

SLOVENSKÁ TECHNICKÁ UNIVERZITA V BRATISLAVE
FAKULTA INFORMATIKY A INFORMAČNÝCH TECHNOLOGIÍ

PETER BRENKUS

SLOVNÍKOVÉ A BRUTE-FORCE ÚTOKY NA HESLÁ OD WIFI SIETÍ

Predmet: Princípy informačnej bezpečnosti
Zodpovedný za predmet: Doc. Ing. Ladislav Hudec, CSc.
Cvičiaci: Ing. Norbert Varga

december 2024

Čestne vyhlasujem, že som túto prácu vypracoval samostatne, na základe konzultácií
a s použitím uvedenej literatúry.

V Bratislave, 1.12.2024

Peter Brenkus

Anotácia

Slovenská technická univerzita v Bratislave

FAKULTA INFORMATIKY A INFORMAČNÝCH TECHNOLOGIÍ

Autor:	Peter Brenkus
Predmet:	Princípy informačnej bezpečnosti
Zodpovedný za predmet:	Doc. Ing. Ladislav Hudec, CSc.
Cvičiaci:	Ing. Norbert Varga
december 2024	

Cieľom tejto práce je analyzovať a porovnať efektívnosť brute-force a slovníkových útokov pri prelomení hesiel WiFi sietí zabezpečených protokolom WPA2. Experimenty boli vykonané na vlastnej domácej sieti v súlade s legislatívnymi a etickými zásadami. Kvôli enormným časovým nárokom brute-force útokov na 8 a 9 miestne heslá bola táto metóda modifikovaná zúžením množiny znakov a využitím predpripravených permutácií. Slovníkové útoky boli testované s využitím databázy bežne používaných hesiel "rockyou.txt". Výsledky experimentov poskytujú náhľad na účinnosť oboch metód v rôznych scenároch, vykresľujú od čoho efektívnosť lámania hesiel závisí a zdôrazňujú dôležitosť výberu silných hesiel na zvýšenie bezpečnosti WiFi sietí.

Obsah

1	Úvod	1
2	Teoretická časť	1
2.1	História WiFi sietí	1
2.2	WPA2 autentifikácia	2
2.3	WPA3 autentifikácia	4
2.4	Techniky lámania hesiel	6
2.5	Voľne dostupné nástroje na lámanie hesiel	7
3	Praktická časť	8
3.1	Potrebné nástroje	8
3.2	Postup monitorovania sieťovej prevádzky	8
3.3	Stavba experimentu	10
3.4	Limitácie experimentu	11
3.5	Príprava experimentu	12
3.6	Vykonanie experimentu	13
3.7	Výsledky experimentu	15
4	Záver	16
4.1	Zhodnotenie výsledkov	16
4.2	Odporúčania pre zvýšenie bezpečnosti	20
	Literatúra	21

Zoznam obrázkov

1	Schéma four-way handshakeu v protokole WPA/WPA2.	3
2	Zjednodušená schéma WPA3 handshakeu.	4
3	Vytvorenie slovníka pre simuláciu brute-force útoku.	12
4	Zdrojový kód skriptu.	13
5	Výstup skriptu.	14
6	Graf časov a vyskúšaných možností pre brute-force útoky.	17
7	Graf časov pre vybrané heslá.	17
8	Graf vyskúšaných možností pre vybrané heslá.	18
9	Graf časov a vyskúšaných možností pre slovníkové útoky.	19

Tabuľka 1: Použité skratky

Skratka	Vysvetlenie
WEP	Wired Equivalent Privacy
WPA	WiFi Protected Access
WPA2	WiFi Protected Access 2
WPA3	WiFi Protected Access 3
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
AES	Advanced Encryption Standard
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
MIC	Message Integrity Code
SAE	Simultaneous Authentication of Equals
PE	Password Element
SS	Shared Secret
KCK	Key Confirmation key
MK	Master Key
MD5	Message Digest 5
SHA	Secure Hash Algorithm 1
SHA-256	Secure Hash Algorithm 256-bit

1 Úvod

WiFi siete predstavujú jeden z najrozšírenejších spôsobov bezdrôtového pripojenia k internetu. Vďaka svojej jednoduchosti, dostupnosti a nízkym nákladom sa stali neoddeliteľnou súčasťou domácností, podnikov a verejných priestorov. Táto technológia, založená na štandardoch IEEE 802.11, umožňuje používateľom pripojiť sa k internetu alebo lokálnym sieťam bez potreby fyzického kábla.

WiFi siete môžu byť verejné, teda voľne prístupné, alebo môžu byť zabezpečené heslom, ktoré slúži ako hlavný mechanizmus na ochranu siete pred neoprávneným prístupom. Mnohí používatelia predpokladajú, že ich sieť je vďaka heslu bezpečná, no v skutočnosti môže byť zabezpečenie často nedostatočné. Slabé alebo predvolené heslá, neaktualizovaný bezpečnostný protokol či nevedomé chyby používateľov môžu viesť k tomu, že útočník dokáže sieť pomerne jednoducho kompromitovať a získať neoprávnený prístup. To poukazuje na dôležitosť nielen správneho zabezpečenia, ale aj pochopenia potenciálnych rizík spojených s používaním WiFi sietí, ktorým sa táto práca venuje.

2 Teoretická časť

V tejto kapitole stručne prejdeme históriu WiFi sietí a ich bezpečnostných opatrení, pozrieme sa bližšie na WPA2 protokol a jeho slabiny, uvedieme opatrenia pre ošetrenie týchto slabín v najnovšom protokole WPA3 a predstavíme si nástroje potrebné na vykonanie útoku na WiFi sieť s protokolom WPA2 a prelomenie jej hesla.

2.1 História WiFi sietí

WiFi siete, ktoré sú založené na štandarde IEEE 802.11, sa od svojho vzniku stretávali s potrebou zaistiť bezpečné pripojenie pre používateľov. Prvým bezpečnostným protokolom, ktorý bol vyvinutý, bol WEP, zavedený v roku 1997. Tento protokol bol navrhnutý s cieľom poskytnúť bezpečnosť porovnateľnú s káblovými sieťami. WEP používa RC4 šifrovací algoritmus na šifrovanie dát a 40-bitový alebo 104-bitový šifrovací kľúč spolu s 24-bitovým inicializačným vektorom.[1–3] Napriek tomu, že bol WEP považovaný za dostatočný pre svoju dobu, jeho implementácia obsahovala závažné chyby, ktoré útočníkom umožňovali prelomenie ochrany v priebehu niekoľkých minút. Najväčšou slabinou WEP bol jeho statický inicializačný vektor, ktorý sa opakoval, čo útočníci dokázali efektívne využiť.[2, 4] Z týchto dôvodov bol WEP oficiálne označený za zastaraný a neodporúčaný v roku 2004.

V reakcii na nedostatky WEP bol v roku 2003 zavedený nový bezpečnostný protokol WPA. Tento protokol priniesol niekoľko vylepšení, najmä použitie TKIP, ktorý dynamicky generuje šifrovacie kľúče pre každú prenosovú reláciu, čím sa eliminuje problém

statických kľúčov jeho predchodcu.[3, 4] WPA tiež obsahoval mechanizmus na detekciu neoprávnených prístupových bodov, čím prispel k zvýšeniu bezpečnosti. Napriek tomu, že WPA bol výrazným zlepšením oproti WEP, bol len dočasným riešením, pretože už v čase jeho zavedenia sa aktívne pracovalo na štandarde WPA2, ktorý mal byť uvedený v krátkom časovom horizonte a priniesť ešte vyššiu úroveň zabezpečenia.

