VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV POČÍTAČOVÝCH SYSTÉMŮ
DEPARTMENT OF COMPUTER SYSTEMS

ROZŠIŘENÍ ODPOSLECHOVÉ SONDY O PODPORU WI-FI

EXTENSION OF THE MONITORING PROBE WITH WI-FI SUPPORT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE **MICHAL FINDRA**
AUTHOR

VEDOUCÍ PRÁCE **Ing. MICHAL ORSÁK**
SUPERVISOR

BRNO 2022

Vysoké učení technické v Brně
Fakulta informačních technologií

Ústav počítačových systémů (UPSY) Akademický rok 2021/2022

Zadání bakalářské práce

Student: **Findra Michal**
Program: Informační technologie
Název: **Rozšíření odposlechové sondy o podporu Wi-Fi**
Extension of the Monitoring Probe with Wi-Fi Support
Kategorie: Počítačové sítě

Zadání:

1. Nastudujte sondu pro zákonné odposlechy vyvíjenou v rámci výzkumu na FIT VUT v Brně.
2. Seznamte se možnostmi rozšíření sondy o Wi-Fi rozhraní (např. pomocí přídavného Wi-Fi USB adaptéru)
3. Navrhněte řešení pro rozšíření odposlechové sondy o podporu odposlechů z tohoto Wi-Fi rozhraní.
4. Implementujte navržené řešení do podoby aktualizačního skriptu nebo balíčku sondy a otestujte navržené řešení.
5. Zhodnoťte výsledky své práce a diskutujte další možná rozšíření.

Literatura:

- Dle doporučení vedoucího práce.

Pro udělení zápočtu za první semestr je požadováno:

- Body 1 až 3 zadání.

Podrobné závazné pokyny pro vypracování práce viz https://www.fit.vut.cz/study/theses/

Vedoucí práce: **Orsák Michal, Ing.**
Konzultant: Korček Pavol, Ing., Ph.D., UPSY FIT VUT
Vedoucí ústavu: Sekanina Lukáš, prof. Ing., Ph.D.
Datum zadání: 1. listopadu 2021
Datum odevzdání: 11. května 2022
Datum schválení: 29. října 2021

Abstrakt

Táto práca sa zaoberá problematikou Wi-Fi sietí a ich zabezpečením s dôrazom hlavne na chyby v jednotlivých zabezpečeniach, ktoré umožňujú odpočúvanie sieťovej komunikácie. V druhej časti je popísaná sonda vyvíjaná Výskumnou skupinou akcelerovaných sieťových technológií na FIT VUT. V poslednej časti je návrh vylepšenia sondy o možnosť získavať sieťovú komunikáciu z bezdrôtového rozhrania s popisom testovania aktuálne dostupných nástrojov a implementáciou rozšírenia sondy.

Abstract

The purpose of this work is to study Wi-Fi networks and their security and to create an extension for network probe, which is able to catch and analyze Wi-Fi traffic developed by The Accelerated Network Technologies (ANT) research group on FIT BUT. Study of software flexprobe components are described with proposal of wireless extension. Wi-Fi standards are described with their flaws and tools to crack Wi-Fi security with ability to intercept traffic on specific netowork. Implementation of wireless extension with testing is described in the last part of this thesis.

Kľúčové slová

Wi-Fi zabezpečenie, WEP, WPA, WPA2, WPA3, sieťová sonda, sieťová analýza, sieťové odpočúvanie, prelamovanie zabezpečenia, bezdrôtové siete

Keywords

Wi-Fi security, WEP, WPA, WPA2, WPA3, network probe, network monitoring, legal traffic interception, security vulnerabilities, wireless networks

Citácia

FINDRA, Michal. *Rozšíření odposlechové sondy o podporu Wi-Fi.* Brno, 2022. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Ing. Michal Orsák

Rozšíření odposlechové sondy o podporu Wi-Fi

Prehlásenie

Prehlasujem, že som túto bakalársku prácu vypracoval samostatne pod vedením pána Ing. Michala Orsáka. Ďalšie informácie mi poskytli členovia skupiny ANT FIT BUT. Uviedol som všetky literárne pramene, publikácie a ďalšie zdroje, z ktorých som čerpal.

.....
Michal Findra
10. mája 2022

Poďakovanie

Poďakovať chcem hlavne vedúcemu práce Ing. Michalovi Orsákovi za pomoc a cenné rady pri tvorení tejto práce.

Obsah

Kapitola 1

Úvod

Použitie Wi-Fi bezdrôtového pripojenia ku sieti je v dnešnej dobe prenosných zariadení ako sú mobily a tablety veľmi rozšírené v domácnostiach, aj na pracoviskách.

Tieto bezdrôtové siete poskytujú podobnú rýchlosť ako siete LAN a bezdrôtové spojenie ich tak užívateľovi robí atraktívnejšie ak je zaistené dostatočné pokrytie signálom. Rýchlosti pripojenia sa v dnešnej dobe v najnovšej verzii Wi-Fi 6 pohybuje pri rýchlosti 9.6Gb/s. Vzhľadom ku rýchlosti je používanie Wi-Fi pripojenia ku sieti komfortnejšou alternatívou nielen pre mobilné zariadenia.

Prenášané dáta sa pri používaní bezdrôtovej Wi-Fi siete šíria priestorom a môže ich takmer hocikto zachytiť, takže je dôležité ich dobre zabezpečiť, aby sa zaistila súkromná komunikácia medzi klientom a prístupovým bodom. Bezpečnostné štandardy zabezpečenia Wi-Fi sietí sa od roku 1997 inkrementálne zlepšujú a rozširujú. Aj napriek tomu sa v dnešnej dobe nájdu chyby a nedostatky od WEP zabezpečenia cez WPA až po najpokročilejšie WPA3 zabezpečenie, ktoré sú bližšie popísané v kapitole 2.

Práca sa zaoberá protokolmi, zabezpečením, spôsobmi odpočúvania a s tým spojenými možnosťami prelomenia zabezpečenia. Pri prelamovaní sú využívané známe nedostatky v týchto protokoloch a nástroje, pomocou ktorých je možné danú zraniteľnosť využiť. Následne oboznámenie sa s vyvíjanou sondou a implementácia rozširujúceho balíka na zachytávanie špecifickej komunikácie z bezdrôtového rozhrania.

Sonda FlexProbe je vyvíjaná Výskumnou skupinou akcelerovaných sieťových technológií ANT na FIT VUT. Cieľom projektu FlexProbe je vytvoriť flexibilnú sieťovou sondu, medzi ktorej cieľové aplikácie patrí hĺbková analýza sieťovej premávky a zákonné odpočúvania v sieti. Použitie legálnych odpočúvaní je špecifikované vysokou selektivitou. Predpokladá se, že žiadanú sieťovú premávku tvoria iba jednotky percent celkovej premávky. Aby bolo možné premávku filtrovať na rýchlosti linky obsahuje sonda akcelerátory implementované v FPGA. Po prefiltrácií na FPGA prebieha dofiltrácia v software časti a export odfiltrovaných dát na zvolené úložné zariadenie.

Kapitola 2

Zabezpečenie Wi-Fi sietí

V dnešné dobe mobilných zariadení a iných prenosných zariadení je potreba bezdrôtového internetu a zabezpečenia bezpečného prenosu dát neustále narastá aj preto, lebo cez zariadenie pripojené ku bezdrôtovej Wi-Fi sieti sa dajú ovládať bankové aplikácie alebo vykonávať iné úkony, ktoré narábajú s citlivými informáciami.

Zabezpečenie bezdrôtového prenosu dát v sieti poskytuje súbor štandardov definovaných Inštitútom pre elektrotechnické a elektronické inžinierstvo (IEEE) 802.11x [2] inak nazývaný aj Wi-Fi, ktorý poskytuje bezdrôtový prístup ku internetu pomocou rádiových vĺn. Výhodou je, že odpadá nutnosť pripojenia fyzickým káblom do siete a zanedbateľná zmena rýchlosti, ktorá je v dnešnej dobe pre bežného užívateľa nepostrehnuteľná. Porovnanie rýchlostí rôznych Wi-Fi verzií je v tabuľke 2.1.

Wi-Fi 3 (802.11g)	Wi-Fi 4 (802.11n)	Wi-Fi 5 (802.11ac)	Wi-Fi 6 (802.11ax)
54 Mb/s	600 Mb/s	3.5 Gb/s	9.6 Gb/s

Tabuľka 2.1: Porovnanie rýchlostí Wi-Fi verzií [5].

Podmienkou používania Wi-Fi pripojenia je byť v dosahu prístupového bodu a mať zariadenie, ktoré podporuje niektorý z bezpečnostných protokolov [20, 16] prístupového bodu.

V tejto kapitole je popísaná štruktúra bezdrôtových sietí a podrobnejšie sú popísané jednotlivé bezpečnostné štandardy a chyby ktoré obsahujú [25].

2.1 Naviazanie spojenia - asociácia

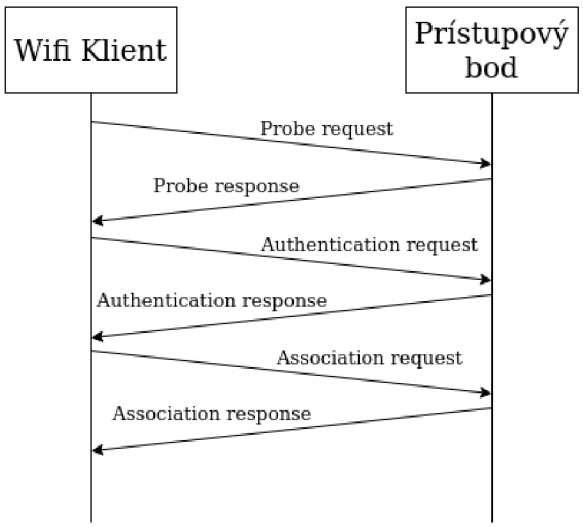
Klienti sa ku bezdrôtovej Wi-Fi sieti pripíjajú cez prístupový bod. Klienti v sieti nemusia byť priamo v dosahu, preto prebieha komunikácia nepriamo použitím prístupových bodov.

Každý prístupový bod predstavuje sieť, ktorá je charakterizovaná ako balíček služieb *Basic Service Set* (BSS) a identifikovateľná pomocou *Basic Service Set Identifier* (BSSID). V praxi je bežné, že MAC adresa prístupového bodu je zhodná s BSSID.

Každý prístupový bod je vrámci WLAN súčasťou *Extended Service Set* (ESS), ktorý je identifikovateľný pomocou *Extended Service Set Identifier* (ESSID). Obvykle je to textový reťazec, ktorý je rozpoznateľný ako názov Wi-Fi siete [2].

Procesu pripojenia zariadenia do siete predchádza proces asociácie zariadenia s prístupovým bodom. Tento proces prebieha v nasledujúcich krokoch a graficky je zobrazený na obrázku 2.1:

1. Prístupový bod vysiela neustále *Beacon frames* - rámce, ktoré obsahujú informácie o sieti. Slúžia ako informácia pre klienta, že daný prístupový bod je v dosahu.
2. Klient zašle *Probe request* - žiadosť na zistenie dostupnosti siete.
3. Reakcia prístupových bodov *Probe response* v dosahu. Párová odpoveď ku každému *Probe request*.
4. Výmena autentizačných rámcov inicializovaná klientom.
5. Klient zasiela asociačnú požiadavku.
6. V prípade prijatia asociačnej požiadavky začína prenos dát.
7. V prípade neúspechu je zaslaný deautentizačný rámec, ktorý vynúti odpojenie klienta od siete.



Obr. 2.1: Postup pri asociovaní zariadeniu ku prístupovému bodu.

Postup autentizácie, ktorý prebieha po úspešnej asociácií je popísaný podrobnejšie pri jednotlivých štandardoch.

2.2 Zabezpečenie WEP

Wired Equivalent Privacy (WEP) je prvý bezpečnostný protokol na zabezpečenie bezdrôtového prenosu. Definovaný je v štandarde IEEE 802.11 [10, 18]. Tento štandard bol pokladaný za hlavný bezpečnostný protokol od roku 1997 do roku 2003, odkedy bol nahradený štandardom WPA, ktorý opravoval chyby v jeho implantácii. WEP je v dnešnej dobe už takmer nepoužívaný štandard a využíva ho iba málo zariadení. Stále ho, ale pre spätnú kompatibilitu podporuje aj väčšina moderných zariadení. V súčasnosti je WEP zabezpečenie možné prelomiť v rade minút až hodín aj na bežnom počítači.

WEP používa zdieľaný kľúč s dĺžkou 40–140 bitov. Proces WEP protokolu vyzerá nasledovne:

1. Je vypočítaná CRC (*Cyclic Redundancy Code*) správa a pridaná ku originálnej správe.

2. Správa je zašifrovaná RC4 algoritmom:
    - Vygenerovanie inicializačného vektoru (IV) - pseudo náhodná sekvencia troch bytov rozširujúca kľúč.
    - XOR funkcia medzi dátami a rozšíreným kľúčom - výsledok šifrovania.
3. Správa a IV sú zaslané prijímateľovi, ktorý opačným postupom získa zasielané dáta.

WEP autentizácia medzi klientom a požadovaným prístupovým bodom môže prebiehať jedným z dvoch následujúcich spôsobov:

- **Open System Authentication**
  Klient neodosiela žiadne údaje prístupovému bodu, takže sa pripojí ku prístupovému bodu bez autentizácie.
- **Shared Key Authentication**
  Autentizácia prebieha v 4 fázach:
    1. Klient pošle prístupovému bodu žiadosť o autentizáciu.
    2. Prístupový bod odošle klientovi naspäť výzvu.
    3. Klient príjme výzvu a zašifruje ju pomocou svojho WEP kľúča a zašle ju späť v nasledujúcej autentizačnej požiadavke.
    4. Prístupový bod pomocou svojho kľúča prijatú odpoveď dešifruje, ak sa zhoduje dešifrovaná správa so zaslanou výzvou, odošle pozitívnu odpoveď.

  Zachytením tejto autentizácie dokáže útočník zistiť použitý kľúč a dešifrovať komunikáciu.

2.2.1 Útoky na WEP zabezpečenie

Tým, že WEP zabezpečenie je najstaršie a je v dnešnej dobe ľahko prelomiteľné existuje mnoho útokov, ktoré ho vedia prelomiť.

Key Recovery útoky - FMS

Fluhrer-Mantin-Shamir útok [12] (FMS) využíva chybu v inicializačnej fáze RC4 šifrovania. Pri určitých kľúčoch je šanca, že niektoré časti kľúča budú pri šifrovaní použité pravdepodobnejšie. Následne útočník odpočúva a zachytáva komunikáciu, kde si ukladá niektoré pakety, podľa štruktúry použitého kľúča.

Čím viac paketov útočník zachytí, tým je väčšia pravdepodobnosť, že sa mu podarí zistiť kľúč. V najhoršom možnom prípade potrebuje útočník okolo jedného milióna paketov.

Nástroje, ktoré využívajú túto chybu:

- WEPCRACK[1]
- AirSnort[2]

[1] http://wepcrack.sourceforge.net"
[2] http://airsnort.shmoo.com

Related Key útoky

Šifrovanie vo WPA prebieha pomocou inicializačného vektora a kľúča. Keďže je RC4 prúdová šifra, tak rovnaký kľúč nesmie byť použitý viackrát. Inicializačný vektor je využívaný, aby sa zabránilo opakovaniu kľúča. Ak je inicializačný vektor krátky, tak je šanca, že sa po určitom čase zopakuje a túto situáciu využíva Related Key Attack [6].

2.3 Zabezpečenie WPA

Wi-Fi Protected Access (WPA) je definovaný v štandarde 802.11i [1]. Tento bezpečnostný štandard vznikol po prelomení WEP zabezpečenia a začal sa oficiálne využívať od roku 1999 [17]. Pre spätnú kompatibilitu s WEP je využívané aj šifrovanie RC4. Narozdiel od WEP, WPA používa nový protokol TKIP a tiež využíva lepšie šifrovanie - 128-bitový šifrovací kľúč a 48-bitový inicializačný vektor.

Vylepšenia sa dočkal aj šifrovací algoritmus CRC-32, lebo sa ukázalo ako nedostatočné, keď sa pomerne výpočtovo lacno dala pozmeniť celá správa a s ňou aj kontrolný súčet. Táto zmena skomplikovala odpočúvanie, lebo kľúč je dynamický dohodnutý a správy výberu kľúča musia byť všetky zachytené, aby sa dala komunikácia dešifrovať treťou stranou.

Temporal Key Integrity Protocol [1] je nový protokol, ktorý vylepšuje bezpečnosť pri šifrovaní vo WEP. Šifra RC4 sa využíva inak ako vo WEP. Vo WPA sa pri šifrovaní využíva zdieľaný kľúč na to, aby sa s ním vygenerovali ďalšie kľúče oproti WEP, kde bol zdieľaný kľúč priamo použitý pri šifrovaní.

Oproti WEP prináša aj nasledujúce výhody:

- silnejšie a spoľahlivejšie generovanie kľúčov,
- priebežné obnovovanie jednotlivých kľúčov,
- kryptografická kontrola integrity – MIC (*Message Integrity Check*) [8],
- novú metódu správy a generovania inicializačných vektorov,
- *tag* funkcia.

TAG funkcia generuje *tag* na základe autentizačného kľúča a zasielaných dát. Vygenerovaný *tag* je zasielaný spolu so správou. TKIP zároveň vykonáva aj kontrolu zasielanej *tag* časti správy. Ak prídu v priebehu jednej sekundy viac ako dve správy s nesprávnym *tag*-om, tak sa musí vykonať reinicializácia autentizácie.

Chyby v zabezpečení WPA sú podobné ako pri zabezpečení WPA2, takže sú zahrnuté v sekcii 2.4.1.

2.4 Zabezpečenie WPA2

WPA2[1] štandard nahrádza WPA štandard. Je využívaný od roku 2004 a ku koncu roku 2020 bol najviac[3] používaným Wi-Fi zabezpečovacím štandardom v Česku s 64% z 3.5 milióna zariadení.

