Jihočeská univerzita v Českých Budějovicích

Přírodovědecká fakulta

Bakalářská práce

Odolnost šifrování standardu WPA3 na platformě Mikrotik RouterOS

Jiří Kudlata

Vedoucí práce: Ing. Jan Fesl Ph. D.
Rok zadání práce: 2022

Bibliografické údaje

Kudlata J., 2022: Odolnost šifrování standardu WPA3 na platformě MikroTik RouterOS. [Resistance of WPA3 encryption on the MikroTik RouterOS platform. Bc. Thesis, in Czech.] - 92 p., Faculty of Science, The University of South Bohemia, České Budějovice, Czech Republic

Anotace

Tato bakalářská práce se zaměřuje na studii bezpečnostních mechanismů používaných novým standardem WPA3 pro dosažení optimálního zabezpečení a popisuje principy, na kterých tyto mechanismy fungují. Dále zkoumá aktuálně dostupné nástroje pro penetrační testování zařízení podporujících WPA3 a pro útoky na tyto zařízení. Práce také popisuje implementaci WPA3 do systému Mikrotik RouterOS a poskytuje doporučení při využití WPA3 na platformě MikroTik.

Klíčová slova

WPA3, Dragonfly, SAE, DoS, Wi-Fi, Dragonblood, MikroTik, RouterOS, Bezpečnost

Annotation

This bachelor thesis focuses on studying the security mechanisms used by the new WPA3 standard to achieve optimal security and describes the principles on which these mechanisms operate. It also examines currently available tools for penetration testing of devices supporting WPA3 and for attacks on these devices. The thesis also describes the implementation of WPA3 into the Mikrotik RouterOS system and provides recommendations for using WPA3 on the MikroTik platform.

Key words

WPA3, Dragonfly, SAE, DoS, Wi-Fi, Dragonblood, MikroTik, RouterOS, Security.

Prohlášení

Prohlašuji, že svoji bakalářskou práci jsem vypracoval samostatně pouze s použitím pramenů a literatury uvedených v seznamu citované literatury.

Datum: Podpis:

Obsah

1 Úvod

Bezpečnost bezdrátových sítí je oblast, která v porovnání s klasickými tj. optickými či metalickými je značně problematická, jelikož není jednoduše možné zabránit odposlechu dat. Již nejméně 20 let je aktuální vývoj řešení, které by zaručilo úroveň zabezpečení srovnatelnou s klasickým médiem. Nejnovějším vyvinutým standardem je zabezpečení nazvané WPA3, které by mělo eliminovat nedostatky předchozího řešení WPA 2, tj. bezpečností slabiny související s nešifrovanými rámci pro řízení provozu a možnosti podvržení identity klientské stanice.

1.1 Cíle

V úvodní části práce zaměřte na detailní studium všech mechanismů, které WPA3 používá pro dosažení optimálního zabezpečení a detailně popište jejich principy. Dále prostudujte aktuální volně dostupné nástroje sloužící k penetračnímu testování zařízení podporujících WPA3, popř. k provádění útoků samotných. Na závěr popište implementaci WPA 3 do systému Mikrotik RouterOS.

Navrhněte smysluplné scénáře pro testování zařízení na platformě Mikrotik RouterOS a proveďte experimentálně možnosti průniku do těchto zařízení. Testování proveďte pro vícero (alepsoň tří) verzí Mikrotik RouterOS, tj. od prvotní verze, která WPA 3 podporovala a až po současnou. Testování bude probíhat automatizovaně anebo semi-automatizovaně prostřednictvím k tomuto vyvinutých skriptů v jazyce Python či Shell.

Na závěr proveďte evaluaci naměřených výsledků a okomentujte je a vyslovte obecná fakticky potvrzená doporučení pro využití pro uživatele plánující nasadit WPA 3 na platformě Mikrotik RouterOS.

2 WPA3

WPA3 je sada protokolů pro autentizaci a šifrování komunikace při komunikaci s bezdrátovými Wi-Fi sítěmi. Bylo vydáno Wi-Fi Aliancí v červnu 2018. Je to nástupce WPA2 a měl by odstranit jeho nedostatky. Používá alespoň 128-bitové šifrování v režimu WPA3 Personal a může používat 192-bitové šifrování u WPA3 Enterprise, což má za následek zvýšení bezpečnosti hesla. Nově oproti WPA2 přichází s technikou Simultanously Authentication of Eaquals (SAE), neboli též Dragonfly Handshake, která nahrazuje 4-cestný handshake a mechnismus výměny klíčů PSK, což zabraňuje útokům formou reinstalaci klíče. Díky tomu že u SAE při připojování nedochází k

výměně známého hesla, mezi AP a klientem, v jakékoliv podobě, je komunikace odolná vůči offline slovníkovým útokům. A protože není možné dopředu odhadnout výměnu klíče a získání klíče relace, je odolný vůči útokům hrubou silou.[1][10]