Definitívnym krokom k zvýšeniu bezpečnosti WiFi sietí bolo zavedenie protokolu WPA2 v roku 2004. WPA2 nahradil RC4 algoritmus pokročilejším šifrovaním AES, ktoré je dodnes považované za vysoko bezpečné. Okrem toho WPA2 používa protokol CCMP, ktorý poskytuje silnú ochranu integrity a dôvernosti dát. WPA2 sa stal štandardom pre bezpečné pripojenie na WiFi siete a je široko používaný dodnes. [2, 3, 5], Avšak aj tento protokol má svoje slabiny, najmä ak používatelia zvolia slabé heslá, ktoré môžu byť prelomené slovníkovým alebo brute force útokom. Keďže je dodnes bežne používaný a podporovaný, práve týmto slabinám sa budeme v tejto práci ďalej venovať.

Najnovšou generáciou bezpečnostných protokolov je WPA3, predstavený v roku 2018. WPA3 priniesol niekoľko významných vylepšení v oblasti bezpečnosti, ktoré reagovali na slabiny WPA2. Jedným z kľúčových prvkov WPA3 je použitie protokolu SAE namiesto tradičného PSK. SAE poskytuje ochranu proti útokom založeným na zachytení dátového prenosu, pretože heslá už nie je možné odvodiť zo zachytených handshakeov. Okrem toho WPA3 zlepšil ochranu pre IoT zariadenia a zaviedol mechanizmy na ochranu siete pred útokmi brute force, ktoré obmedzujú počet pokusov o zadanie hesla.[1, 3]

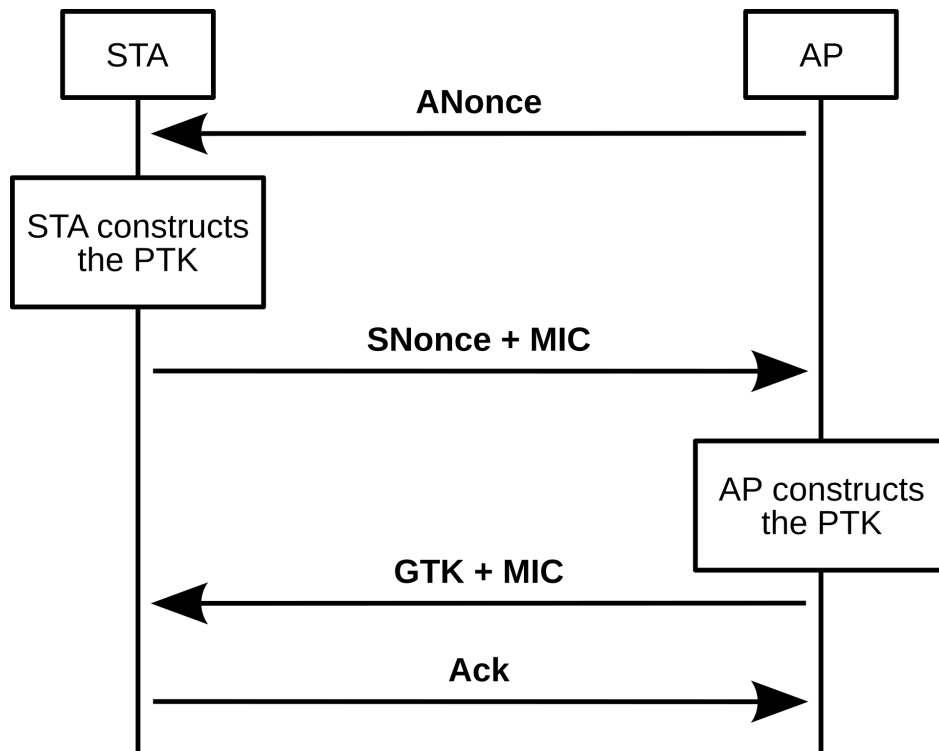
Vývoj bezpečnostných protokolov pre WiFi siete odráža neustále sa meniace výzvy v oblasti kybernetickej bezpečnosti. Od zlyhaní WEP cez dočasné riešenie WPA až po robustný WPA3 je zrejmé, že bezpečnosť WiFi sietí sa musí neustále prispôbovať novým hrozbám a požiadavkám používateľov.

2.2 WPA2 autentifikácia

WPA2 bol predstavený ako významné vylepšenie oproti starším protokolom WEP a WPA. Vďaka použitiu šifrovania AES a protokolu CCMP poskytuje silnú ochranu dát a integritu komunikácie. Tento protokol sa stal štandardom pre zabezpečenie WiFi sietí a dodnes je široko využívaný.[5] Napriek tomu však WPA2 nie je neprelomiteľné. Slabiny sa nachádzajú najmä v spôsobe, akým sa vykonáva autentifikácia. V tejto podkapitole sa zameriame na jeden z najzraniteľnejších aspektov WPA2 – proces tzv. four-way handshake.

Keď sa zariadenie (klient) pokúša pripojiť k zabezpečenej WiFi sieti, WPA2 používa mechanizmus four-way handshake na overenie, či zariadenie a prístupový bod (router) zdieľajú rovnaké heslo. Tento proces umožňuje výmenu šifrovacích kľúčov bez toho, aby

bolo samotné heslo odhalené počas prenosu a je rovnaký ako v protokole WPA.[1, 4]



Obr. 1: Schéma four-way handshakeu v protokole WPA/WPA2.

Handshake prebieha v štyroch krokoch:

1. Inicializácia handshake: Prístupový bod (AP) posiela klientovi náhodné číslo (nonce) známe ako ANonce.

2. Odpoveď klienta: Klient na základe prijatého ANonce vygeneruje vlastné náhodné číslo SNonce a použije ho spolu s heslom PSK na výpočet PTK. Kľúč PTK slúži na šifrovanie komunikácie. Klient odošle svoje SNonce späť prístupovému bodu.

3. Overenie klienta: Prístupový bod vypočíta PTK pomocou hesla, ANonce a SNonce, a odošle klientovi správu s MIC, ktorú môže klient použiť na overenie správnosti kľúča.

4. Ukončenie handshake: Klient potvrdí prijatie správneho kľúča a obe strany začnú šifrovanú komunikáciu.

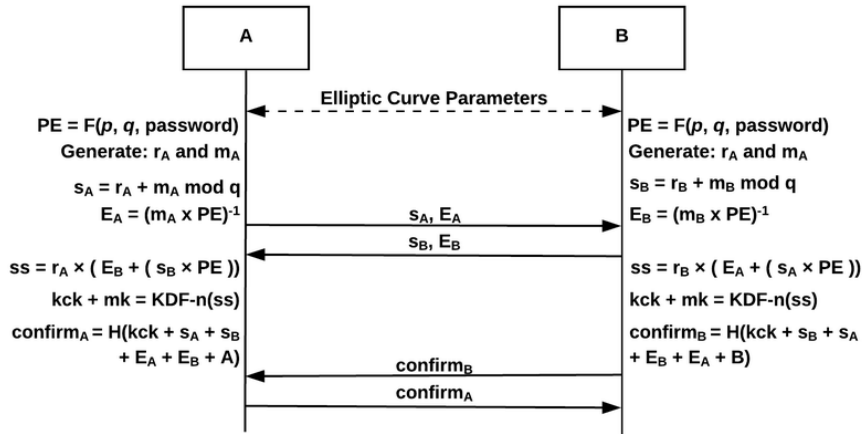
Slabiny WPA2 handshakeu

Aj keď WPA2 pri pripojení klienta samotné heslo neprenáša, implementácia four-way handshakeu obsahuje závažnú slabinu, ktorá môže byť zneužitá útočníkom. Proces propojenia môže byť totiž zachytený útočníkom, ktorý sa nachádza v dosahu siete. Útočník môže dokonca vynútiť handshake tým, že pošle deautentifikačné pakety, čím zariadenia odpojí od siete a donúti ich znovu sa pripojiť.[4]

Keď útočník takto zachytí handshake, môže spustiť off-line útok na heslo. Zachytené údaje sú totiž postačujúce na výpočet všetkých možných hesiel, kým sa nenájde správne heslo. Tento proces je obzvlášť efektívny, ak používateľ zvolil slabé alebo krátke heslo. Pomocou rôznych známych techník lámania hesiel môže útočník získať prístup do siete bez potreby ďalšej interakcie so zariadením.

