VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

BAKALÁŘSKÁ PRÁCE

Brno, 2020 Dominika Šebestová

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

POKROČILÁ DETEKCE FALEŠNÉHO PŘÍSTUPOVÉHO BODU V BEZDRÁTOVÝCH SÍTÍCH
ADVANCED DETECTION OF ROGUE ACCESS POINT IN WIRELESS NETWORKS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR
Dominika Šebestová

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. Radek Fujdiak, Ph.D.

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Bakalářská práce

bakalářský studijní program **Informační bezpečnost**

Ústav telekomunikací

Studentka: Dominika Šebestová ***ID:*** 195172

Ročník: 3 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Pokročilá detekce falešného přístupového bodu v bezdrátových sítích

POKYNY PRO VYPRACOVÁNÍ:

Student bude mít za úkol provést analýzu metod realizace falešného přístupového bodu (AP) i metod jeho detekce v rámci bezdrátových sítích rodiny standardu IEEE 802.11. Teoretickým výstupem bude srovnání jednotlivých metod z pohledu výhod a nevýhod (mj. v rámci detekce). Následně bude proveden vlastní návrh pro pokročilou detekci falešného AP. Bude realizována základní síť a navrženy metody testování. Implementovány tak budou jednotlivé metody realizace falešného AP a vlastní pokročilá metoda detekce. Bude provedena demonstrace odhalení falešného AP a optimalizace vlastního řešení pro zahrnutí všech zvolených typů falešných AP. Výsledkem pak bude vlastní řešení schopné detekovat falešné AP realizované vybranými metodami.

DOPORUČENÁ LITERATURA:

[1] SCHULTZ, Corey P.; PERCIACCANTE, Bob. Kali Linux Cookbook. Packt Publishing Ltd, 2017.

[2] ALAMANNI, Marco. Kali Linux wireless penetration testing essentials. Packt Publishing Ltd, 2015.

Termín zadání: 3.2.2020 ***Termín odevzdání:*** 8.6.2020

Vedoucí práce: Ing. Radek Fujdiak, Ph.D.

doc. Ing. Jan Hajný, Ph.D.
předseda rady studijního programu

ABSTRAKT

Cílem bakalářské práce je seznámit se s dostupnými možnostmi realizace *Rogue Access Point* (RAP) a detekčními metodami, sloužícími k odhalení takových bodů ze strany klienta nebo serveru a z principu nastudovaných metod vytvořit detekční metodu, schopnou odhalit různé typy *Evil Twin* (ET). Zabývá se implementací detekční metody založených na vlastnostech TCP spojení a metody sledující datové rámce, konkrétně jejich příchozí čas, specifickou délku a zdrojovou i cílovou MAC adresu. Spojením vlastností těchto metod vznikla všestranná detekční metoda na straně klienta, která je otestována na experimentální síti.

KLÍČOVÁ SLOVA

Falešný přístupový bod, ET, RAP, Python, detekce

ABSTRACT

The aim of the bachelor's thesis is to get acquainted with the available implementation options of *Rogue Access Point* (RAP) and the detection methods used to detect such points from the side of the client or server, and from the principles of the studied methods implement a solution that is able to detect various types of the *Evil Twin* (ET). The thesis covers implementation of detection methods based on TCP connection properties and a method monitoring data frames, specifically their arrival time, specific length and source and destination MAC address. Connection of these methods creates an universal detection methods on the client's side that is tested on the experimental network.

KEYWORDS

Fake Access Point, ET, RAP, Python, detection

ŠEBESTOVÁ, Dominika. *Pokročilá detekce falešného přístupového bodu v bezdrátových sítích*. Brno, 2020, 44 s. Bakalářská práce. Vysoké učení technické v Brně, Fakulta elektrotechniky a komunikačních technologií, Ústav telekomunikací. Vedoucí práce: Ing. Radek Fujdiak, Ph.D.

PROHLÁŠENÍ

Prohlašuji, že svou bakalářskou práci na téma „Pokročilá detekce falešného přístupového bodu v bezdrátových sítích“ jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.

Jako autorka uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušila autorská práva třetích osob, zejména jsem nezasáhla nedovoleným způsobem do cizích autorských práv osobnostních a/nebo majetkových a jsem si plně vědoma následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, včetně možných trestněprávních důsledků vyplývajících z ustanovení části druhé, hlavy VI. díl 4 Trestního zákoníku č. 40/2009 Sb.

Brno ....

podpis autorky

PODĚKOVÁNÍ

Rád bych poděkovala vedoucímu mé bakalářské práce panu Ing. Radkovi Fujdiakovi, Ph.D. za odborné vedení, konzultace, trpělivost a podnětné návrhy k práci.

Obsah

Seznam obrázků

Seznam tabulek

Seznam výpisů

Úvod

Bakalářská práce se zabývá problematikou falešných přístupových bodů v bezdrátových sítích. S růstem zájmu o IoT zařízení rostou i požadavky na vlastnosti nynějších Wi-Fi sítí a lze tedy očekávat i nárůst počtů přístupových bodů v rámci jedné sítě. *Rogue Access Point* (RAP), neboli falešný přístupový bod má několik podtypů. Nebezpečí některých typů RAP spočívá v tom, že je realizují důvěryhodné osoby, například zaměstnanci. Neznalostí způsobená chyba v zabezpečeni může vyvolat dalekosáhlé následky. Stačí do kabelové sítě v kanceláři připojit špatně zabezpečený router a vybavený útočník může pohodlně získávat data z firemní sítě z lavičky pod oknem budovy.

V případě úmyslně nastrčených bodů, je otázkou několika málo minut najít na internetu vhodný hardware a stovky návodů popisujících realizaci *Evil Twin* (ET). Nainstalovat v kavárně nebo obchodním centru otevřenou síť, vyčkat na oběti a získat jejich osobní údaje, hesla nebo jim podstrčit nevyžádanou reklamu. Falešné přístupové body jsou také populárním a efektivním způsobem dosažení Man In the Midle pozice. Ta lze využít pro provedení celé škály útoků. Příkladem je útok phishing (nastrčení falešné webové stránky namísto například internetového bankovnictví).

V první části projektu je shrnuto zabezpečení bezdrátových sítí včetně nového WPA3. Vysvětleny jsou falešné přístupové body neboli RAP, včetně jejich podtypu ET. Shrnuty jsou výhody a nevýhody volně dostupných nástrojů pro realizaci RAP. Rozebrán je přístup k jejich detekci ze strany klienta i ze strany serveru a jejich konkrétní zástupci. Praktickým výstupem této práce je realizace vlastní metody pro detekci ET, založené na metodě SLFAT a vlastnostech TCP spojení, její otestování na vybraných metodách realizace falešných přístupových bodů. To vše, včetně použitého softwaru a popisu experimentální sítě je popsáno v kapitole 3. Vlastní metoda dokáže detekovat ET připojené na původní legitimní Access Point nebo 3G/LTE modem. Využívá jak pasivní tak aktivní způsoby detekce. Při implementaci jsou využity nástroje operačního systému Kali Linux, Python knihovnu wifi, knihovnu OS a knihovnu requests.

1 IEEE 802.11

IEEE 802.11 je číselné označení, pod kterým nalezneme specifikace standardů WLAN (bezdrátovou lokální síť), publikuje je *Institute of Electrical and Electronic* (IEEE). První verze byla vydána v roce 1997. Pracuje na 1. fyzické vrstvě a MAC podvrstvě 2. linkové vrstvy referenčního modelu ISO/OSI. Jednotlivé revize standardu definují např. přenosovou rychlost, modulační techniku a použité kmitočtové pásmo. Používá se 2,4 GHz pásmo, novější verze pak 5 GHz nebo kombinované. V různých zemích světa je pak povoleno používat různé kanály těchto pásem. Revizí tohoto protokolu existuje velká škála. Zabývají se úpravou vlastností přenosu, bezpečností, regulací vysílacího výkonu, podporou *Požadavky na kvalitu služeb* (QoS) a mnohým dalším [1].

1.1 Revize

IEEE 802.11a

První revize standardu, vydaná v roce 1999. Kvůli problému vzájemného rušení bezdrátových sítí s jinými domácími spotřebiči bylo přidáno 5 GHz pásmo. Revize také umožnila rychlost až 54 Mbit za sekundu. Dnes je nedostačující jak skrze rychlost, tak i skrze problém s vysokým počtem zařízení. Používala tehdy novou modulaci OFDM [2], [3].

IEEE 802.11b

Revize vydaná současně s IEEE 802.11a, pracovala na původním pásmu 2,4 GHz, maximální rychlost byla 11 Mbit za sekundu. Díky nižší ceně hardwaru se oproti IEEE 802.11a stala velmi populární [2], [3].

IEEE 802.11g

Používá identickou modulaci OFDM, jako IEEE 802.11a a podporuje i stejnou maximální rychlost. Ovšem používá pásmo 2,4 GHz a je zpětně kompatabilní pro zařízení podporující IEEE 802.11b. Zároveň se zlepšily některé vlastnosti, jako například pokrytí [2], [3].

IEEE 802.11n

První revize, která uměla pracovat zároveň s 2,4 GHz a 5 GHz pásmem. Přinesla také velké zrychlení přenosu, dosahující až 450 Mbit za sekundu, při použití tří antén, a vyšší spolehlivost. Používá modulaci *Multiple-input multiple-output* (MIMO), což umožnilo přenášet výrazně větší objemy dat [2], [3].

IEEE 802.11ac

Revize jak oprvní nabídla rychlost v řádech Gbit za sekundu, používá 5 GHz pásmo, které není používáno tak často jako 2,4 GHz a nedochází tak ke vzájemnému rušení více sítí. Původní revize z roku 2013 dostala v roce 2016 další vylepšení. Jednotlivé kanály mohou pracovat až s 160 MHz, optimálně alespoň s 80 MHz [3].

IEEE 802.11ah

Revize určená pro čidla a ústředny, která potřebují přenášet méně dat na větší vzdálenost. Jedná se o 900 MHz bezdrátovou síť, která je i skrze nízkou energetickou náročnost nebo lepší šíření skrze překážky, vhodná například pro IoT zařízení. Nejedná se o globalizovaný standard [3].