Díky SAE tedy útočník nedokáže dešifrovat zaznamenanou komunikaci i kdyby se mu podařilo získat heslo k síti a nemůže ani sledovat cizí komunikaci. Při použití WPA3 je podmínkou použití zabezpečených řídících rámců (PMF), které zabezpečují síťový provoz proti jejich podvrhnutí a například odhlášení připojeného klienta od sítě. WPA3 si zachovává kompatibilitu s WPA2 ale neumožňuje používání zastaralých protokolů WEP a TKIP.[30][10]

2.1 SAE (Simultaneous Authentification of Equals)

SAE neboli též Dragonfly Handshake je funkce authentikace používaná při vyjednávání o připojení. Patří mezi standardy 802.11s a když v roce 2018 Wi-Fi Alliance oznámila vznik WPA3, tak SAE bylo použito jako náhrada 4-cestného vyjednávání výměny klíčů PSK.[1]

Nejdříve byl implementován pro použití v mesh sítích, kde je využíván pro zabezpečené propojení jednotlivých bodů sítě, kdy si jednotlivé body sítě, v tomto případě AP, ověří že každý bod zná heslo a dojde k vytvoření silného kryptografického klíče pomocí kterého dojde k vytvoření session-key (klíč relace) používaného k zabezpečené komunikaci v mesh síti.[3]

Je to na hesle založená authentikační metoda, využívající principu Password Authenticated Key Exchange (PAKE), která řeší jak dvě strany mohou navázat zabezpečené, authentikované spojení. K tomu využívá tzv.: „důkaz o nevědomosti“ (Zero-knowledge proofs). Kdy na základě sdíleného tajemství, v našem případě hesla k wifi síti, dokáží deterministickou metodou vytvořit silný kryptografický klíč s vysokou entropií, kdy na základě tohoto klíče, který není užit při komunikaci mezi stranami, si dokáží oprávněnost komunikace. K tomu aby to dokázali, se využívá matematická metoda výměny klíčů Diffie-Hellman.[3]

SAE je varianta authentikačního algoritmu Dragonfly Key Exchange definovaného v RFC 7664, který do výše zmíněného mechanismu přidává náhodnou složku a tak je kryptografický klíč při každém navázaném spojení jiný.[1]

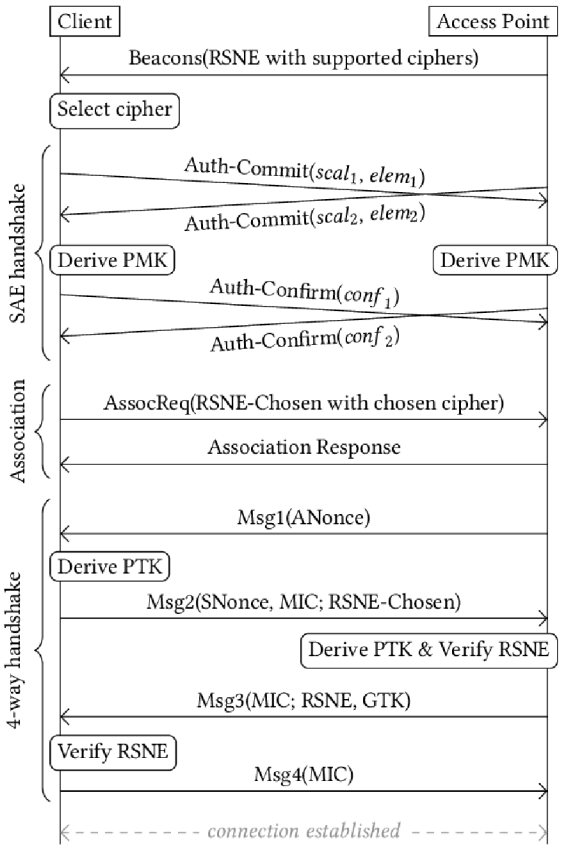
Generování klíče je založeno na sadě parametrů které definují cyklickou skupinu (finite cyclic group). Skupiny jsou založeny na Finite Fine Cryptography (FFC) nebo Elliptic Curve

Cryptography (ECC). V případě ECC je využíváno prvočíslo nejméně 3072 (skupiny 15 až 18) a nebo délce 256 bitů (skupiny 19 – 21).

SAE garantuje následující bezpečnostní vlastnosti:

- Po úspěšném provedení SAE handshaku, účastníci spojení sdílejí silný kryptografický klíč zvaný „pairwise master key“(PMK)
- Žádný útočník, který pasivně nebo aktivně odposlouchává a manipuluje s handshakem nemůže získat heslo a nebo odvozený PMK
- V případě uhodnutého PMK, je tento klíč použit pouze v jednom handshake, a tím pádem není možné využití využít offline slovníkový útok k uhodnutí klíče a následné dešifrování zaznamenané komunikace.
- Případné prozrazení hesla k wifi síti nevede k možnému dešifrování odposlechnuté komunikace nebo odvození PMK

2.1.1.1 SAE Handshake



Obrázek 1: SAE Handshake [31]

SAE zavádí tzv SAE commit a SAE confirm rámce mezi klientem a AP. Využívá Basic Service Set (BSS) kdy klient vždycky jako první posílá commit rámec. Pokud si obě strany vzájemně odešlou confirm rámec, je potvrzeno navazování spojení. Každý rámec z těchto dvou typů obsahuje číslo authentikačního algoritmu (3), authentikační sekvenci (1 pro Commit a 2 pro Confirm) a kód statusu (hodnota mezi 0 a 65535) kdy 0 znamená úspěšný. Kód 1 až 107 znamená nějakou chybu a kódy 114,115, 124,127 a 130 až 65535 jsou rezervovány pro budoucí použití.