2.3 WPA3 autentifikácia

Na rozdiel od WPA2, WPA3 používa nový mechanizmus autentifikácie s názvom SAE. SAE eliminuje zraniteľnosti handshakeu WPA2 tým, že namiesto tradičných PSK autentifikácií využíva princípy výmeny kľúčov pomocou eliptických kriviek. Tento proces zaisťuje, že heslá nie sú nikdy priamo prenášané cez sieť ani neexistuje možnosť ich odvodenia zo zachytených dát. Na obrázku nižšie je uvedená schéma tohto procesu.[1, 3]



Obr. 2: Zjednodušená schéma WPA3 handshakeu.

Krok 1: Inicializácia parametrov

Každé zariadenie (označené ako A a B) si vygeneruje svoje vlastné náhodné hodnoty:

• Zariadenie A:

- Generuje náhodnú hodnotu r_A a výpočet m_A .
- Spočíta $s_A = r_A + m_A \bmod q$, kde q je veľkosť skupiny eliptickej krivky.
- Vypočíta inverzný prvok $E_A = (m_A \times PE)^{-1}$, kde PE je odvodený z hesla pomocou funkcie $F(p, q, \text{password})$, ktorá mapuje heslo na bod na eliptickej krivke.

- **Zariadenie B:**

- Podobne ako A, generuje r_B , m_B , s_B , a E_B .

Obidve zariadenia si následne vymenia svoje hodnoty s_A , E_A a s_B , E_B .

Krok 2: Výpočet spoločného tajomstva

Po výmene parametrov obe zariadenia vypočítajú spoločné tajomstvo SS :

- **Zariadenie A:**

$$ss = r_A \times (E_B + (s_B \times PE))$$

- **Zariadenie B:**

$$ss = r_B \times (E_A + (s_A \times PE))$$

Týmto spôsobom obe zariadenia získajú rovnakú hodnotu ss bez toho, aby museli priamo preniesť svoje heslá alebo iné citlivé informácie.

Krok 3: Generovanie kľúčov

Zdieľané tajomstvo ss sa použije na odvodenie kľúčov:

- **Kľúčové komponenty:** KCK a MK sú generované pomocou Key Derivation Function $KDF-n(ss)$.

Krok 4: Potvrdenie autentifikácie

Každé zariadenie vyšle druhému autentifikačné potvrdenie ($confirm_A$ a $confirm_B$), ktoré obsahuje:

$$confirm = H(kck + s_A + s_B + E_A + E_B + device)$$

Tieto potvrdenia zabezpečujú, že komunikácia medzi zariadeniami bola úspešne autentifikovaná a že obe strany majú rovnaké kľúče.

Výhody SAE Handshake

- **Ochrana hesla:** Heslo nie je nikdy prenášané v akejkoľvek podobe, čo eliminuje možnosť jeho zachytenia.
- **Odolnosť voči offline útokom:** Použitie eliptických kriviek a SAE zabezpečuje, že útočník nemôže vykonať offline útok na zachytené údaje.

2.4 Techniky lámania hesiel

Proces lámania hesiel je založený na pokusoch o nájdenie správnej kombinácie znakov, ktorá zodpovedá zachyteným autentifikačným údajom. Úspešnosť útoku závisí od použitej techniky, výpočtového výkonu a zložitosti samotného hesla. Medzi najčastejšie používané techniky lámania hesiel patria:

- Slovníkový útok
- Brute force útok
- Hybridný útok
- Rainbow tabuľky

Slovníkový útok je jednou z najznámejších a najpoužívanějších metód lámania hesiel. Pri tomto útoku sa využíva preddefinovaný zoznam (slovník) bežne používaných hesiel, ktorý útočník postupne porovnáva so zachytenými údajmi z handshake. Slovníkové útoky sú účinné najmä proti slabým heslám, ktoré sú jednoduché, krátke alebo bežne používané (napr. "12345678", "password"). Úspešnosť tejto metódy závisí od kvality a veľkosti použitého slovníka. Táto metóda však zlyháva, ak je heslo dostatočne dlhé, komplexné alebo nie je bežne používané.[6]

Brute force útok, alebo útok hrubou silou, je technika, pri ktorej útočník postupne skúša všetky možné kombinácie znakov, kým nenájde správne heslo. Táto metóda garantuje prelomenie hesla, pokiaľ útočník disponuje dostatočným výpočtovým výkonom a časom. Brute force útok je však výrazne náročný pri komplexných a dlhých heslách. Napríklad, ak je heslo dlhé 8 znakov a obsahuje malé a veľké písmená, čísla a špeciálne znaky, počet možných kombinácií sa pohybuje v miliardách. Úspešnosť brute force útoku je preto závislá od zložitosti hesla a výpočtovej sily dostupného hardvéru.[6]

Rainbow tabuľky sú predgenerované tabuľky hashov, ktoré umožňujú útočníkom rýchlo overiť zhodu medzi hashmi a potenciálnymi heslami. Táto metóda je efektívna najmä v prípadoch, keď útočník má prístup k veľkému množstvu dát a času na ich predgenerovanie. Pri WPA2 sa však rainbow tabuľky stávajú menej praktickými, pretože handshake obsahuje unikátne náhodné hodnoty (nonce), ktoré bránia opakovanej použiteľnosti predgenerovaných hashov.[6]

Hybridný útok kombinuje prvky slovníkového a brute force útoku. Namiesto generovania všetkých možných kombinácií znakov útočník použije základný slovník hesiel a aplikuje naň pravidlá, ktoré pridávajú, modifikujú alebo kombinujú znaky. Napríklad heslo password môže byť testované aj ako Password123 alebo p@ssw0rd. Hybridné útoky sú účinné, ak používatelia vytvárajú heslá založené na známych vzoroch s malými úpravami.[6]

Okrem vyššie spomenutých techník útočníci používajú na zistenie hesiel aj ďalšie spôsoby, ako phishing alebo sociálne inžinierstvo. Vzhľadom na to, že tieto metódy sú postavené na podvodoch či manipulácii, a nie na technikách lámania hesiel, sú mimo zámeru tejto práce.[6]

2.5 Voľne dostupné nástroje na lámanie hesiel

Vďaka širokej dostupnosti open-source nástrojov sú techniky lámania hesiel voľne dostupné každému, kto má počítač. Medzi najznámejšie bežne používané nástroje patria John the Ripper, Hashcat a Aircrack-ng, ktoré poskytujú efektívne možnosti pre analýzu hesiel a testovanie bezpečnosti sietí.