IEEE 802.11af

Používá nevyužívané frekvence pro televizní vysílání. Podobně jako IEEE 802.11ah je používána pro přenos menších objemů dat na větší vzdálenost. Jelikož se, podobně jako u IEEE 802.11ah, nejedná o globalizovaný standard je použití problematické skrze jiné rozdělení frekvenčních pásma skrze různé pravidla v jiných státech [3].

IEEE 802.11ad

Určená pro přenos velkých objemů dat na velmi krátkou vzdálenost. Myšlenkou je bezdrátový standard srovnatelný s přenosem po optických vláknech. Výroba zařízení je finančně náročná a poptávka není vysoká. Revize není globalizovaná [3].

IEEE 802.11i

Revize z roku 2014, jejímž cílem bylo nahradit stávající neúčinné zabezpečení bezdrátových sítí. V bezdrátových sítích se začaly používatsilnější kryptografické protokoly, jako např. AES. Vychází z ní WPA i WPA2, více v podkapitole 1.2 [2], [4].

1.2 Zabezpečení IEEE 802.11

Patřičné zabezpečení protokolu IEEE 802.11, dále jen "Wi-Fi", je v dnešní době nezbytné. S větším rozmachem používání bezdrátových sítí rostla i snaha obejít jejich zabezpečení. Z bezdrátovými sítěmi se setkáváme ve školách, na letištích, úřadech a jiných veřejných místech. Signál se z antény šíří všemi směry, skrze plášť budovy do veřejných prostor, kde je přístupný bez jakékoliv nutnosti fyzické manipulace se zařízením. Tento fakt a také velká popularita bezdrátových zařízeních, útočníkům usnadnila práci. Na otevřených sítích je snadné zachytávat veškerou komunikaci, s běžně dostupným hardwarem a nástroji např.

Z GitHubu. Na internetu jsou volně dostupné návody, jak získat přístup i do kryptografií chráněné sítě. I po mnoha letech upozorňování, spousta domácností i firem stále zabezpečení podceňuje a neuvědomuje si, jaké riziko bezdrátová síť představuje pro všechna jejich zařízení včetně těch, připojených ke kabelové síti.

Proto se společně s rozvojem bezdrátových sítí vyvíjely i protokoly pro jejich zabezpečení. První metoda zabezpečení WEP se po letech používání ukázala jako nedostatečná a musela být rychle nahrazena novým protokolem, který by na několik let zajistil bezpečí přenášených dat. Těmito nástupci se staly WPA1, WPA2 a nově i WPA3, které přinesly kvalitnější možnosti zabezpečení do firemní sféry, použitím zásad autentizačního standardu 802.1X [5].

1.2.1 WEP (Wired Equivalent Privacy)

Vychází z původního standardu IEEE IEEE 802.11 a pracuje na 2. linkové vrstvě. Používá proudovou šifru RC4, kterou zvlášť šifruje každý paket. Pro kontrolu integrity dat používá kontrolní součet CRC-32. Klíč má délku 40 bitů nebo 104 bitů což odpovídá maximální délce hesla 13 ASCII znaků, dále se ke klíči připojuje 24 bitový inicializační vektor. Byl prolomen v roce 2001 a jeho použití se nedoporučuje.

WEP2 má klíč i inicializační vektor zvětšený na 128 bitů. Cílem bylo zvýšit obranu proti útoku hrubou silou a vyřešit problém s malou velikostí inicializačního vektoru. **WEP plus** je vylepšení, které zabraňuje použití tzv. slabých inicializačních vektorů, je účinné pouze, pokud je použito na obou komunikujících stranách. **Dynamic WEP** dynamicky mění klíče. Byl inspirací pro budoucí WPA TKIP [6], [7].

1.2.2 WPA1 (Wi-Fi Protected Access)

V roce 2003 nahradilo algoritmus WEP, nikdy však nepředstavovalo plnohodnotnou náhradu. Jeho úkolem bylo fungovat jako bezpečný protokol bez nutnosti měnit hardware. Vychází z verze IEEE IEEE 802.11i. Jako novinku představil dva režimy, jeden režim pro osobní a druhý pro firemní použití. **WPA-Personal** určený pro domácnosti nebo malé firemní sítě, používá předsdílené heslo o 8 až 63 znacích. **WPA-Enterprise** ke klasickému modelu klient a přístupový bodu přidává autentizační server. Použití nalezl ve větších firemních sítích, jelikož zajišťuje silnou autentizační metodu pomocí EAP. Klientovi není před autentizací od serveru, s vyjímkou EAP, umožněna jakákoliv komunikace na síti [7], [8].

1.2.3 WPA2

Implementace revize IEEE 802.11i z roku 2004, dnes stále používaný protokol. Byl navržen s cílem, aby vydržel bezpečný co možná nejdéle. Používá šifru AES a CCMP, což oproti

předchozím protokolům pro zabezpečení navýšilo nároky na výpočetní výkon zařízení.

Autentizace

WPA2 nabízí dvě možnosti autentizace, režim PSK s předsdíleným klíčem nebo Enterprise režim využívající autentizační server podle standardu 802.1X. V případě PSK musí každý uživatel znát, pro všechny stejné, heslo. V režimu s autentizačním serverem se nejprve vzájemně ověří přístupový bod a klient. Poté je mezi autentizačním serverem a klientem pomocí EAP ustanoven PMK. Z PMK nebo PSK je při 4-way handshake odvozen PTK.

PSK režim klient se přihlašuje pomocí 8 až 63 znaků dlouhého hesla. Z hesla, SSID a jeho délky je vypočítán PSK. Před falešnými přístupovými body uživatele chrání pouze v případě, kdy útočník nezná přesdílené heslo. Na veřejných místech, kde je síť heslem chráněna, ale heslo je zveřejněno, je nebezpečí falešného AP vysoké.

Enterprise režim každý klient má vlastní jméno a heslo pro přihlášení do sítě. Přístupový bod, vystupující jako autentizátor, používá dva porty, jeden pro službu a druhý pro autentizaci. Dokud se klient úspěšně nepřihlásí, do sítě je mu otevřen pouze druhý port. Klient a přístupový bod komunikují pomocí EAP. Přístupový bod pak předává požadavky klienta autentizačnímu serveru. Pokud je klient úspěšně ověřen, je tato informace předána přístupovému bodu. Obě zařízení ziskají PMK a pokračují s 4-way handshake [9].

4-Way Handshake se používá pro ustanovení dočasného klíče PTK nebo GTK, který slouží pro multicastovou komunikaci. PTK je kolekcí dalších klíčů, které jsou použity pro jedno konkrétní spojení a po jeho zániku jsou zničeny [10]. Průběh je následující:

1. Přístupový bod zasílá nonce value (náhodný řetězec), která nesmí být použita vícekrát. Klient má všechny potřebné parametry pro generování PTK.
2. Klient zašle vlastní nonce value a *Message Integrity Code* (MIC), ten zajistí potvrzení integrity dat a autentizaci. Přístupový bod zná vše potřebné pro vygenerování PTK.
3. Pokud je ověření MIC úspěšné, klientovi může volitelně zaslat *Group Transient Key* (GTK). Je zaslán příkaz pro klienta nainstalovat PTK, případně GTK.
4. Klient nainstaluje PTK, případně GTK, zkontroluje MIC u 3. zprávy a zašle potvrzení.

1.2.4 WPA3

V lednu 2018 byl světu představen nový protokol WPA3. Staví na úspěchu WPA2, který doplňuje o modernější možnosti autentizace, silnější kryprografii pro citlivá data klientů,

použití nejnovějších protokolů, ochranu PMF (Protected Management Frames, rámce managementu multicastu a unicastu), autentizace na základě hesla. Protokol nabízí dva režimy, osobní a enterprise.

Osobní režim představuje silnější ochranu na základě snadno zapamatovatelných hesel, nahrazení předsdíleného klíče (PSK u WPA2) novým mechanismem *Simultaneous Authentication of Equals* (SAE), který šifruje komunikaci mezi zařízením a AP už od zaslání první žádosti o připojení. Je odolnější proti brute-force útokům, ochrání tedy heslo i před, u WPA2 oblíbeným, slovníkovým útokem. Pro lepší ochranu hesla generuje odlišné PMK pro každého klienta a AP. Forward secrecy zajistí, že i po případném získání hesla útočníkem, nebude možné dešifrovat dříve přenesená data.

Enterprise režim používá silnější klíče s minimální délkou 192 bitů, nový protokol pro autentizace, *Elliptic Curve Diffie-Hellman* (ECDH) a *Elliptic Curve Digital Signature Algorithm* (ECDSA), využívajících 384 bitovou eliptickou křivku pro ustanovení hesel, ochranu rámců managementu s pomocí 256 bitového kódu ověření zprávy.

Wi-Fi Easy Connect je služba usnadňující připojení IoT zařízení do bezdrátové sítě. Z těchto zařízení je totiž uživatel limitován chybějícím displejem a klávesnicí, aby tedy mohl zařízení pohodlně připojit, použije svůj chytrý telefon. Díky QR kódu na IoT zařízení a na routeru dojde k bezpečnému propojení těchto zařízeních [11].

Wi-Fi CERTIFIED Enhanced Open je velkou novinkou v přístupu k otevřeným sítím. Tato certifikace zajišťuje, pro uživatele transparentní, šifrování dat. Implementace *Opportunistic Wireless Encryption* (OWE) vyžaduje použití chráněných rámců managementu PMF na straně přístupového bodu i stanice. Užívání OWE by pro uživatele nemělo být odlišné od klasické otevřené sítě, AP by po tzv. přechodnou dobu mělo nabízet otevřené připojení s OWE i bez něj, s rozdílným *Název bezdrávové sítě* (SSID). Po uplynutí přechodné doby budu otevřené sítě, jak je známe, označeny za zastaralé [12].

Už v červenci 2019 byl zveřejněn výzkum Mathyho Vanhoefa (autor KRACK attack, který významně ovlivnil WPA2), zabývající se analýzou bezpečnosti použitého Dragonfly handshake a návrhem změn v protokolu WPA3 pro zajištění lepší ochrany [13].