Předtím než strana odešle commit, musí vygenerovat sdílené tajemství zvané „Password Element“ (PWE) které je vypočítáno pomocí metody „hunting and pecking) která opakovaně vytváří frázi pomocí hashovací funkce SHA256 za použití MAC klienta, MAC AP, známého hesla (P) a počítadla (C) které se při každém průchodu navýší o 1. SHA256(MACk, MACAP, P, C) z výsledné hodnoty se za požití derivační funkce, kde fráze je použita jako klíč, vytvoří souřadnice x na eliptické křivce, které je dosazeno do rovnice:

$$y2=x3+ax+b \bmod p$$

a je zkontrolováno jestli existuje řešení y. Pokud ano, tak bod (x,y) na křivce je PWE. Pokud řešení nebylo nalezeno, tak C se zvýší o 1 a výpočet je opakován. Z důvodu odvrácení útoků založených na čase výpočtu, se vždy provede alespoň 40 iterací i když výsledek byl nalezen dříve.

Obě strany vygenerují dvě náhodná čísla a prvočíslo (r, mask, q). Po dosazení do vzorečku

$$(r+mask) \bmod q$$

obě strany vypočítají skalární hodnotu. Dále vypočítají element

$$Element = -mask * PWE$$

smažou hodnotu „mask“. Následně si pomocí SAE Comitu vymění svoje group ID, skalární hodnotu a Element a ověří jejich správnost. Skalár musí splňovat podmínku $1<Scalar<q$, a pro skupinu ECC musí Element splňovat podmínku že to je celočíselné kladné číslo menší než p, protože Element musí ležet na přímce a nesmí být bodem v nekonečnu.

Pokud by se stalo že hodnoty Scalaru a Elementu jsou shodné, tak je to považováno za tzv. „reflection attack“ a přijímací strana musí přerušit handshake. AP musí také odmítnout commit rámec, který obsahuje nepodporované group ID. Když všechny kontroly projdou, tak klienti vypočítají sdílené tajemství K dle:

$$K=r*(Scalar*PWE+Element)$$

pokud je K bodem v nekonečnu, strany musí odmítnout authentikaci. Souřadnice x bodu K se použije jako vstup hashovací funkce pro získání bodu k

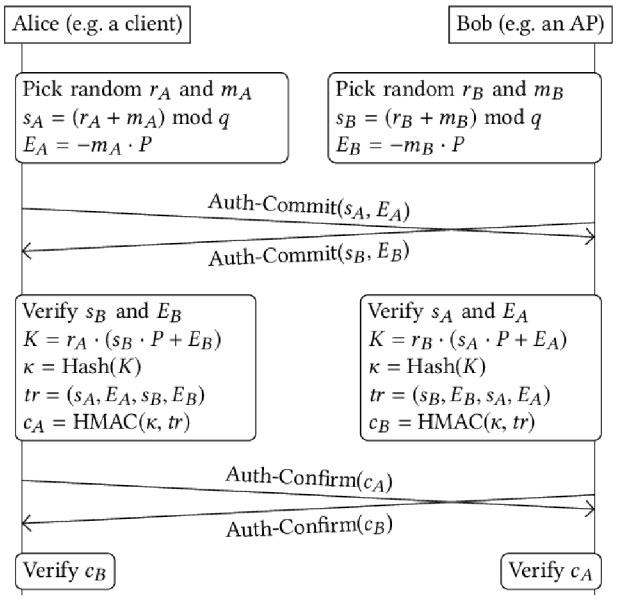
$$k=Hash(Kx)$$

Většinou k je rozděleno do 2 256-bitových podklíčů, které jsou použity pro výpočet potvrzovacího tokenu a PMK, označovány jako „key confirmation key“ (KCK)

Při výměně SAE Confirm rámců obě strany ověří že vypočítali stejné tajemství k a znají tedy stejné heslo P. Většinou se pro výpočet potvrzovacího tokenu použije algoritmus HMAC s klíčemi KCK.

$$c=HMAC\text{-}SHA256KCK(Scalarklient,Elementklient,ScalarAP,ElementAP,SC)$$

a posláno protistraně. V Confirm rámci je hodnota „Send-Confirm“ která obsahuje hodnotu již zaslaných potvrzovacích rámců, to poskytuje ochranu proti injektování nebo změně již zaslaných rámců. Pokud je ověření rámců úspěšné, je podklíč k použit jako PMK a handshake je dokončen.



Obrázek 2: SAE Handshake2 [31]

2.1.2 SAE-PK

SAE-PK je rozšíření SAE authentikace. Doplňkové označování vyžadováno pro SAE-PK je uvedeno v 802.11 Autentizační rámce které obstarávají Commit a potvrzovací rámce SAE.