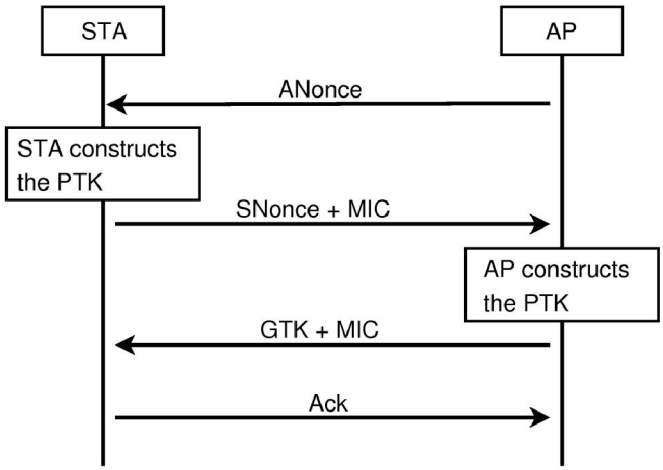
[3] https://www.wifileaks.cz/statistika.php

WPA2 štandard musí spĺňať použitie zabezpečovacieho protokolu CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*), ktorý je založený na štandarde pokročilého šifrovacieho algoritmu AES a poskytuje dôvernosť dát, autentizáciu, integritu a ochranu odpovedí. Zariadenia podporujúce WPA2 môžu podporovať aj TKIP z WPA, čo pre spätnú kompatibilitu väčšina zariadení splňuje.

Používa nový šifrovací algoritmus AES [7], ktorý má vyššiu réžiu, takže sa nedá použiť na starších sieťových kartách. Autentizácia prebieha cez štvorfázový *handshake*, ktorý je zároveň aj častým miestom útokov a jeho schéma je zobrazená na obrázku 2.2. Od roku 2006 musí každé nové Wi-Fi certifikované zariadenie podporovať WPA2 zabezpečenie.

Pripojenie klienta ku prístupovému bodu prebieha následovne:

1. Prístupový bod zašle *ANonce* správu klientovi, ktorý vytvorí PTK *(Pairwise Transient Key)*.
2. Klient zašle *SNonce* správu prístupovému bodu spolu s MIC, ktorý obsahuje autentizáciu.
3. Prístupový bod vytvorí PTK a zašle GTK *(Group Temporal Key)*, sekvenčné číslo a MIC späť klientovi.
4. Klient zašle potvrdenie prístupovému bodu.



Obr. 2.2: Schéma štvorfázového *handshake* [26].

2.4.1 Chyby a metódy prelamovania zabezpečenia WPA2

WPA2 je v dobe písania tejto práce najrozšírenejší štandard a postupy pri priebehu autentizácie a šifrovania sú dobre známe, to vytvorilo možnosť na množstvo útokov na toto zabezpečenie [4, 19].

Zraniteľnosť slovníkovými útokmi

Oproti WEP zabezpečeniu, ktoré je možné v dnešnej dobe prelomiť v rozsahu niekoľkých minút, sú zabezpečenia WPA a WPA2 ťažko prekonateľné a často aj nemožné [35]. Útok prebieha na zabezpečovacie heslo pomocou slovníkov metódou hrubej sily. Vhodne zvolená

alebo zostavená predikátová databáza môže výrazne urýchliť proces prelamovania hesla, ale rýchlosť nie je aj tak možné vopred vyhodnotiť.

Útočník môže využiť priebeh autentizácie klienta ku prístupovému bodu počas štvorfázového *handshake*, a vykonávať útok na zabezpečovacie heslo metódou hrubej sily off-line mimo dosahu prístupového bodu, na vopred zachytenej sieťovej komunikácií. Útočník môže zasielať deautentizačné rámce, ktoré odpoja pripojeného klienta, ktorého následné znovu pripojenie vyvolá štvorfázový *handshake*, ktorého pakety je možné použiť na prelamovanie.

Vyplývajúca nevýhoda je, že ku prístupovému bodu musí byť pripojený aspoň jeden klient. Útočník po útoku získa zašifrované heslo, na ktoré následne vykoná slovníkový útok pomocou dostupných slovníkov alebo menej efektívnou metódou hrubej sily. Zašifrované heslo je možné získať aj pri niektorých prístupových bodoch požiadaním prístupového bodu o PMKID (Pairwise Master Key Identifier), ktorý obsahuje predzdieľaný kľúč[28].

Tento typ útoku ponúka množstvo nástrojov a medzi najznámejšie patria AirCrack 4.3 alebo Hashcat[4] a na generovanie slovníkov sa používa napríklad nástroj John the Ripper[5].

Pfishing

Pfishing je sociálne zameraný útok, pri ktorom sa útočník pokúša získať heslo priamo od užívateľa. Klient môže kliknúť na podstrčený odkaz, kde bude vyzvaný, aby zadal opätovne prihlasovacie údaje ku bezdrôtovej sieti. Tento odkaz môže byť súčasťou emailov alebo odkazov na sociálnych sieťach. Množstvo týchto emailov a odkazov je odfiltrovaných použitím vstavaných antivírových programov.

Tento typ útoku je ponúkaný v rade nástrojov na penetračné testovanie ako je napríklad Wi-Fi pineapple[6].

Man In The Middle útok

Pri tomto type útoku útočník odpočúva komunikáciu v sieti tak, že sa stáva aktívnym členom pri komunikácií klienta so serverom. Všetká komunikácia teda prechádza od klienta ku prístupovému bodu cez útočníka, ktorý môže jednotlivé správy zachytiť, čítať a prípadne modifikovať podľa vlastnej potreby. Tento typ útoku je taktiež implementovaný vo vyššie spomenutom Wi-Fi pineapple.

2.5 Zabezpečenie WPA3

WPA3 zabezpečenie [2] bolo oficiálne predstavené[7] v januári 2018 a v júni 2018 nahradilo starší štandard WPA2. WPA3-Personal používa 128-bitové zabezpečenie a WPA3-Enterprise 192-bitové zabezpečenie. WPA3 nahrádza výmenu kľúčov Pre-shard key (PSK) používanú vo WPA2 bezpečnejšou metódou Simultaneous Authentication of Equals (SAE). Hlavnými výhodami SEA oproti PSK je, že ak sa podarí útočníkovi prelomiť zdieľaný kľúč, tak nebude vedieť spätne dešifrovať zachytenú komunikáciu (Forward secrecy [21]) a vďaka SEA nie je možné zachytiť štvorfázový *handshake*.

WPA3 tak isto podporuje aj PMF (Protected Management Frames), takže znemožňuje útočníkovi deautentizovať klienta zo siete. SEA funguje na princípe vylepšenej Dif-

[4] https://hashcat.net/hashcat/

[5] https://www.openwall.com/john/

[6] https://shop.hak5.org/products/wifi-pineapple

[7] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

fie–Hellmanovej výmeny kľúčov, ktorá je tiež cieľom útokov. SAE sa inak nazýva aj Dragonfly handshake.

Prehľad a porovnanie šifrovania, zabezpečenia integrity dát a autentizácie zobrazuje nasledujúca tabuľka:

Názov štandardu	Autentizácia	Šifrovanie	Intgrita
WEP 2.2	Zdieľané kľúče	RC4 (40b IV, 104b kľúč)	CRC
WPA Personal 2.3	PSK	RC4 + TKIP (128b kľúč)	MIC
WPA Enterprise 2.3	EAP	RC4 + TKIP (128b kľúč)	MIC
WPA2 Personal 2.4	PSK	AES + CCMP (128b kľúč)	CBC-MAC
WPA2 Enterprise 2.4	EAP	AES + CCMP (128b kľúč)	CBC-MAC
WPA3 Personal 2.5	SAE	AES + CCMP (128b kľúč)	CBC-MAC
WPA3 Enterprise 2.5	EAP	AES + GCMP (128b kľúč)	GMAC-256

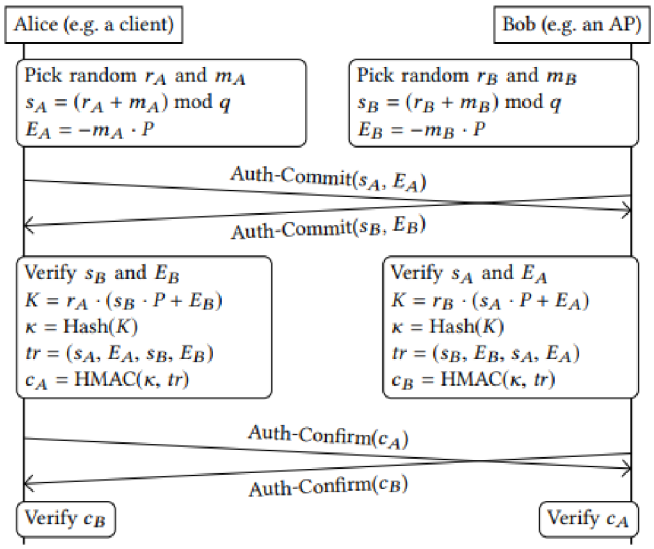
Tabuľka 2.2: Porovnanie bezpečnostných štandardov.

2.5.1 WPA3 Diffie–Hellman výmena kľúčov

WPA3 používa Diffie-Hellman [11, 29] výmenu kľúčov. V štandardnej Diffie-Hellman výmene kľúčov je verejne známe číslo g (generátor), p (zahashované heslo). Obe strany si vygenerujú svoje náhodné číslo (a, b) a vykonajú následovné umocnenie g^a, g^b. Táto časť sa nazýva *Commit phase*.

Umocnené číslo potom odošlú opačnej strane, ktorá ho zase umocní (g^{a^b}, g^{b^a}). Následne obe strany urobia modulo p vypočítanej hodnoty a porovnajú si ich. Obe strany dostanú rovnaký výsledok ak mali pôvodne rovnaké heslo. Táto časť sa nazýva *Confirm phase*.

Na obrázku 2.3 je znázornená výmena kľúčov vo WPA3. Obe strany môžu inicializovať spojenie, preto sú šípky obojsmerne.



Obr. 2.3: Diffie-Hellman výmena kľúčov vo WPA3 [32].

Prvok p môže byť vytvorený pomocou jednej z dvoch kryptografických skupín:

– MODP skupiny (MODulo Prime)

– Eliptické krivky - ponúkajú vyššiu bezpečnosť oproti MODP skupinám[8]

2.5.2 Chyby a metódy prelamovania zabezpečenia WPA3

Práca [30] predstavená na konferencii USENIX Security 2021 obsahuje prehľad všetkých novo zistených chýb v zabezpečovacích štandardoch z výskumu FragAttacks[9] a z nich vyplývajúce útoky na Wi-Fi zabezpečenie.

Autor skriptov Mathy Vanhoef zverejnil[10] sadu skriptov, ktoré testujú zistené chyby. Dostupný je aj *Live Image*[11] s používanými upravenými drivermi, na ktorých dané útoky testuje. Uvedené sú aj podporované sieťové karty.

Nástroj obsahuje viac ako 45 testov, ktoré zisťujú, či je nejaká chyba dostupná a je využiteľná na niektorý zo zistených útokov.

Tým, že je WPA3 najnovší štandard, tak časový rozdiel medzi objavením chyby a opravením je relatívne krátky, aby bolo výhodné implementovať útoky na WPA3 využívajúce danú chybu do vyvíjanej sondy FlexProbe.

DDoS útok

Autentifikácia vo WPA3 je výpočtovo náročný proces a to je možné zneužiť na vykonanie Distributed Denial of Service (DDoS) útoku na prístupový bod. Pri bežne používaných krivkách musí stále prebehnúť 40 iterácií, v ktorých sa vykonávajú výpočtovo náročne operácie. Vo výskume v roku 2020 [32] na profesionálnom prístupovom bode stačilo, aby o pripojenie žiadalo osem adries za sekundu a došlo k preťaženiu CPU, takže prístupový bod nemohol spracovávať ďalšie požiadavky. Ak sa použila menšia krivka, tak CPU prestalo prijímať ďalšie požiadavky pri 70 adresách za sekundu.

Downgrade útok

Pri *downgrade* útokoch sa zariadenie, ktoré nepodporuje WPA3 zabezpečenie pokúša pripojiť ku prístupovému bodu, ktorý je zabezpečený pomocou WPA3 zabezpečenia. Niektoré prístupové body vedia znížiť zabezpečenie z WPA3 na nižšie zabezpečenie (napr. WPA2), takže sa vynúti pripojenie s nižším zabezpečením ako WPA3 a autentizujú klienta s rovnakým heslom, ktoré potom útočník vie zistiť.

Packet injection

Zasielaním upravených *plaintext frame*, ktoré sa podobajú na *handshake frame*, môžu byť zachytené a použité prístupovým bodom. Vložené pakety môžu spôsobiť DDoS útok alebo Man in the Middle útok.

[8] https://www.watchguard.com/help/docs/help-center/en-US/Content/en-US/Fireware/bovpn/manual/diffie_hellman_c.html

[9] https://www.pcmag.com/news/most-wi-fi-devices-released-since-1997-are-vulnerable-to-fragattacks

[10] https://github.com/vanhoefm/fragattacks

[11] https://github.com/vanhoefm/fragattacks#id-live-image

Aggregation útok

Tento útok sa týka všetkých zabezpečení cez WPA2, tak aj WPA3 zabezpečenia. Pri úspešnom útoku je možné vložiť vlastné dáta za prenášaný paket a tým napríklad vynútiť Man in the Middle útok.

Pri zasielaní paketov je v hlavičke uložená informácia o tom, či je paket zaslaný samostatne (*aggregated=false*) alebo je viac paketov zreťazených za sebou s jednou hlavičkou (*aggregated=true*). *Aggregated flag* nie je šifrovaný, takže môže byť útočníkom zmenený, čo môže mať za následok vloženie paketov od útočníka za pôvodne zaslané pakety.

Útočník musí byť počas priebehu útoku v dosahu zariadenia a prístupového bodu. Klient sa musí pripojiť na útočníkov server, čo sa dá dosiahnuť napríklad kliknutím na odkaz alebo obrázok. Následne server zašle požiadavku a útočník podsunie svoje pakety za pôvodné pakety. Výsledkom je napríklad, že sa klient pripojí na podsunutý útočníkov DNS server.

Pri zabezpečení niektorých routerov nie je potrebné, aby klient klikol na odkaz a pripojil sa k útočníkovmu serveru, ale stačí zasielať špeciálne upravené EAPOL rámce.

Fragmentation útok

Pri úspešnom útoku, je útočník schopný pripojiť vlastné dáta ku pôvodnej prenášanej komunikácií. Ak je pri Wi-Fi prenose zasielaný rámec väčší než MTU, tak sa rozdelí na menej menších fragmentov, z ktorých každý vie byť skontrolovaný samostatne a prípadne zaslaný znovu pri strate. V hlavičke sa nachádzajú údaje o fragmentoch, aby bolo možné zložiť fragmenty nazad do pôvodného rámcu.

Pri zasielaní fragmentov po odpojení klienta ostanú fragmenty uložené v prístupovom bode. Pomocou *MAC spoofing* sa dá pripojiť na server a zaslať škodlivé pakety, pomocou ktorých po následnom pripojení klienta do siete je možne podsúvať ďalšie pakety.

Ku fragmentácii dochádza zriedka (viac používané vo Wi-Fi 6 [13]), takže tento typ útoku nie je veľmi prakticky využiteľný. Táto zraniteľnosť je tu už od doby WEP zabezpečenia, ktoré bolo predstavené v roku 1997 a stále nie je opravená.

2.6 Detekcia útokov

Na zrýchlenie útokov, ktoré vyžadujú opätovnú autentizáciu, zasiela útočník deautentizačné rámce, ktoré zapríčinia odpojenie klienta od siete. Pri jeho opätovnom pripojení môže útočník zachytiť a zneužiť štvorfázový *handshake*.

Zasielané deautentizačné rámce je možné detekovať použitím napríklad voľne dostupným programom Wireless IDS[12] (Intrusion Detection System). Tento typ programu zachytáva okolitú premávku a vyhodnocuje riziká.

[12] https://github.com/SYWorks/wireless-ids

Kapitola 3

Sonda FlexProbe 10g

Cieľom projektu FlexProbe [34] je umožniť selektívne zachytávanie aplikačných dát. K tomu je potrebné identifikovať užívateľa na základe aplikačného identifikátoru (NID), ako je napr. e-mailová adresa, a umožniť zachytávanie dát konkrétneho toku TCP alebo UDP použitého v súvislosti so zachytávaným identifikátorom. Zachytené dáta sú exportované do zberného miesta, tzv. *Law Enforcement Monitoring Facility* (LEMF).

Knižnica software modulov na filtráciu sieťovej premávky na úrovni aplikačných protokolov musí dáta spracovávať na rýchlosti linky (10Gb/s). Vzhľadom na nemožnosť dôkladného parsovania protokolov rýchlosťou linky, sonda detekuje žiadanú sieťovú komunikáciu heuristikami, ktoré sú tvorené pravidlami obsahujúce regulárnych výrazy. Regulárnymi výrazmi sú vyhľadávané charakteristické rysy jednotlivých protokolov.

Dáta zachytené zo siete sú predspracované v rámci hardware, ktorý detekuje výskyt NID a protokolov v jednotlivých sieťových tokoch. Tak identifikuje protokoly, pri ktorých je treba ukladať dáta skôr než sa takýto identifikátor objaví, aby bolo odpočúvanie úplne.

Pomocou hardware a software codesignu je dosiahnuté spracovanie dát na rýchlosti linky za predpokladu, že sa k detailnejšiemu spracovaniu dostane len časť dát.

Na obrázku 3.3 je schéma 10g sondy s vyznačenou PaSt časťou.

3.1 Architektúra

Architektúra sondy sa skladá z viacerých samostatne implementovaných častí. Na začiatku vstupujú pakety cez zvolený typ sieťového rozhrania do Sondy. Pakety prechádzajú do akcelerátoru Filtra cez časti sondy *Protocol Identifier* (PI), ktorá detekuje jednotlivé protokoly a cez *Pattern match* (PM), ktorá vyhľadáva užívateľom zadané regulárne výrazy.

Filtračná jednotka funguje v režime "white list"(bez pravidla nič neprepúšťa). Filtrácia prebieha vo časti sondy Filter [34] sondy sa skladá z častí:

- Filter - Filtrovacie jadro samotnej filtračnej funkcionality, obaľuje obe použité filtrovacie tabuľky.
  - L3 Table - filtrovanie podľa maskovanej IPv4/IPv6 adresy, obojsmerné vyhodnotenie: porovnáva sa postupne zdrojová aj cieľová IP adresa paketu (2 výsledky na paket).
  - L4 Table - filtrovanie podľa presnej zhody nad klasickou IPv4 päticou, obojsmerné vyhodnotenie dvojice (IP,port). Filter podporuje možnosť automatického

pridania pravidla na základe výstupu Patern Match alebo Protocol Identifier jednotky.