Práce WPA3 Connection Deprivation Attacks upozornila na nebezpečí, hrozící v přechodné době, kdy budou zařízení současně používat WPA2 i WPA3. Evil Twin může padělat Beacon rámce legitimního AP a změnit hodnotu *Robust Security Network Element* (RSNE), tedy informaci o použitém zabezpečení, a tak neumožnit připojení klienta pomocí WPA3. Toto je odhaleno při 3. zprávě 4-way handshake, kdy je připojení přerušeno kvůli rozporu v hodnotě RSNE [14].

2 Falešné přístupové body

Falešný přístupový bod, známý také jako *Rogue Access Point* (RAP), je bod připojený do sítě bez souhlasu a vědomí administrátora. Může se jednat o zařízení nainstalované oprávněným uživatelem sítě, který si neuvědomuje bezpečnostní rizika. Pokud je takové zařízení chybně nakonfigurované, může umožnit jednoduchý průnik neautorizované osoby do lokální sítě. Proto by měl konfiguraci každého takového zařízení schvalovat správce sítě [15].

Dále se může jednat o zařízení nastrčené útočníkem se záměrem uškodit, omezit šířku pásma ostatním sítím, sbírat citlivé údaje pomocí analyzátoru paketů nebo phishing útoků, tedy útoků, kdy je uživatel namísto chtěné webové stránky přesměrován na kopii této stránky. Často se jedná o sociální síť nebo web bankovní instituce, účel je obvykle získat přístup k přihlašovacím údajům uživatele. Další možností phishing útoku je Captive Portal Attack, který vytvoří falešnou stránku zobrazující se po připojení uživatele do bezdrátové sítě [16].

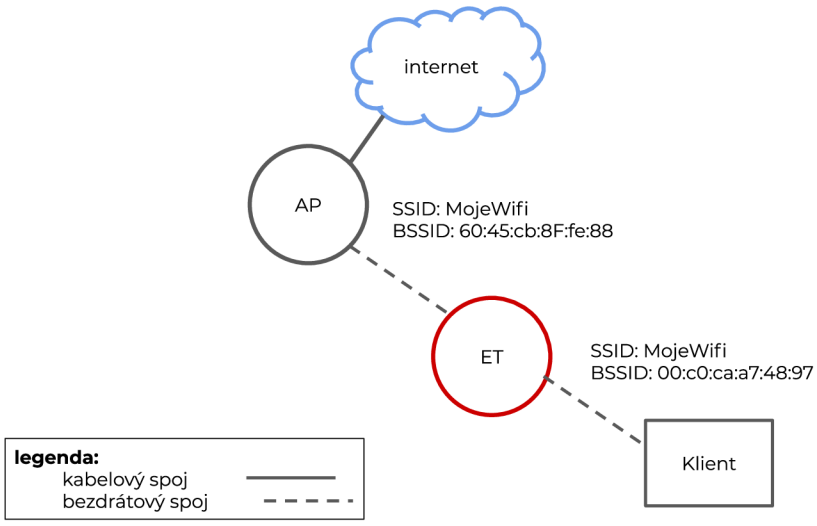
2.1 Rogue Access Point

Dělíme do čtyř kategorií:

1. Chybně nakonfigurovaný AP – vzniká nevědomou a neúčelnou chybnou konfigurací zařízení administrátorem, zastaralým nebo chybným ovladačem či firmwarem zařízení. Další možností je špatně nastavené zařízení využívající ad hoc síť.
2. Neautorizovaný AP – příkladem je AP fungující na pracovišti bez vědomí správce sítě. V případě, že bude používáno pro pracovní účely, může tvořit bezpečnostní hrozbu.
3. Phishing AP – obvykle má stejné SSID, využití zejména pro MITM (Man In The Middle) útoky. Realizován bývá notebookem nebo mikropočítačem s dvěma bezdtárovými síťovímy kartami, z nichž jedna musí podporovat tvorbu přístupových bodů.
4. Kompromitovaný AP – pokud útočník získá heslo k síti, může v ní nainstalovat libovolný počet AP, vyžadujících stejné přihlašovací údaje jako originální síť. Falešné AP tak získají v očích uživatelů na důvěryhodnosti [15].

2.1.1 Evil Twin

Podtypem RAP je ET, který je úmyslnou kopií legitimního AP, má tedy stejný parametr SSID a často kopíruje i MAC adresu. V jeho případě vidí uživatel v nabídce připojení přes Wi-Fi pouze jednu síť, namísto dvou se stejným jménem, a automaticky se připojuje k AP s vyšší sílou signálu. Útočník může využít tzv. deautentizační útok, kdy své oběti donutí



Obr. 2.1: Evil Twin s identickým SSID jako legitimní AP.

odpojit se od legitimního připojení. Je-li potřeba pokrýt Wi-Fi signálem velké prostory, je často nainstalováno několik AP se stejným SSID, což ztěžuje detekci případného falešného bodu. Důležité je, aby byl uživateli poskytnut přístup k internetu a on tak připojení využil. Toho lze docílit buď připojením Evil Twin na již existující originální přístupový bod (viz obrázek 2.1 nebo např. poskytnutím připojení přes mobilního operátora. Vlastní připojení může pomoci obejít některé způsoby detekce falešného AP. Podstatná je také volba stejného zabezpečení jako originální AP, aby se v nabídce sítí k připojení nevyskytl jako duplicita [17].

2.2 Metody realizace falešných přístupových bodů

Falešný přístupový bod je možné realizovat manuálně pomocí linuxových nástrojů hostapd a dnsmasq nebo využitím softwaru dostupného z platformy GitHub. Hostapd (Host access point daemon) je velmi flexibilní a i s obyčejnou síťovou kartou umožňuje vytvořit AP s plnohodnotným Wi-Fi zabezpečením i autentizačním serverem. V kombinaci s nástrojem dnsmasq (realizace lokálního DNS serveru a DHCP serveru), který se vyznačuje jednoduchou konfigurací a nízkou náročností na hardware, vytváří falešný AP, který věrně napodobí legitimní bod. Podle plánovaného způsobu zneužití se tyto dva nástroje mohou doplnit například o Apache (web server) a mysql (databázový systém) [18]. Pro realizaci je možné použít také již existující řešení z GitHubu.

Fake-AP Výše zmiňované nástroje Hostapd a dnsmasq využívá i nástroj Fake-AP od autora thelinuxchoice. Nástroj vhodný pro aktivní způsoby detekce, jelikož jeho součástí

je předpřipravený *Man In the Midle* (MITM). Umožňuje nastavit SSID a kanál AP, neumožňuje však změnu MAC adresy [19].

Fluxion Účelem dalšího nástroje Fluxion je realizace útoku Captive portal. Captive Portal je webová stránka zobrazovaná po připojení k bezdrátové síti. Může sloužit k přihlášení uživatele, poučovat o pravidlech poskytovatele služby, fungovat jako reklama nebo může být nastrčená útočníkem cílem získat citlivé údaje. Při konfiguraci útoku je umožněno využít pro Captive Portal stránku i zabezpečení SSL certifikátem. Pro podstrčení této stránky oběti je využit právě falešný AP, nástroj automaticky kopíruje parametry vybrané sítě a pomocí nástroje Hostapd nebo Airbase-ng realizuje falešný AP [20].

Wifiphisher V pythonu psaný Rogue Access Point framework Wifiphisher pro snadné dosažení MITM pozice při penetračním testování, umožňuje použít předpřipravené phishing webové útoky nebo oběť infikovat malwarem [21].

WiFi-Pumpkin Framework sloužící pro snadnou tvorbu falešných přístupových bodů, umožňujících připojení oběti k internetu pro větší důvěryhodnost falešné sítě. Nabízí množství předchystaných útoků, od deautentizačního, přes rogue AP, ARP Poisoning (změna párování IP a MAC adres v lokálních sítích) až po útok Captive Portal a mnohé další [22].

create_ap Pro falešný AP je možné provést veškerá DNS a DHCP nastavení. Posledním nástrojem je create_ap také z GitHub, podporuje revize IEEE 802.11n a IEEE 802.11ac, více o nich v sekci 1.1 [23].

2.2.1 Beacon rámec

Každý přístupový bod periodicky zasílá zprávu, obsahující informace o síti, všem zařízení v okolí (broadcast), aby tak informoval o existenci bezdrátové sítě. Tato zpráva obsahuje informace o konfiguraci a možnostech sítě, tedy parametry sítě důležité pro připojení zařízení nebo např. vybraní AP se silnějším signálem, je-li jich v síti více [24]. Beacon rámec patří k řídícím, tedy management rámcům protokolu IEEE 802.11 a obsahuje následující parametry:

- SSID – název sítě,
- BSSID – MAC adresa zařízení,
- Timestamp – čas odeslání rámce,
- Beacon Interval – čas mezi periodickým odesláním 2 rámců,
- Supported Rates a Extended Supported Rates – podporované rychlosti přenosu v Mbit za sekundu,

Tab. 2.1: Přehled výhod a nevýhod nástrojů pro realizaci RAP.

	výhody	**nevýhody**
fake-AP	neumožňuje aktivní detekci RAP	nelze změnit BSSD
Fluxion	podpora 5 GHz	nelze změnit BSSD, neumožní aktivní metody detekce, využití pro jeden konkrétní útok, deautentuzační útok na legitimní AP
Wifiphisher	několik předpřipravených útoků, možnost doplnit o vlastní modul s útokem	nelze změnit BSSD
Wifi-Pumpkin	možnost změnit BSSD, DHCP nastavení, kvalitní dokumentace, videonávody, možnost spustit bez jakéhokoli MITM útoku	v dubnu 2020 ukončena podpora, nepodporuje kanály 12, 13 a 14, nepodporuje 5 GHz
creat_ap	rychlé ovládání přes terminál, kvalitní dokumentace, možnost jednoho síť. rozhraní pro připojení k internetu i tvorbu AP, podpora 5 GHz	nelze změnit BSSD

- DS Parameter set – aktuálně využívaný kanál,
- Capabilities Information – vlastnosti, které musí zařízení splnit pro připojení k síti,
- Radio information – informace o použité frekvenci, síle signálu,
- Country Information – regulace vlastností přenosu dané státem,
- a další.