John the Ripper je jeden z najpopulárnejších nástrojov na prelomenie hesiel, ktorý sa používa na testovanie ich odolnosti. Tento nástroj dokáže pracovať s rôznymi typmi hashov a šifrovaní, vrátane hesiel operačných systémov, súborových systémov a ďalších. Podporuje slovníkové útoky, brute force útoky aj hybridné útoky. Je vysoko konfigurovateľný, čo umožňuje používateľovi definovať pravidlá, ktoré prispôbia generovanie hesiel na základe špecifických potrieb. Vďaka jeho efektívnosti a možnosti paralelného spracovania je vhodný na použitie na bežnom hardvéri aj v profesionálnych prostrediach. John the Ripper je dostupný ako open-source a je aktívne udržiavaný komunitou, čo zaručuje pravidelné aktualizácie a rozšírenia.[7]

Hashcat je ďalší výkonný nástroj na prelomenie hesiel, ktorý sa špecializuje na rýchlu analýzu hashov. Na rozdiel od Johna the Rippera je Hashcat optimalizovaný na využitie grafických kariet, čo dramaticky zvyšuje jeho výpočtový výkon. Hashcat podporuje tisíce algoritmov hashovania vrátane MD5, SHA-1, SHA-256, bcrypt, a WPA2 handshake. Podobne ako John the Ripper, aj Hashcat umožňuje vykonávať slovníkové útoky, brute force útoky a hybridné útoky. Hashcat je často využívaný bezpečnostnými špecialistami na analýzu hesiel vo veľkých dátových súboroch a jeho podpora hardvérovej akcelerácie ho robí jedným z najrýchlejších nástrojov v tejto oblasti.[8]

Aircrack-ng je balík nástrojov špeciálne navrhnutý na testovanie bezpečnosti bezdrôtových sietí. Aircrack-ng umožňuje zachytávať dátový prenos v sieti, analyzovať pakety a vykonávať útoky na heslá WiFi sietí chránených WEP, WPA alebo WPA2.[9]

Najdôležitejšou funkciou Aircrack-ng je schopnosť zachytiť WPA/WPA2 handshake, čo je kľúčový krok pri lámaní hesiel zabezpečených WiFi sietí. Po zachytení handshakeu je možné použiť slovníkový útok na prelomenie hesla. Okrem toho Aircrack-ng obsahuje nástroje na vynútenie deautentifikácie klientov zo siete, čo umožňuje simulovať nové pripojenie a získať handshake rýchlejšie. Tento nástroj sa stal štandardom pri testovaní bezpečnosti WiFi sietí a je široko používaný komunitou etických hackerov aj profesionálnych testerov bezpečnosti.

3 Praktická časť

V tejto kapitole sa budeme venovať lámaniu hesiel od WiFi sietí zabezpečených pomocou WPA/WPA2 protokolu. Prejdeme si hardvérové aj softvérové nástroje potrebné na vykonanie útoku na sieť, postup monitorovania sieťovej prevádzky, postup, stavbu a limitácie experimentu, automatizáciu a uvidíme výsledky.

3.1 Potrebné nástroje

Ako sme už spomenuli v predošlej kapitole, na rozlúsknutie hesla od WiFi siete zabezpečenej cez WPA/WPA2 je potrebné najprv zachytiť handshake. Z toho vyplývajú dve základné požiadavky:

1. Útočník musí byť schopný zachytávať sieťovú prevádzku
2. Útočník musí byť v dosahu cieľovej WiFi siete

Schopnosť zachytávať sieťovú prevádzku, tzv. monitorovací režim, nie je bežnou vlastnosťou WiFi kariet zabudovaných v notebookoch alebo stolných počítačoch. Tento režim vyžaduje špeciálny hardvér – externý WiFi adaptér s vnútorným čipom usporiadaným na túto úlohu. Pre účely experimentu bol použitý externý WiFi adaptér Alfa AWUS036NHA s čipom Atheros AR9271.

Okrem hardvéru sú potrebné aj softvérové nástroje, ktoré umožňujú ovládať špecifické funkcie WiFi adaptéra. Softvér zohráva kľúčovú úlohu pri zachytávaní dátovej prevádzky, analyzovaní získaných údajov a následnom vykonávaní útoku. Pre účely experimentu bola použitá špecializovaná linuxová distribúcia Kali Linux, ktorá je určená pre penetračné testovanie a bezpečnostné analýzy. Táto distribúcia obsahuje širokú škálu predinštalovaných nástrojov, potrebných na analýzu a testovanie bezpečnosti WiFi sietí, na experiment boli použité nástroje z balíka Aircrack-ng.

3.2 Postup monitorovania sieťovej prevádzky

Monitorovanie sieťovej prevádzky je kľúčovým krokom pri analýze bezpečnosti WiFi sietí. Tento proces zahŕňa zachytávanie dát prenášaných medzi zariadeniami v sieti, čo umožňuje identifikovať potenciálne zraniteľnosti, ako aj zachytiť handshake potrebný na prelomenie hesla. Nasledujúci postup opisuje kroky, ktoré boli vykonané počas experimentu.

Príprava na monitorovací režim

Pred prechodom WiFi adaptéra do monitorovacieho režimu je potrebné vypnúť všetky procesy, ktoré by mohli rušiť experiment alebo blokovat používanie adaptéra v tomto režime. Na tento účel bol použitý príkaz:

```
airmon-ng check kill
```

Tento príkaz identifikuje a ukončí procesy, ktoré by mohli rušiť prácu nástrojov ako Airmon-ng alebo Airodump-ng. Typicky ide o služby spravujúce bezdrôtové pripojenie, napríklad NetworkManager. Po ukončení týchto procesov je adaptér pripravený na prechod do monitorovacieho režimu.

Prechod do monitorovacieho režimu

Následovný krok je prechod WiFi adaptéra do tzv. monitorovacieho režimu, ktorý umožňuje zachytávanie všetkej sieťovej prevádzky v dosahu adaptéra, vrátane paketov, ktoré nie sú priamo adresované zariadeniu útočníka. Na tento účel bol použitý nástroj Airmon-ng, ktorý je súčasťou balíka Aircrack-ng.

```
airmon-ng start wlan1
```

Týmto príkazom bol WiFi adaptér prepnutý do monitorovacieho režimu, pričom wlan[číslo] predstavuje názov sieťového rozhrania. V prípade úspešného prechodu sa v systéme vytvorí nové rozhranie, zvyčajne označené ako wlan[číslo]mon.

Identifikácia cieľovej siete

Po aktivovaní monitorovacieho režimu je potrebné identifikovať cieľovú WiFi sieť. Na tento účel bol použitý nástroj Airodump-ng, ktorý poskytuje prehľad všetkých sietí v dosahu adaptéra.

```
airodump-ng wlan1mon
```

Tento príkaz zobrazí zoznam sietí vrátane SSID (názvu siete), MAC adresy prístupového bodu (BSSID), použitých bezpečnostných protokolov a kanálu siete. Po identifikovaní cieľovej siete bola zvolená konkrétna sieť na ďalšiu analýzu. Samozrejme pre účely tohto experimentu som pracoval so svojou domácou sieťou, inak by to bolo nelegálne.

Zachytávanie dátovej prevádzky

Na zachytávanie paketov v cieľovej sieti opäť slúži nástroj Airodump-ng. Tento nástroj umožňuje filtrovanie paketov na základe BSSID cieľovej siete a kanála, na ktorom sieť operuje.

```
airodump-ng -c [kanál] --bssid [BSSID] -w [súbor] wlan1mon
```

Uvedený príkaz berie tieto argumenty:

- `-c [kanál]` – špecifikuje kanál cieľovej siete, napríklad 3
- `-bssid [BSSID]` – MAC adresa prístupového bodu.
- `-w [súbor]` – názov súboru, do ktorého sa budú ukladať zachytené pakety.

Tento krok umožňuje priebežné ukladanie sieťovej prevádzky na analýzu a zároveň zachytenie handshakeu potrebného pre ďalšie kroky. Príkaz má kontinuálny výstup do konzoly, ktorý blokuje zadávanie ďalších príkazov používateľom a ukončuje sa stlačením kombinácie klávesov `Ctrl + C` (táto kombinácia odošle procesu signál `SIGINT`, čím sa proces preruší). Po detekovaní WPA/WPA2 handshakeu v dátovej prevádzke sa táto udalosť zobrazí priamo vo výstupe príkazového riadku.

Je potrebné spomenúť, že počas experimentu nebola využitá funkcia na injektovanie paketov do siete, keďže nebolo potrebné odosielať deautentifikačné pakety. Vzhľadom na to, že experiment prebiehal na mojej domácej sieti, jednoducho som zariadenie manuálne odpojil a následne znovu pripojil, vďaka čomu prebehol potrebný handshake.