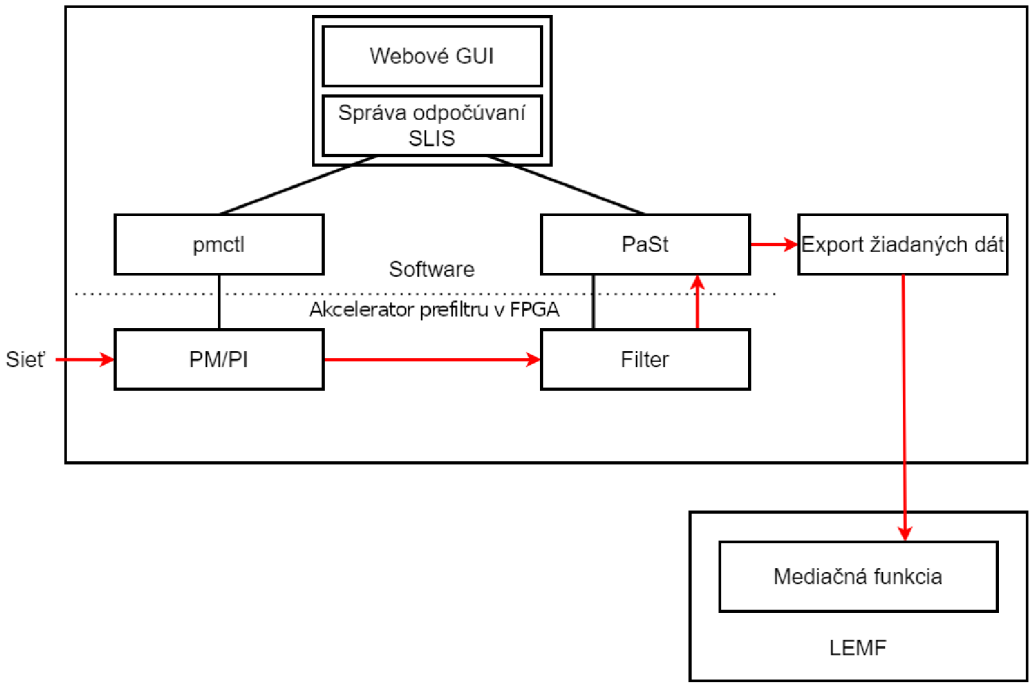
Vo filtri sa môžu nachádzať tri základné typy pravidiel:

- L3 pravidlá - filtrovanie na základe IP adries, celé pätice
- L4 dočasné pravidla - filtrovanie konkrétneho toku (podľa IP adries, portov a čísla protokolov), pravidlo je aktívne len dokým nevyprší jeho TTL, podle informácií z PI môže byť pravidlo do filtra pre daný tok pridané, prípadne se môže resetovať TTL
- L4 trvalé pravidlá - filtrovanie konkrétneho toku (podle IP adries, portov a čísla protokolov), pridané pravidlo je aktívne dokým nie je vymazané, pravidlo je pridané na základe jednotky PM (ak bol nájdený hľadaný identifikátor)

Pri efektívnej spolupráci hardware a software, kde hardware vykonáva efektívnu prefiltráciu tak, aby boli splnené požiadavky na spracovanie vstupného príjmu dát na rýchlosti 2 Gb/s a zároveň pamäťovo náročná analýza aplikačných protokolov prebiehala predovšetkým v software je potrebné zaistiť splnenie následujúcich požiadaviek:

- Hardware musí byť schopný identifikovať potenciálne žiadanú sieťovú premávku a poskytnúť software všetky dáta toku od detekcie momentu, že ide o potenciálne žiadanú sieťovú premávku.
- Software musí byť schopný rozoznať žiadanú sieťovú premávku detailnejšou analýzou dát. Cieľom je finálne určenie premávky určenej na odpočúvanie Tá je poskytnutá výstupným rozhraním orgánom činným v trestnom konaní, v štandardoch ETSI označované ako LEMF [3].
- Ak software identifikuje, že časť sieťovej premávky bola pomocou hardware vyhodnotená ako vhodná na odpočúvanie, ale detailnejšia analýza dát ukázala, že nejde o žiadanú sieťovú premávku (tzv. *false positive*), software musí mať možnosť získavanie dát tohto toku v hardware filtri zrušiť.

Obrázok 3.1 ukazuje architektúru komunikácie medzi hardware a software. Čiernymi čiarami je označená konfigurácia a červenými orientovanými šípkami odovzdávanie dát získavanej sieťovej premávky.



Obr. 3.1: Všeobecná schéma architektúry komunikácie medzi software a hardware [34].

3.2 Konfigurácia

Konfigurácia odpočúvania prebieha cez GUI sondy. Odpočúvania sú aktivované a deaktivované na základe časových intervalov platnosti odpočúvania. Je potrebné konfigurovať nasledujúce dve časti:

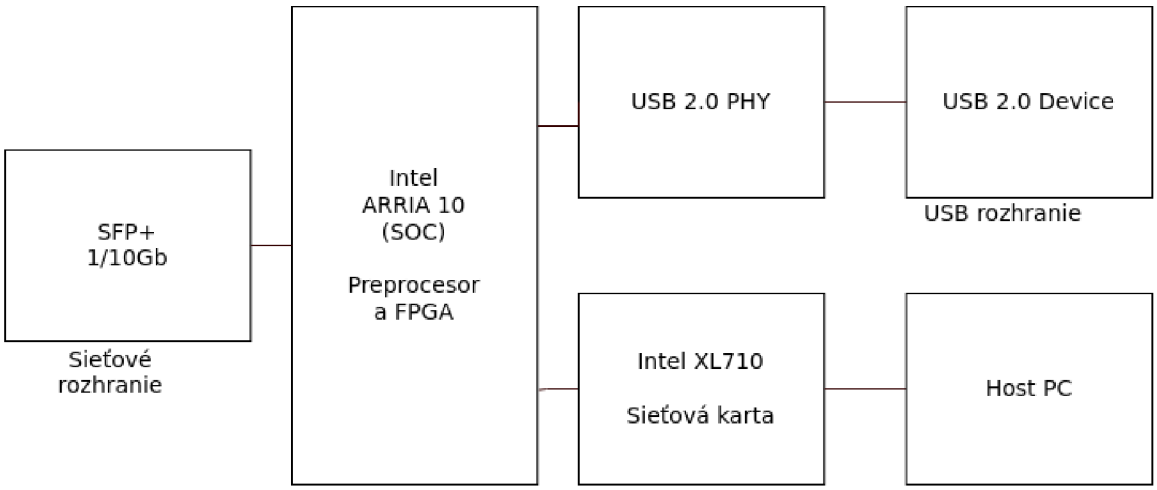
- Jednotku, ktorá zaisťuje *pattern match* (PM) identifikátorov určených na odpočúvanie. Táto jednotka je konfigurovaná nástrojom *pmctl*.
- Software na spracovanie aplikačných protokolov - *Packet Stack* (PaSt). Tento software vykonáva konfiguráciu filtra a analýzu aplikačných protokolov a vykonáva konečné rozhodnutie o exporte zachytených dát do LEMF.

3.3 Hardware

Jednotlivé software balíky, ktoré ovládajú príslušne hardware komponenty [34]:

Názov aplikácie	**Účel hardware**
dispatcherctl	preposielanie paketov z hardware do software
eeprom_write	skript na konfiguráciu eeprom na sonde
ledctl	signalizačné LED diódy
piclt	detekcia aplikačných protokolov v prichádzajúcich paketoch
pmctl	detekcia regulárnych výrazov v prichádzajúcich paketoch
sp1fltctl	filtrovanie prichádzajúcich paketov na báze pätíc a trojíc
statsctl	jednoduché počítanie štatistík premávky vo WLAN
tsuctl	časové značky pre prichádzajúce pakety

Na obrázku 3.2 je zobrazená zjednodušená hardware schéma pôvodnej sondy. Kompletný technický návrh schémy je dostupný tu[1].



Obr. 3.2: Zjednodušená hardware schéma FlexProbe sondy [34].

Ku každému paketu prenášanému z hardware do software sú pridané ku vlastnému obsahu paketu aj ďalšie meta informácie:

- časová značka prijatia paketu,
- informáciu o tom, že paket spôsobil pridanie pravidla do hardware filtru,
- informáciu o preplnení hardware filtra,
- informáciu o zmazaní pravidla z filtra, ktoré bolo pridané na základe detekcie potenciálneho začiatku odpočúvania a ktorému vypršalo TTL,
- informáciu o tom, či sa v pakete našiel niektorý z identifikátorov určených na odpočúvanie,
- informáciu o tom, či sa v pakete našiel niektorý z identifikátorov označujúcich potenciálny začiatok odpočúvania,
- zoznam aplikačných protokolov, ktoré by sa mali novým paketom zaoberať.

3.4 Software

Software sondy FlexProbe sa skladá z viacerých balíkov, názov danej aplikácie a jej príslušná zodpovednosť je popísaná v tabuľke č. 3.1.

Software riadením odpočúvaných tokov sa zaoberá program konkrétne *Packet Stack* (PaSt).

[1] https://ant-dev.fit.vutbr.cz/redmine/attachments/download/2538/cn_fit_flexprobe_a1_sch_a5_210505.pdf

Názov aplikácie	Zodpovednosť
slis	Správa aktívnych odpočúvaní
past	L7 analýza paketov
sprobe_launcher	Management jednotlivých procesov na platforme a webové GUI
sprobe_dumper	Software na ukladanie žiadanej premávky v mediačnej funkcií
lib1spflt	Nástroje a knižnice na ovládanie filtrov v hardware

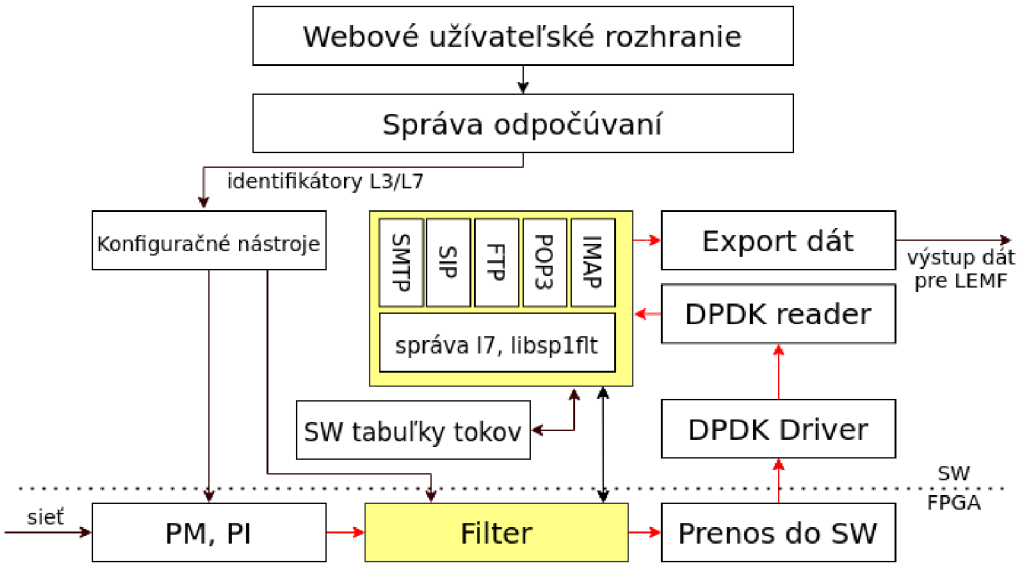
Tabuľka 3.1: Funkcionalita jednotlivých častí software FlexProbe.

3.4.1 L7 analyzátor Packet Stack (PaSt)

Packet Stack (PaSt) je software, ktorý spravuje informácie o tokoch detekovaných hardware časťou, vykonáva dofiltrovanie, buffering dát a exportuje dáta do LEMF. Software PaSt vykonáva:

- Spracováva pakety získané hardware na detailnejšie preskúmanie.
- Spravuje tabuľku tokov, ktorá je uložená v hardware filtri (zmaže zachytávanie tokov, ktoré nie sú určené na export a pridáva toky nájdené spracovaním aplikačného protokolu súvisiaceho s odpočúvaním, napr. v prípade protokolu SIP a FTP).
- Analyzuje obsah spracovávaných paketov a na ich základe pridáva a odoberá záznamy z tabuľky tokov a taktiež z hardware filtra. Zároveň určuje, ktoré pakety sú potrebné na export do LEMF.
- Ukladá si pakety od začiatku potenciálneho začiatku odpočúvania až po dobu, keď je určené, či je daný paket predmetom odpočúvania alebo nie.

Na obrázku 3.3 je žltou vyznačená časť PaSt vrámci sondy.



Obr. 3.3: Zahrnutie PaSt vrámci 10g sondy [34].

PaSt je implementovaná v jazyku C++. Pre PaSt existuje emulátor Sprobe(FlexProbe) emulátor (Spem), unittesty a sada integračných testov.

3.4.2 Beh programu PaSt

Inicializácia

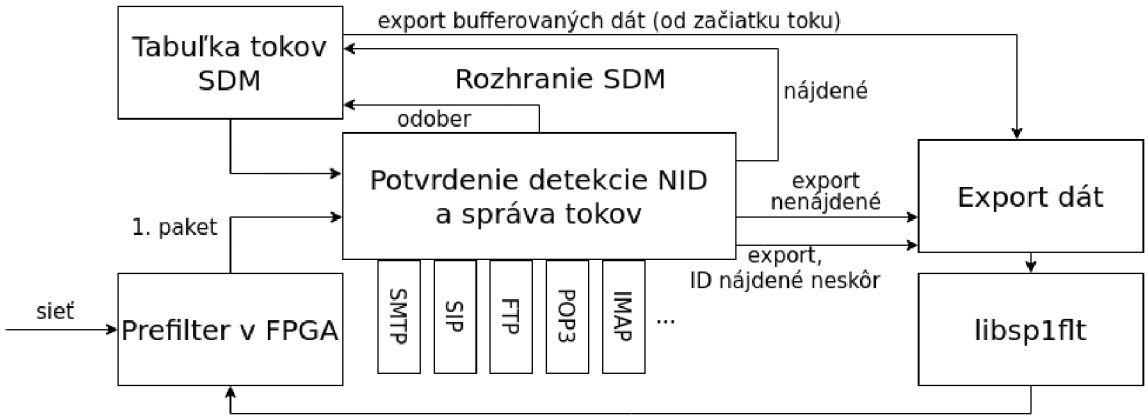
Po štarte programu PaSt načíta hľadané NID-y zo súborov zadaných v parametroch. Každý druh NID je uložený v špecifickom súbore.

Ak je špecifikovaný LEMF, spojí sa PaSt s LEMF pomocou TCP. PaSt tiež inicializuje parsery jednotlivým protokolom, pre ktoré sú nakonfigurované NID-y. Zmenu konfigurácie je možné urobiť zmenou NID v zadaných súboroch a zaslaním signálu SIGUSR1.

Spracovanie paketov

Hlavný cyklus programu zabezpečuje hlavný cyklus PaSt, toto spracovanie paketov v PaSt časti zobrazuje obrázok 3.4. V každej iterácií sa:

1. načíta nový paket zo vstupu,
2. vyhodnotí sa maska parsera, ktorý má o daný paket záujem uložená vo Flow Table (FT) (pre nové toky nulová) a *PATTERN ID* zo software,
3. vykoná sa spracovanie paketov aplikačnými parsermi,
4. parser spolu s FT na úrovni aplikačných protokolov vyhodnotí, čo sa má s daným paketom stať (priamy export, uloženie do FT, export všetkých uložených rámcov, uvoľnenie rámcov uložených v FT apod.),
5. v prípade paketov získaných pomocou PI bez aktuálnej detekcie NID sa pakety ukladajú do FT, dokiaľ nedôjde ku detekcii NIDu pomocou PM alebo signalizácii hardware o odstráneniu pravidla.



Obr. 3.4: Grafické zobrazenie procesu spracovania paketov v PaSt [34].

Správa filtrov

V prípade, že prijatý paket spôsobil pridanie pravidla do filtra, vytvorí PaSt nový záznam v tabuľke tokov. V prípade, že vypršalo dočasné pravidlo detekujúce potenciálny začiatok odpočúvania, uvoľňuje PaSt pamäť obsadenú týmto tokom.

Tabuľky 3.2 a 3.3 zobrazujú jednotlivé pravidlá pre konkrétny spôsob odobratia filtra:

Typ	**Kto pridáva**	**Kedy odobrané**	**Dĺžka aktivity pravidla**
Žiadaná sieťová premávka	PM, PaSt (napr. RTP)	TCP FIN, či rozhodnutie parseru v PaSti	Skôr dlhodobé, krátkodobé *false positives*
Pravidlo zachytávania odpočúvania (PZO)	PI	Maximálny počet paketov, potenciálna transformácia na žiadanú sieťovú premávku	Krátkodobé; môžu zostať aktívne pre toky kratšie než limit
Špecifikácia dátového kanálu FTP	PI	Po prvom pakete z hardware, zostávajú v software	Po prvom pakete z hardware, zostávajú v software

Tabuľka 3.2: Pravidlá pre konkrétny spôsob odobratia filtra (1/2) [34].

Typ	**Priorita spracovania (irelevantná)**	**Preventívne mazanie**	**Kritické mazanie**
Žiadaná sieťová premávka	Kritická	2 hodiny	30 minút a polenie intervalu až po hodnotu 1 minúta
PZO	Stredná, dlhodobo nízka	10 minút	1 minúta
Špecifikácia dátového kanálu FTP	Nízka, predpokladá se zväčša zahodenie	-	Vlastný systém

Tabuľka 3.3: Pravidlá pre konkrétny spôsob odobratia filtra (2/2) [34].

Či došlo k založeniu nového toku alebo bol prijatý paket toku, ktorý bol už videný, PaSt si uloží čas prijatia posledného paketu k toku prislúchajúcemu prijatému paketu.

PaSt odoberá odpočúvania z hardware filtru, ak nastane niektorá z nasledujúcich skutočností:

- Všetky parsery aplikačných dát označia sieťovú premávku ako patriacu inému aplikačnému protokolu. Takéto dáta sú v hardware označené ako *false positive* a ďalšie spracovanie v software by bolo zbytočné.
- Boli detekované príznaky FIN v oboch smeroch toku TCP.
- Aplikačný parser, ktorý rozpoznal konkrétny aplikačný protokol detekoval koniec odpočúvaného celku a ďalšie dáta v toku je nežiadúce ďalej exportovať.
- Bolo detekované preplnenie filtrov. V takom prípade sú z filtrov vymazané toky, pri ktorých neprišli pakety už príliš dlhú dobu. Pri blížiacom sa preplnení hardware filtra se zmažú toky, pri ktorých dáta neprišli dlhšie než jednu hodinu. Pri akútnom nedostatku pamäte, kvôli ktorému nedošlo ku vloženiu pravidla do hardware filtra pre práve spracovávaný paket, sú vymazávané aj toky s nižšou dobou nečinnosti (dlhšou než 30 minút aj kratšou, ak sa v tabuľke tokov žiaden taký nenájde, najmenej však jednu minútu neaktívne).

