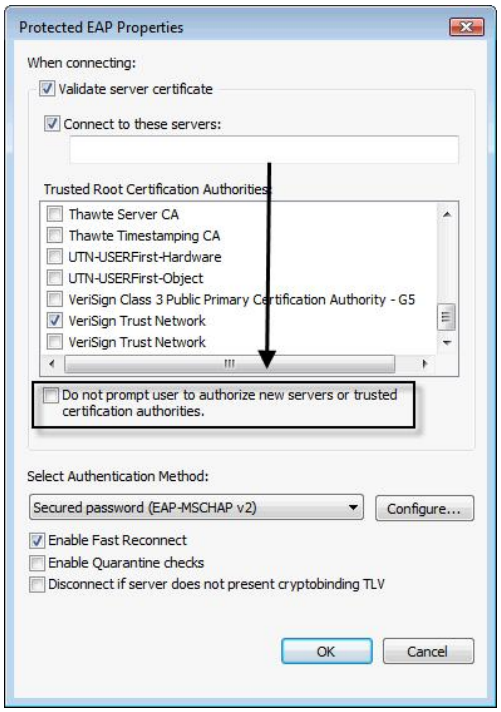
Metoda EAP-PEAP je dnes považována za bezpečnou. I když existuje její zranitelnost prostřednictvím útoku RADIUS impersonation, lze tomuto útoku předejít vhodnou konfigurací klienta:

- Klient povinně ověřuje certifikát RADIUS serveru.
- Ověření certifikátu probíhá v plném rozsahu včetně kontroly vydavatele certifikátu.
- Klient ověří atribut CN[25] v certifikátu, zda-li souhlasí s FQDN[26] RADIUS serveru.

Správnou konfiguraci klienta je možné zajistit prostřednictvím nástroje Group Policy, který je součástí doménové hiearchie Active Directory (implementace doménové struktury společností Microsoft). Zároveň je politikami možné vynucovat určitá nastavení, včetně nemožnosti změny běžným uživatelem (viz. doporučené nastavení 23). V rámci nasazení role Active Directory Certificate Services je možné vytvářet vlastní interní certifikační autority a prostřednictvím ní provádět distribuci kořenových certifikačních autorit přímo na klienty (za předpokladu, že nechceme využívat komerční, placené certifikáty vydávané veřejnými certifikačnímu autoritami). Důležitým prvkem je opět nastavení silných hesel uživatelů, která lépe odolají případnému útoku hrubou silou. Posledním doporučením je využití možnosti skrytí uživatelského jména náhodným či anonymním řetězcem v nešifrované fázi ustavení spojení.

[25]Common Name, atribut obsahující jméno serveru pro který je vydán

[26]Fully Qualified Domain Name, celé jméno serveru v DNS včetně dané domény ke které patří



Obrázek 23: Nastavení klienta OS Windows pro zamezení útoku RADIUS impersonation

2.2.5 EAP-TLS

Mechanismus EAP-TLS je jediný z diskutovaných v rámci této práce, který využívá pro ověření pouze certifikáty. Klient je ověřován vlastním certifikátem, server se vůči klientovi ověřuje taktéž certifikátem. Ověření certifikátem poskytuje této metodě status neprolomitelná, odolá i RADIUS impersonation útoku popisovaným u metody EAP-PEAP.

Nasazení ověřovací metody EAP-TLS má však jednu nevýhodu, díky které se metoda příliš nerozšířila. Ověřování certifikátem namísto uživatelského jména a hesla s sebou nese nutnost mít ve společnosti precizně vybudovou infrastrukturu pro generování certifikátů koncovým klientům, včetně případných procesů zneplatnění certifikátu při ztrátě, odcizení apod. V případě plného využití certifikátů podepisovaných veřejnou certifikační autoritou pak i značně nákladné řešení. Klientské certifikáty mohou být uloženy na klientském zařízení v registrech, souborovém systému nebo na čipové kartě či tokenu. V případě lokálního uložení na daném zařízení pak přináší nutnost přenést certifikát na všechna zařízení, která budou pro autentizaci používána.

Doporučení na závěr

Metoda EAP-TLS je sama o sobě bezpečná, aniž bychom museli řešit nějaká omezení či předem dané konfigurační postupy. Důležitou roli hraje způsob, jakým bude klientský certifikát uložen na koncovém zařízení. Nejbezpečnější variantou je uložení na tokenu či čipové kartě, při její ztrátě se totiž nálezce či únosce k certifikátu nedostane, aniž by zadal „tajný klíč“ chránící úložiště certifikátů.

2.2.6 Shrnutí

V této kapitole jsme popsali do hloubky jednotlivé zranitelnosti metod používaných pro ověřování s výjimkou metod pro filtrování MAC adres a skrývání SSID. Tyto metody nepředstavují pro zkušeného útočníká žádný problém a jejich překonání je otázka několika minut. Mohou být použity jako doplňující prvek, nikoliv ale stěžejní.

Z pohledu míry bezpečnosti je jasně nejvhodnější metoda EAP-TLS, avšak míra složitosti nasazení této metody výraznou měrou přispívá k malé rozšířenosti této metody. I díky tomu je dnes nejvíce zastoupena metoda EAP-PEAP, která je při správné konfiguraci klienta považována za bezpečnou a nepředstavuje při implementaci vysoké nároky na nasazení. Její výhodou je i široká podpora napříč všemi operačními systémy. Bez ohledu na zabezpečení dané metody však ale platí pravidlo dostatečně silného hesla uživatele.

Následuje souhrnná tabulka 3 porovnávající klíčové vlastnosti ověřovacích metod EAP vůči reálné implementaci v jednotlivých mechanismech. Legendu pak udává tabulka 4.

	EAP-MD5	**EAP-LEAP**	**EAP-FAST**	**EAP-PEAP**	**EAP-TLS**
Míra bezpečnosti*	Nízká	Nižší	Vyšší	Vysoká	Vysoká
Dynamická výměna klíčů	NE	ANO	ANO	ANO	ANO
Zabezpečený tunel	NE	NE	ANO	ANO	ANO
Serverový certifikát	NE	NE	Volitelně	ANO	ANO
Klientský certifikát	NE	NE	NE	NE	ANO
Dvoufázové ověření	NE	ANO	ANO	ANO	ANO

Tabulka 3: Přehled zabezpečení jednotlivých metod EAP ve standardu 802.1X

1	2	3	4	5
Nízká	Nižší	Střední	Vyšší	Vysoká

Tabulka 4: Přehled úrovní zabezpečení pro hodnocení metod EAP

3 BEZPEČNOSTNÍ AUDIT–JAK NA TO

S rozvojem technologií jsou již dnes odvětví, která se pro své fungování bez podpory obecně IT systémů neobejdou. Pro řadu firem a společností se tak v současné době pojem bezpečnost stal velmi aktuálním tématem. Bezpečnost je dnes řešena z mnoha různých důvodů, všechny mají ale stejný cíl–zajistit dostupnost systémů po celou dobu jejich provozu. Pojmem bezpečná IT infrastruktura tak můžeme chápat souhrn pravidel, která jsou schopna zajistit důvěrnost, integritu, dostupnost, autenticitu a nepopiratelnost.

Pro zjištění stavu zabezpečení jednotlivých IT systémů je nutné provést jejich kontrolu a ověřit, zdali a do jaké míry jsou jednotlivá bezpečností hlediska splněna. Touto problematikou se zabývá bezpečnostní audit. Jedná se komplexní úkon, jenž není prováděn nahodile, ale podle předem jasně daných metologických postupů. Tyto postupy jsou vytvářeny cíleně pro testování konkrétních zranitelností daných částí IT systémů (bezpečnost týkající se síťových prvků, informačních systémů, databází, apod.)

V této kapitole rozebereme základní pojmy týkající se problematiky bezpečnostního auditu, penetračního testování, metologie testování, uvedeme základní typy testů a jejich rozdělení z různých úhlů pohledu. Na závěr se zaměříme již konkrétně na problematiku bezpečnostního auditu bezdrátových sítí s doporučením pro využití konkrétních nástrojů pro provedení sady penetračních testů zaměřujících se na standard 802.1X a ověřovací metody EAP. Při psaní této kapitoly jsme převážně vycházeli z publikace [21].

3.1 Základní pojmy

V úvodu jsme uvedli 5 základních hledisek, která s bezpečností IT systémů jednoznačně souvisí:

- **důvěrnost**–je zajištěna v případě, pokud k datům mají přístup pouze vyhrazená skupina osob či jednotlivců;
- **integrita**–zaručuje přenesení dat v nezměněném, konzistentním stavu;
- **dostupnost**–zajištění adekvátního přístupu a ochrana před jeho neoprávněným zamezením;
- **autenticita**–ověření, že subjekt je tím, za koho se vydává;
- **nepopiratelnost**–vyloučení možnosti popřít dřívější provedení nějaké operace.

Pro správné pochopení principů bezpečnostního auditu vysvětlíme ještě další pojmy:

Bezpečnostní audit

Komplexní proces obsahující kontrolu daného systému či aplikace podle předem daných postupů. Výsledkem auditu je report se souhrnem zranitelností, na které je testovaný systém náchylný, u větších společností je však zpravidla porovnávána definovaná bezpečnostní politika se zjištěnou realitou. Jde tedy o to, které její požadavky a podmínky jsou splněné a které nikoliv, případně z jakého důvodu. Cílem bezpečnostního auditu je:

1. Zjistit skutečný a aktuální stav zabezpečení systémů organizace;
2. Definovat rizika, která ohrožují bezpečnost systémů organizace;
3. Na základě vyhodnocení rizik získat podklady pro definování bezpečnostních politik organizace.

Bezpečnostní audit není jen o kontrole práce IT oddělení společnosti, jeho primárním přínosem je:

1. **Minimalizace rizik**–Díky zajištění vyšší úrovně bezpečnostního standardu organizace dojde k minimalizaci rizik spojených se ztrátou způsobených ať již havárií systému, napadením škodlivého softwaru či hackery, ale také chybami pracovníků, případně jejích jednáním v rozporu se zákonem.
2. **Ochrana investic**–Organizace si tak zajistí, že jejich investice do know–how nebudou moci být zcizeny a využity v rozporu se zákonem. Zároveň si organizace buduje důvěryhodnější vztah se svými obchodními partnery či potenciálními investory.
3. **Zvýšení produktivity**–Díky stanovení bezpečnostních politik a jejich vynucení se minimalizuje možnost zaměstnanců zneužívat prostředky IT zaměstnavatele v rozporu se zájmy organizace. To vede ke zvýšení produktivity zaměstnanců.[27]
4. **Řízení přístupu**–Zaměřuje se na detailní popis oprávnění skupin či jednotlivců k určitým zdrojům. Audituje jejich využití s cílem jejich procesní optimalizace.
5. **Provozní a bezpečnostní dokumentace**–Je součástí reportu z bezpečnostního auditu, zaměřuje se na detailní popis současné infrastruktury s ohledem na nastavené bezpečnostní politiky daných prvků a způsobu, jakým jsou tyto prvky provozně využívány.

[27]Zdroj: `http://www.root-it.cz/bezpecnostni-audit.asp`

Penetrační testování

Penetrační testování je metodika (taktika) proaktivního testování IT systémů na různé druhy zranitelnosti. Simuluje tak reálné útoky (typu packet injection, Man-in-the-Middle, Denial of Service–DoS apod.) se snahou nalézt a odhalit slabiny a zranitelnosti systému dříve, než je objeví skutečný útočník. Při zjištění zranitelností je však útok proveden jen na úrovni etického hackingu za účelem detailního zmapovaní zranitelností pro aplikování příslušného nápravného opatření. Penetrační testy mohou probíhat i bez vědomí IT oddělení, cílem této techniky je ověření, jakým způsobem a jak rychle dokážou zodpovědné týmy za provoz systémů na tento útok reagovat.

3.2 Metologie testování

Metologie testování je rozdělena na několik částí. Různé zdroje zabývající se penetračním testováním určité fáze dělí na více podfází, typicky jsou zastoupeny fáze čtyři:

1. Cíl a rozsah penetračního testu
2. Sběr dat
3. Skenování a exploitace
4. Report

3.2.1 Typy testů

Testování slouží k odhalování chyb a zranitelností, které vzniknou při vývoji systému a nasazení. Typicky jsou tyto chyby neúmyslné a při testování se na ně nemusí přijít. Často i chyby mohou vznikat nevhodnou konfigurací. Jednotlivé testy se pak zaměřují na určitou problematiku a zkoumají potencionální slabiny. Dělí se do několika základních kategorií podle způsobu provedení:

- **Manuální**–Jsou prováděny s interakcí testera, výhodou je možné testování pomocí sofistikovanějších a složitějších metod a postupů, které automaticky testovat nelze. Nevýhodou je časová náročnost na provádění.
- **Automatizované**–Jsou spouštěny automatizovaně, jejich výhodou je jednak menší časová náročnost, jednak provádění těchto testů zpravidla nevyžaduje ruční zásah, mohou je tedy vykonávat i méně zkušení testeři. Zároveň jsou automatické testy

vyvinuty profesionály v oboru na dané téma, dokáží tak velmi detailně rozkrýt případnou zranitelnost.