3.3 Stavba experimentu

Experiment bol navrhnutý tak, aby simuloval realistické scenáre prelomenia hesiel WiFi sietí a zároveň poskytol merateľné údaje o efektivite slovníkových a brute-force útokov. Testované boli štyri rôzne druhy hesiel, pričom pre každý druh boli vytvorené tri rôzne inštancie. Týmto spôsobom bolo možné analyzovať, ako rôzne typy a variácie hesiel ovplyvňujú čas potrebný na ich prelomenie a úspešnosť zvolených metód útoku.

Typy hesiel použité v experimente:

1. Náhodné heslo (8 miest) – Heslo generované náhodne, obsahujúce malé a veľké písmená a čísla. Tento typ hesla je zameraný na vyzdvihnutie brute-force útoku.
2. Slovníkové heslo (8 miest) – Heslo vybrané zo známeho slovníka `rockyou.txt`, ktorý obsahuje veľkú databázu bežne používaných hesiel. Toto heslo je zamerané na vyzdvihnutie slovníkového útoku.
3. Náhodné heslo (9 miest) – Rovnaký princíp ako pri 8-miestnom náhodnom hesle, avšak s vyšším počtom znakov, čo zvyšuje zložitosť útoku.
4. Slovníkové heslo (9 miest) – Rovnaký princíp ako pri 8-miestnom slovníkovom hesle, avšak s vyšším počtom znakov, čo zvyšuje zložitosť útoku.

Každé z dvanástich testovaných hesiel bolo podrobené obom typom útokov, slovníkovému aj brute-force. Pre každý útok bol zaznamenaný čas a počet vyskúšaných možností, pričom v prípade neúspešného pokusu bol čas označený ako `-`.

3.4 Limitácie experimentu

Dĺžky hesiel testovaných v tomto experimente boli podmienené obmedzeniami môjho routera, ktorý podporuje minimálne 8-miestne heslá. Aby som pokryl viac rôznych dĺžiek hesiel a otestoval ich vplyv na čas potrebný na prelomenie, musel som testovať heslá s dĺžkou 8 a 9 znakov.

Tento prístup však prináša problém pri brute-force útokoch. Počet všetkých možných permutácií hesiel je exponenciálne závislý od dĺžky hesla a veľkosti množiny povolených znakov. Pre heslá obsahujúce malé a veľké písmená, číslice a špeciálne znaky je veľkosť množiny povolených znakov 94. Na základe výpočtov:

- Pre 8-miestne heslo je možné vytvoriť $94^8 = 6,095,689,385,410,816$ rôznych kombinácií.
- Pre 9-miestne heslo je možné vytvoriť $94^9 = 572,994,802,228,616,704$ rôznych kombinácií.

Počet možných kombinácií je tak obrovský, že na mojom hardvéri by úplné vyčerpanie všetkých možností pomocou brute-force útoku trvalo nereálne dlhý čas. Pri mojej rýchlosti spracovania ≈ 10000 hesiel za sekundu by pre 9-miestne heslo, ak by skutočná kombinácia bola posledná v množine, útok trval približne 1,8 milióna rokov. Navyše, vytvorenie a uloženie slovníka s takýmto množstvom hesiel by ďaleko presahovalo kapacitu môjho disku.

Na vyriešenie tejto výzvy som namiesto čistého brute-force útoku použil slovníkový útok, ktorý sa k brute-force útoku len približuje. Optimalizácie vykonané na zníženie počtu kombinácií boli nasledovné:

- Obmedzenie množiny znakov: Množinu možných znakov som zúžil na malé a veľké písmená a číslice, čím som znížil veľkosť množiny z pôvodných 94 znakov na 62 znakov (26 malých písmen + 26 veľkých písmen + 10 číslic). Táto redukcia dramaticky znížila počet možných permutácií.
- Generovanie permutácií znakov hesla: Vzhľadom na to, že som poznal testované heslá, použil som príkaz `crunch` na generovanie všetkých možných permutácií znakov konkrétneho hesla. Napríklad, pre heslo `mtpqb7Dv` som vytvoril slovník obsahujúci všetky možné permutácie jeho znakov.

```
(kali@kali)-[~]  
$ crunch 8 8 v7bqtmpD -o 8random-01.txt  
Crunch will now generate the following amount of data: 150994944 bytes  
144 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 16777216  
  
crunch: 100% completed generating output
```

Obr. 3: Vytvorenie slovníka pre simuláciu brute-force útoku.

- Zavedenie opakovania znakov: Pri 9-miestnych heslách som zaviedol mierne opakovanie znakov, aby som znížil počet permutácií. Ak by heslo obsahovalo výlučne unikátne znaky, množstvo kombinácií by bolo stále príliš vysoké.
- Oddelenie procesov: Generovanie slovníkov som oddelil od samotného procesu prelomenia hesla. Týmto spôsobom čas potrebný na vytvorenie permutácií neovplyvnil čas potrebný na samotné prelomenie hesla.

Týmito opatreniami som zabezpečil, že experiment sa uskutočnil v časovo zvládnu-teľných rámcoch, pričom bol zameraný na získanie praktických poznatkov o efektívite brute-force a slovníkových útokov. Hoci experiment zjednodušoval niektoré aspekty reálnych podmienok, poskytol cenné údaje pre základné pochopenie problematiky pre-lomenia hesiel.

3.5 Príprava experimentu

Každé z hesiel použitých v experimente si vyžadovalo vykonanie presne definova-ných krokov, aby bolo možné získať potrebné dáta na testovanie efektivity útokov. Príprava pre každé heslo zahŕňala následovné činnosti:

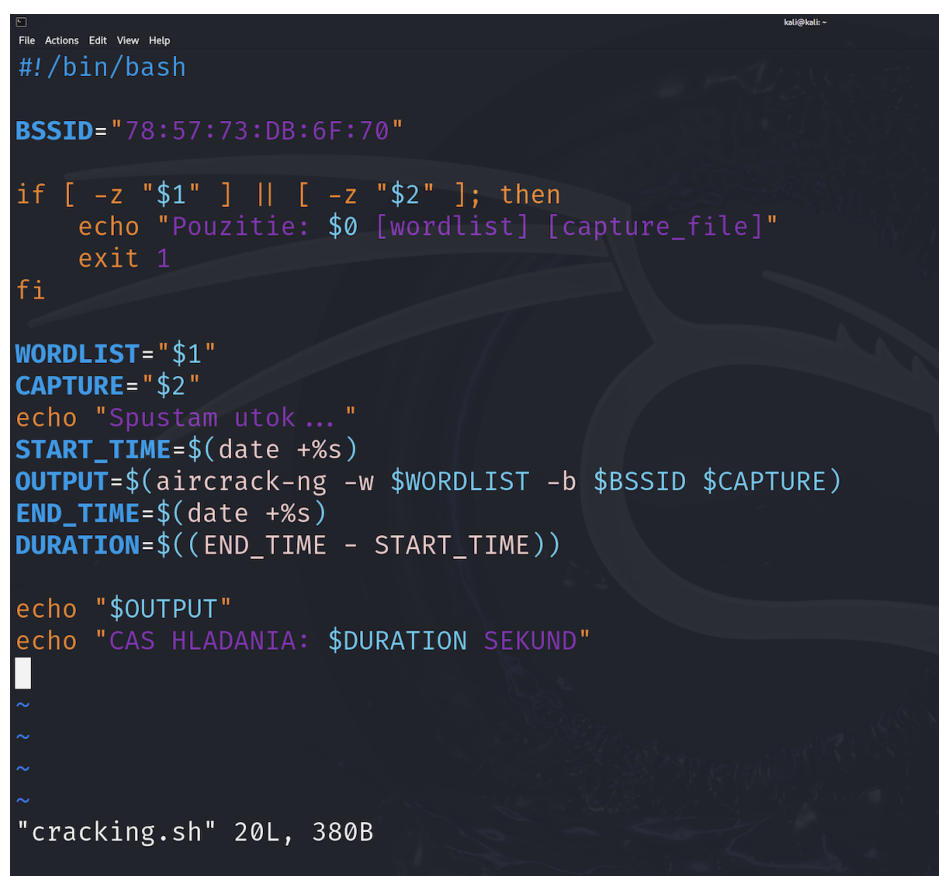
1. Zmena hesla WiFi siete: Pre každé z hesiel som musel manuálne zmeniť heslo na svojom WiFi routeri. Toto zabezpečilo, že testované heslo bolo aktuálne použité na zabezpečenie siete.
2. Začatie zachytávania dátovej prevádzky: Pomocou nástroja **Airodump-ng** som spustil proces zachytávania dátovej prevádzky na príslušnej WiFi sieti. Tento krok bol potrebný na prípravu na zachytenie WPA2 handshake.
3. Odpojenie a znovupripojenie zariadenia: Po začatí zachytávania dát som svoje zariadenie (stolný počítač) odpojil od WiFi siete a následne ho znovu pripojil. Tento krok bol nevyhnutný na generovanie WPA2 handshake, ktorý je kľúčový pre testovanie útokov.