Když AP pošle SAE potvrzovací zprávu klientovi, rámec obsahuje veřejný klíč AP, modifikovanou hodnotu (wrapped using a Key Encryption Key derived from the SAE keyseed) , a digitální podpis který se skládá z SAE veřejných hodnot používaných AP i klientem, veřejného klíče AP a modifikátoru a MAC adresu AP i klienta podepsanou privátním klíčem

STA ověřuje identitu pomocí veřejného klíče pomocí otisku (fingerprint) zakódovaného v hesle pomocí Base32 a přidání oddělovacího znaku a znaku kontrolního součtu.

Digitální podpis poslaný AP dovolí stanici výměnu SAE klíčů s AP za použití ověřeného veřejného klíče AP.[11]

Pokud stanici selže ověření přijatého veřejného klíče od AP, nebo selže ověření digitálního podpisu, dojde k přerušení authentikace. Jinak když je authentikace úspěšná, navázané spojení PMKSA(Pairwise Master Key Security Association) je použito pro 802.11 (znovu)asociaci.

Odolnost vůči útoku (second preimage attack on the fingerprint) je vylepšená hashovacím rozšířením, kdy otisk je zkráceným výstupem hashovací funkce z veřejného klíče AP, SSID a 16-

ti oktetovým modifikátorem který je určen náhodně. The Modifier is found randomly by one-time brute-force search (when the password is initially generated) and is a value that results in the first 8*Sec bits of the fingerprint being equal to zero. This allows a fingerprint of effective length (8*Sec + 19*λ/4 - 5)-bits to be represented in only 5λ bits (where base32 encoding results in a λ-character password excluding separators), using λ/4 bits to redundantly encode Sec and one of the characters (5 bits) for the checksum.[11]

2.1.2.1 Podpora

Zařízení které podporuje SAE-PK musí podporovat WPA3-Personal, a pokud je na zařízení zapnuta podpora pro WPA3 osobní nebo tranzitní režim, tak může podporovat SAE-PK.

Fungování AP

AP podporující SAE-PK s nastavením pro použití SAE-PK s heslem s podporou SAE, musí používat stejné heslo i když není pro přihlášení k AP SAE-PK použito. Pokud AP má povoleno přihlašování heslem, tak to platí pro jakékoliv přihlašování na základě hesla.

Pokud se každé heslo používá se SAE nebo PSK je to heslo SAE-PK a AP musí bit označený jako "SAE-PK Passwords Used Exclusively" v rozšířených možnostech AP mít nastaven na 1. [11]

2.1.2.2 Proces generování údajů k ověření

Údaje k ověření obsahují:

- pár veřejného/privátního klíče k AP (K_AP/k_AP)
- odpovídající 128-bitový modifikátor M, nalezení speciální hodnoty pro Sec
- odpovídající SEA-PK heslo
- volitelný identifikátor hesla SEA, který identifikuje výše zmíněné údaje

Stejná sada údajů je nastavena na všech AP v síti se stejným SSID

Minimálně heslo, a pokud je použit identifikátor hesla, tak i ten je distribuován všem klientům. Pokud je použito přihlašování pomocí QR kódu, tak klient dodatečně obdrží veřejný klíč AP (K_AP)

Privátní klíč se v infrastrukturní síti nesmí dostat mimo AP. Pokud síť obsahuje více AP, tak pár klíčů a modifikátor jsou distribuovány mezi těmito AP, ale jakým způsoben není ve specifikaci obsaženo.

Stejný pár klíčů (K_AP/k_AP) je použit pro více hesel pokud se používají ve stejné síti. (např. Nalezením náhodných modifikátorů)

Zařízení které podporuje SAE-PK musí podporovat ECDSA P-256 AP veřejný klíč. Podpora SAE-PK pro použití ostatních ECDSA klíčů které jsou 256-ti bitové a delší je volitelná.

Zařízení které podporuje SAE-PK s ECDSA klíčem delším než 256-bitů by mělo mít povoleno skupinu SAE 20 a zařízení používající klíč delší než 384-bitů má povoleno skupinu SAE 21

AP který je nastaven pro používání klíčů delších než 256-bitů by měl mít zakázáno použití SAE skupin které používají délku klíče menší než 192-bitů, pokud se nepoužívají hesla které tyto skupiny využívají na BSS. A AP který používá délku klíče delší než 384-bitů by měl mít zakázáno používat klíče kratší než 256-bitů, pokud nejsou použity k jiným heslům nastavených na BSS.[11]

Zařízení by nemělo odmítnout použití SEA skupiny nebo odmítnout SEA potvrzovací zprávu pouze na základě toho, že síla SEA-PK a SEA skupiny neodpovídá.