- **Semiautomatizované**–Představují kombinaci mezi manuálními a automatickými testy. Jdou cestou kompromisu mezi oběma řešeními a aplikují se tam, kde není jednoznačně možné použití manuální či automatické metody.

Další dělení může být podle úrovně znalosti o testovaném systému:

- **Black-box testy**–Nejpoužívanější typ testování. Simulují vnější přístup útočníka, který zná potenciální vstupy a výstupy systému, nezná ale vnitřní implementaci, resp. konfiguraci. Výhodou tohoto přístupu je vysoká míra variability, útočník nepotřebuje znát konkrétní konfiguraci prvků, topologii sítě apod. Nevýhodou je potřeba velmi obsáhlé znalosti testera pro zkoumání.
- **White-box testy**–Testy jsou založeny na znalosti architektury, v případě počítačových sítí má útočník k dispozici topologii sítě, počet a typ připojených zařízení, znalosti vnitřních firemních politik, konfiguraci jednotlivých síťových prvků apod. Díky této metodě lze hledat zranitelnosti přímo v konfiguraci, případně provádět její optimalizaci.
- **Grey-box testy**–Kombinace obou výše uvedených přístupů. Útočník přistupuje k systému zvenčí, avšak má informace o vnitřní infrastruktuře.

3.3 Metodika OSSTMM

OSSTMM (Open Source Security Testing Methodology Manual)[28] je metodika pro provádění bezpečnostních testů a měření. Zastřešuje ji ISECOM (Institute for Security and Open Methodologies), neziskový institut pro bezpečnost. OSSTMM je jednou z volně šiřitelných metodik. Většina komerčních firem zabývajících se bezpečnostním auditem má vyvinuté své vlastní metodiky, které však tvoří její know–how a nezveřejňují je. V roce vzniku této práce (2018) je k dispozici OSSTMM verze 3 [10], v přípravě je verze 4 (v současné době jako draft).

OSSTMM se zabývá několika odvětvími, pro která má zadefinované metodiky:

1. Information security testing (jak organizace funguje, kolik dat musí spravovat, profily zaměstnanců);

[28] `http://www.isecom.org`

2. Process security testing (co všechno o sobě organizace navenek prozrazuje, sociální inženýrství);
3. Internet technology security testing (skenování sítě, hledání bezpečnostních slabin, pokusy o průnik a získání citlivých dat);
4. Communications security testing (telefony, hlasové schránky, faxy);
5. Wireless security testing (elekromagnetické vyzařování, Wi-fi, Bluetooth, bezdrátové periferie);
6. Physical security testing (zabezpečení prostor, dveře, ploty, monitorovací zařízení, alarmy).

Metodika Wireless security testing zabývající se testováním bezdrátových sítí a jejich periferií definuje další podoblasti (ve verzi OSSTMM celkem patnáct), které mohou být testovány a sledovány v rámci bezpečnostního auditu. I když je oblast testování bezdrátových sítí komplexně popsána, jednotlivé metodiky obsahují pouze obecné postupy co testovat, nedefinují už však jakým způsobem.

Metodika OSSTMM je tak popsána velmi abstraktním způsobem, nezabývá se ani metologií pro testování bezdrátových sítí založených na standardu 802.1X. Z tohoto důvodu si vytvoříme metodiku vlastní, popsanou v kapitole 3.4.

3.4 Metodika auditu bezdrátové sítě s využitím 802.1X

V kapitole 3.3 jsme přiblížili otevřenou metodiku OSSTMM. Vzhledem k vysoké míře abstrakce u této metodiky není její využití pro velmi konkrétní a úzce specifikované testování vhodné. Vhodnějšími adepty tak mohou být technologické metodiky, které vzhledem k jejich úzkému zaměření na konkrétní činnost umí přesně definovat, co je předmětem testování, jakým způsobem bude testování probíhat a případná doporučení z výsledků vyplývající. Příkladem technologicky zaměřené metodiky může být metodika OWASP (Open Web Application Security Project)[29] s primárním zaměřením na auditování a penetrační testování webových aplikací.

[29] `https://www.owasp.org`

Vzhledem k absenci technologické metodiky pro bezpečnostní audit a penetrační testování bezdrátových sítí založených na standardu 802.1X si zadefinujeme v rámci této kapitoly metodiku vlastní.

Základem této metodiky pro bezpečnostní audit a penetrační testování budou komponenty architektury 802.1X s využitím v bezdrátových sítích:

- Klient (supplicant)
- Autentizátor
- Autentizační server (RADIUS)

Detailněji je architektura 802.1X popsána v kapitole 1.6 a na obrázku 11. Cílem této metodiky bude zjištění míry zabezpečení bezdrátových sítí založených na ověřování uživatelů prostřednictvím standardu 802.1X a ověřovacího mechanismu EAP. V případě zjištění nedostatečných bezpečnostních mechanismů pro přenos citlivých dat jako jsou přihlašovací údaje poukáže na možnosti zvýšení stupně zabezpečení příslušnými mechanismy.

Z podstaty fungování ověřování uživatelů v sítích založených na 802.1X je metodika rozložena do několika fází:

1. **Zjištění použité metody EAP**
2. **Získání uživatelského jména**
3. **Prolomení uživatelského hesla**
4. **Audit komponent architektury 802.1X**

Zjištění použité metody EAP

Zjištění konkrétního typu metody EAP je základem pro další postup v rámci bezpečnostního auditu. Typ metody EAP značí způsob, jakým budou přenášena uživatelská jména a hesla v rámci procesu autentizace. Typ použité EAP metody je zasílán klientem při připojení k bezdrátové síti v otevřeném tvaru. Lze jej tak odchytit pasivním odposlechem sítě. Navíc lze vynutit deautentizaci již připojených klientů, a zajistit si tak větší vzorek klientů prověřených bezpečnostním auditem.

Získání uživatelského jména

V závislosti na zvolení typu EAP metody klientem se již proces získání uživatelského jména liší. Standardně je v rámci EAP uživatelské jméno přenášeno v otevřené podobě a lze tak

pasivním odposloucháváním odchytit. Výjimkou mohou být však metody, které sestavují mezi klientem a autentizačním serverem šifrované spojení s využitím možnosti skrytí uživatelského jména (problém popisuje obrázek 20). V počátečním sestavování šifrovaného tunelu lze využít anonymizace uživatelského jména a reálné uživatelské jméno zaslat až v šifrované podobě.

Prolomení uživatelského hesla

Fáze spočívající v aktivním útoku s cílem prolomení uživatelského hesla. Přesný sled kroků při útoku je daný použitou metodou a existencí případné zranitelnosti u dané metody. Detailní popis zranitelností u jednotlivých ověřovacích mechanismů s možností jejich zneužití je rozebrán v kapitole 2.2.

Audit komponent architektury 802.1X

Fáze zaměřující se na konfiguraci jednotlivých síťových prvků (bezdrátový přístupový bod–autentizátor a autentizační server–RADIUS server) v rámci whitebox testování. Předmětem auditu je aktuální softwarová vybavenost (verze firmware) na daných prvcích, povolené autentizační metody na RADIUS serveru, způsob, jakým je řešeno logování (zda–li je řešeno s využitím vzdáleného logserveru, např. syslog) pro dohledání případných incidentů, typ nastaveného pokročilého šifrování přenosu dat (pokud vůbec). Zároveň může být v této fázi řešeno procesní řízení–seznam osob, které mají oprávnění konfigurovat prvky, sbírat logovací údaje apod.

3.5 Shrnutí

V této kapitole jsme popsali základní pojmy, které jsou spojeny s bezpečnostním auditem, rozebrali, co se skrývá pod pojmy bezpečnostní audit, penetrační testování a uvedli záměr s jakým cílem jsou tyto techniky prováděny. V rámci metologie jsme seznámili čtenáře s typy testů, které mohou být v rámci auditu prováděny, a popsali otevřené metodiky zabývající se prováděním bezpečnostních auditů. Od obecných metodik jsme se na závěr dostali ke konkrétním a naznačili jsme svou vlastní metodiku, v rámci které se v této práci budeme zabývat dále. Cílem nebylo detailně popsat metodiku krok za krokem (což

by v detailním pohledu vydalo na celou publikaci), ale uvést způsob, jakým je možné provádět bezpečnostní audit v sítích využívající pro ověřování uživatelů standard 802.1X. Následující kapitola je věnována návrhu komplexní architektury zabývající se problematikou bezpečnostního auditu v sítích 802.1X.

4 ARCHITEKTURA TESTŮ PRO AUDIT 802.1X SÍTÍ

V předchozích kapitolách jsme se zabývali bezdrátovými sítěmi a jejich bezpečností z různých úhlů pohledu, většina z nich byla ale pouze v teoretické rovině. V kapitole 1 jsme popsali jednotlivé mechanismy zabezpečení bezdrátových sítí se zaměřením na bezdrátové sítě podporující ověřování prostřednictvím standardu 802.1X. V kapitole 2 jsme na tuto kapitolu navázali a do detailu popsali princip ověřování v sítích 802.1X včetně zranitelností, které se v ověřovacím frameworku či jednotlivých ověřovacích mechanismech vyskytují. V předchozí kapitole 3 se v úvodní části zabýváme obecně metodologií bezpečnostních auditů s detailním pohledem na celý proces auditu, popisujeme jednotlivé typy testovacích mechanismů, včetně veřejně dostupných metodik. Nakonec, vzhledem k vysoké abstrakci dostupných metodik, si vytvoříme metodiku vlastní, zabývající se konkrétně a do detailu tématem bezpečnosti bezdrátových sítích a procesu autentizace uživatelů v nich samotných založených na standardu 802.1X. Tato vlastní metodika je základem pro praktickou část této práce.

Cílem této kapitoly je analyzovat možnosti využití existujících nástrojů a vytvořit architekturu testů pro bezpečnostní audit bezdrátových sítí založených na standardu 802.1X dle předem navržené vlastní metodiky. Bezpečnostním auditem bezdrátových sítí je v tomto kontextu myšlen proces analýzy zabezpečení sítě v odhalení používaných ověřovacích metod protokolu EAP, detekce uživatelských jmen připojovaných klientů a případný pokus o odhalení hesel těchto klientů při zjištění existence zranitelnosti u dané metody v rámci etického hackingu. Jednotlivé fáze bezpečnostního auditu byly navrženy v rámci vlastní metodiky v kapitole 3.4.

V této kapitole v části analýza návrhu rozebereme detailně jednotlivé fáze auditu dle předem navržené vlastní metodiky (kapitola 3.4), z praktického pohledu popíšeme, jakým způsobem lze bezpečnostní audit provést (pasivní versus aktivní režim), navrhneme řešení pro detekci použité autentizační metody, odchycení uživatelského jména a v případě nalezení zranitelné metody poukážeme na možnosti využití této zranitelnosti v rámci etického hackingu. Inspirací při psaní této kapitoly byla publikace [15].

4.1 Analýza požadavků

Při vytváření návrhu architektury jsme striktně museli dodržet předem navrženou metodiku bezpečnostního auditu, která tvoří předlohu pro kompletní návrh celé architektury. Bezpečnostní audit je složen z několika fází, které na sebe vzájemně navazují. Úkolem první fáze je zjištění použité EAP metody. Tato fáze má zásadní vliv na další průběh, neboť jednotlivé EAP metody využívají jiné technické řešení procesu autentizace, kterému je potřeba další průběh přizpůsobit. V dalším kroku probíhá detekce použitého uživatelského jména[30], které je standardně v rámci EAP přenášeno v čitelné, nezabezpečené podobě[31].

Abychom při provádění bezpečnostního auditu zachytili co nejvyšší počet klientů, potřebujeme v návrhu zohlednit i již připojené klienty. V rámci bezdrátových sítí lze provést deautentizaci klienta z přístupového bodu. Snahou tohoto procesu je, aby se klient pokusil znovu připojit k přístupovému bodu a mohli jsme jej do auditu zahrnout.