4. Zachytenie handshake: Po opätovnom pripojení zariadenia som zachytil WPA2 handshake pomocou nástroja **Airodump-ng**. Zachytené dáta som uložil do súboru s príponou **.pcap**, ktorý slúži ako vstupný súbor pre ďalšie kroky analýzy a testovania.
5. Príprava "brute force" slovníkov: Pre náhodne generované heslá som vytvoril špecifické slovníky na vykonanie brute-force simulácie, tak ako je to opísané v predošlej podkapitole.

Tieto kroky som vykonal pre každé z dvanástich testovaných hesiel, pričom všetky získané **.pcap** súbory a generované slovníky boli organizované a pripravené na nasledujúcu fázu experimentu, ktorá zahŕňala samotné lámanie.

3.6 Vykonanie experimentu

Na automatizáciu prelomenia hesiel som vytvoril Bash skript, ktorého zdrojový kód je uvedený na priloženom obrázku nižšie. Skript zjednodušuje proces útoku na heslo pomocou nástroja **aircrack-ng**, pričom vypisuje čas potrebný na prelomenie hesla aj výstup príkazu o úspešnosti prelomenia hesla.



```
#!/bin/bash

BSSID="78:57:73:DB:6F:70"

if [ -z "$1" ] || [ -z "$2" ]; then
    echo "Použitie: $0 [wordlist] [capture_file]"
    exit 1
fi

WORDLIST="$1"
CAPTURE="$2"
echo "Spustam utok ..."
START_TIME=$(date +%s)
OUTPUT=$(aircrack-ng -w $WORDLIST -b $BSSID $CAPTURE)
END_TIME=$(date +%s)
DURATION=$((END_TIME - START_TIME))

echo "$OUTPUT"
echo "CAS HLADANIA: $DURATION SEKUND"

~
~
~
~

"cracking.sh" 20L, 380B
```

Obr. 4: Zdrojový kód skriptu.

Popis a použitie skriptu

Skript prijíma dva vstupné parametre. Prvým je slovník hesiel, respektíve cesta k súboru obsahujúcemu zoznam hesiel na vykonanie útoku. Druhým je súbor vo formáte .pcap, ktorý obsahuje zachytené dáta z WPA/WPA2 handshakeom.

Výstup skriptu

Výstup skriptu poskytuje prehľad o priebehu útoku a jeho výsledkoch. Zobrazuje kľúčové informácie, ako počet testovaných kombinácií, rýchlosť spracovania, celkový čas hľadania, odhadovaný zostávajúci čas a konečný výsledok. Okrem toho obsahuje aj technické detaily o generovaných kľúčoch a parametroch spojených s WPA2 handshake. Na obrázku nižšie je uvedený ukážkový výstup pre jedno z testovaných hesiel.

```
Aircrack-ng 1.7

[00:30:32] 19527168/40353607 keys tested (10491.76 k/s)

Time left: 33 minutes, 5 seconds                                48.39%

KEY FOUND! [ capricorn ]

Master Key      : F4 39 F1 6F 17 B0 9E 26 25 ED 70 17 AD B1 5B F8
                  FF C2 AC EE F2 29 17 6E 9F B6 3F 1A E2 FA 68 DB

Transient Key   : 49 84 9B 88 97 D8 81 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC      : FE 96 EF F8 82 22 2B 1E 8F 36 14 5D 66 2E 40 A6

CAS HLADANIA: 1861 SEKUND
```

Obr. 5: Výstup skriptu.

Praktické využitie v experimente

Tento skript som použil pre každé testované heslo v rámci experimentu. Pre slovníkové heslá som použil predom pripravený slovník `rockyou.txt` a pre náhodné heslá som použil vlastné generované slovníky s permutáciami znakov hesla. Výsledné časy prelomenia hesla, prípadne informácia o neúspechu (-), boli následne zaznamenané do excelovej tabuľky. Automatizácia pomocou skriptu výrazne zjednodušila proces a umožnila zamerať sa na analýzu výsledkov.

Testované heslá

Nižšie je uvedená tabuľka so zoznamom testovaných hesiel spolu s ich typom (dĺžka a druh hesla):

Heslo	Typ hesla
mtpqb7Dv	8-miestne náhodné
H7Dk2PqX	8-miestne náhodné
P3xL1aN2	8-miestne náhodné
williams	8-miestne slovníkové
grabass1	8-miestne slovníkové
FIANCE22	8-miestne slovníkové
mtpvb7Dvm	9-miestne náhodné
W4Xn7Xk7B	9-miestne náhodné
P8Rm2L8Z	9-miestne náhodné
capricorn	9-miestne slovníkové
grabapunk	9-miestne slovníkové
kaitlynn4	9-miestne slovníkové

Tabuľka 2: Zoznam testovaných hesiel a ich typov.

3.7 Výsledky experimentu

Nižšie uvedená tabuľka obsahuje výsledky experimentu, kde pre každé heslo je čas potrebný na prelomenie pomocou brute-force a slovníkového útoku zaznamenaný v sekundách. Hodnoty - označujú, že útok bol neúspešný, čiže nenašiel správne heslo. Stĺpec # Možností zaznamenáva koľko rôznych možností bolo vyskúšaných.

Heslo	Brute-force		Slovníkový	
	Čas (s)	# Možností	Čas (s)	# Možností
mtpqb7Dv	1130	11,862,552	-	14,344,392
williams	155	1,665,864	0.1	798
mtpvb7Dvm	2483	26,014,504	-	14,344,392
capricorn	1861	19,527,168	0.1	786
H7Dk2PqX	875	9,209,584	-	14,344,392
grabass1	79	900,880	739	7,772,495
W4Xn7Xk7B	3642	38,144,952	-	14,344,392
grabapunk	9295	97,196,856	740	7,799,457
P3xL1aN2	1254	13,086,228	-	14,344,392
FIANCE22	276	2,970,896	1054	11,080,387

P8Rm2L8Z	1360	14,275,112	-	14,344,392
kaitlynn4	9247	96,704,920	633	6,598,420

Tabuľka 3: Výsledky experimentu.

4 Záver

V tejto kapitole zhodnotíme výsledky získané počas experimentu a poskytneme odporúčania pre zvýšenie bezpečnosti hesiel WiFi sietí na základe zistených informácií.

4.1 Zhodnotenie výsledkov

Výsledky experimentu ukazujú rôzne úrovne efektivity brute-force a slovníkových útokov pri prelomení hesiel rôznej dĺžky a zložitosti. Na základe zozbieraných údajov je možné identifikovať niekoľko dôležitých poznatkov.