2.3 Metody detekce falešných přístupových bodů

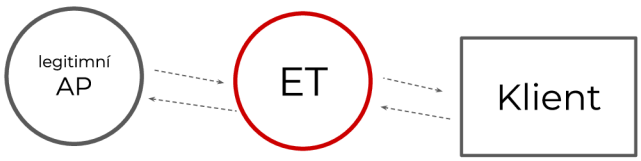
Existují dva základní přístupy a to ze strany klienta a serveru, každý přináší jiné výhody a nevýhody.

2.3.1 Detekce na straně klienta

Klient je oproti serveru omezen svými oprávněními, výpočetním výkonem a také nedisponuje specializovaným hardwarem. Výhodou je, že kdykoliv si klient není jistý důvěryhodností připojení, může ji sám ověřit. Síť v souvislosti s těmito typy detekce nepotřebuje žádné speciální nastavení. Naopak nevýhody spočívají v nemožnosti porovnat AP s databází legitimních zařízení administrátora sítě, klientský přístup může být znevýhodněn svými privilegii v síti. Detekce na straně klienta se může dále dělit na **aktivní** způsob, kdy klient komunikuje s podezřelým AP a **pasivní** způsob, při kterém se zaměřuje na data získaná při monitorování veškerého síťového provozu v okolí [25].

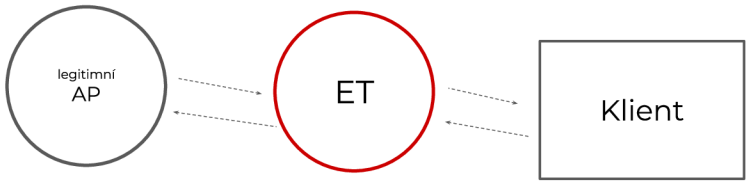
Round Trip Time

zkráceně RTT označuje čas, po který paket putuje mezi klientem a AP.



Obr. 2.2: Probe žádost a odpověď u legitimního AP [25].

Pokud je klient připojen na falešný přístupový bod, zabere mu cesta o jeden bezdrátový skok víc než v případě připojení na legitimní AP, tedy získá po cestě určité zpoždění, znázorněno na obr. 2.3. Tento skok vzniká při cestě paketu z legitimního AP na AP falešný. Je-li po několika opakovaných pokusech u jednoho AP střední hodnota doby zpoždění vyšší, je velmi pravděpodobné, že se jedná o AP nastrčené útočníkem. Tato metoda využívá žádosti DNS lookup a Probe žádost (aktivní skenování okolí, s cílem získat seznam dostupných AP) a odpovědi na ně. Je používán Lokální DNS server, protože při dotazu na něj je možné použít nerekurzivní dotaz, který dovoluje použít pouze lokální server a naměřené zpoždění tedy není zkresleno provozem na vnější síti. Při každém pokusu je doporučeno použít dotaz na jiné doménové jméno. Metoda není účinná pokud je falešné AP připojeno k internetu přes vlastní připojení, například mobilního poskytovatele



Obr. 2.3: Probe žádost a odpověď u ET, dochází k jednomu skoku navíc [25].

ani přímé připojení falešného bodu kabelem do původní sítě. Hlavní výhodou metody je, že nevyžaduje žádný specializovaný hardware, tedy ani bezdrátovou síťovou kartu podporující monitorovaní sítě. Na místo DNS lookup dotazu je možné použít i ping nebo traceroute. Z těch je však možné, že falešné AP nebude dotazy přeposílat na legitimní bod, odpověď pro ping vygeneruje sám nebo v případě traceroute napodobí MAC adresu legitimního bodu a tak vznikne dojem, že je přímo připojený na výchozí bránu. Zprávy pro ping i tracerout navíc můžou být zablokováný síťovým administrátorem [26].

DNS server zajišťuje překlad zapamatovatelných názvů, jako vutbr.cz, na IP adresy. DNS lookup se dělí na dva základní typy. První je rekurzivní, v případě, kdy dotazovaný DNS server nezná odpověď, začne ji vyhledávat u nadřazených DNS serverů. Nerekurzivní typ ve stejném případě zašle zprávu host not found.

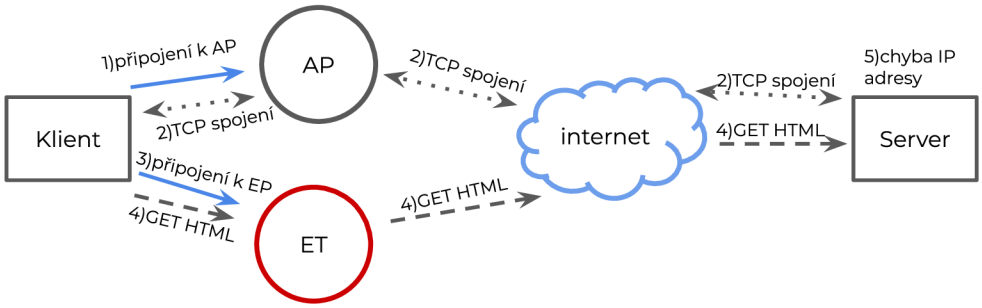
Received Signal Strengths and Sequential Hypothesis

Využívá měření síly přijatého signálu, ten je získán buďto aktivním dotazováním na přístupové body nebo pasivním zachytáváním Beacon rámců. Metoda se skládá ze třech částí: sběru dat o signálu, normalizace sesbíraných dat pro vyšší přesnost metody a klasifikační části, jež určuje, které signály mají vysokou korelaci oproti hodnotám signálu, které byly experimentálně získány při přítomnosti RAP. Pro sběr o síle signálu jsou sbírána data z Beacon rámců, které AP vysílá 10 – 100 krát za sekundu. Beacon rámce uvádí v parametru Radio information údaje o síle signálu. Normalizace dat o síle signálu je statistická metoda pro eliminaci, pro bezdrátové sítě charakteristické výkyvy. Díky překážkám, vzdálenosti od AP nebo odrazem signálu se mohou vyskytnout příliš nízké hodnoty nebo časté přerušení signálu. Při klasifikaci vyjde najevo, jestli má signál dva zdroje nebo jen jeden. Je měřena vzdálenost dvou náhodně zvolených sekvencí přijatého signálu. Pokud je jejich vzdálenost vyšší než prahová hodnota rozdílu, znamená to, že obě zvolené sekvence spolu vysoce korelují. Vysoce korelující signály jsou klasifikovány jako

různé signály vyslané falešným přístupovým bodem. Prahová hodnota je definována na základě výsledku experimentů, kdy bylo určeno jak moc podobné sekvence jsou definované jako více signálů. Určení této hodnoty při experimentu, umožňuje detekci falešného AP bez nutnosti předešlého učení algoritmu na konkrétní síti [27].

Metoda na bázi spojení přes TCP

Metoda prozradí přítomnost falešného přístupového bodu s vlastním internetovým připojením, tedy použití odlišné výchozí brány než u legitimního AP. V prvním kroku se uživatel připojí na první AP. Klient naváže TCP spojení se serverem, např. google.com. Po úspěšném navázání připojení se klient přepojí na druhý AP a zašle serveru příkaz GET HTML, což je žádost o znovu stažení indtex.html. Je-li druhý AP připojen na stejnou výchozí bránu jako první, klient obdrží odpověď 200 OK. V tomto případě se v síti falešný AP s vlastním připojením nenachází. V případě, kdy je druhý AP nastrčený útočníkem,



Obr. 2.4: Průběh detekce ET na základě TCP spojení, scénář s přítomností ET.

odpověď od serveru neobdrží a spojení se po uplynutí timeout uzavře s Errno 110. To je způsobeno odlišným zdrojem připojení obou AP. Lokální sítě obvykle klientům přidělují privátní IP adresy. Při komunikaci se zařízeními mimo LAN je nutné privátní IP adresu zaměnit za veřejnou. Za tímto účelem existuje Network Address Translation případně Port Address Translation. Z NAT je zdrojová adresa klienta zaměněna za veřejnou adresu výchozí brány. Při použití PAT je navíc změněno i číslo zdrojového portu. Změna AP v průběhu TCP spojení nijak neovlivňuje informace o tomto spojení uložené v soketu na straně serveru a klienta. V případě změny výchozí brány se obě skutečnosti změní a dotaz

tedy neodpovídá vlastnostem TCP spojení, uložených v soketu. Server na dotaz tedy nereaguje. Metoda přítomnost falešného AP odhalí, ale není schopna určit, o které konkrétní zařízení se jedná. Nelze použít na scénář, kdy je falešný AP připojený na legitimní AP [28].

BiRe – Bi-directional SYN Reflection

Klient při navazování TCP spojení se serverem zasílá zprávu s příznakem SYN, na nějž server odpovídá s příznakem SYN a ACK. Metoda využívá dvě bezdrátové síťové karty, podporující monitorovací mód. Obě se připojí do sítě a obdrží vlastní IP adresu. Z karty A je pak na server odeslána zpráva s příznakem SYN, ve které je zaměněna zdrojová IP adresa za adresu síťové karty B. Karta B po celou dobu monitoruje komunikaci na WLAN a čeká na odpověď. Za správnou odpověď je považována pouze ta, která má správně všech 6 položek (zdrojová MAC adresa, cílová MAC adresa, zdrojová IP adresa, cílová IP adresa, zdrojový port, cílový port) a dorazí v předem daném časovém limitu. Poté se proces opakuje s rozdílem, že zpráva s příznakem SYN je zaslána z karty B. Obdrží-li odpověď s SYN a ACK obě karty, jsou obě AP prohlášeny za legitimní. Pokud odpověď obdrží pouze jedna karta, v síti je detekována přítomnost falešného přístupového bodu, připojeného na legitimní AP. V případě, kdy odpověď neobdrží karta A ani karta B, jedná se o falešné AP s vlastním připojením k internetu. Metoda má tři komponenty. V prvním dojde k zaměření přístupových bodů se stejným SSID. V případě výskytu více než dvou AP jsou postupně otestovány všechny zařízení. Reflexní komponenta zajišťuje odesílání SYN zpráv a monitorováním sítě za účelem nalezení validních odpovědí. Poslední rozhodovací komponenta je zodpovědná za detekováním falešného AP a rozlišení způsobu jeho připojení [29].