4.1.1 Pasivní režim

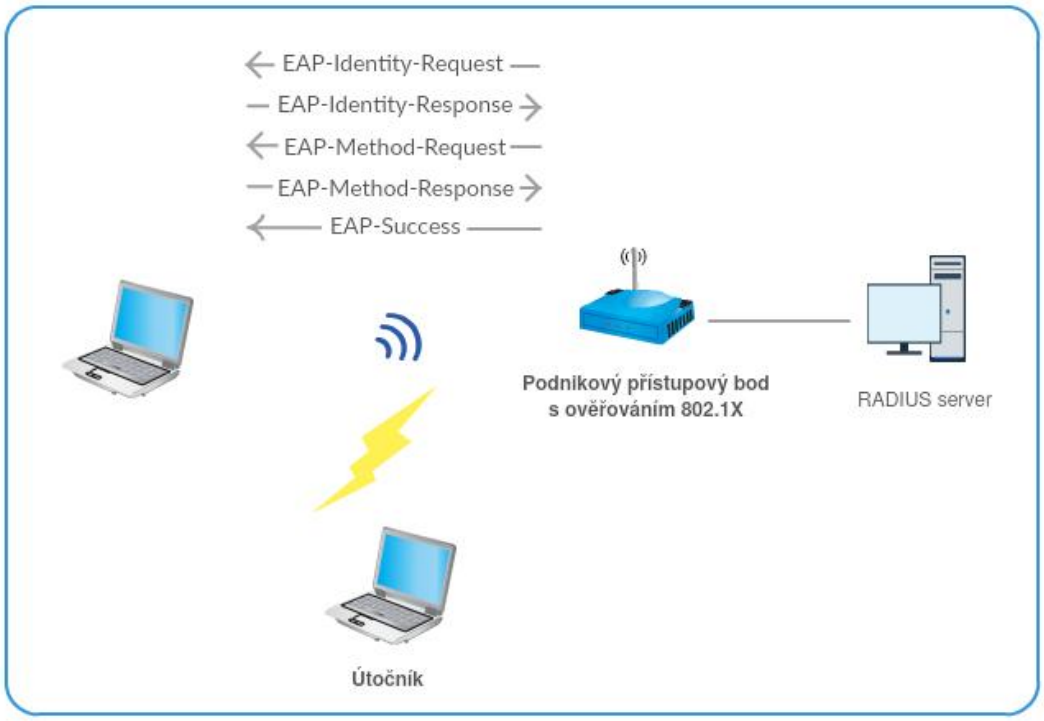
V případě pasivního režimu jde o metodu, při které je bezdrátový síťový adaptér přepnutý do monitorovacího módu a umožňuje tak odposlouchávat komunikaci v bezdrátových sítích, které má v dosahu. V monitorovacím režimu adaptér sekvenčně přepíná mezi všemi kanály[32] a dokáže tak odchytit komunikaci všech sítí v dosahu. Lze však při konfiguraci bezdrátového adaptéru napevno nastavit kanál a tímto způsobem si tak vyfiltrovat bezdrátovou síť, na kterou se chce zaměřit. Probíhající komunikaci je možné v reálném čase přímo hned analyzovat nebo ji pouze zachytit pomocí specializovaných nástrojů (např. Wireshark) do souborů typu pcap a komunikaci analyzovat posléze. Výhodou tohoto řešení je odchycení kompletních rámců *Challenge/Response* obsahující typ ověřovací metody, kterou klienti pro autentizaci využívají, uživatelské jméno[33] a u některých metod i hash uživatelského hesla. Vzhledem k potřebě získat pro bezpečnostní audit vzorek co nejvíce klientů a jediným okamžikem, kdy je možné data pro bezpečnostní audit sesbírat, je moment autentizace klientů k bezdrátové síti, je v pasivním režimu možnost zaslat požadavek na deautentizaci klientů z přístupového bodu. Předpokladem tohoto kroku je fakt, že

[30] V některých literaturách fáze pojmenovaná jako enumerace uživatelských jmen

[31] Pokud neuvažujeme využití funkcionality skrytí identity

[32] Pro WiFi na frekvenci 2.4GHz je pro Českou republiku možné použití kanálů 1–13

[33] Pokud není použita technika skrytí identity

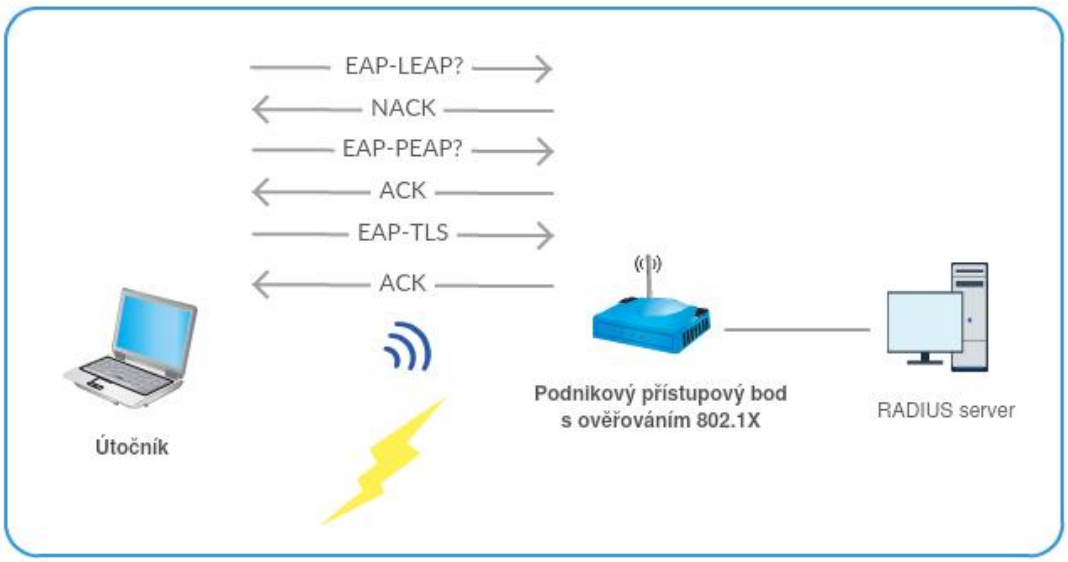


Obrázek 24: Princip detekce metody EAP v pasivním režimu

se bezdrátový adaptér klienta pokusí ihned o znovusestavení spojení, čímž dosáhneme požadovaného efektu. Pasivní režim je jedním z nejvyužívanějších režimů při bezpečnostních auditech a penetračních testech. Z pohledu úrovně znalosti o testovaném systému se jedná o blackbox testování. Princip činnosti v pasivním režimu znázorňuje obrázek 24.

4.1.2 Aktivní režim

Aktivní způsob detekce EAP metody se od pasivního režimu liší principem proveditelnosti. Zatímco u pasivního režimu dochází k odposlechu komunikace v bezdrátové síti, u aktivního režimu se testovací nástroj chová jako klient (suplikant) a aktivně se snaží navazovat spojení s příslušným přístupovým bodem dané bezdrátové sítě. Sekvenčně se tak snaží procházet seznam EAP metod a čeká na kladnou či zamítavou reakci ze strany autentizátoru, resp. autentizačního serveru. Tímto způsobem dokáže enumerovat povolené EAP metody. Nevýhodou tohoto přístupu je absence možnosti získání seznamu uživatelských jmen, případně hesel. Hlavním a klíčovým užitím aktivního způsobu enumerace je možnost kontroly konfigurace infrastruktury přímo ze strany klientů a může sloužit jako doplňkový kontrolní nástroj pro porovnání výsledků s pasivním režimem auditu. Z pohledu úrovně



Obrázek 25: Princip detekce metody EAP v aktivním režimu

znalosti o testovaném systému se jedná stejně jako u pasivního režimu o blackbox testování. Princip činnosti v aktivním režimu znázorňuje obrázek 25.

4.1.3 Výstup bezpečnostního auditu

Součástí každého bezpečnostního auditu je report, závěrečná zpráva, shrnující poznatky z bezpečnostního auditu. Pro tyto účely je nejvhodnější zvolit výstup do strojově čitelného formátu, který lze dále zpracovávat. Jako nejvhodnější variantou se tak nabízí výstup do formátu XML, který splňuje možnost dalšího zpracování a zároveň nabízí i možnost transformace do graficky formátovaného výstupu.

4.2 Analýza využití existujících nástrojů

V předchozí kapitole 4.1, zabývající se analýzou požadavků pro architekturu testů, jsme definovali funkční požadavky architektury pro audit bezdrátových sítí založených na standardu 802.1X. Z definovaných požadavků budeme v této části práce zkoumat možnosti využití existujích nástrojů splňujících výše uvedené požadavky.

Obrázek 26: Ukázka výstupu z aplikace crEAP [22]

4.2.1 Detekce EAP metody

Detekce použité autentizační metody je klíčovou součástí bezpečnostního auditu, neboť udává sled dalších kroků v části penetračního testování. V rámci této práce jsme se zabývali dvěma nástroji, které problematiku detekce použitých EAP metod v sítích 802.1X řeší. V této části se na jednotlivé aplikace podíváme detailněji a budeme zkoumat možnosti jejich uplatnění pro připravovanou architekturu testů.

crEAP

Volně dostupný nástroj z repozitáře[34] napsaný v jazyce Python, který umožňuje detekci používaných EAP metod v síti. V případě, kdy zjistí použití nezabezpečené nebo nedostatečně zabezpečené metody EAP, pokusí se shromáždit uživatelské jméno, popřípadě handshake z autentizace klienta. V pasivním režimu umožňuje odposlouchávání komunikace v reálném čase (live capture) z rozhraní bezdrátového adaptéru nebo umožňuje předat zachycenou síťovou komunikaci ve formátu pcap souboru jako parametr. Velkou nevýhodu při analýze tohoto nástroje jsme našli v absenci implementace aktivního režimu detekce EAP metody popsané v kapitole 4.1.2 a možnosti uložení výstupu do souboru ve formě grafického reportu nebo strojově čitelné podoby (např. XML) pro další zpracování. Na obrázku 26 je uveden výřez z aplikace crEAP na standardní výstup do konzole (převzato z [22]).

Nástroj crEAP tak nesplňuje funkční požadavky vyplývající z analýzy a z tohoto důvodu je nevhodný pro využití v architektuře pro testování.

[34] `https://github.com/Shellntel/scripts/blob/master/crEAP.py`

EAPeak, EAPscan

Rodina nástrojů na úrovni implementace velmi podobná předchozímu nástroji `crEAP`, jedná se však o sadu komplexnějších nástrojů s plnou podporou všech definovaných funkčních požadavků jak z pohledu způsobu detekce EAP metody (aktivně, pasivně), tak možností výstupu do souboru ve formátu XML umožňující další zpracování. Vstupem obou aplikací je název sítě (SSID), BSSID (MAC adresa) přístupového bodu a název rozhraní bezdrátového adaptéru, přes který bude s přístupovým bodem komunikovat.

Pasivním odposlechem bezdrátové komunikace s cílem analyzovat použité EAP metody se zabývá nástroj `EAPeak`[35]. Jedná se o konzolovou aplikaci umožňující analyzovat odposlouchávanou komunikaci v reálném čase nebo ji zachytávat do pcap souborů a analyzovat později parametrickým předáním na vstup aplikace. Pro aktivní enumeraci povolených EAP metod využijeme sesterskou aplikaci `EAPscan`[36]. Z pohledu funkcionality se jedná o shodnou aplikaci jako nástroj `EAPeak`, obě napsané v jazyce Python s využitím podpůrných knihoven Scapy a M2Crypto. První verze těchto nástrojů se objevila v roce 2011, v rámci této práce jsme použili verze 0.1.6 . Tyto nástroje nejsou součástí základní instalace distribuce Kali Linux, jsou však k dispozici v oficiálním repozitáři, z kterého jsme vycházeli.

Vzhledem ke splnění všech funkčních požadavků vyplývajících z analýzy využijeme tyto nástroje jako klíčovou část v architektuře testů pro audit 802.1X sítí.

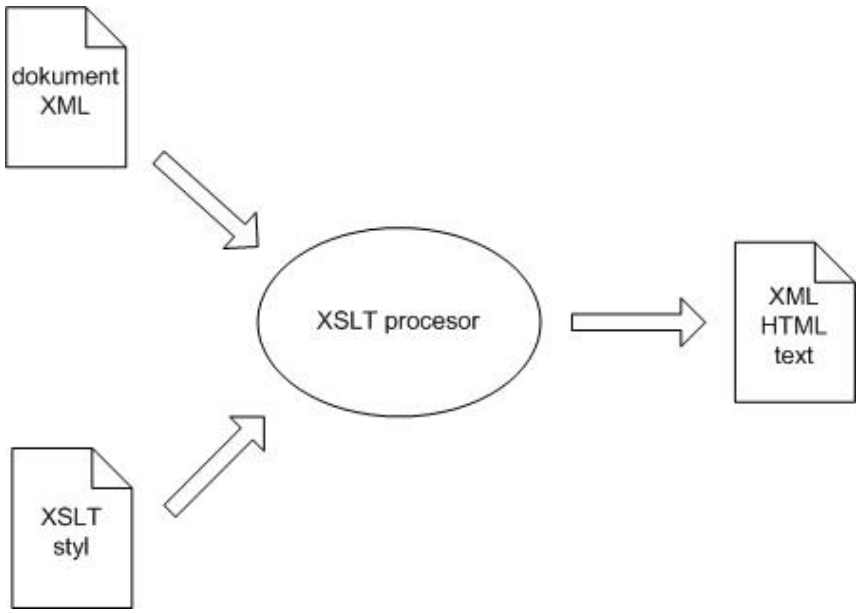
4.2.2 Grafický výstup–report

Jak jsme již zmínili v kapitole 4.2.1, nástroje `EAPeak` a `EAPscan` umožňují uložit výstup do souboru ve formátu XML. Pro potřeby dalšího strojového zpracování je tento formát dat nejlepší možnou volbou, jako podklad pro závěrečnou zprávu z bezpečnostního auditu ale není vhodný. Z tohoto důvodu jsme si implementovali vlastní rozšíření a s výhodou využili právě výstup ve formě XML pro transformaci do grafické podoby. K tomuto účelu využijeme technologii XSLT[37], která slouží k převodům zdrojových dat ve formátu XML do libovolného jiného požadovaného formátu, nejčastěji HTML.