128-bitový modifikátor využívá datový typ unsigned integer (M) by měl být nalezen prvotním nastavením M na náhodnou hodnotu a podle potřeby zvyšovat hodnotu M o 1 dokud hodnota M není nalezena, pro kterou platí že první Sec oktety otisku se rovnají 0.

$$\text{Fingerprint} = L(\text{Hash}(\text{SSID} \parallel M \parallel K\_AP), 0, 8*\text{Sec} + 19*\lambda/4 - 5)$$

kde:

- L(S, F, N) je funkce extrahující bity od F do F+N–1 řetězce bitů S začínající z leva
- Hash() je funkce implementující hashovací algoritmus, kde záleží na délce veřejného klíče AP K_AP, použitím ECC sloupce pro délku ECDSA klíče
- Sec je rozšiřující bezpečnostní parametr, rovný číselné hodnotě 3 nebo 5
  - λ by měla být $\lambda = 4*n$, kde n je číslo větší nebo rovno 3, a $8*\text{Sec} + 19*\lambda/4 - 5 <=$ HashLen, kde HashLen je výstup hashovací funkce Hash()
- SSID je sekvence oktetů rovnající se síťovému SSID
- K_AP je veřejný klíč AP, reprezentovaný certifikátem v DER podobě podle ASN.1 SubjectPublicKeyInfo. Kódování je definovánu v RFC 5480 pro ECDSA, kde subjectPublicKey je komprimovaný formát. ASN.1 reprezentace pro ECDSA P-256 klíč je následující:

  AlgorithmIdentifier ::= SEQUENCE { algorithm ecPublicKey, parameters secp256r1 } SubjectPublicKeyInfo ::= SEQUENCE { algorithm AlgorithmIdentifier, subjectPublicKey BIT STRING } Heslo by poté mělo být definováno takto: PasswordBase = Base32(P(0) || P(1) || … || P(λ/4-1)) Heslo = AddSeparators(PasswordBase || ChkSum)

kde:

- když i< (λ/4-1), P(i) = Sec_1b || L(Fingerprint, 8*Sec+(19*i), 19)
- když i=(λ/4-1), P(i) = Sec_1b || L(Fingerprint, 8*Sec+(19*i), 14)
- Sec_1b je 1-bitové číslo rovno 1 když Sec=3, a rovno 0 když Sec=5
- Base32() je base32 kódovací funkce (5 bitů na znak) používající malá písmena dle US-ASCII abecedy
- ChkSum je base32 znak roven výstupu Verhoeffova algoritmu kde:
  - vstup je PasswordBase, tvořen malými písmeny kódovaných v base32
  - dihedrální skupina je složená z 32 skupin s 16-ti úhly a permutace je (1 2)(7 11 13 5 20 23 9 6 27 15 21 25 14 10 8 31 26 4 16 22 12 29 18 24 28 17 3 30 19 0)
  - POZNÁMKA: násobení d(j, k) v této dihedrální skupině je provedeno pomocí vzorce:
    d(j, k) = (j + k) mod 16 kde j<16 a k<16
    d(j, k) = ((j + k) mod 16) + 16 kde j<16 a k>=16
    d(j, k) = ((j - k) mod 16) + 16 kde j>=16 a k<16
    d(j, k) = (j - k) mod 16 kde j>=16 a k>=16
  - POZNÁMKA: inverzní operace inv(j) v této dihedrální skupině je provedena pomocí vzorce:
    inv(j) = 16 - j kde j<16
    inv(j) = j kde j>=16
- AddSeparators() v této funkci která vkládá znak „-“ (ASCII 0x2D) za každé čtyři znaky US-ASCII vstupního řetězce, kromě ukončujícího znaku.

POZNÁMKA: Délka vstupu do funkce base32 nemusí být ve výsledku celočíselná hodnota oktetů. Implementace může dovolit dosazení 0 do vstupu a zkrácení výstupu tak že 5λ-bit vstup vždycky povede k λ výstupu.

2.1.3 PMF (Protected Management Frames)

PMF bylo vytvořeno ze standardu 802.11w a brání klienty proti disassociaci, deauthentikaci z bezdrátové sítě. Tímto má za úkol bránit klienty proti spojení s útočníkem podvrhnutým AP u útoků typu Man-in-the-Middle. Standard 802.11w chrání řídící rámce tak, že přidává do rámce část MIC (Message Integrity Check) během handshake. Tato ochrana je povinná pro rámce WPA3.

Pokud AP podporuje zabezpečení řídících rámců, dá o tom klientským stanicím vědět pomocí BEACON rámce. Pokud klient také podporuje PMF, tak o tom dá vědět zahrnutím parametru PMKID do rámce dotazu na připojení, který jinak chybí.

2.1.4 Anti-clogging mechanismus

Z důvodu toho, že AP musí provést náročné výpočty při příjmu první zprávy SAE handshakeu. Má útočník možnost provádět tzv. DoS útoky, kdy zahlcuje AP falešnými SAE Commit rámci, což vede k vysoké zátěži na straně AP. Pro snížení rizika byl použit mechanismus ochrany proti zahlcení, který využívá výměnu "cookies" mezi zařízeními. Pokud je počet aktivních spojení překročen, AP odpoví novým SAE Commit rámcem obsahujícím "cookie". Toto cookie musí být odeslána zpět klientskou stanicí. Pokud cookie není platné, tak AP odmítne nové spojení. Nicméně, tento mechanismus nemusí být dostatečný, pokud útočník získá platné cookie a použije ho pro falešné spojení. [29]