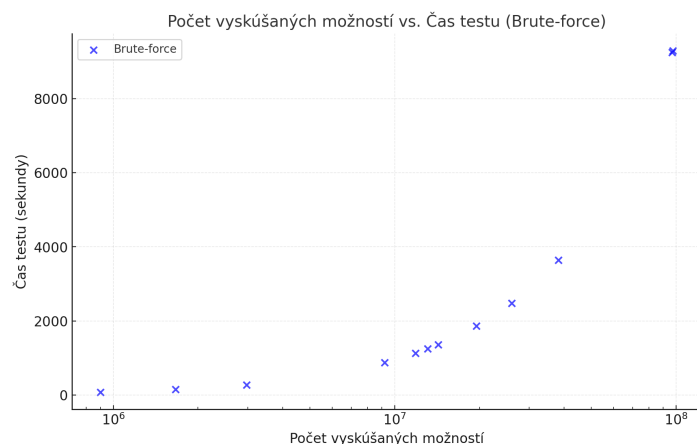
Brute-force útoky

Počet vyskúšaných možností mal zásadný vplyv na čas potrebný na prelomenie hesiel touto metódou. S narastajúcim počtom možností, ktoré boli testované sa predlžoval čas trvania testu, pričom najkratší test bol vykonaný na hesle „grabass1“, kde brute-force útok prešiel 900,880 možnosťami a trval iba 79 sekúnd. Na druhú stranu najdlhší test bol brute-force útok na heslo „grabapunk“, kde bolo testovaných 97,196,856 možností a proces trval až 9,295 sekúnd, čo predstavuje 2 hodiny, 34 minút a 55 sekúnd.

Obrovský rozdiel medzi týmito dvoma testami vyzdvihuje význam zložitosti hesla a veľkosti vyhľadávacieho priestoru na čas potrebný na prelomenie hesla. Testy ukazujú, že efektívnosť útoku je úzko spätá s kombináciou dĺžky a zložitosti hesla.

Grafické zobrazenie

Na grafe na obrázku 5 je možné vidieť vzťah medzi počtom vyskúšaných možností na osi x a časom testu v sekundách na osi y pre brute-force testy. Je vidieť významnú koreláciu medzi rastom dĺžky vykonania testu a rastom počtu vyskúšaných možností.



Obr. 6: Graf časov a vyskúšaných možností pre brute-force útoky.

Na presnejšiu analýzu tohto vzťahu treba ešte odizolovať jednu premennú, a to vyhľadávací priestor. Keďže rôzne heslá v mojich testoch mali rôzne dĺžky a rôzny stupeň opakovania znakov, počty všetkých ich permutácií sa tiež líšia. To docielime tak, že vybereme heslá, ktoré majú rovnaký počet možných permutácií, konkrétne tieto tri:

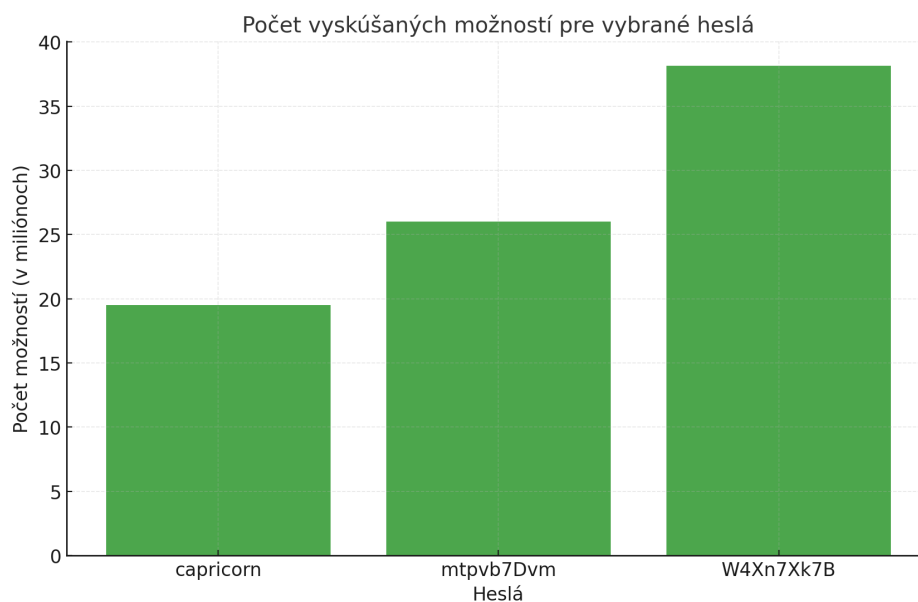
1. capricorn
2. mtpvb7Dvm
3. W4Xn7Xk7B

Všetky tri heslá majú 9 znakov, z toho dva znaky obsahujú dva krát, čiže počet všetkých ich permutácií je $7^9 = 40,353,607$. Na nasledujúcom grafe je znázornený čas brute-force testov pre tieto heslá.



Obr. 7: Graf časov pre vybrané heslá.

Na treťom grafe je zobrazený počet vyskúšaných možností brute-force testov pre tieto heslá.



Obr. 8: Graf vyskúšaných možností pre vybrané heslá.

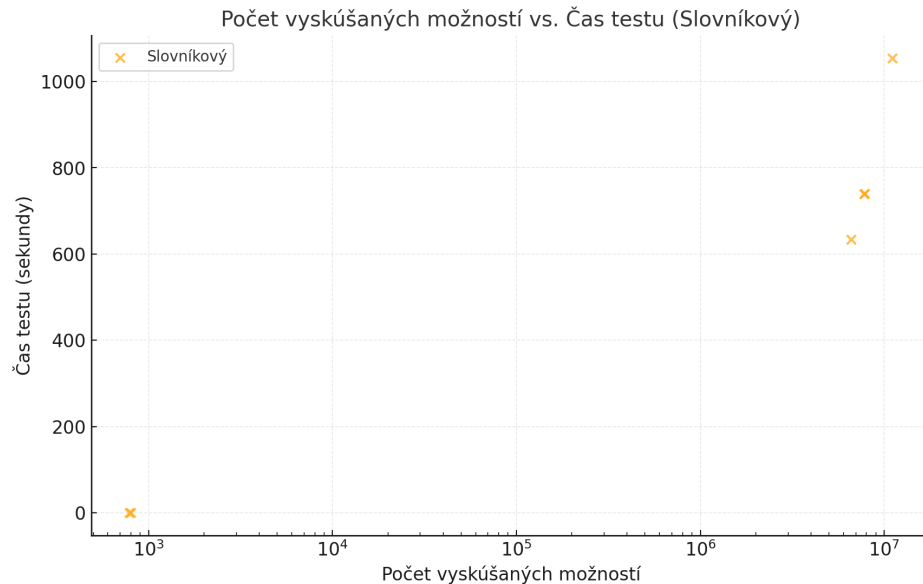
Ako môžeme vidieť, nárast času potrebného na nájdenie týchto hesiel je rovnaký ako nárast vyskúšaných možností. Kombináciou analýzy času a počtu vyskúšaných možností sme nadobudli obraz o efektívnosti brute-force útokov. Pri heslách s rôznymi dĺžkami a zložitou, ako aj pri heslách s rovnakými dĺžkami a zložitou, je najdôležitejším faktorom pre tento typ útoku počet vyskúšaných možností. Z toho vyplýva, že efektívnosť brute-force útokov je predvídateľná podľa celkového počtu všetkých možností hesla.

Slovníkové útoky

Ako je z tabuľky výsledkov už na prvý pohľad zjavné, slovníkové útoky sú neúspešné, ak sa heslo, ktoré sa snažíme prelomiť, v slovníku nenachádza. Na druhú stranu, ak sa heslo v slovníku nachádza, čas potrebný na jeho prelomenie je výrazne kratší v porovnaní s brute-force útokmi. Napríklad heslo „capricorn“ bolo prelomené za 0,1 sekundy s použitím slovníka obsahujúceho toto heslo, pričom brute-force útok na to isté heslo trval až 1,861 sekundy a prešiel vyše 19 miliónov možností. Podobne, heslo „grabapunk“ bolo v slovníkovom útoku prelomené za 740 sekúnd po vyskúšaní 7,799,457 možností, čo je výrazne kratší čas oproti 9,295 sekundám pri brute-force útoku, ktorý musel prejsť 97,196,856 možností.