[35] Dostupný z repozitáře `https://github.com/securestate/eapeak`

[36] Dostupný z repozitáře `https://github.com/securestate/eapeak/blob/master/eapscan`

[37] eXtensible Stylesheet Language Transformations



Obrázek 27: Transformace XML dokumentu prostřednictvím technologie XSLT [13]

Pro zpracování (převod) XML dokumentu do požadovaného formátu (využijeme formát HTML, který je pro potřeby výstupu z bezpečnostního auditu nejvhodnější) potřebujeme následující 3 komponenty:

- **XML dokument:** Soubor, obsahující zdrojová data ve formátu XML–v našem případě výstupní data z nástrojů `EAPeak` a `EAPscan`.
- **XSLT styl:** Předpřipravená šablona vytvářející výsledný styl transformovaného dokumentu. Obsahuje kaskádové styly (CSS), HTML a XSL (eXtensible Stylesheet Language) značky.
- **XSLT procesor:** Softwarová implementace XSLT procesoru zprostředkovávající převod ze zdrojového XML dokumentu prostřednictvím XSLT stylu do požadovaného cílového formátu.

Ilustrace transformace XML dokumentu do požadovaného formátu prostřednictvím technologie XSLT je uvedena na obrázku 27 (převzato z [13]).

Při vytváření šablony XSLT stylu jsme využili pro grafický vzhled volně dostupnou sadu nástrojů **Bootstrap**[38] a javascriptovou knihovnu **jQuery** [39]. Transformaci prostřednictvím XSLT procesoru implementujeme v jazyce Python s využitím knihovny `lxml`[40]. Využijeme

[38] `https://www.getbootstrap.com/`

[39] `http://www.jquery.com/`

[40] `http://www.lxml.de/`

tak stejnou platformu, ve které jsou implementovány nástroje `EAPeak` a `EAPscan` pro detekci EAP metody.

4.2.3 Slovníkový útok–odhalení hesla

Slovníkový útok je technika v oblasti počítačové bezpečnosti a kryptoanalýzy, která spočívá ve snaze uhodnout heslo tak, že útočník zkouší pravděpodobná hesla z připraveného seznamu. Tento seznam je nazýván slovníkem. Jedná se o potenciálně efektivnější metodu než útok hrubou silou. Pro tyto účely využijeme připravený slovník z distribuce Kali Linux, o které se zmiňujeme v kapitole 4.2.5. Jeho umístění a způsob použití bude specifikován v kapitole 5.

eapmd5pass, asleap

Nástroje využívající slovníkový útok (`eapmd5pass` a `asleap`) jsou z dílny autora Joshua Wright, který se zabývá výzkumem v oblasti bezdrátových technologií. Jako první upozornil na zranitelnost u metody EAP-LEAP, kterou demonstroval právě s nástrojem `asleap`.

Nástroj `eapmd5pass`, jak již z názvu napovídá, je napsán pro odhalování hesel, která byla odchycena při použití autentizační metody EAP-MD5. Tato metoda používá pro přenos hesla jeho převod na hash prostřednictvím metody MD5.

Nástroj `asleap` je napsán pro odhalování hesel, která byla odchycena při použití autentizační metody EAP-LEAP. Tato metoda používá pro přenos hesla jeho převod na hash prostřednictvím modifikované metody MS-CHAPv1, umí však odhalit hesla, jejichž hash byl vytvořen metodou MS-CHAPv2 (využívá metoda EAP-PEAP).

4.2.4 Podpůrné nástroje

aircrack-ng

Aircrack-ng je balík nástrojů, který je alfou omegou pro penetrační testování bezdrátových sítí. Obsahuje nástroje pro deautentizaci klientů, odchytávání komunikace na bezdrátových sítích a ukládání do pcap souborů, odhalování WEP, WPA klíčů, a další. V naší architektuře jsme využili nástroje `aireplay-ng` a `airodump-ng` pro deautentizaci připojených

bezdrátových klientů a odchytávání bezdrátové komunikace. Pro přepnutí bezdrátové karty do monitorovacího módu pak nástroj `airmon-ng`. V rámci referenční distribuce Kali Linux, na které je celá architektura postavena a testována, jsou tyto nástroje již připraveny a není potřeba je zvlášť doinstalovat.

4.2.5 Aplikační prostředí

Penetrační testování je dost specificky založený obor, který vyžaduje specifické programové vybavení. Vzhledem k potřebě často zasahovat přímo do samotné síťové komunikace na úrovni práce s datovými rámci (druhá vrstva ISO/OSI síťového modelu), případně modifikace samotných paketů, jsou pro tento obor vhodnější unixové platformy. Díky této skutečnosti je většina nástrojů dostupná právě a pouze na této platformě. Pro bezpečnostní audit bezdrátových sítí jsme při návrhu architektury zvolili linuxovou distribuci Kali Linux, která je pro penetrační testování přímo navržena. Obsahuje v základní instalaci předpřipravenou sadu nástrojů, které jsou v navržené architektuře využívány bez nutnosti jejich dodatečné instalace či konfigurace. Zároveň je možné tuto distribuci provozovat v „live“ režimu nastartováním z DVD či flash disku bez nutnosti instalace na disk PC. Pro penetrační testování jsme využili poslední dostupnou verzi této distribuce, která v době psaní této práce byla k dispozici (`kali-linux-2018.1-amd64.iso`). ISO instalační obraz pro 64-bitové systémy je dostupný na přiloženém DVD, viz. příloha 5.6.2.

4.3 Penetrační testování

Cílem penetračního testování je prověření cílového systému na všechny známé zranitelnosti. V případě bezdrátových sítí s autentizací pomocí 802.1X je tím primárním cílem autentizační server RADIUS, autentizátor (přístupový bod) a klient (resp. nastavení klientského suplikantu). Způsob penetračního testování se liší v závislosti na použité EAP metodě vzhledem k odlišným způsobům možného útoku. V této části se zaměříme na penetrační testování dvojího typu, v prvním případě na metody EAP-MD5 a EAP-LEAP, následně pak na metodu EAP-PEAP.

Metody EAP-MD5 a EAP-LEAP

Metody EAP-MD5 a EAP-LEAP mají společný základní princip ověřování klientů, a to pomocí uživatelského jména a hesla. Liší se však ve způsobu, jakým je přenášeno uživatelské heslo. Obě metody při procesu autentizace nevytváří šifrovaný tunel, komunikaci mezi klientem a autentizačním serverem lze odposlechnout. Bezpečnostní slabiny metod byly popsány v kapitolách 2.2.1 (EAP-MD5) a 2.2.2 (EAP-LEAP). Základem pro penetrační testování bude odchycení rámců *Challenge/Response*, získání uživatelského jména, které je přenášeno v otevřeném tvaru (tyto kroky jsou společné pro obě metody) a použití slovníkového útoku na odchycený hash hesla z přenášené komunikace. Penetrační test provedeme s využitím nástrojů:

1. `aireplay-ng` (deautentizace klientů)
2. `airodump-ng` (odchycení komunikace–řetězce *Challenge/Response*)[41]
3. `EAPeak` (detekce použité EAP metody a extrakce uživatelského jména)
4. Slovníkový útok na hash hesla ze zachycených rámců:
    a) `eapmd5pass` pro EAP-MD5
    b) `asleap` pro EAP-LEAP

Všechny nástroje jsou detailně popsány v kapitole 4.2.

Metoda EAP-PEAP

Klíčovým rozdílem u metody EAP-PEAP oproti předchozím je výměna autentizačních údajů mezi klientem a autentizačním serverem v šifrované podobě. Z tohoto důvodu jsou autentizační údaje neodchytitelné[42]. Za určitých předpokladů je však možné provést na metodu EAP-PEAP útok RADIUS impersonation[43]. Bezpečnostní slabiny metody byly detailně popsány v kapitole 2.2.4. Penetrační test cílený na metodu EAP-PEAP využívá modifikovaou verzi RADIUS serveru `freeradius-wpe`[44] spočívající v automatickém ukládání přihlašovacích údajů připojovaných klientů do logovacího souboru. Abychom klienty přinutili ověřovat se vůči podvrženému RADIUS serveru, vytvoříme ještě podvržený

[41] Tento krok lze přeskočit a spustit EAPeak v live módu, při kterém je ve výchozím stavu bezdrátová komunikace odchycena do pcap souboru a zároveň ihned analyzována.

[42] Za předpokladu využití funkce skrytí identity.

[43] V některých literaturách označovaný jako AP impersonation.

[44] `http://www.willhackforsushi.com/?page_id=37`

přístupový bod, který vysílá stejný název sítě tak, aby přístupový bod distribuoval signál s vyšší úrovní signálu než původní. Po deautentizaci se klienti začnou připojovat k přístupovému bodu s vyšší úrovní signálu. Penetrační test provedeme v následujícím sledu kroků s využitím nástrojů:

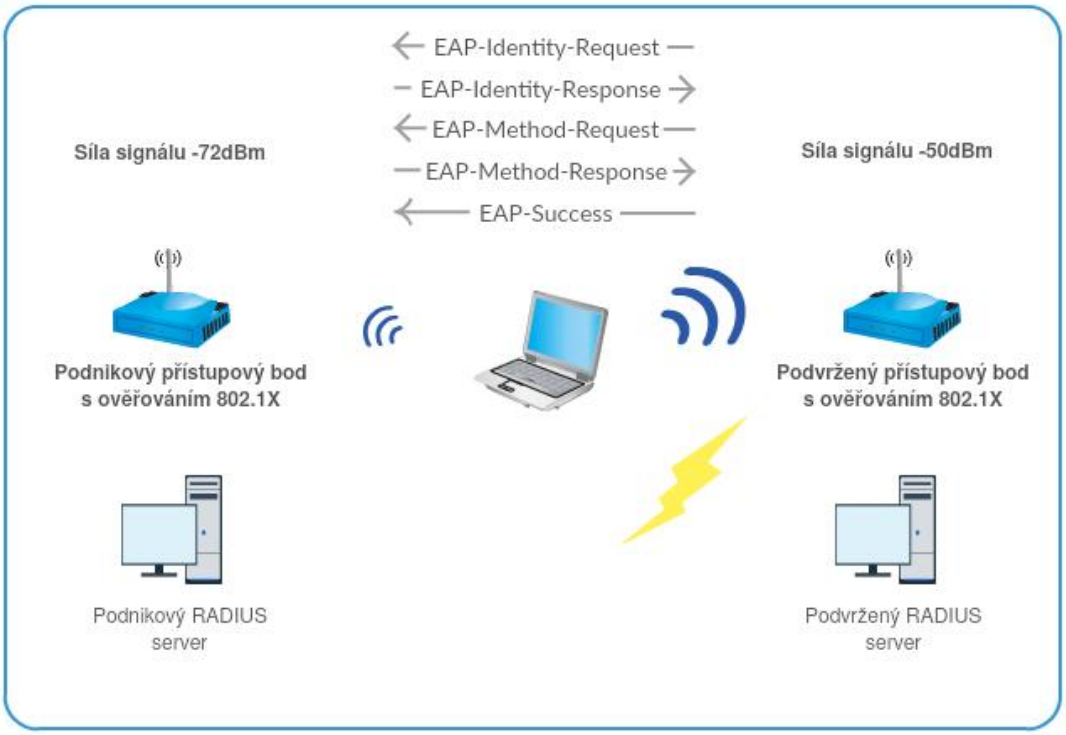
1. Příprava infrastruktury pro provedení útoku RADIUS impersonation za účelem ukládání přihlašovacích údajů poskytnutých klientem při procesu autentizace:
   a) `hostapd-wpe` softwarové řešení, které lze realizovat pomocí jednoho PC (NB) s bezdrátovou WiFi kartou
   b) `freeradius-wpe` kombinace hardwarového a softwarového řešení, pro provedení útoku budeme potřebovat hardwarový přístupový bod (blackbox) a PC s nainstalovým podvrženým RADIUS serverem
2. `aireplay-ng` (deautentizace klientů)
3. Zjištění uživatelského jména z logovacího souboru RADIUS serveru
4. Slovníkový útok na hash hesla z logovacího souboru pomocí `asleap`

Schematický princip útoku RADIUS impersonation je naznačen na obrázku 28. Podmínkou, aby mohl být penetrační test úspěšný, je nastavení suplikantu klienta bez ověřování autencity serveru. V případě, že klient ověřuje autenticitu serveru, je metoda EAP-PEAP bezpečná a útok nelze provést.