Spracovanie paketov patriacich do jedného toku

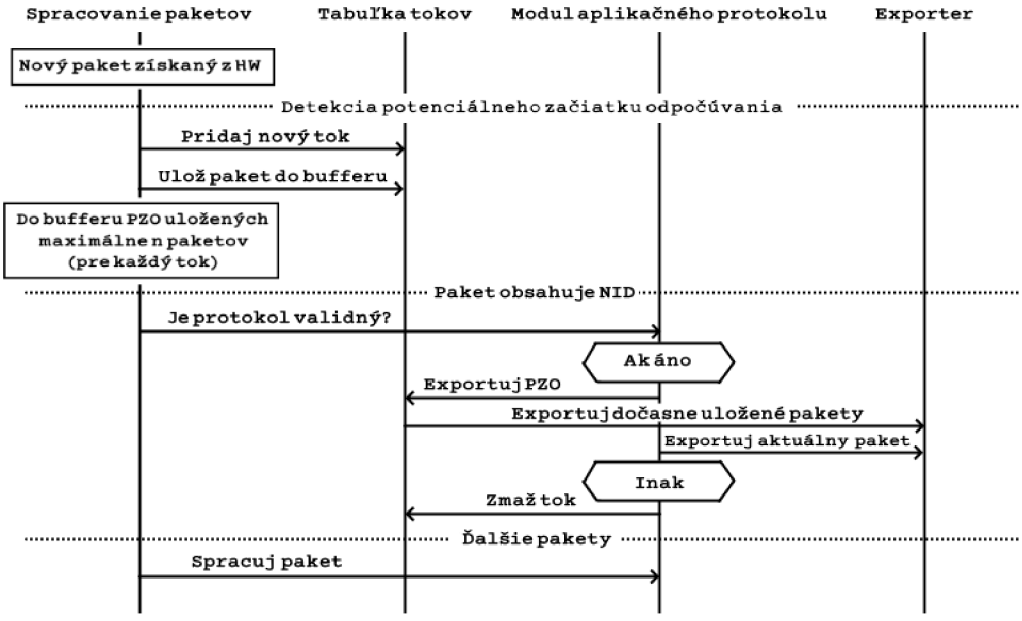
Po obdržaní paketov PaSt skontroluje, či už má pre daný tok uložené nejaké informácie. Ak ide o nový tok, tak pre neho založí záznam. V prípade, že se jedná o tok, ktorý bol hardware vyhodnotený ako potenciálny začiatok odpočúvania, sa prvých N paketov uloží na neskoršie vyhodnotenie.

Ak hardware v pakete nájde niektorý z hľadaných NID, tak sa v rámci PaSt overuje prítomnosť hľadaného NID pomocou regulárnych výrazov špecifických pre konkrétny aplikační protokol 3.4.2.

Ak sa PaSt podarí overiť, že spracovávaný paket je naozaj určený k odpočúvaniu, je táto informácia uložená do tabuľky tokov a paket je exportovaný vrátane všetkých paketov od posledného detekovaného potenciálneho začiatku odpočúvania.

Ak sa zistí, že spracovávaný paket nepatrí do hľadaného protokolu, napr. preto, že sa hľadaný reťazec vyskytol iba v inom kontexte (a nie ako aplikačný identifikátor), je ďalšie spracovanie tohoto toku ukončené a pravidlo na zachytávanie toku je odobrané z hardware.

Toky, u ktorých sa nepotvrdí, že by mali byť zachytávané a zistí sa, že bod potenciálneho začiatku odpočúvania v skutočnosti nie je bodom začiatku odpočúvania sú odstránené z hardware aj software pamäti v momente prijatia N paketov. Protokoly, ako je SMTP, ktoré môžu identifikátory prenášať vo viacerých paketoch, umožňuje firmware SDM detekovať, že sa ešte neukončil prenos identifikátorov a hardware následne posiela dáta viacerých paketov. V prípade SMTP sa každý z adresátov e-mailu prenáša špecifickým príkazom typicky umiestneným vo vlastnom pakete. Graficky je tento proces zobrazený následovne:



Obr. 3.5: Spracovanie paketov v PaSt.

Tabuľka tokov

Tabuľka tokov je implementovaná ako objekt triedy `flow_table`. Pre každý aktívny tok spracovaný PaSt existuje záznam v tabuľke tokov (objekt `flow_map`). Pre každý tok sa evidujú predovšetkým IP adresy, porty, protokol L4, časová značka posledného paketu a maska

parserov majúcich o tento tok záujem. Ďalej je možné si do tabuľky uložiť dáta zviazané s konkrétnym parserom protokolov, či pakety potenciálne určené na export dát.

Objekt `flow_map` zaisťuje prístup k jednotlivým položkám tabuľky v konštantnom čase $\mathcal{O}(1)$ bez ohľadu na veľkosť tabuľky.

Spracovanie aplikačných protokolov

Hardware dostupný v rámci FlexProbe vykonáva prefiltráciu dát a do software posiela iba dáta, pri ktorých existuje predpoklad na ich odpočúvanie. Hardware posúva pakety určené na spracovanie pomocou aplikačných parserov z nasledujúcich dôvodov:

- hardware jednotka Pattern Match (PM) našla v tomto pakete výskyt predom nakonfigurovaného NIDu,
- hardware jednotka Protocol Identifier (PI) našla v pakete regulárny výraz, ktorý identifikuje možný začiatok odpočúvania, ak sa v danom bloku aplikačného protokolu neskôr nájde identifikátor určený k odpočúvaniu,
- zdrojová a cieľová IP adresa, protokol L4 a zdrojový a cieľový port paketu odpovedajúce predom určeným pravidlám vo filtri,
- zdrojová IP adresa, protokol L4 a zdrojový port paketu odpovedajú predom určeným pravidlám vo filtri,
- cieľová IP adresa, protokol L4 a cieľový port paketu odpovedajúce predom určeným pravidlám vo filtri.

Podporované aplikačné protokoly:

- Protokol SMTP [14] - Podporované zachytávanie od `MAIL FROM` pre e-mail, v ktorom se objavuje hľadaná e-mailová adresa v `MAIL FROM` alebo v `RCPT TO`. Zachytáva sa až do konca SMTP toku.
- Protokol POP3 [23] - Zachytávanie celého sedenia POP3 (ak nie je použité kódovanie base64) alebo zachytávanie konkrétneho e-mailu pri detekcií *Internet Mail Format* (príkaz `RETR`).
- Protokol IMAP [22][9] - Zachytávanie celého sedenia IMAP (ak nie je použité kódovanie base64) alebo zachytávanie konkrétneho e-mailu pri detekcií *Internet Mail Format*.
- Protokol FTP [24] - Zachytávanie celého sedenia FTP (podľa prihlasovacieho mena) alebo zachytávanie prenosu konkrétneho súboru príkazy `RETR` a `STOR` (iba informácie z riadiaceho kanálu).
- Protokol SIP [27] - Zachytávanie sedenia od detekcie identifikátoru (`SUBSCRIBE`, `INVITE`, `NOTICE`) po prvý výskyt identifikátoru `BYE`.

Načítanie a export dát

Manažment čítania zo vstupu a odosielania paketov do LEMF jednotky má na starosti trieda *dispatcher*. *Dispatcher* funguje vo dvoch módoch:

- Ak sa všetky pakety úspešne podarilo odoslať, tak sa bude čítať iba zo vstupného rozhrania.
- Ak nastala situácia, že sa prerušilo spojenie s LEMF (aspoň jeden paket sa nepodarilo odoslať). V tomto prípade sa dispatcher pokúša spojenie s LEMF opäť nadviazať a pakety určené na export priebežne ukladá do bufferu. Keď sa spojenie znovu naviaže, tak sa dispatcher najprv pokúsi odoslať prvý paket z bufferu a až potom čítať zo vstupu (tento mechanizmus by mal zaistiť priebežné odosielanie paketov a zároveň nezaseknúť čítanie zo vstupu). Cieľom mechanizmu je postupne odosielať nazhromaždené dáta bez obmedzenia spracovania vstupu.

Kapitola 4

Nástroje na prelamovanie zabezpečenia a odpočúvania Wi-Fi sietí

V tejto kapitole budú popísané nástroje, ktoré boli skúmané a niektoré budú použité na prelomenie zabezpečenia a následné zachytávanie paketov, ktoré budú zasielané do PaSt 3.4.1.

4.1 Password Cracker

Nástroj Password Cracker je sada Pyton skriptov [15], ktoré zaobaľujú Aircrack a ďalšie nástroje na prelamovanie Wi-Fi zabezpečenia. Vyvíjaný vrámci výskumu v ak. roku 2020/21.

Nástroj používa v základe knižnicu Libpcap[1]. Knižnica dokáže spracovávať pakety rýchlosťou až 13,9 milióna paketov za sekundu na jednom CPU jadre[2].

Na zachytávanie paketov je nutné, aby Wi-Fi karta podporovala monitorovací mód, ktorý slúži k zachytávaniu komunikácie ostatných pripojených staníc vo Wi-Fi sieti. To znamená, že nevyžaduje asociáciu s prístupovým bodom.

Pre niektoré typy útokov je potrebné, aby Wi-Fi karta podporovala *Packet Injection*, ktorý slúži k vysielaniu ľubovolných paketov.

Bežné Linuxové distribúcie obsahujú aplikácie (napr. NetworkManager), ktoré si môžu vynucovať prístup ku hardware Wi-Fi karty, čoho dôsledkom je zmena nastavenia karty a prepnutie z monitorovacieho režimu naspäť do bežného režimu.

Ak tento prípad nastane, tak sa preruší zachytávanie paketov a program je prerušený. Dá sa tomuto nežiadanému stavu zabrániť použitím nástroja airmon-ng a pred spustením programu ukončiť takéto procesy príkazom:

```
airmon-ng check kill
```

4.1.1 Beh programu

Beh programu po nakonfigurovaní filtrov a nastavení prebieha následovne:

1. Spustenie monitorovacieho módu - nastavenie sieťového rozhrania a filtra.
2. Zachytenie Beacon rámca - získanie ďalších údajov (SSID, kanál, etc.).

[1] https://www.tcpdump.org/
[2] https://libtins.github.io/benchmark/

3. Deautentizácia klienta a zachytenie štvorfázového autentizačného *handshake* - ak používa prístupový bod TKIP albo CCMP šifrovanie. Tento bod sa vykoná len ak je nastavené aktívne sondovanie, inak program čaká, kým nezachytí autentizáciu.

4. Zachytávanie paketov.

4.1.2 Použitie programu

Po stiahnutí a rozbalení nástroja obsahuje repozitár `./web-api/` všetky potrebné súbory a inštalačný skript `installer.sh`.

Program používa slovníkové útoky, ktoré sú bližšie popísané v kapitole 2.4.1. Slovníky nie sú vzhľadom na veľkosť obsiahnuté pri skripte, ale je nutné ich ručne stiahnuť a vložiť do zložky `./web-api/dicts/`.

Medzi často používané slovníky patrí slovník `rockyou.txt`[3] alebo je možné použiť špeciálne vytvorený slovník pre konkrétnu situáciu, resp. klienta, ktorého heslo chceme získať.

Program je následne spustený príkazom

```
python3 -m cracking_server.server --host 127.0.0.1 --port 3000
--interface <interface_name>
```

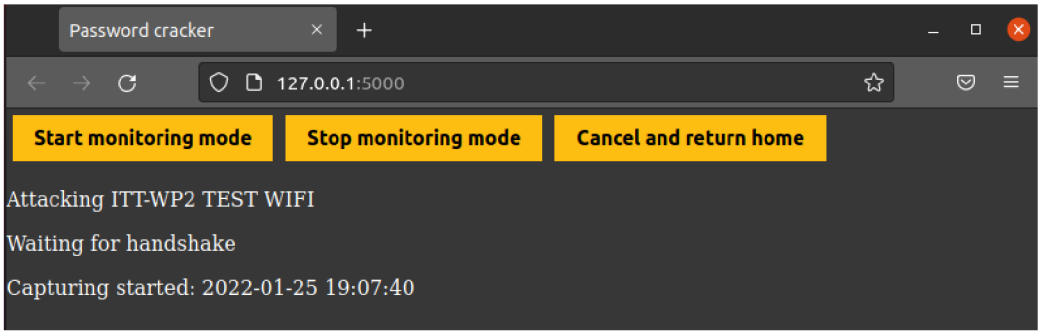
Tento príkaz lokálne na porte 3000 spustí rozhranie na ovládanie a konfiguráciu programu. Prepínač `--interface` nastavuje sieťový adaptér, ktorý sa má použiť. Sieťový adaptér musí podporovať monitorovací režim.

Stlačením tlačidla `Start monitoring mode` sa nastaví karta do monitorovacieho režimu a stlačením tlačila `Scan` sa po zvolenom intervale (v základom nastavení 10 sekúnd) získa zoznam dostupných sietí v okolí.

Zo všetkých dostupných sietí, viď obrázok 4.1 sa zvolí konkrétna sieť, na ktorú sa bude útočiť. Ak je zadaná adresa servera na prelamovanie, tak sa použije ten, inak sa začne prelamovať lokálne. Zvolí sa, či má prebiehať zasielanie deautentizačných rámcov alebo nie, parametre zasielania a spustí sa útok ako na obrázku 4.2.

Obr. 4.1: Zobrazenie dostupných sietí.

[3] https://gitlab.com/kalilinux/packages/wordlists/blob/kali/master/rockyou.txt.gz

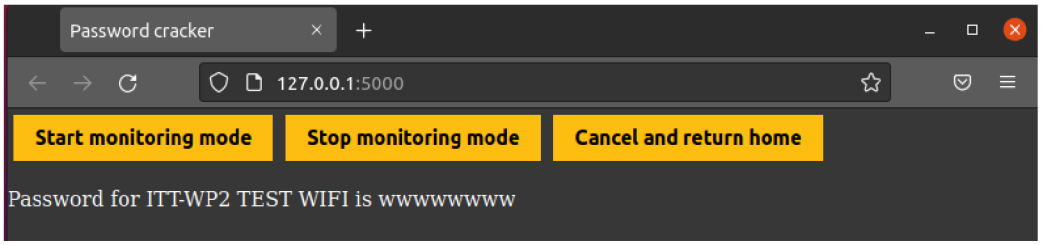


Obr. 4.2: Spustenie útoku.

V prípade chyby komunikácie sa získaný *handshake* uloží lokálne a dá sa spustiť prelamovanie neskôr.

Testovanie nástroja *Password Cracker* prebiehalo lokálne v kontrolovanom virtuálnom prostredí použitím sieťovej karty `Linksys WUSB54GC v1 802.11g [Ralink RT73]`, prístupového bodu Android 9 a klientskými zariadeniami Android 12, Fedora 34 a sieťovej karty Comet Lake PCH-LP CNVi Wi-Fi.

Prístupový bod bol nakonfigurovaný s WPA2 zabezpečením a útok prebiehal pomocou slovníka, ktorý obsahoval heslo. Otestované bolo aj dešifrovanie hesla na inom zariadení z uloženého zachyteného handshake, obrázok 4.3 zobrazuje úspešné prelomenie hesla.



Obr. 4.3: Heslo zistené zo slovníka.

4.2 Nástroj KRACK

Vrámci získavanie paketov z Wi-Fi siete bol počiatočne diskutovaný a zvolený nástroj KRACK [31][4], ktorý vykonáva rovnomenný typ útoku (Key Reinstallation Attacks).

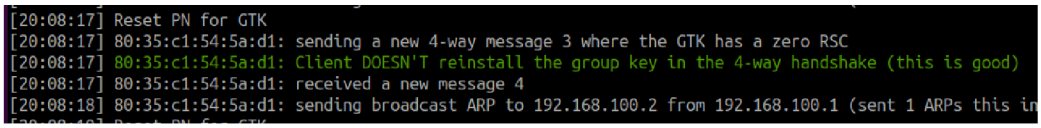
Tento útok využíva chybu v implementácií kryptografických protokolov, keď je možné použiť už aktuálne používaný kľúč. To spôsobí obnovu parametrov asociovaných s daným kľúčom, ako sú *transmit nonce* a *receive replay counters*.

Najrozšírenejšie zabezpečenie WPA2 aj WPA používa štvorfázový handshake pri generovaní nového kľúča. Štvorfázový handshake sa používa už od roku 2004 a doteraz nebol miestom, ktoré mohlo byť bodom, kde dôjde ku prelomeniu zabezpečenia. KRACK útok však využíva štvorfázový handshake ako miesto v ktorom dochádza ku znovupoužitiu už používaného kľúča, dôsledkom toho je útočník schopný odpočúvať premávku bez znalosti hesla a bez nutnosti vykonávať výpočtovo náročne prelamovanie hesla.

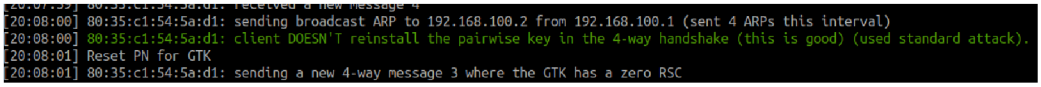
[4] https://github.com/vanhoefm/krackattacks-scripts

4.2.1 Testovanie nástroja KRACK

Testovanie nástroja KRACK prebiehalo lokálne v kontrolovanom virtuálnom prostredí použitím sieťovej karty Linksys WUSB54GC v1 802.11g Adapter [Ralink RT73]. Testované boli najprv zariadenia s aktuálnym software (Android 11, Android 9, iOS 13, Fedora 34), kde pri všetkých boli oba pokusy o reinštaláciu IV neúspešné, ako je možné vidieť na obrázkoch 4.4 a 4.5. Na zariadenie Samsung Galaxy J1, ktoré malo poslednú bezpečnostnú záplatu z roku 2017(2017-03-01) a odvtedy nebolo pripojené na internet bolo možné reinštalovať *pairwise key*, viď obrázok 4.6.



Obr. 4.4: Pokus o reinštaláciu group key.



Obr. 4.5: Pokus o reinštaláciu pairwise key.

Obr. 4.6: Úspešný pokus o reinštaláciu pairwise key pri starom zariadení.

Testovaním bolo zistené, že chyba, ktorú tento nástroj testuje už naďalej nepretrváva pri aktuálnych zariadeniach a nie je teda nijak vhodné tento nástroj naďalej používať a skúmať.

4.3 Sada nástrojov Aircrack-ng

Aircrack-ng[5] je sada nástrojov určených na vyhodnotenie a prácu s Wi-Fi zabezpečením. Všetky nástroje používajú rozhranie príkazového riadku, takže je možné ich funkcionalitu zaimplementovať aj do robustnejších aplikácií.