ET detector

Cílem je detekovat podezřelý přístupový bod, který často přesměrovává pakety. Metoda se tedy zaměřuje na falešný AP připojený na legitimní přístupový bod. Při tomto scénáři je falešné AP nuceno přesměrovat veškerou komunikaci připojeného klienta (oběti) na původní přístupový bod. ET Detector pasivně monitoruje okolní síťový provoz. Detekce začíná výběrem Wi-Fi sítě k testování, zvolena je síť s alespoň dvěma AP se shodným parametrem SSID a bez zabezpečení heslem. Každé AP ve vybrané síti má svoji hash tabulku rozlišenou pomocí BSSID. Kdykoliv je zachycen paket, je z něj získáno sekvenční číslo a ACK, z kterých vypočítá a uloží hash hodnotu. Při přeposílání falešný AP tyto hodnoty nemění, což po čase ET Detector odhalí při porovnávání hash hodnot v tabulkách různých AP. Podle pořadí poté odhalí, které AP přesměrovává pakety. Uživatel může využít možnosti sekundárního testování konkrétního zařízení, kdy je za pomoci dalšího zařízení připojeného k podezřelému AP, realizováno připojení k specifické IP adrese získané

od ET Detectoru. Data pro toto testování jsou sbírány ve stejný čas jako data pro hash tabulky. Jedná se o cílové IP adresy TCP paketů. Zachytí-li ET Detector specifickou IP adresu ve dvou různých paketech zaslaných na dvě různé AP, vyhodnotí adresáta prvního paketu (jedno z AP) jako falešné [30].

SLFAT – Special Length Frame Arrival Time

Detekční metoda složená ze čtyř komponent. První je monitorovací, která zachytává okolní komunikaci a z ní pakety odeslané podezřelými AP. Zaznamenaná komunikace je rozdělena do souborů na základě původu a obsahuje kontrolní, managementové a datové rámce. Kvůli možným odlišnostem v použitém kanálu jednotlivých AP je pro tento úkon doporučeno použít dvě síťové karty. Filtrovací komponenta vybírá pouze datové rámce specifické, nejméně se vyskytující délky. Jsou to rámce, které se v souboru jednotlivých AP vyskytnou maximálně 20 krát. Z těchto vybraných rámců jsou uložena data do slovníku. Klíčem je vždy délka rámce a hodnotou je další slovník, obsahující cílovou MAC adresu a čas přijetí rámce. Pro oba AP existují separátní slovníky. Posledním krokem filtrovací komponenty je průnik obou slovníků na základě klíčové hodnoty, tedy délky rámců. Třetí komponenta, procesní, detekuje podezřelé přesměrovávání zpráv. Metoda předpokládá připojení falešného AP na AP originální sítě. Z toho vyplývá, že rámce odeslané útočníkem budou mít vyšší čas přijetí paketu. Hodnota intervalu mezi přijetím dvou rámců stejné speciální délky je metodou určena na nejvýše 0,6 s. Pro dva rámce, jejichž časy se maximálně o tuto hodnotu liší je zaznamenána dvojce MAC adres, cílová adresa dřívějšího rámce a zdrojová adresa později přijatého rámce, a počet výskytů pro tuto dvojici. V poslední rozhodovací komponentě je rozpoznána vysoká hodnota počtu výskytů určité dvojce, indikuje přítomnost Evil Twin, MAC adresy pak ukazují na jeho síťová rozhraní [31].

Tab. 2.2: Přehled vlastností detekcí na straně klienta.

metoda/zaměření detekce	**RAP připojený na originální AP**	**RAP s vlastním připojením**	**pasivní/aktivní detekce**
Round Trip Time	ano	ne	aktivní
Received Signal Strengths and Sequential Hypothesis	ano	ano	obě možnosti
Metoda na bázi spojení přes TCP	ne	ano	aktivní
BiRe	ano	ano	aktivní
ET detector	ano	ne	obě možnosti
SLFAT	ano	ne	pasivní

2.3.2 Detekce na straně serveru

Servery disponují velkou pamětí a silou výpočetního výkonu. Pro klienty je tento přístup výhodný, jelikož nemusí použít žádný specializovaný hardware nebo software. Nevýhodou je, že klient nemá informaci, které AP jsou legitimní či škodlivé [25].

Hidden Markov Model

Příchozí i odchozí provoz na výchozí bráně Wi-Fi sítě je monitorován. Mezi legitimním a falešným AP rozhoduje statistika, založená na základě dat získaných z průměru časů příchodů paketů. Model přístupové body v síti označuje stavy good, probed a compromised. Ve stavu good nejeví AP žádné známky neobvyklého chování. Stav probed znamená, že je důvěryhodnost AP testována, např. pomocí skenování portů. Compromised označuje stav, kdy je AP nedůvěryhodný. V první fázi je potřeba model trénovat, počáteční parametry sítě mohou být dodány správcem sítě, dále jsou dodána data, která vznikla např. během DoS útoků na síti, využívajících právě RAP. Po tréninku na těchto datech je model schopen nalézt RAP, je-li přes něj prováděn DoS útok [32].

Detekce s využitím časové charakteristiky

Používá charakteristiku síťového provozu na centrálním uzlu – switchi (nutná podpora podsítí). Switch sleduje síťový provoz na jednotlivých portech v obou směrech, časová charakteristika jednoho portu je uchována v řadě stavových proměnných. Metoda pracuje s rozdílem přenosu dat v části sítě, která je realizována pouze kabelem a částí sítě, kde je použit bezdrátový přístupový bod. Časová charakteristika síťového provozu na portu s připojeným AP bude ovlivněna vyšší nespolehlivostí přenosového média, rozdílem přenosových rychlostí mezi kabely a Wi-Fi, mohutností provozu, rušením frekvenčního pásma nebo zpožděním, způsobeném čekáním na uvolnění přístupu k médiu. Vyskytnou-li se na některém portu výrazné změny, lze očekávat přítomnost AP. Tato metoda funguje pouze díky datům z fyzicky uchopitelné části sítě a je tedy nezávislá na šíření signálu od AP [33].

Clock Skew

Clock Skew je označení pro rozdíly zdroje hodinového signálu v digitálních obvodech, způsobené fyzickými odlištnostmi v řezu krystalu křemene. Ty jsou zapříčiněny nepřesností mechanického procesu řezání, což způsobuje, že i dva velmi podobné krystaly mají rozdílné hodinové signály. Metoda používá časové značky v beacon rámcích a odpovědích na ně k zisku jedinečné hodnoty Clock Skew daného přístupového bodu. V případě, kdy je obvykle konstantní posun hodin narušen výrazným skokem, je indikována přítomnost dalšího AP. Metoda zavádí parametr threshold, což je rozdíl mezi skokem a konzistentní

inkrementací, pro jehož výpočet stačí hodnoty z 50 až 100 paketů. Podle threshold jsou data rozdělena do datových množin a přiřazena konkrétním pracujícím AP. Z nichž je pomocí jedné ze dvou metod (případně kombinací) určen Clock Skew falešného nebo více falešných AP [34].

Hybrid Framework

Spojuje výhody detekčního přístupu s použitím kabelové i bezdrátové části sítě. Metoda používá dva moduly – distribuovaný fungující na jednotlivých přístupových bodech sítě a centrální, pracujícím na výchozí bráně LAN sítě. Distribuovaný modul pasivně sbírá rámce na bezdrátové části sítě. Ty jsou poté předzpracovávány, hledají se duplicitní nebo u administrátora neregistrované MAC dresy nebo falešné rámce managementu, v této části jsou odhaleny RAP čtvrtého typu – kompromitované. Finální zpracování spočívá v odhalení všech čtyř kategorií RAP, jsou kontrolovány např. možné deautentizační útoky na uživatele. Druhý, centrální modul využívá skenování portů. Na konzoli připojené k výchozí bráně, běží program dotazující se na port 80 (HTTP), všechny zařízení, včetně AP, zašlou v odpovědi svou IP adresu a jméno výrobce. Seznam je poté porovnán s whitelistem administrátora. Pokud má RAP port 80 zakázaný, využívá metoda detekci s využitím časové charakteristiky [35].

Tab. 2.3: Přehled vlastností detekcí na straně serveru.

metoda/zaměření detekce	**RAP připojený na originální AP/na stejnou síť**	**RAP s vlastním připojením**
Hidden Markov Model	ano	ne
Detekce s využitím časové charakteristiky	ano	ne
Clock Skew	ano	ano
Hybrid Framework	ano	ne

3 Vlastní metoda detekce falešného přístupového bodu

V této kapitole bude popsána pokročilá metoda detekce, která je praktickým výstupem této práce. Představeny budou její vlastnosti, problémy při realizaci, použitý software, síť a hardware, na které byla metoda testována a výsledky těchto testů.

3.1 Popis vlastní detekční metody

Vlastní metoda se zaměřuje na Evil Twin přístupové body, které úmyslně napodobují nastavení legitimního AP. Cílem bylo odhalit přítomnost ET získávajícího přístup k internetu přes původní přístupový bod napadnuté sítě i variantu, kdy má útočník zajištěno vlastní připojení. Vybrán byl přístup k detekci ze strany klienta, konkrétní metody pak podle zaměření na typ připojení RAP v tabulce 2.2. Pro přehlednost budou zopakovány klíčové vlastnosti zvolených metod Special Length Frame Arrival Time a detekce založené na TCP spojení.

SLFAT

- Jedná se o pasivní detekci, kdy uživatel neriskuje připojení na ET.
- K implementaci postačí jedna síťová karta (používá-li ET stejný kanál), podporující monitorovací režim, ideální jsou však karty dvě.
- Pro zachycení dat je možné použít dobře známé nástroje pro monitorování sítě, jako Wireshark nebo TShark.
- Zaměřuje se na scénář, kdy je Evil Twin připojeno na legitimní Access Point.
- Detekci je možné provádět z jednoho místa.
- Při úspěšné detekci odhalí MAC adresy použité útočníkem.