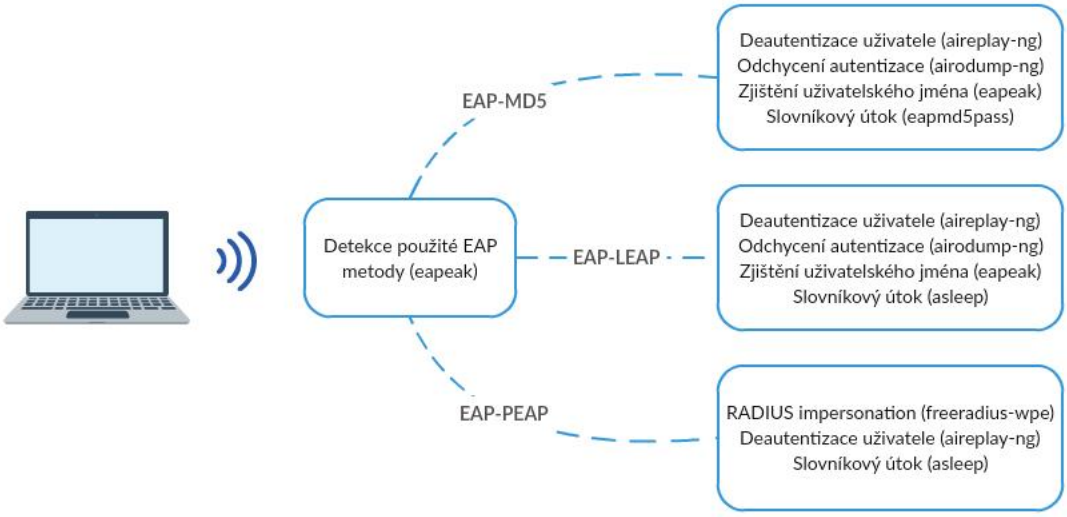
Všechny nástroje jsou detailně popsány v kapitole 4.2.

4.4 Shrnutí

Konečný návrh celé architektury zobrazuje obrázek 29. Je zde vidět detailní pohled na pořadí provedení jednotlivých fází dle navržené metodiky, navržené nástroje plně pokrývající potřebnou funkcionalitu pro provedení bezpečnostního auditu v závislosti na použité autentizační metodě (EAP-MD5, EAP-LEAP, EAP-PEAP). V rámci jednotlivých fází je tak provedena deautentizace klienta, odchycení autentizačních rámců při následném procesu reautentizace, získání uživatelského jména z autentizačních rámců a pokus o provedení slovníkového útoku (u metod EAP-MD5 a EAP-LEAP) a pro metodu EAP-PEAP provedení útoku typu RADIUS impersonation. Jádrem bezpečnostního auditu je nástroj EAPeak, který celý proces auditu zaštiťuje.



Obrázek 28: Princip útoku typu RADIUS impersonation



Obrázek 29: Konečný návrh architektury testů pro audit 802.1X sítí

5 BEZPEČNOSTNÍ AUDIT PODNIKOVÉ SÍTĚ

V této kapitole se zaměříme na provedení bezpečnostního auditu dané síťové infrastruktury. Pro audit využijeme navrženou metodiku v kapitole 3 s provedením pomocí navržené architektury v kapitole 4. Cílem této kapitoly je tak ověřit v praxi navrženou metodiku auditování z pohledu procesního řízení a navrženou architekturou testů pro faktické provedení auditu podnikových sítí založených na standardu 802.1X.

Abychom mohli v rámci bezpečnostního auditu provést otestování autentizačních metod, které se dnes již v sítích nepoužívají vzhledem k jejich zranitelnostem, byl audit proveden v předem připraveném laboratorním prostředí. Testovanou infrastrukturu tvořil bezdrátový přístupový bod simulující podnikovou bezdrátovou síť s nastaveným ověřováním pomocí 802.1X, autentizační server tvořila virtualizovaná distribuce Kali Linux s instalovaným balíčkem `freeradius`. Klient byl zastoupen notebookem s OS Windows 7 s integrovanou WiFi kartou. Počítač útočníka provádějící pasivní odposlech a zprostředkovávající podvrženou síť při útoku *RADIUS impersonation* zastoupil druhý notebook, taktéž s využitím integrované WiFi karty.

V navazujících podkapitolách je detailně popsána příprava infrastruktury a samotný průběh bezpečnostního auditu.

5.1 Příprava infrastruktury pro provedení auditu

Konfigurace přístupového bodu

Jak jsme již uvedli v úvodu kapitoly, podnikovou bezdrátovou síť v laboratorním prostředí tvořil bezdrátový přístupový router (blackbox zařízení). V rámci jeho konfigurace, standardní cestou přes webové rozhraní, jsme jej využili pro zprostředkování rolí DHCP, DNS serveru a brány do internetu. Konfiguraci WLAN jsme nastavili pro ověřování přes RADIUS server dostupným v rámci vnitřního LAN subnetu s předem definovaným sdíleným tajemstvím mezi autentizačním serverem (RADIUS) a autetizátorem (přístupový bod, resp. router).

Konfigurace notebooku klienta

Klientem, který se připojuje k bezdrátové síti, jsme zvolili notebook s OS Windows 7. Vzhledem k tomu, že v této verzi OS již zranitelné metody pro ověřování EAP-MD5 a EAP-LEAP nejsou ve výchozí instalaci dostupné, je potřeba je určitými kroky v systému povolit či doinstalovat.

I když metoda EAP-MD5 nebude v rámci této kapitoly testována, uvedeme alespoň způsob, jakým je možné ji v operačním systému povolit. Úprava spočívá v přidání patřičných klíčů do souboru registru, skrze nástroj `regedit` dostupný v OS. Přesný postup je uveden pod odkazem[45].

V případě metody EAP-LEAP či EAP-FAST (proprietární řešení od společnosti Cisco) je zapotřebí provést doinstalaci z balíčku „Surface Tools for IT“ dostupného na webu[46]. Přesný návod, jak lze v OS Windows dané metody povolit, je uveden v bodě [47] (z důvodu sazby dokumentu je odkaz zkrácen).

Konfigurace notebooku útočníka

Notebook útočníka pro pasivní odposlech je vybaven linuxovou distribucí Kali Linux s doinstalovanými aplikacemi `EAPeak` a `EAPscan` rozšířené o vlastní implementaci generování grafických HTML reportů (za předpokladu spuštění s parametrem `--xml`)[48]. Jejich postup instalace je uveden v příloze 5.4. Ostatní využívané nástroje jsou standardně distribuovány ve výchozí instalaci a není potřeba je zvlášť instalovat (i v případě využití Kali Linux jako Live distribuce–tento scénář je v navržené architektuře podporován).

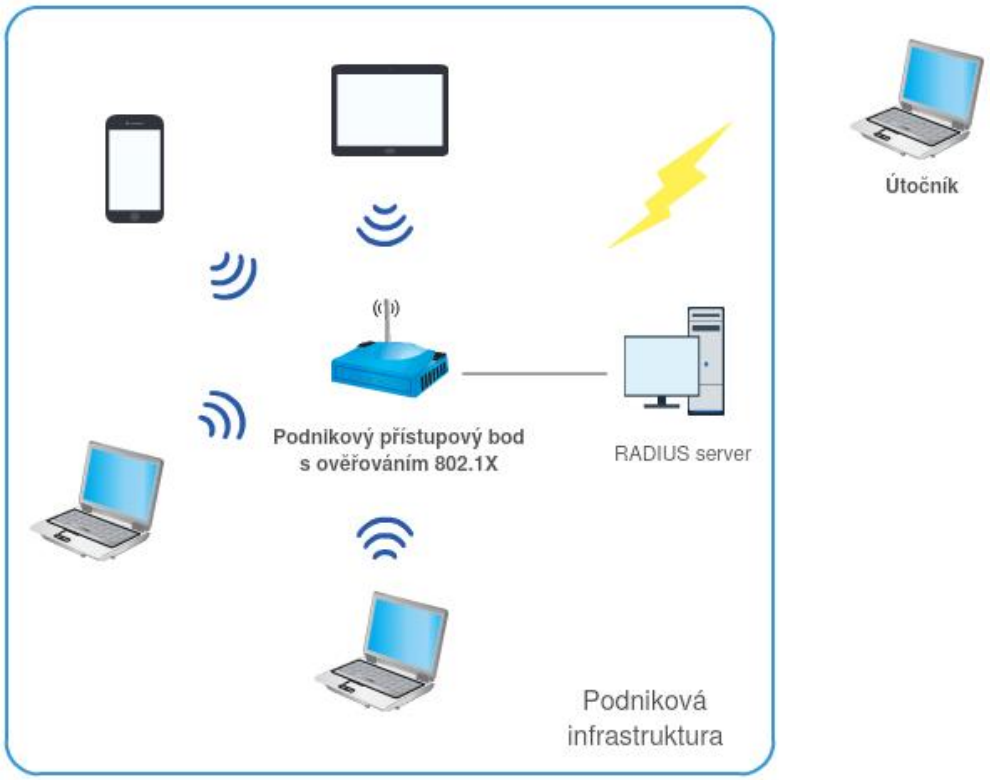
Schéma infrastruktury laboratorního prostředí pro bezpečnostní audit podnikové sítě je uvedeno na obrázku 30.

[45] `http://support.microsoft.com/kb/922574`

[46] `https://www.microsoft.com/en-us/download/details.aspx?id=46703`

[47] `https://www.bit.ly/2rF26JE`

[48] Zdrojové soubory jsou k dispozici na přiloženém DVD–viz. příloha 5.6.2



Obrázek 30: Infrastruktura LAB prostředí pro provedení bezpečnostního auditu

5.2 Detekce používaných EAP metod

Nastavení monitorovacího režimu

Prvním krokem, který musíme provést, je přepnutí WiFi karty notebooku útočníka do tzv. monitorovacího režimu. Tento režim nám zajistí možnost odchytávání celé komunikace v rámci nastaveného WiFi kanálu bezdrátové karty, nebo v rámci konkrétního přístupového bodu dle BSSID. Přepnutí do tohoto režimu provedeme pomocí nástroje `airmon-ng` dostupném v balíku `aircrack-ng`[49]. Nástroj je součástí distribuce Kali Linux, není potřeba jej tedy doinstalovávat. V notebooku útočníka je bezdrátová karta v rámci OS identifikována jako *wlan0*, změnu režimu tak provedeme dvojicí příkazů:

```
1: airmon-ng check kill

2: airmon-ng start wlan0
```

[49] `https://www.aircrack-ng.org/`

První příkaz provede kontrolu závislých služeb, které by mohly při přepnutí do monitorovacího režimu karty způsobit problémy (typicky služba wpa_supplicant, případně network-manager). Pomocí druhého příkazu provedeme faktické přepnutí. Úspěšné nastavení monitorovacího režimu lze ověřit příkazem `iwconfig`.

Získání informací o dostupných sítích, odchycení komunikace

V dalším kroku potřebujeme získat informace o cílové WiFi síti, nad kterou chceme provést bezpečnostní audit. Klíčové jsou parametry SSID a BSSID sítě. Pro získání informací použijeme nástroj `airodump-ng` na rozhraní *wlan0mon*.

```
airodump-ng wlan0mon
```

Výsledkem bude výpis všech dostupných sítí (skenování probíhalo přes všech 13 kanálů, pokud nebude upřesněno parametrem jinak) s informacemi o jejich SSID a BSSID. Ze seznamu vybereme cílovou síť a spustíme zachytávání komunikace v této síti do souboru:

```
airodump-ng -c 1 -d 00:23:69:da:36:1a -w audit.pcap wlan0mon
```

Parametr `-c` definuje kanál, na kterém cílová síť vysílá; `-d` BSSID sítě, u které chceme komunikaci zachytávat a `-w` zachycenou komunikaci uloží do souboru požadovaného názvu.