Jednotlivé skripty sa zaoberajú rôznymi oblasťami Wi-Fi zabezpečenia:

- Monitorovanie - Zachytávanie paketov a ich následný export do textových súborov určených na ďalšie spracovanie.
- Útok - *Replay attacks*, deautentizácia, falošné prístupové body a ďalšie útoky pomocou vkladania paketov (*packet injection*)
- Testovanie - Kontrola vlastnosti Wi-Fi sieťových kariet a ich ovládačov (schopnosť zachytávania paketov, vkladania paketov).
- Prelamovanie - WEP, WPA a WPA-PSK (WPA1 a WPA2)

[5] https://www.aircrack-ng.org/

Sada Aircrack-ng skriptov obsahuje približne 19 samostatne fungujúcich skriptov a ďalšie menšie nástroje, ktoré uľahčujú prácu s touto sadou. Bližšie sú rozobrané niektoré podstatnejšie skripty a tie, ktoré sú použité v práci.

4.3.1 Airodump-ng

Skript Airodump-ng[6] slúži hlavne na zachytávanie paketov a zachytávanie 802.11 rámcov. Tak isto je vhodný aj na zachytávanie WEP inicializačných vektorov a WPA *handshake*, ktoré môžu byť následne použité skriptom Aircrack-ng 4.3 na prelomenie zabezpečenia.

Výstup programu môžu byť súbory v rôznych formátoch obsahujúce detaily o všetkých klientoch a prístupových bodoch, ktorí boli počas behu skriptu zachytený v dosahu.

Skrátený ukážkový výstup skriptu airodump-ng so zmenenými názvami sietí a BSSID zachytený z terminálu zobrazuje 4.1. Sieťová karta musí podporovať a byť zapnutá v monitorovacom režime.

```
\$ sudo airodump-ng wlx00c0cab02383

CH 13 ][ Elapsed: 30 s~][ 2022-04-10 10:12

BSSID              PWR Beacons #Data, #/s CH   MB  ENC CIPHER AUTH ESSID

C8:3A:35:48:XX:XX  -2      48     0    0  9  135  WPA2 CCMP  PSK  Test
6C:C4:9F:30:XX:XX -40       3     0    0  6  130  WPA2 CCMP  MGT  Name1

BSSID              STATION            PWR  Rate   Lost    Frames  Probes

6C:C4:9F:32:XX:XX  80:35:C1:54:XX:XX  -24 6e- 1e     0        3
```

Výpis 4.1: Ukážka výstupu zachytávania dostupných sietí.

4.3.2 Airmon-ng

Hlavným účelom skriptu Airmon-ng[7] je kontrola, či sieťová karta podporuje monitorovací režim a ovládanie prepínania medzi monitorovacím režimom a klasickým režimom sieťovej karty.

Medzi ďalšiu podstatnú funkcionalitu patrí aj možnosť kontroly bežiacich procesov, ktoré by mohli interferovať monitorovaciemu režimu. Jedná sa o procesy, ktoré vyžadujú, aby sieťová karta bežala v klasickom režime a pri detekcii, že sa jej režim zmenil sa snažia zmeniť jej režim nazad. To môže mať za následok neočakávané správanie skriptov, ktoré používajú danú sieťovú kartu v monitorovacom režime.

[6] https://www.aircrack-ng.org/doku.php?id=airodump-ng
[7] https://www.aircrack-ng.org/doku.php?id=airmon-ng

```
$ sudo airmon-ng start wlx00c0cab02383

PHY     Interface       Driver          Chipset

phy2    wlx00c0cab02383 mt76x2u         MediaTek Inc.
        (mac80211 monitor mode vif enabled on [phy2]wlan0mon
        (mac80211 station mode vif disabled for [phy2]wlx00c0cab02383)
```

Výpis 4.2: Ukážka výstupu zmeny režimu sieťového adaptéra.

```
$ sudo airmon-ng check kill

Killing these processes:

    PID Name
    740 wpa_supplicant
  20414 avahi-daemon
  20416 avahi-daemon
```

Výpis 4.3: Ukážka výstupu ukončenia nežiadúcich procesov.

4.3.3 Aireplay-ng

Skript Aireplay-ng[8] zasiela vopred pripravené rámce, ktorých účelom je napr. deutentifikovať klienta za účelom zachytenia WPA *handshake*, falošné prihlásenie, zasielanie podvrhnutých ARP paketov.

Pri zasielaní deautentizačných paketov, je potrebné zadať MAC adresu klienta a prístupového bodu a prípadne nastaviť počet zasielaných paketov. Sieťová karta musí podporovať a byť zapnutá v monitorovacom režime. Ukážkový výstup zasielania a prijatia deautentifikačných paketov zobrazuje 4.4.

Pri niektorých novších sieťových kartách nemusia byť deuatentizačné pakety prijaté a ku deautentizácií nemusí dôjsť.

```
$ sudo aireplay-ng -0 3 -a 90:9A:4A:B8:F0:67
-c 80:35:C1:54:5A:D1 wlan0mon

11:06:48  Waiting for beacon frame (BSSID: 90:9A:4A:B8:F0:67) on channel 2
11:06:49  Sending 64 directed DeAuth (code 7). STMAC:
          [80:35:C1:54:5A:D1] [ 8|67 ACKs]
11:06:50  Sending 64 directed DeAuth (code 7). STMAC:
          [80:35:C1:54:5A:D1] [ 0|64 ACKs]
11:06:50  Sending 64 directed DeAuth (code 7). STMAC:
          [80:35:C1:54:5A:D1] [ 1|64 ACKs]
```

Výpis 4.4: Ukážka zasielania deautentikačných rámcov.

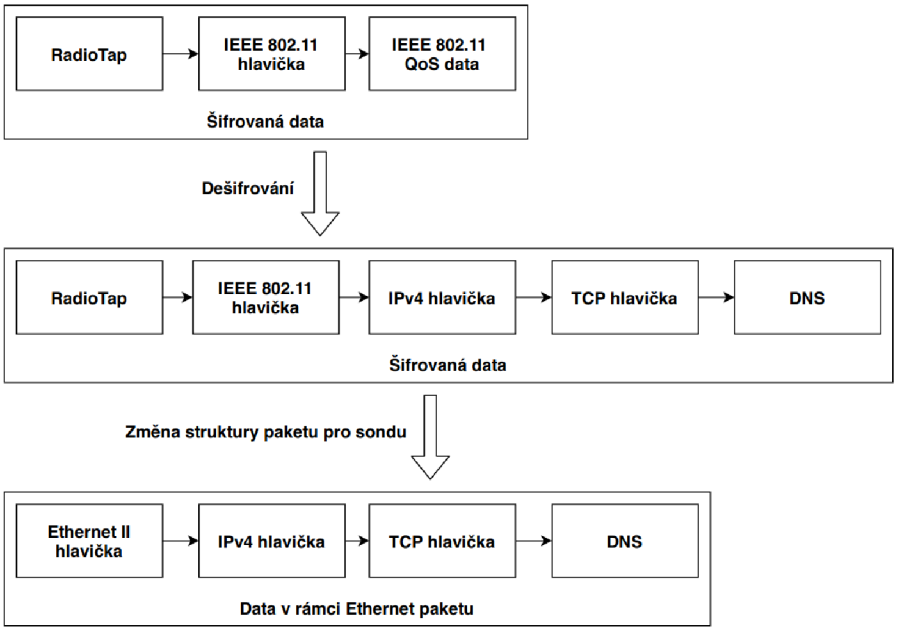
[8] https://www.aircrack-ng.org/doku.php?id=aireplay-ng

4.4 Modifikácia PaSt pre Wi-Fi

Nástroj past-wifi[33] vyvíjaný Petrom Šopfom vrámci bakalárskej práce v roku 2020. Nástroj implementuje rozšírenie l7 analyzátora PaSt popísanej v sekcií 3.4.1 sondy Flexprobe na príjem dát z Wi-Fi siete.

Po spustení nástroja sa inicializuje analyzátor a exportér paketov protokolov aplikačnej vrstvy popísaných v sekcií 3.4.1. Po inicializácii program začne zhromažďovať *Beacon* rámce, z ktorých zisti potrebné informácie. V závislosti na získaných informáciách sa určí šifrovanie a vykonajú potrebné operácie. Pri zabezpečení WPA/WPA2 sa bude čakať na zachytenie štvorfázového handshake. Zo zachyteného štvorfázového handshake budú pomocou zadaného hesla zistené kľúče použiteľné pri dešifrovaní komunikácie. Po ich získaní začne prebiehať dešifrovanie rámcov. Pôvodná časť sondy je vytvorená na prácu s Ethernetovými paketmi a nie s paketmi typu IEEE 802.11. Je teda potrebne pakety orezať až po IP hlavičku a následne ju spojiť so zostrojenou Ethernetovou hlavičkou. Takto zostrojené pakety sú potom posúvané na ďalšie spracovanie sondou. Táto zmena je zobrazená na obrázku 4.7.

Získavaniu kľúčov zo štvorfázového handshake mal obísť nástroj Krack popísaný v kapitole 4.2. Nástroj je však už v dnešnej dobe zastaralý a nepoužiteľný voči aktuálnym zariadeniam, lebo chyby v zabezpečení, ktoré využíva sú už opravené výrobcami zariadení.



Obr. 4.7: Postupná zmena 802.11 paketu na ethernetový paket. Prevzaté z [33].

```
$ sudo ./past-wifi -n wlan0 -b 80:35:C1:54:5A:D1 -c 4C:79:6E:71:D5:95
        -k wwwwwwww -L 127.0.0.1 -P 21103 -A

Interface wlan0 was set to monitor mode.

Collecting beacon frame to gather info...
Found beacon frame!
SSID: TEST-WIFI
Channel: 1
AP is using some sort of encryption, trying to detect...
Detected encryption: CCMP

We have to collect 4-way auth handshake...
Building deauthentication packets...
Sending deauthentication packet (10/10).
All deauthentication packets sent!

Capturing 4-way auth handshake...

Managed to decrypt packet data!
```

Výpis 4.5: Ukážka výstupu nástroja past-wifi.

Testovanie nástroja prebiehalo cez príkazový riadok a ukážkový výstup je zobrazený v 4.5. Výsledkom bolo nájdenie chýb, ktoré viedli ku únikom pamäte a ku nežiadanému správaniu spôsobenému nesprávnymi alebo chýbajúcimi kontrolami pri volaní funkcií z knižnice *lib-pcap*[9].

Nástroj bol vyvinutý na 1g sondu a od jeho vytvorenia nebol udržiavaný. S príchodom verzie 10g sondy došlo ku zmenám v spôsobe komunikácie medzi PaSt časťou a zvyškom sondy a nástroj bol upravený, aby bol kompatibilný s aktuálnou verziou. Zmena nastala v správe pamäti paketov (*buffer*) a ich aktualizácia je súčasťou rozširujúceho balíka.

4.5 Ďalšie nástroje

Zoznam pravidelne aktualizovaných nástrojov zverejnený na github.com dostupný na adrese[10]. Každý z nástrojov v zozname ponúka možnosť vykonať útok na niektorý typ zabezpečenia alebo iným spôsobom získať dáta. Zoznam obsahuje stovky nástrojov, takže nie je možné v reálnom čase otestovať všetky.

4.6 Problémy pri odpočúvaní

Medzi časté komplikácie pri odpočúvaní patrí detekovateľnosť odpočúvaní a technické problémy pri konkrétnych adaptéroch. Ak nie je vykonaná deautentizácia klienta, tak celý odposluch prebieha pasívne a nie je teda detekovateľný. Deautentizácia klienta však celý proces značne urýchľuje, takže nie je nutné čakať na znovupripojenie klienta do siete. Ďalším

[9] https://www.tcpdump.org/
[10] https://github.com/0x90/wifi-arsenal

problémom je nutnosť spúšťať nástroj so špeciálnym oprávnením, aby bolo možné sieťové rozhranie pomocou programu prepnúť do monitorovacieho režimu.

Najväčším problémom je však nutnosť mať kompatibilne a správne nastavený hardware. Zariadenie na odpočúvanie môže z dôvodu nekompatibility odpočúvať premávku iba v obmedzenej miere alebo dokonca vôbec. Medzi časté problémy pri nekompatibilite patria:

- Rozdielna frekvencia – 2.4 GHz alebo 5 GHz.
- Rozdielna šírka pásma – 20/40/80 MHz.
- Rozdielny priestorový tok (Spatial stream) - štyri druhy.
- Rozdielny guard interval – môže byť dlhý alebo krátky, zabezpečuje medzery medzi jednotlivými paketmi.

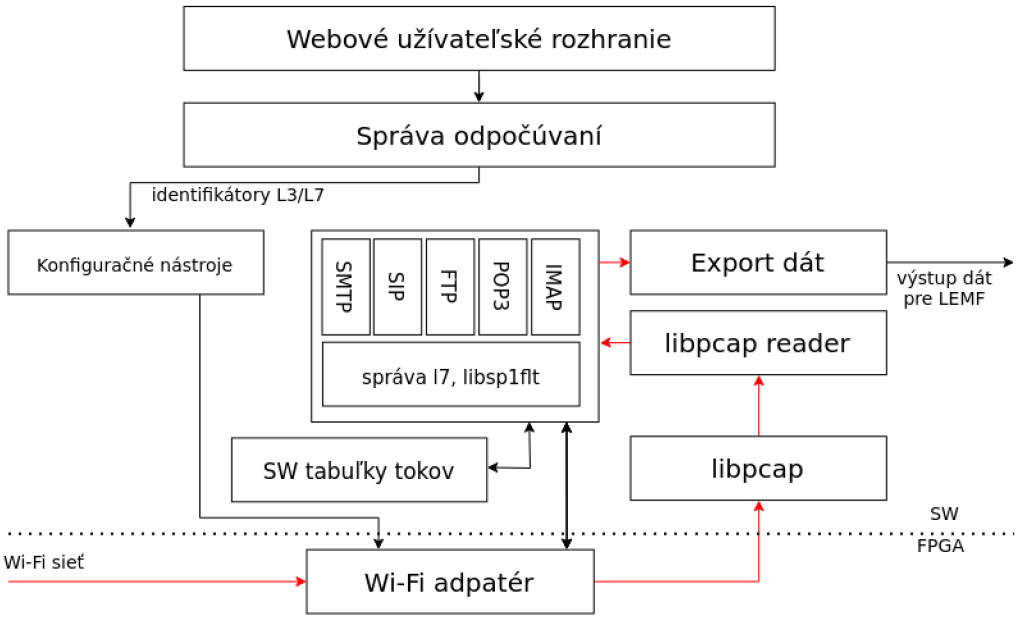
Kapitola 5

Implementácia

Cieľom bakalárskej práce je navrhnúť, implementovať a vytvoriť nástroj na zachytávanie komunikácie z bezdrôtovej siete, ktorý bude rozšírením pre 10g sondu popísanú v kapitole 3, vyvíjanú Výskumnou skupinou akcelerovaných sieťových technológií na FIT VUT[1].

5.1 Návrh rozšírenia sondy

Implementácia rozšírenia zahrňuje úpravu niektorých častí sondy FlexProbe a to L7 analyzátora PaSt, hlavného skriptu na správu obsluhy spúšťania skriptu SPL, skriptu na správu databázy odpočúvaní SLIS a užívateľského rozhrania.



Obr. 5.1: Návrh rozšírenia sondy.

Na obrázku 5.1 je červenými šípkami naznačené ako bude prebiehať cesta paketu v novej architektúre, ktorá používa dáta získané z bezdrôtovej siete. Pakety sa zachytia pomocou pripojeného Wi-Fi adaptéru, ktorý bude používaný časťou software, ktorá bude mať na sta-

[1] https://www.fit.vut.cz/research/group/ant/.cs

rosti prelomenie zabezpečenia a začiatok odpočúvania. Následne budú dáta spracované použitím knižnice libpcap[2], použitím vopred definovaných filtrov, ktoré filtrujú management pakety z Wi-Fi. Po spracovaní dát, budú dáta pripravené v zvolenom formáte na exportovanie.

Tým, že rozšírenie sa týka projektu, ktorý je stále vo vývoji, bol kladený dôraz na to, aby bolo rozšírenie kompatibilné s aktuálnou verziou.

5.2 Použité štandardné nástroje a knižnice

Testovaním a výskumom dostupných nástrojov sa pre jednotlivé časti implementácie zvolil následovné nástroje.

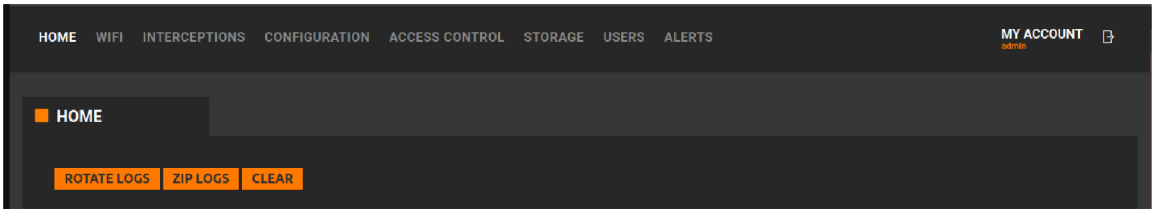
- iwconfig[3] - získavanie zoznamu dostupných bezdrôtových sieťových rozhraní a ich konfigurácia
- ip[4] - správa ovládania bezdrôtových rozhraní
- nástroje zo sady aircrak-ng 4.3
  - airodump-ng - zachytávanie dostupných sietí v dosahu bezdrôtového adaptéra
  - aireplay-ng - zasielanie deutetizačných rámcov na urýchlenie reautentizácie klienta pri zachytávaní handshake
- knižnica pexpect[5] - správa a konfigurácia medziprocesovej komunikácie

5.3 Použitie rozšírenia

Typický príklad použitia rozšírenia za predpokladu, že už je získané povolenie na použitie sondy a situácia si vyžaduje aby sa zachytávala a dešifrovala Wi-Fi komunikácia medzi klientom a prístupovým bodom.

Celá ukážka použitia rozšírenia je v priložených súboroch. Nasledujúci postup popisuje konfiguráciu odpočúvania, ak ešte nebolo pred tým nakonfigurované. Jednotlivé koncové body REST API sú popísané podrobnejšie v sekcií 5.4.2.