Na základě TCP spojení

- Aktivní detekce, je tedy nutné postupně se připojit na všechny body v síti.
- Nevyžaduje žádný specializovaný hardware.
- Jelikož se síťová karta automaticky připojuje na AP s nejsilnějším signálem, je nutné se v průběhu detekce přesouvat.
- Využívá vlastností překladu IP adres z privátních na veřejné k rozpoznání Evil Twin s vlastním připojením k internetu.
- Při odhalení přítomnost ET není ukázáno na konkrétní zařízení.

3.2 Implementace

Průběh obou metod je na sobě nezávislý. První byla implementována detekce na základě TCP spojení. Kdy byla metoda nejprve odzkoušena v terminálu za pomocí nástroje OpenSSH. V python kódu je pak pro zasílání HTML dotazů využit modul requests. V první části program za pomocí knihovny OS a příkazu nmcli vypíše informace o všech okolních Wi-Fi sítích. Uživatel je vyzván, aby zadal SSID sítě, kterou chce otestovat. V tu chvíli je upozorněn, že síťová karta se připojí k AP s nejvyšší silou signálu a doporučením, jak zjistit, kde má které BSSID silnější signál. Poté je zařízení připojeno k prvnímu AP a je navázáno spojení se serverem google.com. Využita je requests funkce session, v které je využíváno jedno spojení po celou dobu jejího trvání. Nemůže se tedy stát, že z druhého AP bude navázáno spojení s vlastním socketem. Uživatel je upozorněn, že spojení je navázáno a vyzván k přesunu blíž k druhému AP. Má na to 30 s, poté je zařízení s použitím nmcli připojeno k druhému AP, pro kontrolu je vypsáno jeho BSSID. Následně je serveru zaslán příkaz GET, obdrží-li na něj uživatel odpověď "200 OK"je druhý AP ve stejné síti jako první, to je možné vidět na výpise 3.1.

Dojde-li k nastavenému timeoutu, je uživatel varován před ET. Žádost `GET` je zaslána s nastaveným timeoutem 30 s, jelikož bez něj trvá zahození spojení serverem kolem 15 minut. Jelikož odpověď serveru po navázání spojení (na prvním AP) přišla do jedné sekundy, je očividné, že klient je připojen z jiné výchozí brány než na začátku spojení. Server tedy nezná informace, nutné pro doručení odpovědi. Klient je varován, před výskytem ET v síti viz výpis 3.2.

Výpis 3.1: Výstup v terminálu tcp_based.py, scénář bez ET.

```
SSID of target network: MojeWifi

WNIC will always connect to AP with strongest signal.
Move around room and use command:
nmcli dev wifi
in terminal to find out
where every AP has strongest signal.

Connecting to first AP with BSSID:
60:45:cb:8F:fe:88
    [2K
Device 'wlan0' successfully activated
with '54686d38-2202-4ea5-8662-4001fb238bd4'.
200
Move to place, where second AP has stronger signal.

Connecting to second AP with BSSID:
60:45:cb:90:21:98
 [2K
Device 'wlan0' successfully activated
with '54686d38-2202-4ea5-8662-4001fb238bd4'.
200

MojeWifi network doesn't␣have␣Evil␣Twin
with␣extrenal␣internet␣connection.
```

Výpis 3.2: Výstup v terminálu tcp_based.py, scénář s ET.

```
SSID of target network: MojeWifi

WNIC will always connect to AP with strongest signal.
Move around room and use command:
nmcli dev wifi
in terminal to find out
where every AP has strongest signal.

Connecting to first AP with BSSID:
60:45:cb:8F:fe:88
    [2K
Device 'wlan0' successfully activated
with '54686d38-2202-4ea5-8662-4001fb238bd4'.
200
Move to place, where second AP has stronger signal.

Connecting to second AP with BSSID:
18:31:BF:D1:26:CA
 [2K
Device 'wlan0' successfully activated
with '54686d38-2202-4ea5-8662-4001fb238bd4'.

HTTPSConnectionPool(host='www.google.com', port=443):
Read timed out. (read timeout=5)

Response from server takes unexpected long time.
Evil Twin warnning!
```

Druhá část, vycházející z SLFAT pracuje se zadáním dat z fáze monitoringu z CSV souboru získaném v programu Wireshark. Oproti původnímu návrhu je vyfiltrování datových rámců realizováno už v kroku monitoringu. Ve Wiresharku je použit filtr `wlan.fc.type==2`, který zobrazí všechny druhy datových rámců. Uživatel musí znát MAC adresy přístupových bodů s duplicitním SSID, aby je označil jako cíle. Poté je vytvořen slovník obsahující všechny délky rámců a jejich četnost. Zadané MAC adresy jsou vyhledány ve sloupci odchozích adres, zkontrolována je četnost výskytu délek a pokud řádek splní obě podmínky jsou informace z něj přidány do slovníku ap1 nebo ap2. Aby mohli být oba slovníky promazány o hodnoty mimo jejich průnik, je pro oba slovníky zvlášť vytvořena struktura set, obsahující seznam všech obsažených délek. Po provedení průniku jsou podle stejných délek a příchozího času s maximálním rozdílem

0,6 s hledány stejné dvojce paketů v rámci odeslaných z obou AP. Pro každou takovou dvojici je zaznamenána dvojce podezřelých MAC adres. Nejvyšší počet nálezů stejných MAC adres ukáže na přítomnost ET.

Výpis 3.3: Výstup v terminálu slfat.py, scénář bez ET.

```
Type path to .csv file:day2_a.csv
Insert MAC address of first target AP:
3c:33:00:a2:56:b8
Insert MAC address of second target AP:
3c:33:00:a2:56:ad
Network is safe.
```

Výpis 3.4: Výstup v terminálu slfat.py, scénář bez ET.

```
Type path to .csv file:day2_b.csv
Insert MAC address of first target AP:
3c:33:00:a2:56:b8
Insert MAC address of second target AP:
00:c0:ca:a7:48:97
Evil Twin detected.
Keep away from those MAC addresses:
00:c0:ca:a7:48:97,14:4f:8a:ed:47:43
```

Použitý software a knihovny

Pro realizaci ET i vlastní detekční metodu byla zvolena linuxová distribuce KALI, určená pro penetrační testování. Nabízí širokou škálu předinstalovaných nástrojů i podporu experimentálních projektů z GitHubu. Z předinstalovaných nástrojů byly využit následující:

- **nmcli** – nástroj pro terminál, pracuje s Network Managerem, reportuje statusy připojení.
- **Airmon-ng** – určený pro přepnutí síťové karty do monitorovacího režimu.
- **Wireshark** – umožňuje monitorovat a analyzovat pakety získané na kabelové i bezdrátové síti. Má grafické uživatelské rozhraní a podporuje řadu filtrů. Bezdrátové sítě monitoruje vždy na jednom vybraném kanále.
- **iwconfig** – pro konfiguraci síťových bezdrátových rozhraní.

Samotná implementace pak probíhala v programovacím jazyku Python 2.7. ve vývojářském prostředí Eclipse. Využity byly tyto knihovny:

- **requests** – umožňuje jednoduchou tvorbu dotazů HTTP/1.1, podporuje SSL zabezpečení, kontrolu certifikátů webových stránek.
- **wifi** – konfigurace bezdrátového síťového rozhraní a usnadnění připojení k síti přímo z Python programu.

- **csv** – modul pro práci se soubory CSV, čtení i zápis do souborů bez nutné znalosti přesně použitého formátu tabulky.
- **os** – usnadnění práce s funkcemi vestavěnými v operačním systému.
- **time** – využita byla konkrétně funkce sleep, pro vynucení zpoždění mezi úkony.

Realizace falešného AP

Všechny nástroje zmíněné v sekci 2.2 byly nainstalovány na virtuální stroj s Kali Linuxem. Pro účely testování byl nejvhodnější nástroj Wifi-Pumpkin a create_ap. Jelikož oba nastroje je možné spustit bez jakéhokoliv předpřipraveného útoku. Je možné provádět s nimi aktivní detekci a při pasivní generovat provoz z jiných zařízení.

3.2.1 Experimentální síť

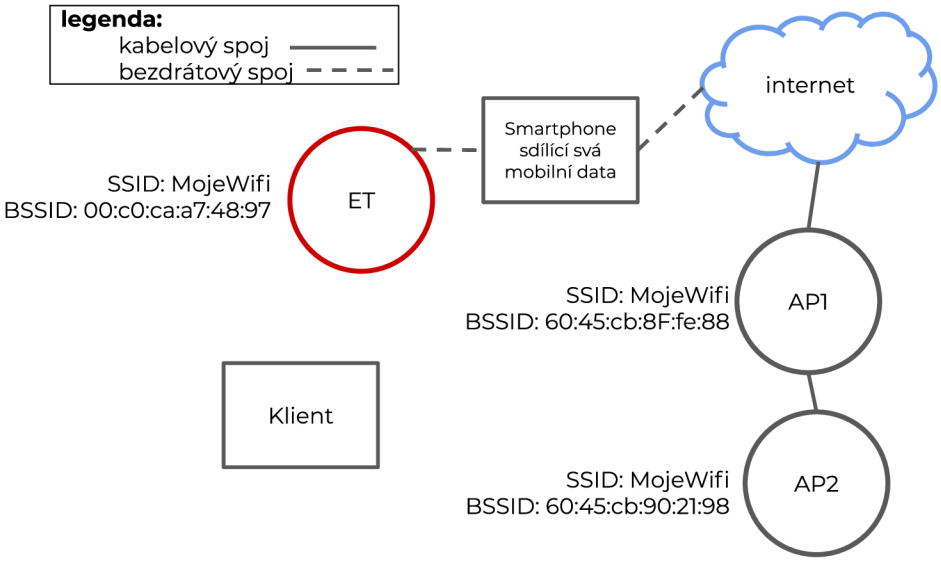
Testování funkčnosti vlastní implementace proběhlo na experimentální síti. Topologie pro testování implementace detekční metody na bázi TCP byla následující. Klient se v průběhu testů přepojoval mezi přístupovými body podle své aktuální polohy. Pro druhou část, zaměřenou na detekci ET připojeného v původní síti, bylo zapojení následující. Klient v tomto případě síť pouze pasivně monitoroval.