Pomocí aplikace `EAPeak` provedeme analýzu zachycené komunikace a získáme seznam asociovaných klientů k dané síti:

```
EAPeak -f audit.pcap
```

Abychom v rámci auditu mohli testovat již připojené klienty potřebujeme zajistit jejich deautentizaci, aby došlo k jejich opětovnému připojení, a mohli jsme tak odchytit i tuto komunikaci. K tomu použijeme nástroj `aireplay` s parametrem `-a` definujícím MAC adresu klienta, kterému zašle deautentizační rámec (parametr `-0`) následovaným parametrem 3 určující počet zaslaných rámců.

```
aireplay-ng -0 3 wlan0mon -a < MAC_address >
```

S tímto příkazem zároveň znovu spustíme zachytávání probíhající komunikace:

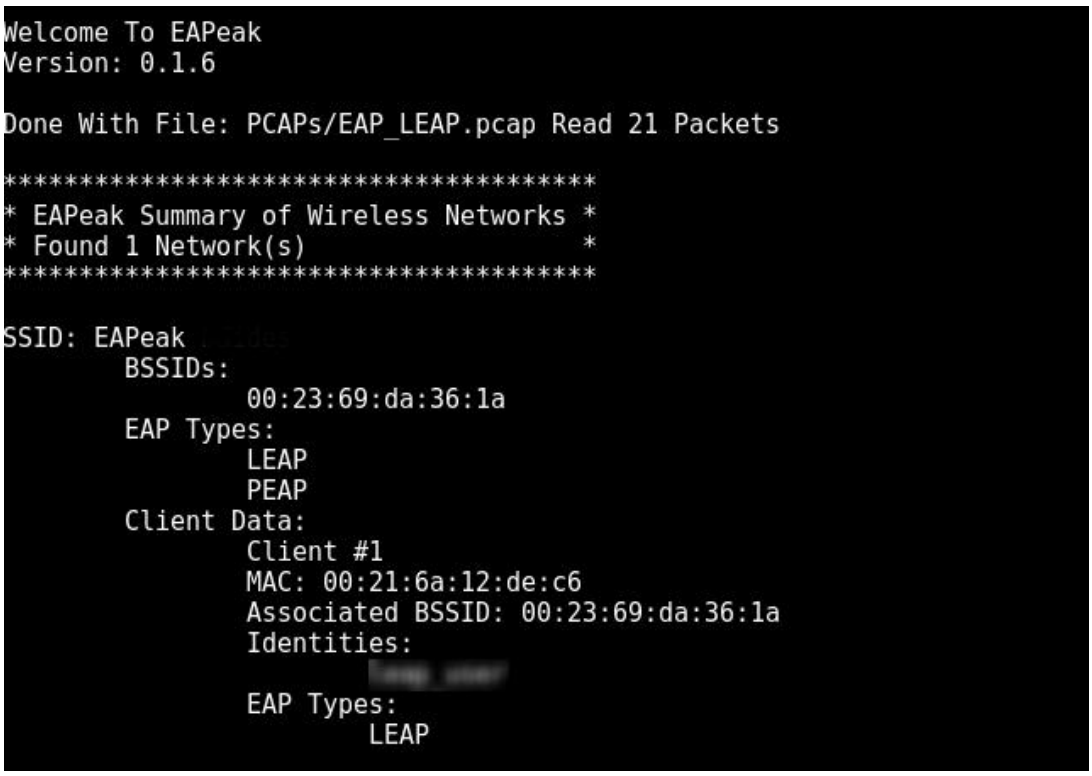
```
airodump-ng -c 1 -d 00:23:69:da:36:1a -w EAP_LEAP.pcap
wlan0mon
```

Zachycenou komunikaci v souboru *EAP_LEAP.pcap* již můžeme považovat za dostatečný vzorek dat (zachycuje všechny klienty, kteří již byli asociováni k přístupovému bodu a zároveň všechny nově se autentizující po dobu probíhajícího odchytávání nástrojem `airodump`). Spustíme nad souborem *EAP_LEAP.pcap* aplikaci `EAPeak` s parametrem `--xml` a získáme XML výstup do souboru a zároveň HTML report s detekovanými EAP metodami použitými klienty včetně seznamu všech uživatelských jmen použitých pro autentizaci. Výstup aplikace `EAPeak` na standardní výstup do konzole (stdout) po provedení analýzy zachycené komunikace je vidět na obrázku 31. Podobu grafického HTML reportu zobrazuje obrázek 32. Dle pravidel etického hackingu nejsou některé údaje zveřejňovány.

```
EAPeak -f EAP_LEAP.pcap --xml
```

Po analýze komunikace na výstupu vidíme použití metody EAP-LEAP, proprietární metody od společnosti Cisco, která již dnes není považována za bezpečnou. V rámci prováděného bezpečnostního auditu byla tato metoda zařazena záměrně pro možnost vykonání penetračního testu nad touto zachycenou komunikací. Zároveň ve výstupu vidíme využívanou metodu PEAP, která bude v kapitole 5.3.2 podrobena pokusu o útok *RADIUS impersonation*.

Ověření, že jsou tyto metody skutečně na RADIUS serveru povoleny, můžeme provést pomocí aplikace `EAPscan`, která simuluje chování klienta a aktivním způsobem se snaží k přístupovému bodu autentizovat pomocí dané metody. Ověření lze provést následovně:



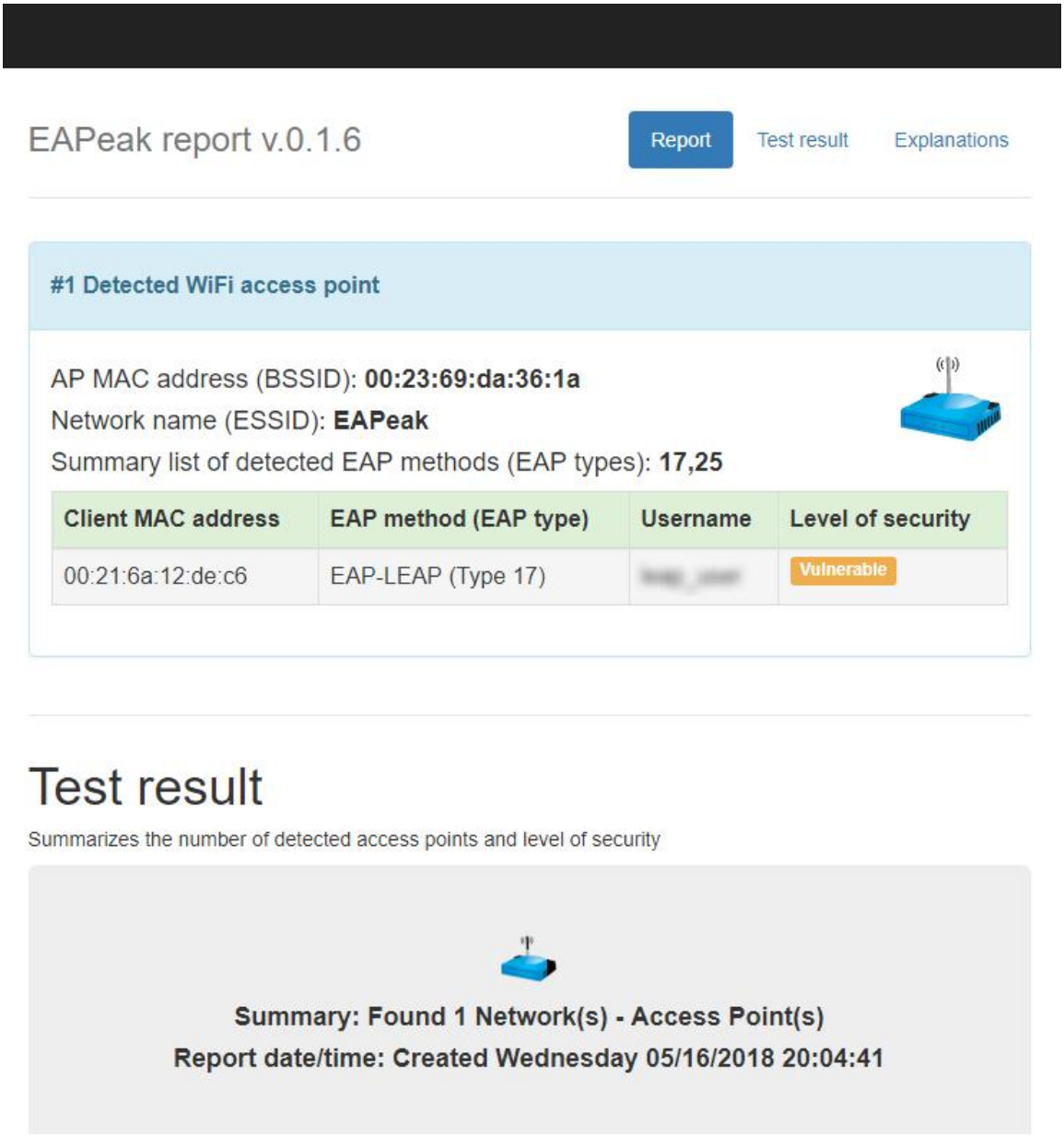
Obrázek 31: Pasivní detekce EAP metody pomocí nástroje EAPeak

```
EAPscan -e EAPeak -b 00:23:69:da:36:1a -i wlan0mon -c 1
```

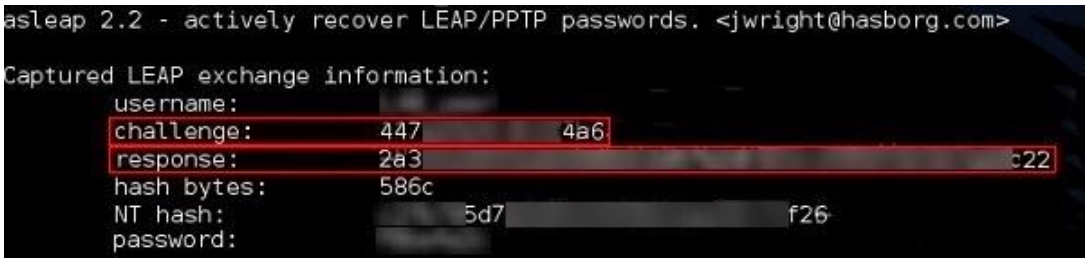
Výstupem aplikace `EAPscan` je sekvenčně seřazený seznam všech dostupných EAP metod, které byly otestovány vůči RADIUS serveru.

5.3 Provedení sady penetračních testů

V předchozí kapitole jsme díky aplikaci `EAPpeak` detekovali používané metody pro autentizaci a získali seznam uživatelských jmen ze zachycené komunikace. Zjistili jsme přítomnost metod EAP-LEAP a EAP-PEAP, které jsou za určitých okolností náchylné na možné zneužití. V této kapitole se v rámci penetračního testování na tyto jednotlivé metody zaměříme a prověříme je sadou bezpečnostních testů aplikovatelných na konkrétní metody.



Obrázek 32: Pasivní detekce EAP metody pomocí nástroje EAPeak–HTML report



Obrázek 33: Získání uživatelského hesla ze zachycené komunikace–metoda EAP-LEAP

5.3.1 EAP-LEAP

Možnosti využití zranitelnosti u metody EAP-LEAP byly popsány v kapitole 2.2.2. Odchycenou komunikaci včetně rámců *Challenge/Response* máme již zachycenou v souboru *EAP_LEAP.pcap*, můžeme tak provést penetrační test s využitím nástroje `asleap`:

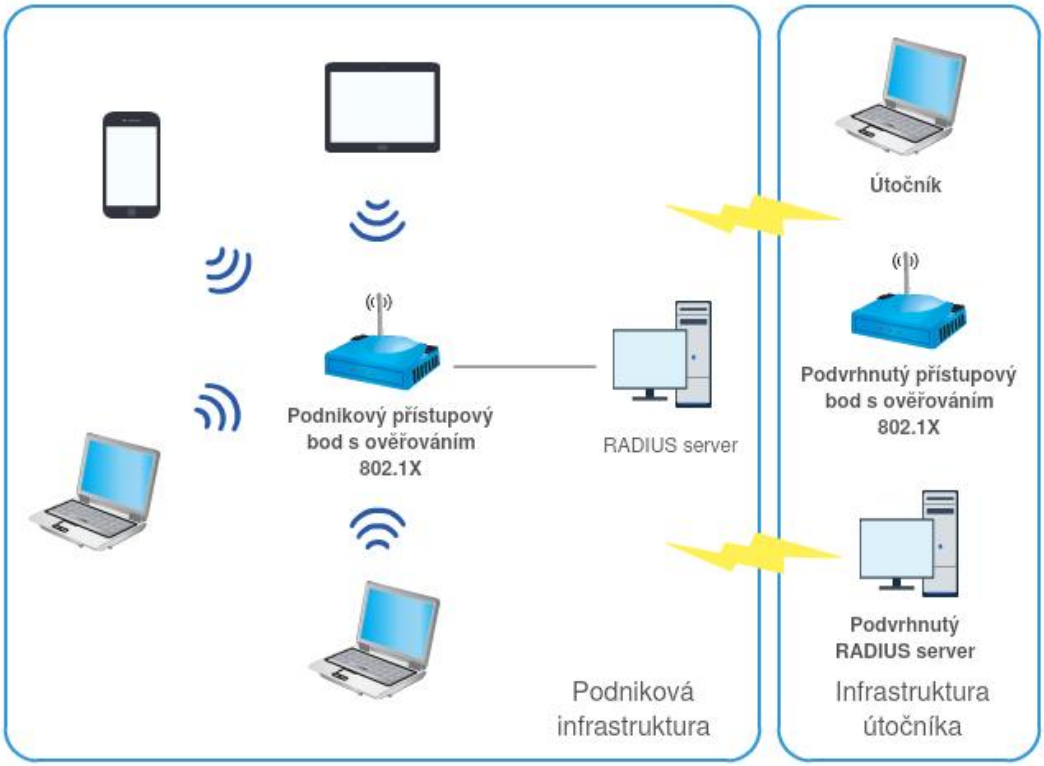
```
asleap -r EAP_LEAP.pcap -W /usr/share/wordlist/rockyou.txt.gz
```

Parametrem `-W` předáváme slovník, který je standardně dodáván s distribucí Kali Linux. Je provedena extrakce rámců *Challenge/Response* a použit slovníkový útok na přenášený hash kód. Pokud je porovnávaný hash shodný s hashem ze slovníku, máme uživatelské heslo. Výstup z nástroje `asleap` je vidět na obrázku 33. Dle pravidel etického hackingu nejsou opět některé údaje zveřejňovány.