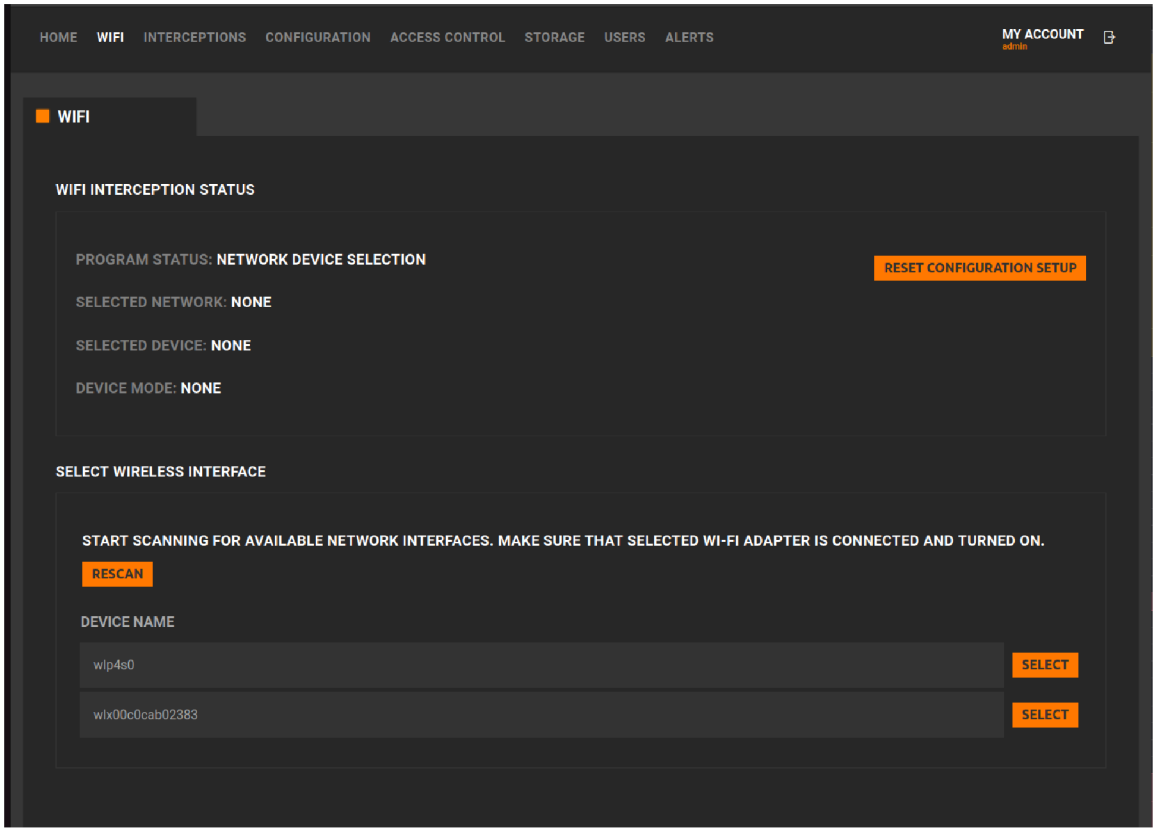
1. Inštaláciou balíčku pre frontend, SLIS, SPL a past-wifi po reštartovaní sondy, bude užívateľské rozhranie aktualizované ako je ukázané na obrázku 5.2. Vo frontend časti na vrchnej lište pribudne záložka `WIFI`.



Obr. 5.2: Užívateľské rozhranie po nainštalovaní rozšírenia.

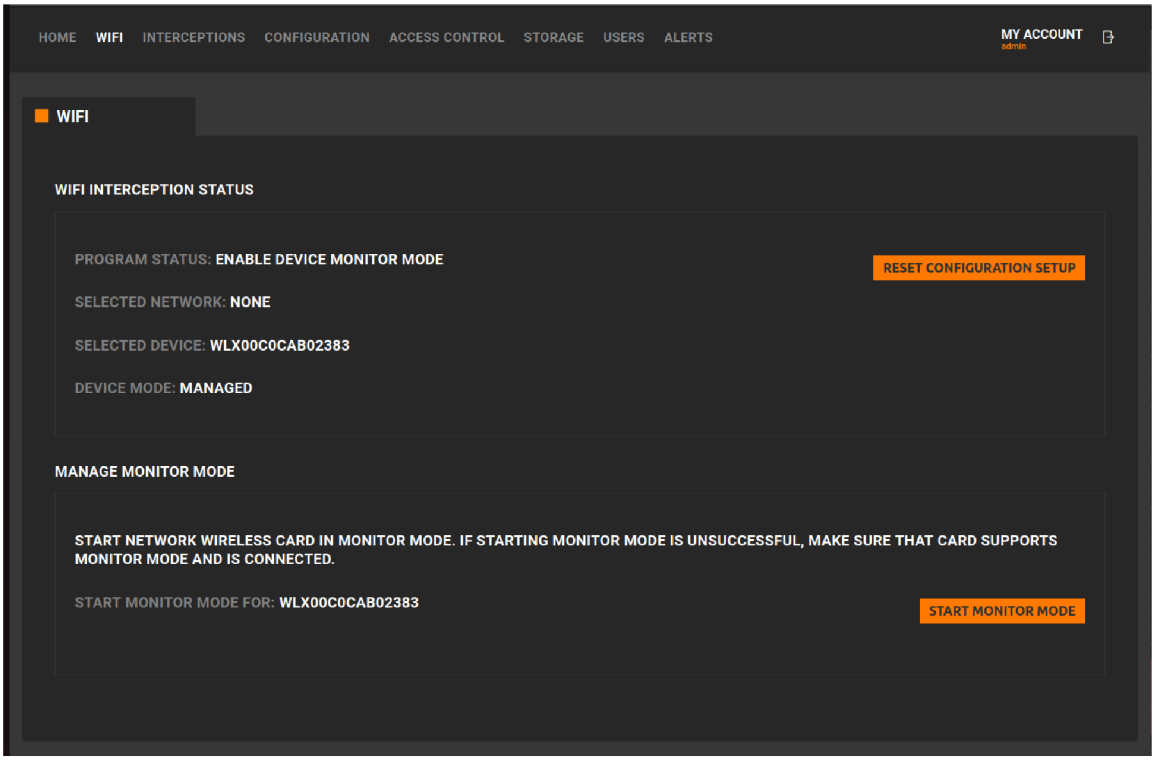
[2] https://www.tcpdump.org/
[3] https://linux.die.net/man/8/iwconfig
[4] https://www.man7.org/linux/man-pages/man8/ip.8.html
[5] https://pypi.org/project/pexpect/

2. V záložke `WIFI` sa najprv zvolí bezdrôtové rozhranie, ktoré bude použité na odpočúvanie. Bezdrôtový sieťový adaptér musí podporovať monitorovací režim. Zoznam sieťových rozhraní je získaní z backend časti pomocou REST API `GET /wifi/devices` a programu `iwconfig`. Ak sa adaptér nezobrazuje na zozname po kliknutí na tlačidlo `SCAN`, je potrebné skontrolovať, či je adaptér správne pripojený a tlačidlom `RESCAN` znovu načítať zoznam, zobrazené na obrázku 5.3.



Obr. 5.3: Užívateľské rozhranie pri výbere bezdrôtového rozhrania.

3. Výber bezdrôtového rozhrania sa potvrdí tlačidlom `SELECT` pri zvolenom rozhraní čo pomocou koncového bodu `/wifi/devicemode` skontroluje režim sieťovej karty. Ak zariadenie nie je v monitorovacom režime na ďalšom stave scény sa zapne monitorovací režim tlačidlom `START MONITOR MODE`, ktorý pomocou REST API koncového bodu `POST /wifi/devicemonitor` a skriptov `ip` a `iwocnfig` zo sekcie 5.2, nastaví monitorovací režim. Ak zlyhá zmena režimu sieťovej karty, bude o tom užívateľ oboznámený chybovou správou a pokračovanie v konfigurácií bude možné až po pripojení vhodnej sieťovej karty. Pred prepnutím režimu sa ukončia bežiace procesy, ktoré by mohli zabrániť úspešnému skenovaniu pomocou REST API `POST /wifi/kill`, zobrazené na obrázku 5.4.



Obr. 5.4: Užívateľské rozhranie pri prepínaní do monitorovacieho režimu.

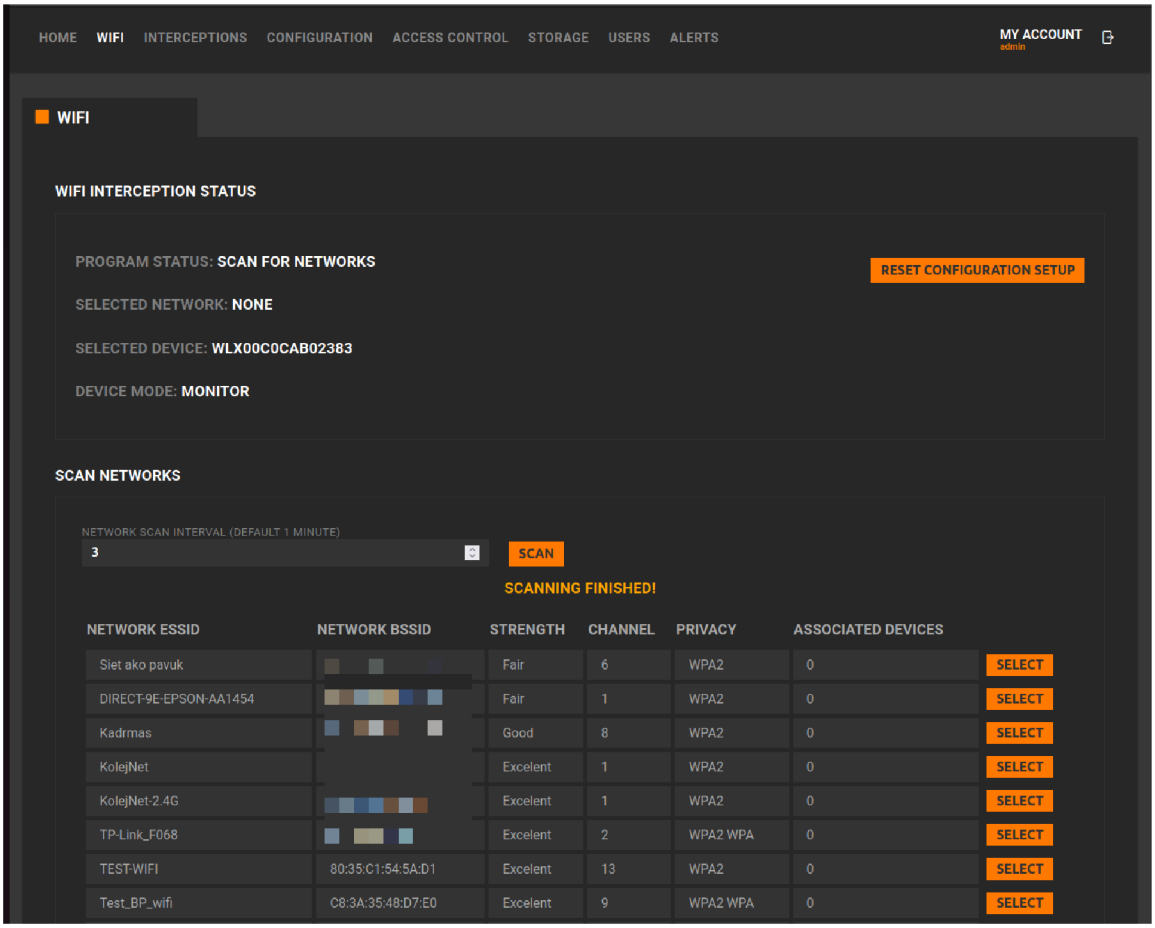
4. Po zmene režimu na monitorovací režim je potrebné zvoliť sieť, ku ktorej bude klient pripojený a na ktorej bude prebiehať odpočúvanie. Základná dĺžka skenovania sietí je jedna minúta, ale táto dĺžka sa dá navýšiť až na 60 minút zadaním čísla v ľavej časti konfiguračnej obrazovky.

   Po zapnutí skenovania sa začnú zobrazovať zachytené dostupné siete v okolí. Skenovanie sa zastaví v momente, keď sa stlačí tlačidlo `STOP SCANNING` alebo vyprší časový limit skenovania nastavený na začiatku skenovania. Správa a zoznam sietí sú získavané použitím REST API `POST /wifi/networks` a nástrojom Airodump-ng popísaným v sekcií 4.3.1. Tento stav scény je zobrazený na obrázku 5.5.

   Pri jednotlivých sieťach je zobrazená aj sila, kanál a zabezpečenie siete.

   Po zastavení skenovania je možné vybrať sieť klknutím na tlačidlo `SELECT` pri zvolenej sieti.

   Ak sa požadovaná sieť nezobrazuje, treba sa uistiť, že je v dosahu sieťového adaptéra.



Obr. 5.5: Užívateľské rozhranie pri skenovaní a voľbe bezdrôtovej siete.

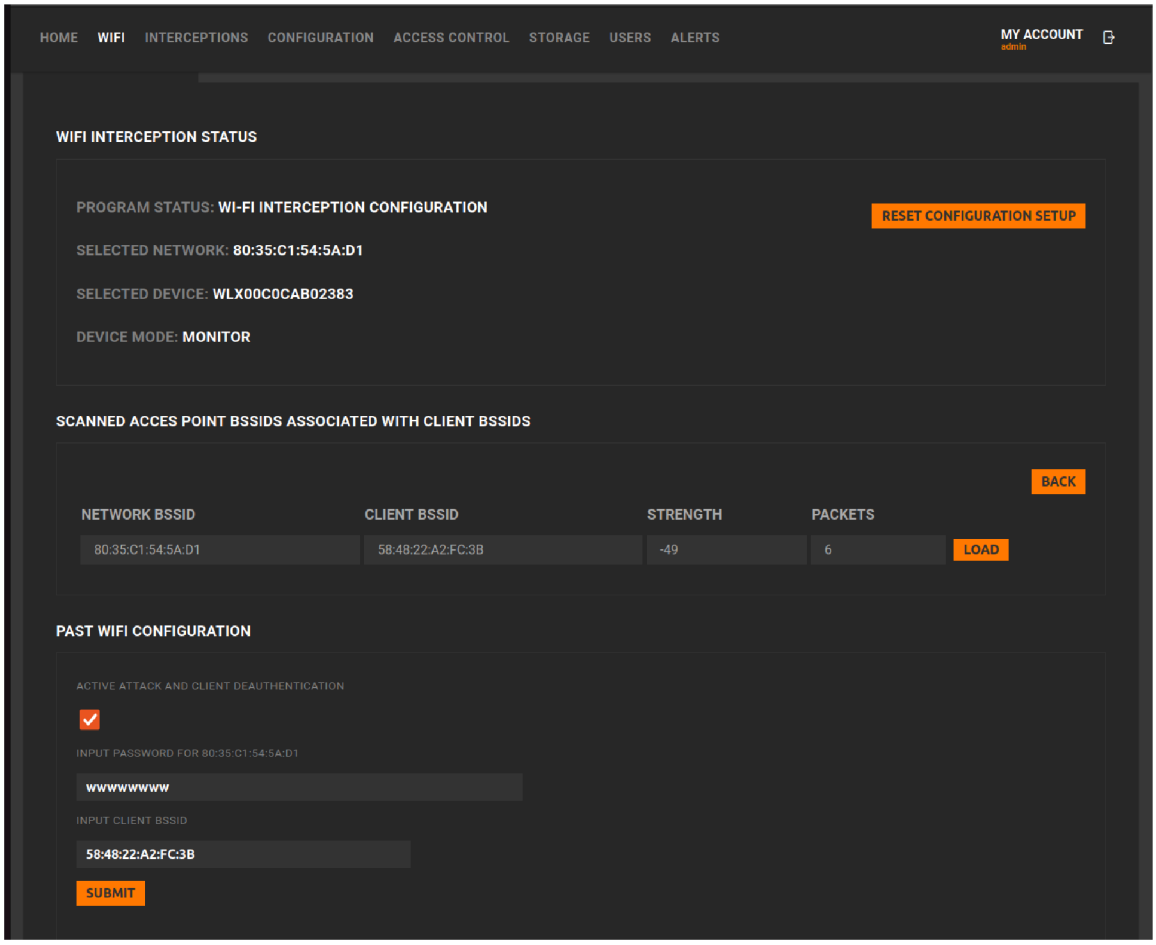
5. Zvolením bezdrôtovej siete, na ktorej sa bude odpočúvať sa dostávame na ďalšiu konfiguračnú scénu. Ak by zvolená sieť nebola požadovaná sieť, tak kliknutím na tlačidlo `BACK` v pravom rohu sa užívateľ vráti na zoznam naskenovaných sietí, kde môže zvoliť inú sieť alebo znovu začať skenovanie.

   Ak užívateľ zvolil požadovanú sieť, tak je potrebné, aby zadal MAC adresu klienta a heslo siete. Ak pri skenovaní bola zachytená komunikácia zvolenej siete s klientom, tak sa všetci asociovaný klienti zobrazia v zozname na vrchu. Po kliknutí na tlačidlo `LOAD` sa MAC adresa asociovaného zariadenia načíta do formulára.

   Ak je formát hesla alebo MAC adresy nesprávny, bude o tom užívateľ upozornený pri potvrdzovaní dát tlačidlom `SUBMIT` a bude možné pokračovať až po vyriešení problému.

   Užívateľ má tak isto možnosť zaslať deautentizačné rámce, ktoré môžu urýchliť deautentizáciu klienta a tým je možné získať *handshake* potrebný na začatie dešifrovania paketov skôr.

   Užívateľské rozhranie pri konfigurácií klienta a hesla je zobrazené obrázkom 5.6.