2.2 Požadavky pro použití WPA3

1. AP nesmí povolit WPA v1 na stejné BSS
2. AP nesmí povolit WEP a TKIP na stejné BSS
3. Při připojování k AP který podporuje SAE a PSK, STA se musí připojit pomocí SAE
4. Na AP kde je povoleno PSK (SHA1 nebo SHA256), by měl být defaultně povolen WPA3-Personal transition mode, pokud není administrátorem určeno aby se použil režim WPA2-Personal

2.2.1 WPA3-Personal only mode

1. AP musí podporovat alespoň SAE v Basic Service Set (BSS)
2. STA musí podporovat alespoň SAE pro vybrání při asociaci
3. AP nesmí povolit PSK, SHA1 a PSK, SHA256
4. STA nesmí povolit vybrání PSK, SHA1 a PSK, SHA256 pro asociaci
5. AP musí povolit Management Frame Protection Capable (MFPC) a Management Frame Protection Required (MFPR)
6. STA musí povolit Management Frame Protection Capable (MFPC) a Management Frame Protection Required (MFPR)
7. STA nesmí povolit oveření pomocí WEP a TKIP

2.2.2 WPA3-Personal transition mode

1. AP musí povolit alespoň PSK, SHA1 a SAE v Basic Service Set (BSS)
2. STA musí povolit alespoň PSK, SHA1 a SAE pro vybrání při asociaci
3. AP by měl povolit PSK, SHA256
4. STA by měla povolit použití pro asociaci PSK, SHA256

5. AP musí povolit Management Frame Protection Capable (MFPC) a zakázat Management Frame Protection Required (MFPR)

6. STA musí povolit Management Frame Protection Capable (MFPC) a zakázat Management Frame Protection Required (MFPR)

7. AP musí odmítnout asociaci pro SAE pokud není použito Protected Management Frames (PMF) pro asociaci

8. STA musí vyjednávat s použitím Protected Management Frames (PMF) při asociaci k AP používající SAE

2.2.3 RSNA

Robus Security Network Association je bezpečnostní protokol používaný v bezdrátových sítích k bezpečnému navázání a udržování spojení mezi AP a klientským zařízením. Poskytuje ochranu proti neoprávněnému přístupu a požaduje po klientské stanici a AP aby se navzájem authentikovali předtím, než začne přenos dat.

RSNA je dostupné jak ve starším WPA2 tak ve WPA3 protokolu. U WPA2 je použito společně s PSK k navázaní zabezpečeného spojení, kdežto u WPA3 je použito společně se SAE k posílení authentikace a znemožnění útoků jako jsou offline slovníkové útoky nebo hádání hesla.

2.2.4 DPP (Device Provisioning Protocol)

Nahrazuje funkci WPS, dostupné na Wi-Fi CERTIFIED Easy Connect™ zařízeních.

Usnadňuje připojení zařízeních , které nepodporují zadávání hesla. Je možné je připojit pomocí naskenováním QR kódu nebo pomocí NFC.

2.3 WPA3 Enterprise

WPA3 Enterprise může používat 192-bitové šifrování při stálém využívání standardu 802.1X pro zabezpečení bezdrátové sítě.

Pro zabezpečení bezpečnosti používá pro:

- šifrování authentikace: 256-bitový Galois/Counter Mode protokol (GCMP-256)
- získání klíče a potvrzení: HMAC-SHA-384
- výměnu klíče a authentikaci: Eliptic Curve Diffie-Hellman (ECDH) výměnu a Elliptic Curve Digital Signature Algorithm (ECDSA) za použití 384-bitové eliptické křivky

- Robust management frame protection: 256-bitový Broadcas/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

2.3.1 GCMP-256

GCMP-256 je šifrovací algoritmus používaný v rámci WPA3 pro zabezpečení Wi-Fi komunikace. Jedná se o rozšíření algoritmu GCMP (Galois/Counter Mode Protocol) používaného v předchozím standardu WPA2. GCMP-256 používá klíč o délce 256 bitů, což je dvojnásobek délky klíče používaného v původním GCMP algoritmu (128 bitů). Tento delší klíč zvyšuje bezpečnost Wi-Fi komunikace proti útokům na šifrování.

2.3.2 HMAC-SHA384

Hash Message Authentication Code (HMAC) je speciílní případ Message Authentication Code (MAC), který zahrnuje kryptografickou hashovací funkci a tajný kryptografický klíč. A může být použit k ověření integrity a pravosti dat. HMAC poskytuje authentikaci za pomoci sdíleného tajemství, namísto digitálního podpisu u asymetrické kryptografie. V tomto případě SHA384 v názvu, označuje hashovací algoritmus použitý k vytvoření hashe na kterém závisí kryptografická odolnost.

HMAC pro svojí funkci využívá dvou průchodů hashovací funkce, kdy nejdříve z tajného klíče jsou odvozeny klíče dva. Při prvním průchodu hashovací funkcí vznikne „interní hash“ ze zprávy a jednoho klíče a následně při druhém průchodu vznikne HMAC kód z interní hashe a druhého klíče.