Nalezení hesla pomocí slovníkového útoku značí, že uživatelské heslo bylo nastaveno velmi jednoduše, bez jakýkoliv známek komplexnosti. Z tohoto důvodu bylo i odhalitelné v rámci slovníkového útoku. V případě potřeby stále využívat metodu EAP-LEAP pro autentizaci je silně doporučováno nastavit v rámci bezpečnostních politik společnosti zásady tvorby uživatelských hesel. Pokud si uživatel vytvoří heslo splňující prvky komplexnosti, slovníkový útok ztrácí na své síle a heslo nemusí odhalit.

5.3.2 EAP-PEAP

I když je metoda EAP-PEAP ve své podstatě bezpečná, pokud není správně nakonfigurována na straně klienta, je možné ji zneužít pomocí útoku typu *RADIUS impersonation*. Tento typ útoku jsme detailně rozebírali v kapitole 2.2.4. Abychom mohli simulovat tento



Obrázek 34: Infrastruktura LAB prostředí pro provedení útoku RADIUS impersonation

typ útoku, musíme částečně modifikovat LAB infrastrukturu. Na notebooku útočníka spustíme nástroj `hostapd-wpe`, který vytvoří softwarově přístupový bod se stejným SSID jako je bezdrátová síť nastavená na přístupovém bodu (blackbox zařízení) (tzv. falešný přístupový bod[50]). Součástí balíčku je i instalace modifikovaného RADIUS serveru, který zapisuje celý proces autentizace klientů (včetně přihlašovacích údajů) do textového souboru. Pro dosažení úspěšnosti útoku je zapotřebí, aby podvržený přístupový bod vysílal z pohledu připojujících se klientů signál s vyšší úrovní. Abychom této potřebě dostáli v LAB prostředí, záměrně snížíme vysílací výkon na přístupovém bodu (blackbox zařízení) na minimum. Schéma infrastruktury LAB prostředí je uvedeno na obrázku 34.

V této fázi již nic nebrání faktickému provedení útoku. Opětovným zasláním deautentizačních rámců donutíme připojené klienty k odpojení od připojeného přístupového bodu a následnému připojení k nově vytvořenému, falešnému. Pokud je suplikant klienta nastaven bez ověření RADIUS serveru, nebude mít problém se ověřit vůči našemu podvrženému RADIUS serveru, který poskytnuté přístupové údaje uloží v logovacím souboru.

[50]Můžeme se setkat i s pojmem Rogue AP.

Obrázek 35: Získání uživatelského hesla ze zachycené komunikace–metoda EAP-PEAP

Máme tak již k dispozici uživatelské jméno v otevřené podobě a potřebujeme pouze zjistit uživatelské heslo. Stejným způsobem jako v případě metody LEAP provedeme slovníkový útok na hash hesla nástrojem `asleap` a pokusíme se heslo odhalit. Pokud měl uživatel nastavené slabé heslo, útok bude úspěšný. Náhled na obsah log souboru podvrženého RADIUS serveru je na obrázku 35.

Doporučením pro znemožnění využití tohoto útoku je mít správně nastavené suplikanty připojujících se klientů pro ověřování poskytnutého certifikátu RADIUS serveru. V případě použití interních certifikátů je zapotřebí mít na klientech vydávající certifikační autoritu importovanou jako důvěryhodnou (např. přes skupinové politiky–Group policy). Druhou zásadou je mít nastavena dostatečně silná uživatelská hesla, jak již bylo zmíněno u metody LEAP.

5.3.3 Audit komponent architektury 802.1X

Vzhledem k provádění auditu v laboratorním prostředí, nikoliv v reálném prostředí bezdrátové sítě, nebyla tato část provedena. V obecné rovině tato část testování spadá do tzv. whitebox testování, kdy je prověřována konfigurace jednotlivých prvků sítě (v případě testování architektury 802.1X jsou těmito prvky klientské zařízení, přístupový bod–autentizátor a autentizační server). Zkoumá se jejich konfigurace, verze instalovaného software (firmware) a v případě nálezu chyby umožňující zneužití, je doporučeno nápravné opatření.

5.4 Shrnutí auditu

Provedli jsme bezpečnostní audit infrastruktury bezdrátové sítě s implementovaným ověřováním uživatelů prostřednictvím standardu 802.1X. Bezpečnostní audit probíhal v laboratorním prostředí v rámci přesně dané vlastní metodiky navržené v kapitole 3. Metodika zahrnuje fáze:

Zjištění použité metody EAP

S využitím navržených nástrojů v rámci architektury pro audit 802.1X sítí jsme detekovali použití dvou metod pro ověřování, metody EAP-LEAP a EAP-PEAP. První z uvedených metod je již dnes považována za zastaralou a nedoporučuje se její využívání z důvodu možné kompromitace přihlašovacích údajů. Druhá metoda, EAP-PEAP, je dnes jednou z nejrozšířenějších, avšak při nevhodné konfiguraci může být taktéž zranitelná. V rámci bezpečnostního auditu a penetračního testování jsme tak na obě metody aplikovali sadu nástrojů, které prokázaly jejich slabiny a zranitelnosti.

Získání uživatelského jména

Uživatelské jméno je u metody EAP-LEAP přenášeno v otevřené podobě. Tento způsob přenosu plyne z návrhu metody a v praktickém auditu jsme tuto skutečnost ověřili. V případě kompromitace hesla je pak tento fakt velmi ulehčující pro zneužití přístupu. Metoda EAP-PEAP umožňuje uživatelské jméno skrýt v rámci funkce „skrytí identity“, avšak v auditu jsme si ověřili, že je přenášeno v otevřené podobě. Klient, který byl pro audit použit, byl notebook s dnes běžně používaným OS Windows 7, do značné míry tak záleží na klientovi, zda-li tuto funkcionalitu umí využít. Metoda EAP-PEAP ji však podporuje.

Prolomení uživatelského hesla

Prolomení uživatelského hesla je disciplína v rámci penetračního testování. Postup, jakým je potenciálně možné prolomit přenášená uživatelská hesla u obou zmíněných metod, jsme v rámci auditu vyzkoušeli a v obou případech úspěšně získali uživatelská hesla. Do značné míry tomu pomohla jednoduchost hesel, která nejsou odolná proti slovníkovému útoku. V rámci etického hackingu jsme však uživatelská jména ani hesla nezveřejnili.

Bezpečnostním auditem jsme ověřili správnost návrhu metodiky pro testování podnikových bezdrátových sítí založených na autentizaci a ověřování uživatelů pomocí 802.1X. Zároveň provedený bezpečnostní audit referenční sítě potvrdil teoretické znalosti o zranitelnostech jednotlivých metod EAP. Výstupem bezpečnostního auditu je automaticky generovaný HTML report zaměřený na úroveň bezpečnosti auditované sítě.

ZÁVĚR

Diplomová práce se zabývá zabezpečením komunikace v podnikových sítích s primárním zaměřením na bezdrátové sítě využívající pro ověřování standard 802.1X. V úvodní, teoretické kapitole 1 jsme rozebrali vývoj standardů bezdrátových sítí, které kromě definice způsobu přenosu po fyzickém médiu zahrnují i principy zabezpečení bezdrátových sítí. Rozebrali jsme způsoby zabezpečení vhodné pro podnikové využití, poukázali na metody, které dnes již není vhodné využívat z důvodu možné kompromitace přenášených dat. Primárně jsme se však zaměřili na zabezpečení sítí založených na autentizaci pomocí standardu 802.1X. Tento způsob ověřování je již od počátku návrhu standardu určen do podnikového prostředí, jednak díky své robustnosti, zároveň ale i pro vyšší nároky na implementaci. V rámci teoretické kapitoly jsme popsali prvky provádějící autentizaci v rámci 802.1X a představili srdce celého systému–autentizační framework EAP. Ten zapouzdřuje jednotlivé metody EAP, které definují způsob, jakým jsou přenášeny přístupové údaje– tedy zabezpečení. V práci se v kapitole 2 zabýváme metodami EAP-MD5, EAP-LEAP, EAP-FAST, EAP-PEAP, EAP-TLS, které jsme podrobili detailnímu zkoumání, co se jejich bezpečnosti týče. V případě, že je metoda za určitých okolností zranitelná, jsme popsali způsob, jakým je možné zranitelnost využít a navrhli i doporučení, jak lze míru zranitelnosti minimalizovat v případě nutného využívání dané metody.

V další části práce (kapitola 3) jsme se obecně zabývali metodikami provádění bezpečnostních auditů. Popsali jsme základní metodiky, které jsou volně dostupné, avšak definující způsob provádění auditu na velmi abstraktní úrovni. Z tohoto důvodu jsme si zavedli metodiku vlastní, zabývající se přímo auditem bezdrátových sítí s ověřováním pomocí 802.1X. Návrh vlastní metodiky je součástí praktické části této práce.

Vlastní metodika auditu vytvořila základ pro jádro praktické části této práce–vytvoření architektury testů pro audit bezdrátových sítí využívající standard 802.1X (kapitola 4). Vlastní metodika definuje v teoretické rovině způsob a metody, jakým má být bezpečnostní audit proveden, architektura testů se zabývá praktickým provedením auditu. Detailně popisuje, jak má být audit proveden u konkrétních metod, jaké nástroje využít pro penetrační testování, poskytuje výstup z bezpečnostního auditu do souboru ve formátu XML pro možnost dalšího zpracování a HTML report jako protokol z bezpečnostního auditu zaměřený na úroveň bezpečnosti auditované sítě.

V závěrečné části práce 5 jsme prakticky ověřili správnost návrhu metodiky a architektury testů pro bezpečnostní audit podnikových sítí v rámci reálného testu nad referenční infrastrukturou. Výstupem bezpečnostního auditu je automaticky generovaný HTML report zaměřený na úroveň bezpečnosti auditované sítě.

Shrnutí výsledků

Bezdrátové sítě jsou přítomny všude kolem nás a předpokládá se jejich masivní rozšiřování. Z pohledu propustnosti a kapacitního přenosu se dnes již vyrovnají metalickým sítím, které vlivem toho mohou ustupovat do pozadí. Téma zabezpečení bezdrátových sítí je tak stále velmi aktuální. Snahou autora této práce bylo poukázat na aktuální možnosti způsobu zabezpečení podnikových sítí LAN, ke kterým bezdrátové sítě dnes již neodmyslitelně patří.

V menších podnikových sítí, kde nemáme k dispozici vybudovanou síťovou infrastrukturu, je situace dnes velmi jednoduchá a z pohledu zabezpečení sítě jasně daná–zabezpečení pomocí WPA2. Tento typ zabezpečení je dostupný již od roku 2004 a od roku 2006 dokonce povinný pro implementaci ze strany výrobců bezdrátových zařízení. Podpora napříč všemi zařízeními tak dnes již je a není důvod využívat starší zabezpečovací mechanismy.

U rozsáhlejších podnikových sítí je situace složitější, neboť síťová infrastruktura bývá zpravidla komplexnější a přechod na jiný způsob zabezpečení může být komplikovaný. Obecně však lze pro bezdrátové sítě dle standardu 802.1X doporučit autentizaci pomocí metody EAP-TLS, která je považována za bezpečnou. Její nasazení však přináší vyšší nároky na implementaci a údržbu vzhledem k využívání klientských certifikátů pro autentizaci. Často tak společnosti dávají přednost metodě EAP-PEAP, která je zároveň jednou z nejrozšířenějších. Je však potřeba důsledně zabezpečit nastavení klientů (suplikantů) tak, aby ověřovali autenticitu RADIUS serveru a nemohla být metoda EAP-PEAP náchylná na útok. Při splnění těchto podmínek můžeme nasazení metody EAP-PEAP doporučit.

POUŽITÁ LITERATURA

[1] Aboba, B.; Blunk, L.; Vollbrecht, J.; aj.: Extensible Authentication Protocol (EAP), [online]. 2004 [cit. 2017-07-25].
URL `https://tools.ietf.org/html/rfc3748`

[2] Apprize.info: Mastering Kali Linux Wireless Pentesting, [online]. 2016 [cit. 2017-07-09].
URL `http://apprize.info/linux/kali/5.html`

[3] ASSOCIATION, I. S.: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, [online]. 2016-12-07 [cit. 2017-07-09].
URL `http://standards.ieee.org/getieee802/download/802.11-2016.pdf`

[4] Benton, K.: The Evolution of 802.11 Wireless Security, [online]. 2010-04-18 [cit. 2017-07-07].
URL
`http://homes.soic.indiana.edu/ktbenton/research/benton_wireless.pdf`

[5] Burda, K.: *Bezpečnost informačních systémů*. Skripta VUT Brno, 2005.