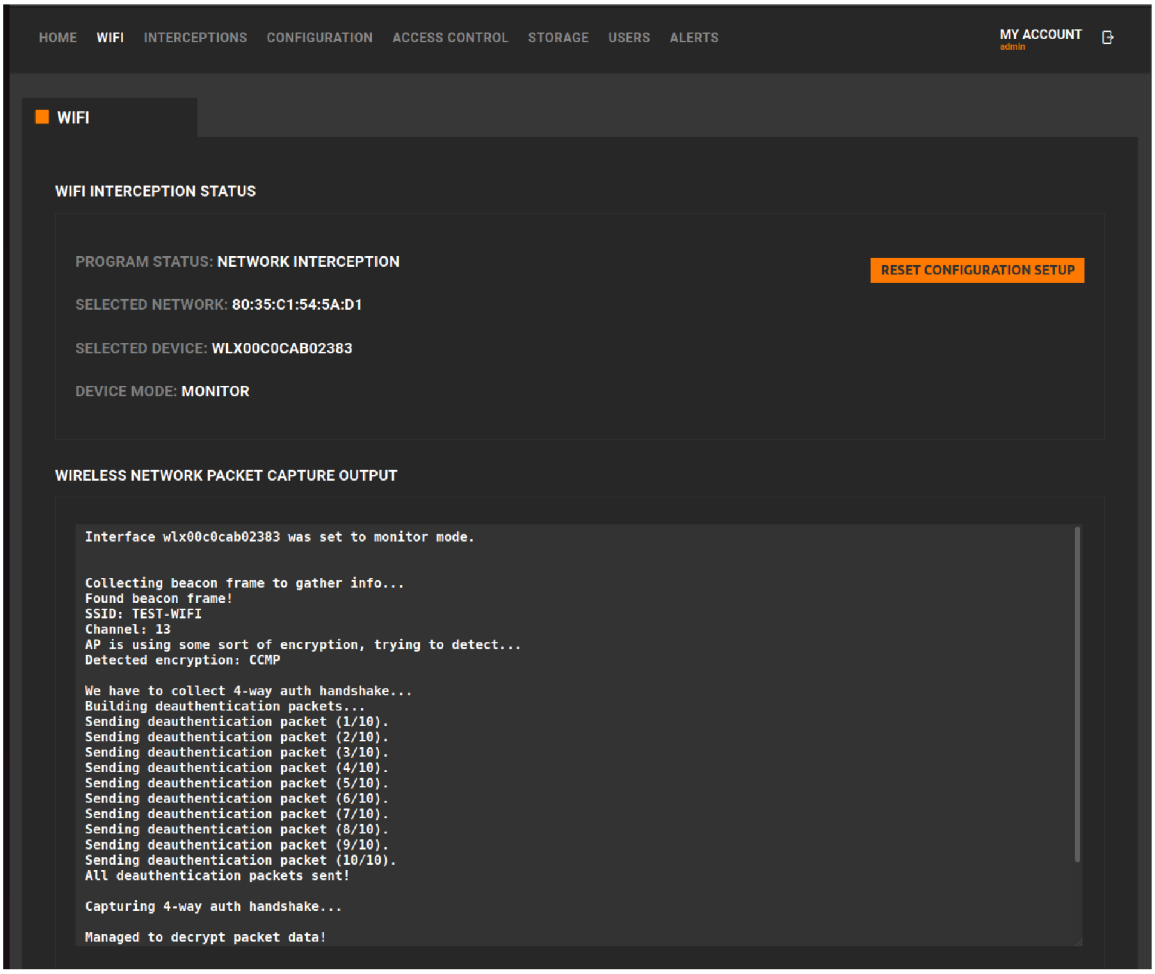
Obr. 5.6: Užívateľské rozhranie pri konfigurácií klienta a hesla.

6. Ak prebehla konfigurácia parametrov úspešne, tak sa po kontrole v backend časti spustí proces `past-wifi` a v stavovom okne zobrazí postup prelamovania Wi-Fi zabezpečenia a záchyty paketov, získavaný z backend časti pomocou REST API koncových bodov, ktorými prebieha nastavenie, alebo resetovanie zvolených parametrov. Najprv musí sonda zachytiť *beacon* rámec, z ktorého vyčíta potrebné parametre. Ak bola zvolená možnosť zaslať deautentizačné rámce, tak sa vytvorí a zašle desať vytvorených rámcov. Následne sa začne zachytávať *handshake*, ktorý zvyčajne prebieha pri pripájaní klienta ku sieti.

   Čas dĺžky procesu zachytávania *handshake* je ovplyvnený tým, kedy bude zariadenie autentizované ku zvolenému prístupovému bodu. Ak boli akceptované deutentizačné rámce, tak zachytenie môže prebehnúť hneď, inak tento proces môže trvať minúty až hodiny.

   Obrázok 5.7 ukazuje užívateľské rozhranie po nakonfigurovaní scény.

   Po úspešnom zachytení *handshake* sa začne podľa vytvorených filtrov na odpočúvanie zachytávať a exportovať požadovaná komunikácia. Odpočúvania je možné vytvárať a konfigurovať v záložke `INTERCEPTIONS`.



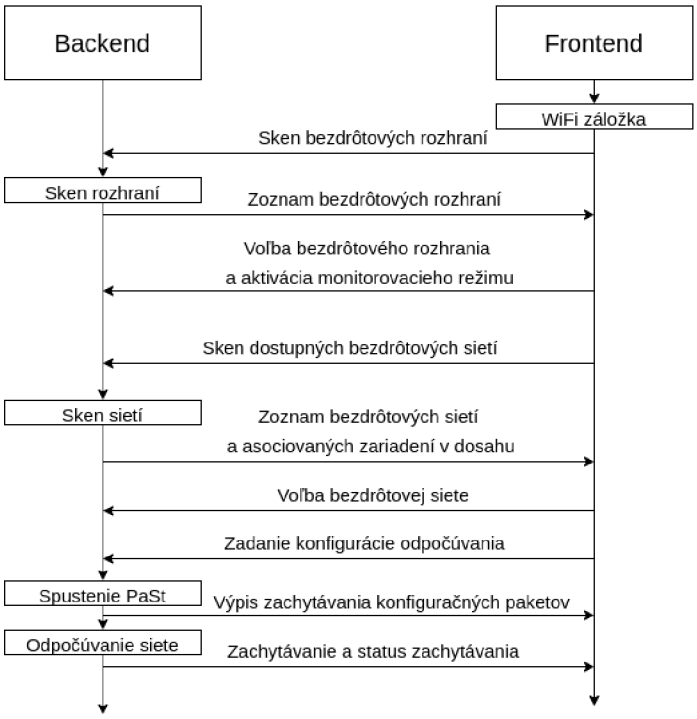
Obr. 5.7: Užívateľské rozhranie po nakonfigurovaní Wi-Fi odpočúvania.

5.4 Časti rozšírenia

Implementácia rozšírenia sa skladala z dvoch častí a to rozšírenia pre *backend* a *frontend*. *Backend* rozšírenie bolo implementované použitím Python3[6] a *frontend* použitím knižnice React[7].

Diagram 5.8 zobrazuje postup pri bežnom postupe konfigurácie Wi-Fi odpočúvania.

[6] https://www.python.org/
[7] https://reactjs.org/

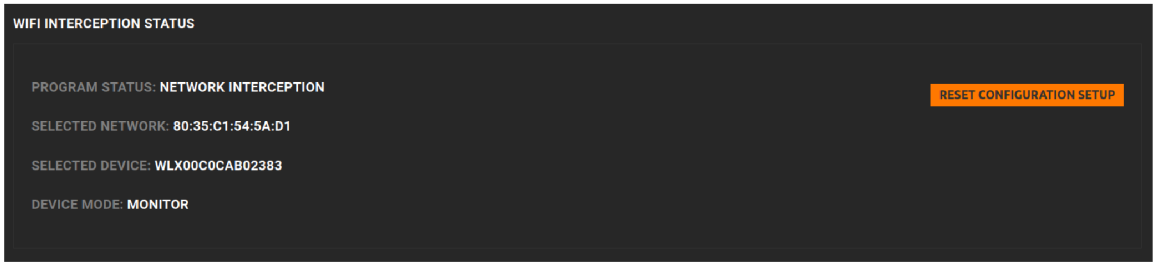


Obr. 5.8: Diagram komunikácie pri konfigurácií odpočúvania WPA/WPA2 siete.

5.4.1 Frontend implementácia

Vo *Frontend* prebehla implementácia vytvorením novej scény. Pridaním tejto scény sa po nainštalovaní rozšírenia zobrazí na hornej lište nová záložka s názvom WIFI.

V Reacte je hlavný komponent App, implementovaný vo funkcii v súbore App.js. Tento komponent dokáže na základe svojho stavu vykresliť konkrétnu scénu, ktorá sa môže skladať z ďalších komponentov a má požadovaný obsah. Zobrazovaný obsah je synchronizovaný s `backend` časťou pomocou API, viď 5.9.



Obr. 5.9: Komponent StatusLine.

Keďže sa konfigurácia berie ako jeden súvislý krok, tak musí prebehnúť celá od voľby bezdrôtového rozhrania cez voľbu siete a zadania parametrov ku spusteniu PaSt časti, aby sa konfigurácia uložila do súboru a mohla byť pri opätovnom spustení znovu načítaná. Vrámci Wi-Fi scény sa podľa aktuálneho kroku zobrazuje jeden z piatich možných stavov scény. Jednotlivé stavy scény zotrvávajú zobrazené, pokiaľ sa nesplnia všetky podmienky konfiguračného kroku v danej scéne.

Každý stav scény má na vrchu scény komponent `StatusLine`, ktorý zobrazuje aktuálne nakonfigurované parametre.

5.4.2 Backend implementácia

Backend je spravovaný pomocou časti sondy SPL. SPL spravuje a zabezpečuje, aby sa procesy jednotlivých častí spustili v správnom poradí a správne medzi sebou komunikovali.

Beh procesov spravuje trieda `ProcessGuard`, ktorá vytvára vlastný proces a v prípade zlyhania procesu, sa ho pokúsi znovu zapnúť, aby sa zabezpečil chod sondy aj bez externého zásahu. Tak isto zabezpečuje aj správne ukončenie programu.

PaSt sa v testovacom prostredí zapne volaním skriptu SPL. Skript SPL postupne naštartuje všetky potrebne procesy medzi ktoré patrí napríklad zber dát, konfigurácia, ale aj inicializácia Hardware.

Hlavná funkcionalita backend časti pre implementácie Wi-Fi rozšírenia je v súbore `wifi.py`. V tomto súbore sú implementované funkcie na voľbu bezdrôtového rozhrania a správy monitorovacieho režimu na ňom, správa a zachytávanie bezdrôtových sietí v dosahu zvoleného rozhrania.

Ku backend časti sa pristupuje pomocou koncových bodov REST API (Application Program Interface). V nasledujúcom zozname sú uvedené novo vytvorené koncové body API na komunikáciu medzi obomi časťami aplikácie. Využívajú sa hlavne metódy `POST` a `GET`.

- GET /wifi/devicemode - vráti režim, v ktorom sa práve sieťový adaptér nachádza.
- POST /wifi/devicemonitor - vráti návratovú hodnotu funkcie aktivácie alebo deaktivácie monitorovacieho režimu na zvolenom sieťovom adaptéri.
- GET /wifi/devices - vráti zoznam pripojených bezdrôtových rozhraní.
- POST /wifi/networks - vráti zoznam sietí v dosahu sieťového adaptéru a asociované zariadenia s konkrétnou sieťou. Možnosť zastavenia skenovania, pri zmene scény.
- POST /wifi/kill - vráti návratovú hodnotu funkcie, ktorá zabezpečuje, aby žiadne procesy nenarušovali priebeh behu programu a prípadne zastaví ich priebeh.

Na komunikáciu a konfiguráciu PaSt Wi-Fi časti slúžia nasledujúce koncové body API:

- POST - /wifi/pastsetup - nastavenie užívateľom zadaj konfigurácie pre PaSt Wi-Fi a spustenie alebo zastavenie procesu
- GET - /wifi/deviceresniff - prístupový bod na získavanie výstupu z spusteného PaSt Wi-Fi procesu
- GET - /wifi/configuration - vráti aktuálnu konfiguráciu z konfiguračného súboru
- GET - /wifi/resetconfiguration - nastavenie konfigurácie PaSt Wi-Fi v konfiguračnom súbore na pôvodné základné hodnoty

Konfigurácia PaSt časti sondy v rozšírení nazvanej `ConfigurationWifi` je implementovaná ako rozšírenie triedy `CONFIGURATION10g` v súbore `configuration.py`. Za účelom vytvorenia novej konfigurácie bola v súbore `probe-platform.py` vytvorená nová platforma

`WIFI`, ku ktorej boli upravené príslušné závislosti v ostatných súboroch rodičovských tried. Novovzniknutá platforma upravuje niektoré funkcie rodičovskej triedy a medzi hlavné zmeny patrí zmena funkcií na správu konfigurácie PaSt Wi-Fi, kde sa v novej platforme musí zachytávať aj výpis z tohoto procesu. Upravená musela byť aj trieda `ProcessGuard`, kde bolo potrebné doplniť funkcionalitu na možnosť zachytávania výstupu z STDOUT do PIPE, odkiaľ sa následne výstup spracuje a zobrazí v užívateľskom rozhraní.

Novo vzniknutá konfigurácia sa ukladá do konfiguračného súboru `config.spl` a je perzistentná a automaticky načítaná po štarte sondy. Zakladaný formát ukladanej konfigurácie Past WiFi je následovný:

- PaSt: <bool>, - PaSt sa používa.
- PaSt_Configured: <bool>, - PaSt je nakonfigurovaná.
- PaSt_data: - Konfigurácia parametrov PaSt.
  - PaSt_AP: <string>, - BSSID prístupového bodu.
  - PaSt_Client: <string>, - MAC adresa klienta.
  - PaSt_Device: <string>, - Názov bezdrôtového rozhrania.
  - PaSt_Pswd: <string>, - Heslo siete.
  - PaSt_Deauth: <bool>, - Aktívne zasielanie deutentizačných paketov.
  - PaSt_Channel: <string>, - Kanál na ktorom sieť vysiela.

Stav konfigurácie PaSt je zistený priamo z parametra konfigurácie `PaSt_Configured` a stav bežiaceho procesu je zistený vrámci procesu `_processes["PaSt"]` na správu procesov. Pri načítaní WIFI scény môže nastať jedna z troch situácií.

1. PaSt nie je nakonfigurovaná v konfiguračnom súbore a nebeží - spustí sa celý proces konfigurácie od začiatku.
2. PaSt je nakonfigurovaná v konfiguračnom súbore a nebeží - preskočia sa kroky spojené s výberom adaptéra a siete a začne sa rovno začiatkom zachytávania výstupu z konfigurácie zachytávania.
3. PaSt je nakonfigurovaná a beží - výpis z konfigurácie PaSt Wi-Fi.

5.5 Testovanie

Zmyslom práce je vytvoriť nástroj na prelamovanie zabezpečenia, čo je z pohľadu legálnosti zakázané, takže všetky testy útokov prebiehali iba na vlastné zariadenia.

5.5.1 Nástroj na správu monitorovacieho režimu

V prvej fáze testovania bolo testované, ktorý z trojice nástrojov Airmon-ng4.3.2, `ifconfig` a `ip link` je najvhodnejší na správu monitorovacieho režimu, výsledky tohto testu sú zobrazené v tabuľke:

	Airmon-ng	ifconfig	ip link
Aktuálny	✓	x	✓
Zmena názvu rozhrania	✓	x	x

Tabuľka 5.1: Porovnanie nástrojov na správu monitorovacieho režimu.

Zmena názvu je nežiadúca vzhľadom na to, že je očakávané, že ak sa nástroj reštartuje tak, v prípade ak je už odpočúvanie v priebehu bude sa v odpočúvaní pokračovať bez nutnej manuálnej konfigurácie. Pri zmene názvu by mohlo dôjsť ku problémom pri výbere z dostupných rozhraní.

Prvotne bol zvolený nástroj `ifconfig`, ale testovaním sa zistila inkonzistencia jeho funkcionality a bol zmenený za nástroj `ip link`, ktorý je implementovaný v aktuálnej verzii. Ďalším prieskumom[8] sa zistilo, že aj najpoužívanejšia Linuxová distribúcia Ubuntu, už `ifocnfig` nemá v základnom balíku súborov a nahradila ho nástrojom `ip link`.

5.5.2 Hardware sieťové zariadenia

Pri testovaní boli použité routre, ktoré sú aj s možnosťami zabezpečenia zobrazené v nasledujúcej tabuľke:

názov	WEP	WPA	WPA2	WPA3
TENDA W311R+	✓	✓	✓	x
Archer AX20	x	✓	✓	✓
TENDA N3	x	✓	✓	x
Belkin F6D4230-4 v1	✓	✓	✓	x
Xiaomi 5 pro (mobile AP)	x	x	✓	x

Tabuľka 5.2: Routre použité pri testovaná a ich vlastnosti.

Pri testovaná boli použité následovné sieťové adaptéry:

názov	rozhranie
d-link dwa-181	USB 3.0
Cisco WUSB54GC	USB 2.0
Alfa AWUS036ACM	USB 3.0
Intel Wi-Fi 6 AX200	PCI express

Tabuľka 5.3: Sieťové adaptéry použité pri testovaní a ich vlastnosti.

Z testovaných adaptérov sa najviac osvedčil adaptér Alfa AWUS036ACM, ktorý bol aj v iných projektoch[9] podobného charakteru kladne ohodnotený. Spĺňa všetky požadované podmienky ako sú ďaleký dosah porovnaním napríklad s druhým testovaným adaptérom D-link dwa-181 a USB 3.0 rozhranie. Výhodou je aj fakt, že adaptéry značky Alfa sa používajú aj pri iných projektoch so zameraním na problematiku prelomenia zabezpečenia. Adaptér D-link dwa-181[10] bol na začiatku zvolený ako hlavný adaptér kvôli podpore WPA3, ale bol nahradený z dôvodu nestability a nedostupnosti Linuxových ovládačov adaptérom Alfa AWUS036ACM[11].

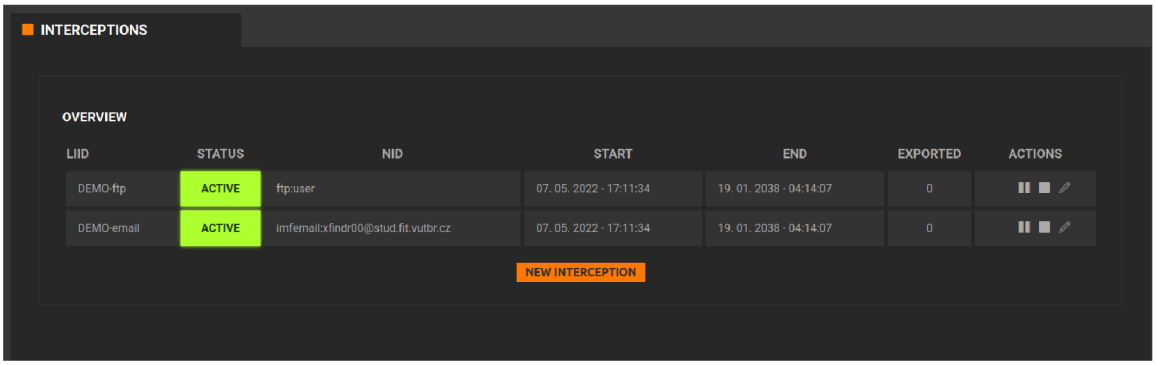
[8] https://ubuntu.com/blog/if-youre-still-using-ifconfig-youre-living-in-the-past
[9] https://github.com/vanhoefm/fragattacks#2-supported-network-cards
[10] https://www.dlink.com/en/products/dwa-181-ac1300-mu-mimo-wi-fi-nano-usb-adapter
[11] https://www.alfa.com.tw/products/awus036acm?variant=36473965936712

5.5.3 Testovanie implementovaného rozšírenia

Po nainštalovaní rozšírenia bolo užívateľské rozhranie otestované manuálne bez automatizovaných testov. Týmto spôsobom bola otestovaná všetka funkcionalita implementovanej backend časti.

Pri testovaní integrácie rozšírenia do sondy boli prostredníctvom webového GUI v záložke `Interceptions` vytvorené testovacie odpočúvania, aby sa overilo, že rozšírenie je nainštalované správne a aj bezdrôtové zachytávanie paketov je správne napojený na zvyšok sondy.