Grafické zobrazenie

Na tomto grafe je zobrazený vzťah času potrebného na nájdenie hesla a počtu vyskúšaných možností pre slovníkové útoky.



Obr. 9: Graf časov a vyskúšaných možností pre slovníkové útoky.

Tu sa dá vidieť rovnaká závislosť ako pri brute-force útokoch. Čím viac možností sa vyskúša, tým dlhšie to trvá.

Porovnanie použitých metód

Obidva vyskúšané druhy útokov majú rovnakú závislosť medzi časovou náročnosťou a vyhľadávacím priestorom. Slovníkové útoky problém enormného vyhľadávacieho priestoru pri neznámom hesle riešia tým, že sa zameriavajú na známe najčastejšie používané heslá, čím výrazne znižujú časové nároky na nájdenie hesla, ale za cenu možného neúspechu.

Brute-force útoky zase skúšajú všetky možnosti, čím maximalizujú teoretickú pravdepodobnosť nájdenia hesla, ale za cenu časovej zložitosti. Treba podotknúť, že na to aby som vôbec mohol porovnávať brute-force útok a slovníkový útok, som musel robiť optimalizácie spomenuté v podkapitole 3.4, v rámci ktorých som z brute force útokov urobil vlastne tiež slovníkové útoky, tým že som výrazne okresal vyhľadávací priestor na základe poznanej dĺžky a znakov hesla. Keby som nepoznal dĺžku a znaky hesla, počet všetkých možností pre brute force útok by bol tak enormne veľký, že by bolo nemožné ich v reálnom čase všetky vyskúšať. Z toho vyplýva, že brute-force útok na neznáme heslo je rovnako neefektívny ako slovníkový útok na heslo, ktoré sa v slovníku nenachádza.

Obidve metódy majú svoje silné a slabé stránky, ktoré predurčujú ich ideálne využitie. Brute-force útoky vynikajú svojou univerzálnosťou a schopnosťou prelomiť akékoľvek heslo za predpokladu dostatočného času a výpočtového výkonu. Ich hlavnou slabinou je však ich extrémna časová náročnosť, ktorá pri väčšom vyhľadávacom priestore môže dosiahnuť nerealizovateľné hodnoty. Preto ideálnym prípadom pre použitie brute-force útoku v praxi je, keď sú dostupné dostatočné informácie o hesle (napríklad počet znakov alebo množina znakov, z ktorých sa skladá), vďaka ktorým je vyhľadávací priestor okresaný, tak ako tomu bolo aj v mojom experimente.

Naopak, slovníkové útoky sú mimoriadne efektívne pri prelomení bežných, často používaných hesiel, ale sú úplne závislé od kvality a rozsahu použitého slovníka. Ich hlavnou slabinou je teda obmedzená použiteľnosť pri unikátnych a silných heslách, ktoré nie sú v slovníku zahrnuté.

Pre prelomenie väčšej sady hesiel by zase mohol byť optimálny prítup kombinácia oboch týchto metód. Slovníkový útok môže slúžiť ako prvá fáza na rýchle prelomenie slabých hesiel, pričom brute-force útok by mohol byť aplikovaný až na heslá, ktoré neboli nájdené slovníkom.

4.2 Odporúčania pre zvýšenie bezpečnosti

Na základe výsledkov získaných počas experimentu je možné poskytnúť niekoľko konkrétnych odporúčaní pre zvýšenie bezpečnosti WiFi sietí. Tieto odporúčania sa týkajú predovšetkým výberu silných hesiel a implementácie modernejších bezpečnostných štandardov.

Používanie silných náhodných hesiel

Jedným z najdôležitejších opatrení na zvýšenie bezpečnosti WiFi siete je používanie dostatočne dlhých, komplexných a náhodne generovaných hesiel. Výsledky experimentu jasne ukázali, že heslá s väčším počtom znakov a vyššou zložitosťou vyžadujú dlhší čas na prelomenie. Napríklad náhodné 9-znakové heslá ako „W4Xn7Xk7B“ mali oveľa väčší počet možných kombinácií v porovnaní s jednoduchšími slovníkovými heslami, čo spôsobilo, že brute-force útok trval výrazne dlhšie. Navyše, heslá, ktoré sa nenachádzali v slovníku, boli proti slovníkovým útokom úplne odolné.

Pre praktické účely sa odporúča vytvárať heslá ako náhodné kombinácie znakov. Takéto heslá by mali obsahovať veľké a malé písmená, čísla a špeciálne znaky a ich dĺžka by mala byť aspoň 8 znakov, aby sa zabezpečil dostatočne veľký vyhľadávací priestor.

Unikátnosť hesiel

Okrem vytvorenia silného hesla je dôležité nepoužívať heslo od WiFi aj pre kontá na rôzne stránky a služby. Všeobecne platí, že heslá treba pravidelne kontrolovať, či náhodou neboli kompromitované pri úniku dát. Aj keď je heslo silné, v prípade jeho kompromitácie môže útočník získať pomerne ľahko neautorizovaný prístup pomocou prelomenia hesla útokom za použitia slovníka s uniknutými heslami. Pravidelná aktualizácia hesiel tiež znižuje riziko takýchto útokov.

Prechod na WPA3 protokol

Aj keď WPA2 bol dlhodobo považovaný za bezpečný štandard, uskutočnenie experimentu ukazuje, že je zraniteľný voči útokom založeným na zachytení handshakeu. Prechod na moderný WPA3 protokol prináša významné bezpečnostné výhody.

Jednou z hlavných výhod WPA3 je použitie protokolu SAE, ktorý eliminuje možnosť útoku na heslo pomocou handshakeu. V protokole SAE sa heslá neodosielajú priamo ani sa z nich neodvodzujú hodnoty, ktoré by útočník mohol použiť na offline analýzu. Okrem toho WPA3 zavádza ochranu proti brute-force útokom tým, že obmedzuje počet pokusov o prihlásenie.

Literatúra

- [1] B. Indira Reddy and VrnS Srikanth. Review on wireless security protocols (wep, wpa, wpa2 & wpa3). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2019. URL <https://api.semanticscholar.org/CorpusID:199017854>.
- [2] A Wiese, A Gibson, and N Kim. Wifi network security protocols. Technical report, Oregon State University, 2020. URL https://web.engr.oregonstate.edu/~kimmich/ECE_476_WiFi_Network_Security_Protocols.pdf.
- [3] Asmaa Halbouni, Lee-Yeng Ong, and Meng-Chew Leow. Wireless security protocols wpa3: A systematic literature review. *IEEE Access*, 11:112438–112450, 2023. doi: 10.1109/ACCESS.2023.3322931.
- [4] CP Kohlios and T Hayajneh. A comprehensive attack flow model and security analysis for wi-fi and wpa3. *Electronics*, 7(11):284, 2018. URL <https://www.mdpi.com/2079-9292/7/11/284/pdf>.
- [5] Glen Sagers. Wpa3: The greatest security protocol that may never be. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 1360–1364, 2021. doi: 10.1109/CSCI54926.2021.00273.
- [6] BeyondTrust. Password cracking 101: Attacks and defenses explained. <https://www.beyondtrust.com/blog/entry/password-cracking-101-attacks-defenses-explained>, 2024. Accessed: November 19, 2024.
- [7] Openwall. John the ripper documentation. <https://www.openwall.com/john/doc/>, 2019. Accessed: November 19, 2024.
- [8] Hashcat. Hashcat documentation. <https://hashcat.net/wiki/doku.php?id=hashcat>, 2024. Accessed: November 19, 2024.
- [9] Aircrack-ng. Aircrack-ng documentation. <https://www.aircrack-ng.org/documentation.html>, 2023. Accessed: November 19, 2024.