[6] Church, C.: EAP Authentication Protocols, [online]. 2009 [cit. 2017-07-25].
URL
`https://layer3.wordpress.com/2009/08/16/eap-authentication-protocols`

[7] Cisco.com: EAP-FAST Authentication with Wireless LAN Controllers and External RADIUS Server Configuration Example, [online]. 2012 [cit. 2017-07-26].
URL `http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/99791-eapfast-wlc-rad-config.html`

[8] Cisco.com: 802.11 Network Security Fundamentals, [online]. 2017 [cit. 2017-07-09].
URL `http://www.cisco.com/en/US/docs/wireless/wlan_adapter/secure_client/5.1.0/administration/guide/C1_Network_Security.html`

[9] Geier, J. T.: *Implementing 802.1X security solutions for wired and wireless networks*. Hoboken, N.J.: Wiley, c2008, ISBN 9780470168608.

[10] Herzog, P.; Barceló, M.: OSSTMM 3–The Open Source Security Testing Methodology Manual, [online]. 2010 [cit. 2017-08-03].
URL http://www.isecom.org/mirror/OSSTMM.3.pdf

[11] Huňka, T.: Technologie počítačových sítí RADIUS, [online]. 2005-01-15 [cit. 2017-07-09].
URL http://www.cs.vsb.cz/grygarek/TPS/projekty/0405Z/RADIUS/

[12] Jensen, M. A.; Wallace, J. W.: A review of antennas and propagation for MIMO wireless communications. *IEEE Transactions on Antennas and Propagation*, ročník 52, č. 11, Nov 2004: s. 2810–2824, ISSN 0018-926X, doi:10.1109/TAP.2004.835272.

[13] Kosek, J.: XSLT v příkladech, [online]. 2014-11-10 [cit. 2018-05-06].
URL http://www.kosek.cz/xml/xslt/

[14] Matthew, G.: *802.11 wireless networks: the definitive guide*. O'Reilly, 2005, ISBN 978-0-596-10052-0.

[15] McCabe, J. D.: *Network analysis, architecture, and design*. Boston: Elsevier/Morgan Kaufmann Publishers, třetí vydání, c2007, ISBN 978-0123704801.

[16] Miller, K. W.; Voas, J.; Hurlburt, G. F.: BYOD: Security and Privacy Considerations. *IT Professional*, ročník 14, č. 5, Sept 2012: s. 53–55, ISSN 1520-9202, doi:10.1109/MITP.2012.93.

[17] Ong, E. H.; Kneckt, J.; Alanen, O.; aj.: IEEE 802.11ac: Enhancements for very high throughput WLANs. In *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*, Sept 2011, ISSN 2166-9570, s. 849–853, doi:10.1109/PIMRC.2011.6140087.

[18] Reynolds, J.: When 802.1x/PEAP/EAP-TTLS Is Worse Than No Wireless Security, [online]. 2010-11-19 [cit. 2017-07-31].
URL https://depthsecurity.com/blog/when-802-1x-peap-eap-ttls-is-worse-than-no-wireless-security

[19] Rigney, C.; Willens, S.; Rubens, A.; aj.: Remote Authentication Dial In User Service (RADIUS), [online]. 2000 [cit. 2017-07-25].
URL https://tools.ietf.org/html/rfc2865

[20] Robyns, P.; Bonné, B.; Quax, P.; aj.: Short Paper: Exploiting WPA2-enterprise Vendor Implementation Weaknesses Through Challenge Response Oracles. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, WiSec '14, New York, NY, USA: ACM, 2014, ISBN 978-1-4503-2972-9, s. 189–194, doi:10.1145/2627393.2627411.
URL http://doi.acm.org/10.1145/2627393.2627411

[21] SELECKÝ, M.: *Penetrační testy a exploitace*. Computer Press, 2012, ISBN 978-80-251-3752-9.

[22] Travis: crEAP–Harvesting Users on Enterprise Wireless Networks, [online]. 2015-10-01 [cit. 2018-05-06].
URL https://www.shellntel.com/blog/2015/9/23/assessing-enterprise-wireless-networks

[23] Vaněk, T.: Zabezpečení bezdrátových sítí IEEE 802.11, [online]. 2013-09-04 [cit. 2017-07-09].
URL http://data.cedupoint.cz/oppa_e-learning/2_KME/043.pdf

[24] Vladimirov, A.; Gavrilenko, K.; Mikhailovsky, A.: *Hacking Exposed Cisco Networks: Cisco Security Secrets and Solutions*. McGraw-Hill/Osborne, 2006, ISBN 0-07-225917-5.

[25] Whitley, T.: ASLEAP to Exploit Vulnerabilities in Cisco LEAP, [online]. 2004 [cit. 2017-07-26].
URL https://www.giac.org/paper/gcih/589/asleap-exploit-vulnerabilities-cisco-leap/106234

SEZNAM PŘÍLOH

PŘÍLOHA A – INSTALACE PROSTŘEDÍ PRO PROVEDENÍ BEZPEČNOSTNÍHO AUDITU

5.5 Požadavky na programové vybavení

Typ aplikace	Název programu	Požadovaná verze
běhové prostředí (OS)	Kali Linux	2018.1
aplikace	EAPeak	0.1.6
aplikace	EAPscan	0.1.6
aplikační prostředí EAPeak, EAPscan	Python	>= 2.6
závislost pro EAPeak, EAPscan	Scapy	poslední verze
závislost pro EAPeak, EAPscan	M2Crypto	poslední verze

Tabulka 5: Požadavky na programové vybavení

5.6 Instalace rozšiřujících aplikací

5.6.1 Předinstalační upozornění

»Před instalací zkontrolujte prostředí pro běh aplikací!

»Minimální požadavky pro správné fungování aplikací jsou popsány v kapitole 5.5

Následující kroky již předpokládají správné nastavení prostředí pro běh aplikací a spuštěnou linuxovou distribuci Kali Linux 64-bit. Je podporována možnost spuštění jako „Live CD“ bez nutnosti fyzické instalace na disk.

5.6.2 Postup instalace

V rámci výchozí instalace distribuce Kali Linux verze 2018.1 je již předpřipravené aplikační prostředí pro běh skriptů napsaných v jazyku Python pro verzi 2.7. V tomto ohledu tak není potřeba žádná příprava prostředí pro běh aplikací–vše je již nachystáno.

Knihovna Scapy

Spustíme si konzoli (shell) a zadáme následující příkaz (instalace probíhá z online repozitáře Kali Linux přes balíčkovací systém .deb–vyžaduje dostupnost konektivity do internetu):

```
root@kali: sudo apt-get install scapy
```

V některých distribucích Kali Linux je již knihovna Scapy nainstalována. Pokud tomu tak je, balíčkovací systém o tom informuje a tento krok je možné přeskočit.

Aplikace EAPeak, EAPscan

Přes konzoli (shell) spustíme z adresáře kde se nachází zdrojové soubory následující skripty:

```
root@kali: python setup.py build &&
           sudo python setup.py install
```

Rozšíření pro automatické generování HTML reportů je součástí zdrojových souborů pro EAPeak a EAPscan. Výchozí konfigurace rozšíření předpokládá umístění zdrojového XSL souboru (`eapeak_template.xsl`) a datového XML souboru (`eapeak_report.xml`) v kořenovém adresáři zdrojových souborů. Výstup v podobě HTML souboru je ukládán taktéž do stejného umístění (`eapeak_report.html`).

RADIUS server–freeradius-wpe

Spustíme si konzoli (shell) a zadáme následující příkaz (instalace probíhá z online repozitáře Kali Linux přes balíčkovací systém .deb–vyžaduje dostupnost konektivity do internetu):

```
root@kali: sudo apt-get install freeradius-wpe
```

Softwarový AP s RADIUS serverem–hostapd-wpe

Spustíme si konzoli (shell) a zadáme následující příkaz (instalace probíhá z online repozitáře Kali Linux přes balíčkovací systém .deb–vyžaduje dostupnost konektivity do internetu):

```
root@kali: sudo apt-get install hostapd-wpe
```

PŘÍLOHA B – SEZNAM EAP METOD DLE TYPOVÉHO OZNAČENÍ

Přiložený seznam všech typů EAP metod, které byly navrženy v rámci jednotlivých RFC dokumentů a mohou být implementovány. Nejvyužívanější typy EAP metod jsou rozebírány v kapitole 1.6.2.

Převzato z `https://www.vocal.com/secure-communication/eap-types`.

EAP Types – Extensible Authentication Protocol Types information

Type	Description	Reference
0	Reserved	RFC 3748
1	Identify	RFC 3748
2	Notification	RFC 3748
3	NAK (Response Only)	RFC 3748
4	MD5-Challenge	RFC 3748
5	OTP, One Time Password	RFC 2289RFC 3748
6	GTC, Generic Token Card	RFC 3748
7	Allocated	
8	Allocated	
9	RSA Public Key Authentication	RFC-draft-ietf-pppext-eaprsa-04.txt
10	RSA Public Key Authentication	RFC-draft-ietf-pppext-eapdss-01.txtNIST FIPS PUB 196
11	KEA	RFC-draft-ietf-pppext-eapkea-01.txt
12	KEA-VALIDATE	RFC-draft-ietf-pppext-eapkea-01.txt
13	EAP-TLS Authentication Protocol	RFC 5216
14	Quest Defender Token	
15	RSA Security SecurID EAP	RFC-draft-josefsson-eap-securid-01.txt
16	Arcot System EAP	
17	Cisco-LEAP	
18	EAP-SIM, GSM Subscriber Identity Modules	RFC 4186
19	SRP-SHA-1 Part 1	RFC-draft-ietf-pppext-eap-srp-03.txt
20	SRP-SHA-1 Part 2	RFC-draft-ietf-pppext-eap-srp-01.txt
21	EAP-TTLS, EAP Tunneled TLS Authentication Protocol	RFC 5281
22	Remote Access Service	
23	EAP-AKA, EAP method for 3rd Generation Authentication and Key Agreement	RFC 4187
24	EAP-3Com Wireless	
25	PEAP, Protected EAP	RFC-draft-josefsson-pppext-eap-tls-eap-06.txt
26	MS-EAP-Authentication (EAP/MS-CHAPv2)	RFC-draft-kamath-pppext-eap-mschapv2-02.txt
27	EAP-MAKE, Mutual Authentication w/Key Exchange	RFC-draft-berrendo-chabanne-pppext-eapmake-01.txt
28	CRYPTOCard	
29	PEAPv0/EAP-MSCHAPv2	RFC-draft-dpotter-pppext-eap-mschap-01.txt
30	DynamID	
31	Rob EAP	
32	EAP-POTP, Protected One Time Password	RFC 4793
33	MS-Authentication-TLV	RFC-draft-hiller-eap-tlv-01.txt
34	SentriNET	
35	EAP-Actiontec Wireless	
36	Cogent Systems Biometrics Authentication EAP	
37	AirFortress EAP	
38	EAP-HTTP Digest	
39	SecureSuite EAP	
40	DeviceConnect EAP	
41	EAP-SPEKE	
42	EAP-MOBAC	
43	EAP-FAST, EAP Flexible Authentication via Secure Tunneling	RFC 4851RFC 5421RFC 5422
44	ZLXEAP, ZoneLabs EAP	
45	EAP-Link	
46	EAP-PAX, EAP Password Authentication eXchange	RFC 4746
47	EAP-PSK, EAP Pre-Shared Authentication and Key Establishment	RFC 4764
48	EAP-SAKE, EAP Shared-secret Authentication and Key Establishment	RFC 4763
49	EAP-IKEv2	RFC 5106
50	EAP-AKA, Improved EAP method for 3rd Generation Authentication and Key Agreement	RFC-draft-arkko-eap-aka-kdf-10.txt
51	EAP-GPSK, EAP Generalized Pre-Shared Key	RFC 5433
52-191	Available via review by designated expert	RFC 3748
192-253	Reserved for allocation via standards action	RFC 3748
254	Expanded Type	RFC 3748
255	Experimental	RFC 3748

PŘÍLOHA C – OBSAH DVD

Přiložené DVD médium obsahuje:

- zdrojové soubory aplikací `EAPpeak` a `EAPscan`–adresář `[src]`
- zdrojové soubory rozšíření pro grafický výstup k aplikacím `EAPpeak` a `EAPscan`–adresář `[src]`
- technickou zprávu v elektronické podobě–adresář `[doc]`
- instalační image distribuce Kali Linux 2018.1 x64 (ISO obraz)–adresář `[img]`