Použitý hardware

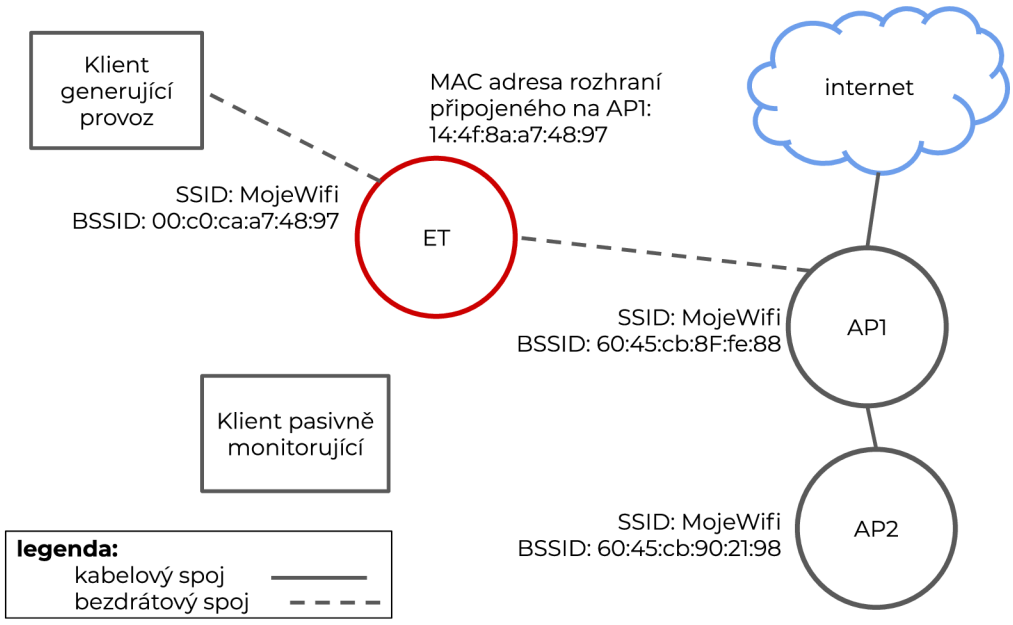
Detekce a realizace ET běžely na virtuálních strojích s OS Kali Linux, hostvaných na noteboocích s Windows 10. Použité USB síťové karty byly Alfa Network AWUS036ACH a TP-LINK TL-WN722N. Oba legitmní přístupové body zastupovaly ASUS RT-AC1200G+.

Režimy bezdrátových síťových karet

- **Běžný režim** – V běžném režimu síťová karta přijímá pouze komunikaci, která je pro ni určená, ostatní pakety zahazuje.
- **Promiskuitní režim** – Síťová karta příjmá veškerou komunikaci, režim je vhodný pro packet sniffing, analyzování datového provozu vhodným programem, například Wiresharkem. Pro použití tohoto režimu je potřeba být přihlášený v dané síti.
- **Monitorovací režim** – Funguje podobně jako promiskuidní režim, ovšem bez nutnosti se do sítě přihlašovat.
- **Master režim** – Dovoluje bezdrátové síťové kartě fungovat jako acess point.



Obr. 3.1: Experimentální síť pro testování vlastní implementace detekční metody na bázi TCP.



Obr. 3.2: Experimentální síť pro testování vlastní implementace detekční metody SLFAT.

Závěr

Cílem bakalářské práce bylo vytvořit vlastní detekční metodu, odhalující falešné přístupové body v bezdrátových sítích, dále také nastudování potřebné teorie k tématům detekčních metod i metod realizace RAP.

V průběhu implementace bylo nutné vypořádat se s několika problémy. Jedním z nich byla nemožnost ovlivnit výběr sítě k připojení zadáním jejího BSSID u implementace metody založené na TCP spojení. Proto byl původní záměr, kdy měl uživatel dobu testovaní sítě strávit na jednom místě, změněn na variantu s přesouváním. U frameworku Wifi-Pumpknin se vyskytl problém, kdy se hodnota parametru MAC adresy neměnila a vždy zůstala na výchozí hodnotě se kterou byl program spuštěn. U použité metody sledující datové rámce, jejich specifické délky a právě MAC adresy (BSSID), ET se změněným BSSID prošel jako legitimní bod, tento scénář se však nepodvedlo otestovat. Tato skutečnost není uvedena v tabulce 2.1, podle diskuzí u nástroje na GitHubu se pravděpodobně jedná o ojedinělý problém. V průběhu zpracovávání této práce, konkrétně v březnu 2020, navíc vyšla nová verze wifipumpkin3 a repozitář původní verze byl označen za zastaralý.

Vlastní implementace byla otestována na experimentální síti. Pro oba programy byl alespoň desetkrát otestován scénář s i bez výskytu ET. Kombinací obou implementovaných metod je možné odhalit ET napodubující SSID, s vlastním připojením k internetu (mobilní poskytovatel) i připojený na původní síť. TCP metoda pouze ukáže na přítomnost ET v síti, neidentifikuje však konkrétní zařízení. Metoda bude fungovat i pro nalezení neautorizovaného RAP..

Literatura

[1] IEEE 802.11. *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-03-12]. Dostupné z: <https://en.wikipedia.org/wiki/IEEE_802.11>

[2] Wi-Fi (802.11x standard). *Tech target* [online]. [cit. 2020-03-12]. Dostupné z: <https://searchmobilecomputing.techtarget.com/definition/Wi-Fi>

[3] RAY, Brian. WiFi's Future: Examining 802.11ad, 802.11ah HaLow (and Others). *Link-labs* [online]. 2018 [cit. 2020-03-12]. Dostupné z:<https://www.link-labs.com/blog/future-of-wifi-802-11ah-802-11ad>

[4] 802.11i. *Tech target* [online]. [cit. 2020-03-13]. Dostupné z: <https://searchmobilecomputing.techtarget.com/definition/80211i>

[5] Wireless security. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2020-03-13]. Dostupné z: <https://en.wikipedia.org/wiki/Wireless_security>

[6] ARASH HABIBI LASHKARI, MIR MOHAMMAD SEYED DANESH a Behrang SAMADI. A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). *2009 2nd IEEE International Conference on Computer Science and Information Technology*. IEEE, 2009, 2009, , 48-52. DOI: 10.1109/ICCSIT.2009.5234856. ISBN 978-1-4244-4519-6. Dostupné z: <https://ieeexplore.ieee.org/document/5234856/>

[7] SARI, Arif a Mehmet KARAY. Comparative Analysis of Wireless Security Protocols: WEP vs WPA. *International Journal of Communications, Network and System Sciences*. 2015, **08**(12), 483-491. DOI: 10.4236/ijcns.2015.812043. ISSN 1913-3715. Dostupné z: <https://scirp.org/journal/doi.aspx?DOI=10.4236/ijcns.2015.812043>

[8] VANHOEF, Mathy a Frank PIESSENS. Practical verification of WPA-TKIP vulnerabilities. *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security - ASIA CCS '13*. New York, New York, USA: ACM Press, 2013, 2013, 427-436. DOI: 10.1145/2484313.2484368. ISBN 9781450317672. Dostupné z: <https://computerresearch.org/index.php/computer/article/view/480>

[9] SAKIB, A.K.M. Nazmus, Shamim AHMED, Samiur RAHMAN, Ishtiaque MAHMUD a Md. Habibullah BELALI. WPA 2 (Wi-Fi Protected Access 2) Security Enhancement: Analysis and Improvement. *Global Journal of Computer Science and*

Technology. Dha ka International University, 2012, **2012**(4), 1-9. ISSN 0975-4172. Dostupné z: <https://dl.acm.org/citation.cfm?doid=2484313.2484368>

[10] Key Management. *Etutorials* [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2018-12-11]. Dostupné z: <etutorials.org/Networking/Wireless+lan+security/Chapter+8.+WLAN+Encryption+and+Data+Integrity+Protocols/Key+Management/#ch08lev3sec15>

[11] Discover Wi-Fi Security. *Wi-Fi Alliance* [online]. [cit. 2020-03-19]. Dostupné z: <https://wi-fi.org/discover-wi-fi/security>

[12] Opportunistic Wireless Encryption Specification. *Wi-Fi Alliance* [online]. [cit. 2020-03-19]. Dostupné z: <https://wi-fi.org/downloads-public/Opportunistic_Wireless_Encryption_Specification_v1.0.pdf/35331>

[13] VANHOEF, Mathy a Eyal RONEN. *Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd*. Los Alamitos, CA, USA, 2020, **2020**(1), 808-824. DOI: 10.1109/SP40000.2020.00031. ISSN 2375-1207. Dostupné z: <https://www.computer.org/csdl/proceedings-article/sp/2020/349700a808/1j2LfVdHRaE>

[14] LOUNIS, Karim a Mohammad ZULKERNINE. WPA3 Connection Deprivation Attacks. *Risks and Security of Internet and Systems: 14th International Conference, CRiSIS 2019, Hammamet, Tunisia, October 29—31, 2019, Proceedings*. 1. Switzerland: Springer International Publishing, 2020, s. 164-176. ISBN 978-3-030-41567-9. Dostupné z: <https://link.springer.com/chapter/10.1007/978-3-030-41568-6_11>

[15] MA, Liran, Amin Y. TEYMORIAN, Xiuzhen CHENG a Min SONG. RAP. In: *The Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness & Workshops - QSHINE '07* [online]. New York, New York, USA: ACM Press, 2007, 2007, s. 1- [cit. 2020-06-07]. DOI: 10.1145/1577222.1577252. ISBN 9781595937568. Dostupné z: <http://portal.acm.org/citation.cfm?doid=1577222.1577252>

[16] Captive Portal Attack. *GitHub* [online]. [cit. 2020-02-11]. Dostupné z: <https://github.com/FluxionNetwork/fluxion/wiki/Captive-Portal-Attack>

[17] AGARWAL, Mayank, Santosh BISWAS a Sukumar NANDI. An Efficient Scheme to Detect Evil Twin Rogue Access Point Attack in 802.11 Wi-Fi Networks. *International Journal of Wireless Information Networks* [online]. 2018, **25**(2), 130-145 [cit. 2020-05-07]. DOI: 10.1007/s10776-018-0396-1. ISSN 1068-9605. Dostupné z: <http://link.springer.com/10.1007/s10776-018-0396-1>