2.3.3 ECDH

ECDH je varianta Diffie-Hellmann protokolu za použití kryptografie eliptických křivek využívající násobení bodů eliptických křivek namísto modulárního umocňování a je označován za tzv. „key agreement“ protokol který umožňuje výměnu sdíleného tajemství mezi dvoumi stranami prostřednictvím nezabezpečeného média. Kdy každá ze stran zná veřejný a soukromý klíč eliptické křivky, které jsou pro to použity. Toto sdílené tajemství může sloužit k odvodění klíče a nebo být použito jako klíč. ECDH je založeno na následující vlastnosti:

$$(a * G) * b = (b * G) * a$$

kdy a a b jsou tajná čísla, neboli soukromé klíče strany a a b, a G je generovaný bod ležící na eliptické křivce. Můžou si strany přes nezabezpečený kanál vyměnit čísla (a * G) pro stranu a a (b * G) pro stranu b, což jsou veřejné klíče stran. Díky tomu si každá ze stran dopočítá sdílené tajemství

sdílené tajemství = (a * G) * b = (b * G) * a neboli

sdílené tajemství = (veř. klíč strany a) * (souk. klíč strany b) = (veř. klíč strany b) * (souk. klíč strany a)

2.3.4 ECDSA

Eliptic Curve Digital Signature Algorithm je kryptograficky bezpečné schéma digitálního podpisu založené na Eliptic Curve Cryptography. Je to asymetrický kryptografický algoritmus který na rozdíl od RSA by měl být teoreticky hůře prolomitelný při použití kratšího klíče, neboli pro zajištění stejné bezpečnosti potřebuje kratší délku klíče. Například podpis s délkou klíče 256-bitů u ECDSA oproti 3072-bitů dlouhém klíči u RSA. [13]

Poskytuje bezpečnou možnost ověření identity odesílatele a integritu odesílané zprávy na bezdrátové síti. U WPA3 je použito k podepsání výměny klíčů Diffie-Hellman mezi klientem a AP, zajišťující že vyměněné klíče jsou autentické. Zajišťuje silné zabezpečení protože umožňuje připojení do sítě pouze autorizovaným zařízením.

Velká výhoda ECDSA je ta, že díky používání kratší délky klíče je zapotřebí méně výpočetního výkonu a tak se jeho použití hodí tam kde máme omezené výpočetní zdroje. [18]

3 WPA3 na MikroTik RouterOS

Podpora WPA3 byla do MikroTik RouterOS přidána s vydáním verze 7.1 6.12.2021. Podporu lze doinstalovat balíčkem pod názvem „wifiwave2“ který zahrnuje podporu pro 802.11ac Wave2, WPA3 a 802.11w management frame protection (vyžaduje ARM CPU a 256MB RAM).[20][21]

Dle zjištění, výše uvedená podpora od RouterOS verze 7.1, platí pouze pro 32-bitové procesory ARM. Pro zařízení s architekturou ARM64 je balíček „wifiwave2“ dostupný až od verze RouterOS 7.3.

3.1 Implementace WPA3

Implementace WPA3 je závislá na balíčku s názvem „wifiwave2“. Tento balíček nahrazuje standardní bezdrátovou konfiguraci. Poskytuje podporu pro využívání standardu Wifi 6 802.11ax a 802.11ac wave2. [8]

3.2 Instalace potřebných balíčků

Pro možnost využívání WPA3 na Platformě MikroTik je nutné manuálně doinstalovat balíček „wifiwave2“, pokud již není na routeru nainstalován z výroby. Abychom tak mohli učinit, je nejprve nutné zajistit, abychom na zařízení MikroTik měli nainstalovaný operační systém podporující WPA3. Pokud tomu tak již není, tak si stáhneme ze stránek https://mikrotik.com/download/ podporovanou verzi, která musí být 7.1 nebo novější. Najdeme si tedy verzi pro platformu ARM a stáhneme soubor označený jako „Main Package“. Následně si otevřeme nástroj pro konfiguraci zařízeních MikroTik s názvem Winbox, pokud ho ještě nemáme v počítači tak si ho rovněž stáhneme. Ve spodní části pod záložkou „Neighbours“ by se nám mělo zobrazit naše zařízení které vybereme a po zadání přihlašovacích údajů klikneme na „Connect“ čímž dojde k přihlášení do zařízení. Nyní si otevřeme okno se staženým RouterOS a pouze ho myší přetáhneme do okna winboxu, tím dojde k nakopírování souboru do našeho zařízení. Pro nainstalování poté po levé straně na záložce „System“ vybereme možnost „Reboot“ kterou následně potvrdíme. Tímto dojde k nainstalování nového systému. Instalace většinou trvá delší dobu než spuštění zařízení a tak musíme dávat pozor abychom si zařízení neodpojili z napájení dříve než bude instalace dokončená. To poznáme obvykle tak, že se nám buď automaticky znovu otevře konfigurace zařízení a nebo se nám naše zařízení opět objeví na záložce „Neighbours“ v programu Winbox. Po opětovném připojení se k zařízení, bychom ještě měli provést aktualizaci jádra systému, kterou provedeme kliknutím na záložku „System/RouterBOARD“ a následně v okně které se objevilo zvolíme „Upgrade“ a volbu potvrdíme. Po zobrazení červeně napsané hlášky v dolní části okna „Firmware upgraded successfully…“ opět restartujeme zařízení. Nyní máme nainstalovanou potřebnou verzi RouterOS abychom mohli nainstalovat balíček „wifiwave2“ vrátíme se na stránku pro stažení softwaru, kde tentokrát pod stejnou verzí jako jsme stáhli RouterOS, nyní stáhneme zip archiv pod nabídkou „Extra packages“. Následně archiv rozbalíme a měli bychom nalézt balíček začínající názvem „wifiwave2-*.npk“ který nainstalujeme stejným způsobem jako výše zmíněný RouterOS. Akorát už není nutno dávat „System/RouterBOARD → Upgrade“. Jestli instalace proběhla úspěšně, si můžeme zkontrolovat na záložce „System/Packages“ kde v otevřeném okně uvidíme všechny nainstalované balíčky.