Boli vytvorené dva testovacie odpočúvania `DEMO-ftp` na zachytávanie FTP paketov a `DEMO-email` na zachytávanie mailovej komunikácie zobrazené obrázkom 5.10.

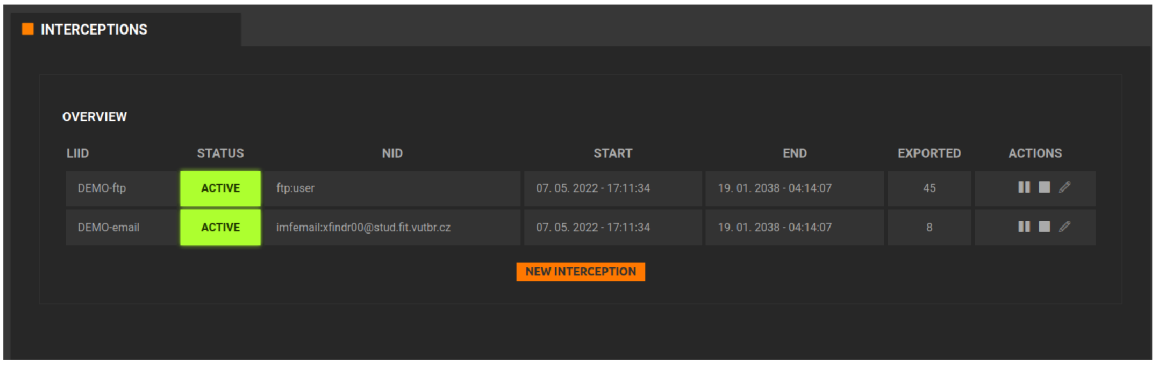


Obr. 5.10: Nakonfigurované odpočúvania.

Testcase mail

Odpočúvanie `DEMO-mail` bolo nakonfigurované na to, aby zachytávalo všetky mailové pakety, obsahujúce mailovú adresu nakonfigurovaného odpočúvania v záložke `Interceptions` (xfindr00@stud.fit.vutbr.cz).

Testovanie zabezpečuje skript `test_imap_mails.py`. Skript vyzve užívateľa na zadanie prihlasovacích údajov na mailový server imap.stud.fit.vutbr.cz, odkiaľ získa jeden mail, čím vytvorí sieťovú premávku a v odpočúvaní sa zobrazí počet zachytených exportovaných paketov, počet zachytených paketov zobrazuje obrázok 5.11.



Obr. 5.11: Ukážka zachytených paketov v záložke *Interceptions*.

Testcase FTP

Odpočúvanie `DEMO-ftp` bolo nakonfigurované na to, aby zachytávalo všetky mailove pakety, obsahujúce login *user*. Jednoduchý FTP server je dostupný po nainštalovaná pip balíčka *python-ftp-server*. Na zariadení, ktoré sa nezúčastňovalo odpočúvania bol spustený FTP server nasledujúcim príkazom, ktorý spustil lokálny FTP server a vypísal prístupové údaje. Spustenie serveru zobrazuje výstup 5.1.

```
$ python3 -m python_ftp_server -d ~/Documents/

Local address: ftp://147.229.221.188:60000
User: user
Password: yKTMgdUqltgDyZJQSWtR
```

Výpis 5.1: Spustenie lokálneho FTP servera.

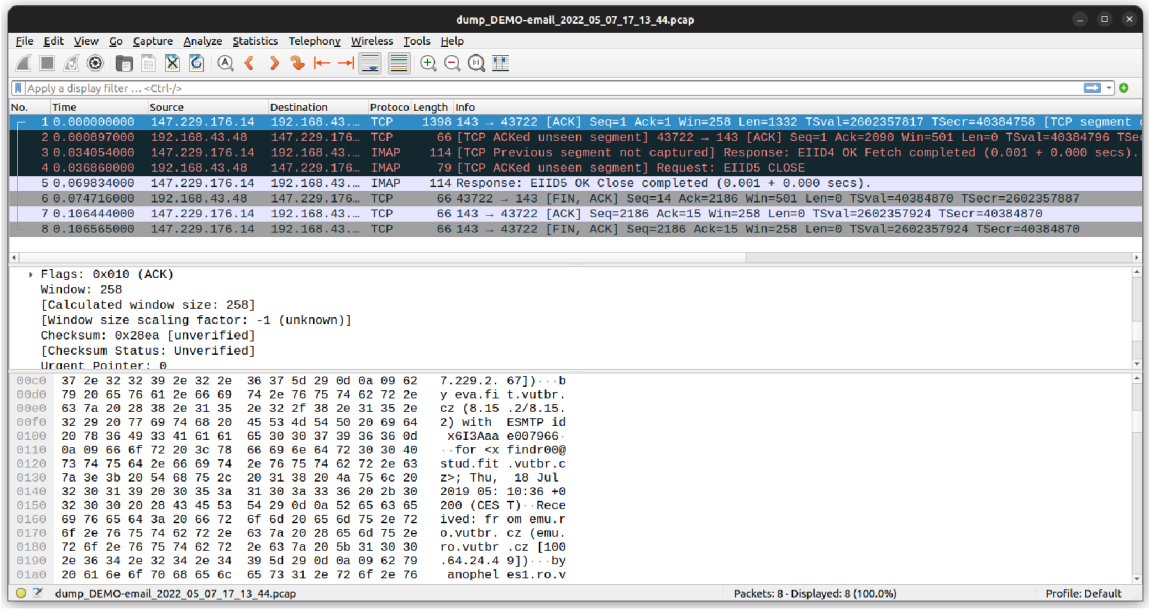
Následne na zariadení, ktoré je odpočúvané sa prihlásil užívateľ na vytvorený FTP server, odkiaľ stiahol textový súbor.

```
$ ftp 147.229.221.188 60000

Connected to 147.229.221.188 (147.229.221.188).
220 pyftpdlib 1.5.6 ready.
Name (147.229.221.188:michal): user
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get Makefile
local: Makefile remote: Makefile
227 Entering passive mode (147,229,221,188,234,163).
150 File status okay. About to open data connection.
226 Transfer complete.
7678 bytes received in 0.00924 secs (831.22 Kbytes/sec)
```

Výpis 5.2: Pripojenie na FTP server a stiahnutie súboru.

Zachytené pakety sú tak isto ukladané podľa názvu odpočúvania s aktuálnym dátumom na cieľové úložné zariadenie v súbore formátu .pcap, ukážka na obrázku 5.12.



Obr. 5.12: Ukážka zachytených paketov v príslušnom .pcap súbore.

Kapitola 6

Záver

V rámci tejto práce bola preskúmaná problematika Wi-Fi zabezpečenia a s tým súvisiacich nástrojov na prelomenie zabezpečenia a odpočúvanie Wi-Fi sietí. Hlavným cieľom bolo zúžitkovať získané znalosti a implementovať rozšírenia pre sieťovou sondu FlexProbe popísanú v kapitole 3, na zachytávanie a analýzu dát aj z bezdrôtového rozhrania. Na odpočúvanie komunikácie vo Wi-Fi sieti je potrební zachytávanú komunikáciu dešifrovať. Na dešifrovanie komunikácie bola použitá knižnica libpcap, lebo má dostatočný výkon a API je kompatibilné s architektúrou PaSt časti sondy FlexProbe.

Počas implementácie boli priebežne testované kombinácie sieťových kariet a prístupových bodov a následne bola zvolená jedna, na ktorej bolo rozšírenie otestované a bude použitá pri nasadení sondy do praxe. Rozšírenie sa týka frontend i backaned časti sondy, kde sa implementovalo okrem konfigurácie a ovládania odpočúvania z bezdrôtovej siete aj nízkoúrovňové ovládanie hardware a portovanie l7 analyzátora (PaSt) sondy.

Implementácia rozšírenia prebiehala na základe poznatkov spísaných v kapitole 2 zaoberajúcich sa štandardami Wi-Fi zabezpečení a chybami v ich implementácií. Chyby v štandardoch viedli ku vzniku nástrojov, ktoré tieto chyby využívajú, aby bolo možné zabezpečenie prelomiť a dostať sa ku pôvodným prenášaným dátam. Vhodné nástroje na implementáciu rozšírenia boli zvolené na základe poznatkov k jednotlivým nástrojom popísaných v kapitole 4.

Rozšírenie je implementované ako sada balíčkov. Ich inštalácia do aktuálnej sondy FlexProbe pridá funkcionalitu podpory získavania dát z Wi-Fi siete. Rozšírenie užívateľského rozhrania je implementované využitím knižnice React.js zakomponované do pôvodného rozhrania sondy, ktoré umožňuje užívateľovi nakonfigurovať parametre na odpočúvanie dát medzi zvoleným klientom a prístupovým bodom, podrobnejšie popísané v sekcií 5.4.1. Nástroj podporuje odpočúvanie sietí, ktoré sú chránené najviac používanými zabezpečeniami WEP a WPA/WPA2. Počas vývoja bol sledovaný aj vývoj útokov na zabezpečenie WPA3 popísaných v sekcií 2.5. Aktuálne dostupné útoky však využívajú iba princípy, ktoré sú už opravené alebo budú v blízkej budúcnosti. To vedie na krátku životnosť nástrojov a tak sa od ich integrácie do výsledného balíka upustilo.

V blízkej budúcnosti je plánované rozšírenie o podporu zachytávania na základe iba IP adresy, to ale vyžaduje obídenie L7 parserov časti PaSt. PaSt je tiež pripravená na rozšírenie o podporu prelamovania WPA3 zabezpečenia. V ďalšej verzií je aj možnosť rozšírenia nástroja o automatické prelamovanie hesla bez nutnosti poznať ho pred začiatkom odpočúvania.

Literatúra

[1] IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements. *IEEE Std 802.11i-2004*. 2004, s. 1–190. DOI: 10.1109/IEEESTD.2004.94585.

[2] IEEE Standard for Information Technology–Telecommunications and Information Exchange between Systems - Local and Metropolitan Area Networks–Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Std 802.11-2020 (Revision of IEEE Std 802.11-2016)*. 2021, s. 1–4379. DOI: 10.1109/IEEESTD.2021.9363693.

[3] *Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery*. TS 102 232-1 V3.26.1. European Telecommunications Standards Institute, March 2022. 53 s. Dostupné z: https://www.etsi.org/deliver/etsi_ts/102200_102299/10223201/03.26.01_60/ts_10223201v032601p.pdf.

[4] Abo Soliman, M. A. a Azer, M. A. A study in WPA2 enterprise recent attacks. In: *2017 13th International Computer Engineering Conference (ICENCO)*. 2017, s. 323–330. DOI: 10.1109/ICENCO.2017.8289808.

[5] Balkonis, M. WIFI evolution "beyond WIFI 6". In:. 2021, s. 21. DOI: 10.1109/ICSPS.2009.87.

[6] Biham, E. New types of cryptanalytic attacks using related keys. *Journal of Cryptology*. Dec 1994, zv. 7, č. 4, s. 229–246. DOI: 10.1007/BF00203965. ISSN 1432-1378. Dostupné z: https://doi.org/10.1007/BF00203965.

[7] Bogdanov, A., Khovratovich, D. a Rechberger, C. Biclique Cryptanalysis of the Full AES. In: Lee, D. H. a Wang, X., ed. *Advances in Cryptology – ASIACRYPT 2011*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, s. 344–371. ISBN 978-3-642-25385-0.

[8] Chen, L., Ji, J. a Zhang, Z. *Wireless Network Security: Theories and Applications*. Springer Berlin Heidelberg, 2013. 46–52 s. SpringerLink : Bücher. ISBN 9783642365119.

[9] Crispin, M. *INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1* [Internet Requests for Comments]. RFC 3501. RFC Editor, March 2003. Dostupné z: http://www.rfc-editor.org/rfc/rfc3501.txt.

[10] Crow, B. P., Widjaja, I., Kim, J. G. a Sakai, P. T. *Wirelesss LAN (802.11)*. First. Institute of Electrical & Electronics Enginee, 1997. ISBN 978-1-55937-935-9.

[11] Diffie, W. a Hellman, M. New directions in cryptography. *IEEE Transactions on Information Theory*. 1976, zv. 22, č. 6, s. 644–654. DOI: 10.1109/TIT.1976.1055638.

[12] Fluhrer, S., Mantin, I. a Shamir, A. Weaknesses in the Key Scheduling Algorithm of RC4. In: Vaudenay, S. a Youssef, A. M., ed. *Selected Areas in Cryptography*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, s. 1–24. ISBN 978-3-540-45537-0.

[13] Khorov, E., Kiryanov, A., Lyakhov, A. a Bianchi, G. A Tutorial on IEEE 802.11ax High Efficiency WLANs. *IEEE Communications Surveys Tutorials*. 2019, zv. 21, č. 1, s. 197–216. DOI: 10.1109/COMST.2018.2871099.

[14] Klensin, J. *Simple Mail Transfer Protocol* [Internet Requests for Comments]. RFC 5321. RFC Editor, October 2008. Dostupné z: http://www.rfc-editor.org/rfc/rfc5321.txt.

[15] Klusáček, J. *Automatizované útoky na WiFi sítě s nízkou detekovatelností a obrana proti nim*. Brno, CZ, 2021. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: https://www.fit.vut.cz/study/thesis/23797/.

[16] Kohlios, C. P. a Hayajneh, T. A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3. *Electronics*. 2018, zv. 7, č. 11. DOI: 10.3390/electronics7110284. ISSN 2079-9292. Dostupné z: https://www.mdpi.com/2079-9292/7/11/284.

[17] Lashkari, A. H., Mansoor, M. a Danesh, A. S. Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA). In: *2009 International Conference on Signal Processing Systems*. 2009, s. 445–449. DOI: 10.1109/ICSPS.2009.87.

[18] Lashkari, A. H., Towhidi, F. a Hosseini, R. S. Wired Equivalent Privacy (WEP). In: *2009 International Conference on Future Computer and Communication*. 2009, s. 492–495. DOI: 10.1109/ICFCC.2009.32.

[19] Liu, Y., Jin, Z. a Wang, Y. Survey on Security Scheme and Attacking Methods of WPA/WPA2. In: *2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*. 2010, s. 1–4. DOI: 10.1109/WICOM.2010.5601275.

[20] Malgaonkar, S., Patil, R., Rai, A. a Singh, A. Research on Wi-Fi Security Protocols. *International Journal of Computer Applications*. Apríl 2017, zv. 164, s. 30–36. DOI: 10.5120/ijca2017913601.

[21] Menezes, A., Oorschot, P. van a Vanstone, S. *Handbook of Applied Cryptography*. CRC Press, 2018. Discrete Mathematics and Its Applications. ISBN 9780429881329. Dostupné z: https://books.google.cz/books?id=YyCyDwAAQBAJ.

[22] Myers, J. *IMAP4 Authentication Mechanisms* [Internet Requests for Comments]. RFC 1731. RFC Editor, December 1994. Dostupné z: https://datatracker.ietf.org/doc/html/rfc1731.

[23] Myers, J. G. a Rose, M. T. *Post Office Protocol - Version 3* [Internet Requests for Comments]. STD 53. RFC Editor, May 1996. Dostupné z: http://www.rfc-editor.org/rfc/rfc1939.txt.

[24] Postel, J. a Reynolds, J. *File Transfer Protocol* [Internet Requests for Comments]. STD 9. RFC Editor, October 1985. Dostupné z: http://www.rfc-editor.org/rfc/rfc959.txt.

[25] Prasad, N. a Prasad, A. *802.11 WLANS and IP Networking: Security, QoS, and Mobility*. Artech, 2005. 1 s. Dostupné z: http://ieeexplore.ieee.org/document/9107165.

[26] Ronder, A. *The 4-way handshake WPA/WPA2 encryption protocol*. 2021. [Online; dostupné Duben 2022]. Dostupné z: https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64.

[27] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J. et al. *SIP: Session Initiation Protocol* [Internet Requests for Comments]. RFC 3261. RFC Editor, June 2002. Dostupné z: http://www.rfc-editor.org/rfc/rfc3261.txt.

[28] Steube, J. *New Attack on WPA/WPA2 Using PMKID*. 2018. [Online; dostupné Duben 2022]. Dostupné z: https://hashcat.net/forum/showthread.php?mode=threaded&tid=7717&pid=41427#pid41427.

[29] Taparia, A., Panigrahy, S. K. a Jena, S. K. Secure key exchange using enhanced Diffie-Hellman protocol based on string comparison. In: *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*. 2017, s. 722–726. DOI: 10.1109/WiSPNET.2017.8299856.

[30] Vanhoef, M. Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation. In: *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, August 2021, s. 161–178. ISBN 978-1-939133-24-3. Dostupné z: https://www.usenix.org/conference/usenixsecurity21/presentation/vanhoef.

[31] Vanhoef, M. a Piessens, F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In:. New York, NY, USA: Association for Computing Machinery, 2017, s. 1313–1328. CCS '17. DOI: 10.1145/3133956.3134027. ISBN 9781450349468. Dostupné z: https://doi.org/10.1145/3133956.3134027.

[32] Vanhoef, M. a Ronen, E. Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. In: *2020 IEEE Symposium on Security and Privacy (SP)*. 2020, s. 517–533. DOI: 10.1109/SP40000.2020.00031.

[33] Šopf, P. *Prolomení hesel do wi-fi*. Brno, CZ, 2020. Bakalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Dostupné z: https://www.fit.vut.cz/study/thesis/22769/.

[34] Výskumná skupina akcelerovaných sieťových technológií FIT VUT. *FlexProbe 10g Wiki*. 2022. [Online; dostupné Duben 2022]. Dostupné z: https://ant-dev.fit.vutbr.cz/redmine/projects/flexprobe/wiki.

[35] Zhang, L., Yu, J., Deng, Z. a Zhang, R. The security analysis of WPA encryption in wireless network. In: *2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*. 2012, s. 1563–1567. DOI: 10.1109/CECNet.2012.6202145.

Príloha A

Obsah priloženého pamäťového média

Súbor `readme.md` obsahuje popis inštalácie balíka na cieľovom zariadení, kde už je nainštalovaná aktuálna verzia sondy FlexProbe.

Zložka `rozsirenie/` obsahuje súbory z ktorých sa podľa postupu v `readme.md` dá vytvoriť inštalačný balík pre jednotliví časti sondy.

Zložka `testy/` obsahuje skripty na testovanie odpočúvaní. Každý skript obsahuje v nápovede informáciu o svojej funkcionalite.

Zložka `text/` obsahuje zdrojové súbory LaTex textu tejto práce.

Súbor `demo_video.mp4` obsahuje ukážku funkcionality programu od konfigurácie cez zachytenie a ukážku exportovaných dát.

```
CD-ROM
├── readme.md
├── demo_video.mp4
├── rozsirenie/
├── testy/
└── text/
```