[18] How to Hack WiFi with Rogue Access Point. *rootsh3ll* [online]. [cit. 2020-02-14]. Dostupné z: <https://rootsh3ll.com/how-to-hack-wifi/>

[19] Fake-AP. *GitHub* [online]. [cit. 2020-02-14]. Dostupné z: <https://github.com/thelinuxchoice/fakeap>

[20] Fluxion. *GitHub* [online]. [cit. 2020-02-14]. Dostupné z: <https://github.com/FluxionNetwork/fluxion>

[21] Wifiphisher. *GitHub* [online]. [cit. 2020-02-14]. Dostupné z: <https://github.com/wifiphisher/wifiphisher>

[22] WiFi-Pumpkin: Framework for Rogue Wi-Fi Access Point Attack. *GitHub* [online]. [cit. 2020-02-14]. Dostupné z: <https://github.com/P0cL4bs/WiFi-Pumpkin>

[23] Create_ap. *GitHub* [online]. [cit. 2020-02-14]. Dostupné z: <https://github.com/oblique/create_ap>

[24] *Beacon frame monitoring*. US 9,398,519 B2. Dostupné z: <https://patents.google.com/patent/US9398519B2/en>

[25] ANMULWAR, Sweta, Shalvi SRIVASTAVA, Shrinivas P. MAHAJAN, Anil Kumar GUPTA a Vinodh KUMAR. Rogue access point detection methods: A review. In: *International Conference on Information Communication and Embedded Systems (ICICES2014)* [online]. IEEE, 2014, 2014, s. 1-6 [cit. 2020-05-07]. DOI: 10.1109/ICICES.2014.7034106. ISBN 978-1-4799-3834-6. Dostupné z: <http://ieeexplore.ieee.org/document/7034106/>

[26] HAN, Hao, Bo SHENG, Chiu C. TAN, Qun LI a Sanglu LU. A Timing-Based Scheme for Rogue AP Detection. *IEEE Transactions on Parallel and Distributed Systems* [online]. 2011, **22**(11), 1912-1925 [cit. 2020-05-08]. DOI: 10.1109/TPDS.2011.125. ISSN 1045-9219. Dostupné z: <http://ieeexplore.ieee.org/document/6007016/>

[27] KIM, Taebeom, Haemin PARK, Hyunchul JUNG a Heejo LEE. Online Detection of Fake Access Points Using Received Signal Strengths. In: *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)* [online]. IEEE, 2012, 2012, s. 1-5 [cit. 2020-05-08]. DOI: 10.1109/VETECS.2012.6240312. ISBN 978-1-4673-0990-5. Dostupné z: <http://ieeexplore.ieee.org/document/6240312/>

[28] NAKHILA, Omar, Erich DONDYK, Muhammad Faisal AMJAD a Cliff ZOU. User-side Wi-Fi Evil Twin Attack detection using SSL/TCP protocols. In: *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC)* [online]. IEEE, 2015, 2015, s. 239-244 [cit. 2020-05-08]. DOI: 10.1109/CCNC.2015.7157983.

ISBN 978-1-4799-6390-4. Dostupné z: <http://ieeexplore.ieee.org/document/7157983/>

[29] LU, Qian, Ruobing JIANG, Yuzhan OUYANG, Haipeng QU a Jiahui ZHANG. BiRe: A client-side Bi-directional SYN Reflection mechanism against multi-model evil twin attacks. *Computers & Security* [online]. 2020, **88** [cit. 2020-05-09]. DOI: 10.1016/j.cose.2019.101618. ISSN 01674048. Dostupné z: <https://linkinghub.elsevier.com/retrieve/pii/S0167404819301658>

[30] HSU, Fu-Hau, Chuan-Sheng WANG, Yu-Liang HSU, Yung-Pin CHENG a Yu-Hsiang HSNEH. A client-side detection mechanism for evil twins. *Computers & Electrical Engineering* [online]. 2017, **59**, 76-85 [cit. 2020-05-09]. DOI: 10.1016/j.compeleceng.2015.10.010. ISSN 00457906. Dostupné z: <https://linkinghub.elsevier.com/retrieve/pii/S0045790615003559>

[31] LU, Qian, Haipeng QU, Yuzhan OUYANG a Jiahui ZHANG. SLFAT: Client-Side Evil Twin Detection Approach Based on Arrival Time of Special Length Frames. *Security and Communication Networks* [online]. 2019, **2019**, 1-10 [cit. 2020-05-10]. DOI: 10.1155/2019/2718741. ISSN 1939-0114. Dostupné z: <https://www.hindawi.com/journals/scn/2019/2718741/>

[32] SHIVARAJ, Gayathri, Min SONG a Sachin SHETTY. A Hidden Markov Model based approach to detect Rogue Access Points. In: *MILCOM 2008 - 2008 IEEE Military Communications Conference* [online]. IEEE, 2008, 2008, s. 1-7 [cit. 2020-05-10]. DOI: 10.1109/MILCOM.2008.4753358. ISBN 978-1-4244-2676-8. Dostupné z: <http://ieeexplore.ieee.org/document/4753358/>

[33] BEYAH, R., S. KANGUDE, GEORGE YU, B. STRICKLAND a J. COPELAND. Rogue access point detection using temporal traffic characteristics. In: *IEEE Global Telecommunications Conference, 2004. GLOBECOM '04* [online]. IEEE, 2004, s. 2271-2275 [cit. 2020-05-10]. DOI: 10.1109/GLOCOM.2004.1378413. ISBN 0-7803-8794-5. Dostupné z: <http://ieeexplore.ieee.org/document/1378413/>

[34] JANA, S. a S.K. KASERA. On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews. *IEEE Transactions on Mobile Computing* [online]. 2010, **9**(3), 449-462 [cit. 2020-05-12]. DOI: 10.1109/TMC.2009.145. ISSN 1536-1233. Dostupné z: <http://ieeexplore.ieee.org/document/5210105/>

[35] MA, L., A. Y. TEYMORIAN a X. CHENG. A Hybrid Rogue Access Point Protection Framework for Commodity Wi-Fi Networks. In: *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications* [online]. IEEE, 2008, 2008, s. 1220-1228

[cit. 2020-05-13]. DOI: 10.1109/INFOCOM.2008.178. ISBN 978-1-4244-2026-1. Dostupné z: <http://ieeexplore.ieee.org/document/4509773/>

Seznam symbolů, veličin a zkratek

ACK number acknowledgement number

AES Advanced Encryption Standard

AP Access Point

ASCII American Standard Code for Information Interchange, kódovácí tabulka pro znaky

BiRe Bi-directional SYN Reflection

BSSID MAC adresa přístupového bodu bezdrátové sítě

CCMP Counter Cipher Mode with Block Chaining Message Authentication Code Protocol

CRC-32 Cyclic redundancy check, hashovácí funkce pro detekci chyb během přenosu

CSV Comma Separated Values

DNS Domain Name Server

DoS Denial of Service

EAP Extensible Authentication Protocol

ECDH Elliptic Curve Diffie-Hellman

ECDSA Elliptic Curve Digital Signature Algorithm

ET Evil Twin

GHz jednotka frekvence (kmitočtu)

GTK Group Transient Key

HTTP Hypertext Transfer Protocol

IEEE Institute of Electrical and Electronic

IoT Internet of Things

KRACK Key Reinstallation Attacks

LAN Local Area Network

MAC	Media Access Control
MIC	Message Integrity Code
MIMO	Multiple-input multiple-output
MITM	Man In the Midle
NAT	Network Address Translation
OFDM	Orthogonal Frequency Division Multiplexing
OWE	Opportunistic Wireless Encryption
PAT	Port Address Translation
PMF	Protected Management Frames
PMK	Pairwise Master Key
PSK	Preshared Key
PTK	Pairwise Transient Key
QoS	Požadavky na kvalitu služeb
RAP	Rogue Access Point
RC4	proudová šifra
RSNE	Robust Security Network Element
RTT	Round Trip Time
SAE	Simultaneous Authentication of Equals
SLFAT	Special Length Frame Arrival Time
SSID	Název bezdrávové sítě
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Privacy
WLAN	bezdrátová lokální síť
WPA	Wi-Fi Protected Access

Seznam příloh

A Uživatelská příručka

Po stažení souborů na počítač s OS Linux je potřeba u obou souborů umožnit jejich spuštění příkazem `sudo chmod +x <název souboru>`. Poté je možné soubory pustit příkazem `sudo ./<název souboru>`.

A.1 tcp_based.py

Pro běh je nutné nainstalovat modul requests pomocí příkazu `pip install requests`. Před spuštěním je doporučeno zjistit v kterých částech místnosti či prostoru je signál jednotlivých AP vyšší pomocí `nmcli dev wifi`. Po spuštění tcp_based.py, je uživatel vyzván k zadání SSID, které chce prověřit a dále jsou veškeré infromace a instrukce zobrazeny v konzoli. Na 8. a 9. řádku kódu je jako string uložena adresa serveru a rozhraní. V případě hlášky Connection refused může pomoci změnit server nebo také příkaz `systemctl restart NetworkManager.service`. Poku chceme program využít pro hledání neautorizovaného RAP viz výčet 2.1, je potřeba v řádcích s `os.system('nmcli d wifi connect '+name+' password "")` přepsat proměnnou name konkrétním názvem sítě, jednou např. firemní sítí a v druhém případě sítí podezřelou.

A.2 slfat.py

Program pracuje s daty vyexportovanými z Wiresharku. Pro monitorování provozu na okolních sítích je potřeba změnit režim bezdrátové síťové karty příkazy: `sudo airmon-ng check kill`, `sudo airmon-ng start wlan0` a `sudo airmon-ng`. Pro vyfiltrování potřebných paketů je použit filtr `wlan.fc.type==2`. Modul pro práci se soubory CSV je třeba nainstalovat příkazem `pip install python-csv`. Po zadání cesty k CSV souboru do programu je vše plně automatizováno.

B Obsah elektronické přílohy

- tcp_based.py
- sflat.py