3.3 Konfigurace

Budeme předpokládat že již máme naše zařízení MikroTik nakonfigurované jako router/access point podle toho jak potřebujeme a že nám za ním funguje připojení k internetu. V další konfiguraci se budeme věnovat pouze nastavení bezdrátové části. Se zaměřením hlavně na základní nastavení a nastavení související s WPA3. Při Popisování funkčnosti se budu převážně věnovat hodnotám, které v aktuální části nastavení mohu změnit.

3.3.1 Nastavení WiFi

V levé části programu Winbox klikneme na „Wireless“, otevře se nám okno, kde hned na první záložce „Wifi Wave2“ se nám v případě routeru s 2,4 i 5GHz pásmem, zobrazí dvě rozhraní s názvem „wifi1“ a „wifi2“ pro vstup do konfigurace u vybraného rozhraní na něj dvojklikem klikneme a zobrazí se nám okno kde hned na první záložce „General“ vidíme název rozhraní, který můžeme změnit, dále pak velikost MTU která je ve výchozím nastavení 1500 a pokud jí nechceme změnit, tak pole ponecháme prázdné. Následně můžeme nastavit hodnotu „L2MTU“ která nám vyjadřuje velikost Ethernetového rámce bez hlavičky s MAC adresou rozhraní. Dále zde můžeme změnit MAC adresu rozhraní, možnost povolit, zakázat nebo jinak pozměnit chování rozhraní při dotazování klientů na ARP tabulku a timeout těchto dotazů. A na závěr pro nás nejpodstatnější parametr „Mode“ ktrým si zvolíme jestli chceme aby naše zařízení pracovalo v režimu přístupového bodu (AP) nebo klientské stanice (station).

Na další záložce „Configuration“ vidíme parametr „Configuration:“ k tomuto se vrátíme později, dále pak „SSID:“ kde si nastavujeme název naší wifi sítě, „Country:“ zvolíme zemi ve které se nacházíme, hodnota má vliv na přednastavení frekvenčního pásma a vysílacího výkonu v kterém AP bude provozováno, abychom vyhověli povoleným hodnotám v našem regionu. Parametrem „Chains:“ můžeme omezit počet použitých vysílacích polarizací antény, ovšem pouze v rozsahu podporovaném hardwarem, ve výchozím nastavení se využívají všechny dostupné polarizace. Parametrem „Tx Chains:“ můžeme upravit počet polarizací využívaných pro vysílání a „Tx Power:“ nám udává vysílací výkon v dBm, ovšem opět nemůžeme překročit maximální hodnoty podporované hardwarem. A na závěr volbou „Hide SSID:“ můžeme určit, zda-li ve vysílacích rámcích BEACON budeme prozrazovat jméno naší sítě okolním stanicím.

Na záložce „Channel“ opět přeskočíme první volbu „Channel:“, dále pak můžeme nastavit frekvenční pásmo parametrem „Band:“. Na výběr máme z možností:

- 2GHz AX/(G)/(N)

- 5GHz A/(A/N)/(AC)/(AX)

Na záložce „Security“ opět jako první máme možnost zvolit přednastavený profil. Dále pod názvem „Authentication Types“ si rozbalíme nabídku, kde vidíme možnosti zabezpečení. (WPA PSK, WPA2 PSK, WPA EAP, WPA2 EAP, WPA3 PSK, OWE, WPA3 EAP, WPA3 EAP 192)

Pod názvem „Encryptions“ se nám rozbalí nabídka s možností vybrat si které šifry budeme podporovat pro unicastové vysílání. Ve výchozím stavu i když není zvolena žádná šifra se použije CCMP. V další nabídce „Group Encryption:“ volíme šifru která se použije pro multicastové vysílání. Ve výchozím stavu se použije CCMP. U volby „Group Key Update:“ můžeme zvolit po jaké době se změní dočasný klíč pro broadcastovou komunikaci, ve výchozím stavu to je 5 minut. V řádku „Passphrase:“ si volíme heslo pro přihlášení k WiFi. Volbou „Disable PMKID:“ můžeme zakázat hodnotu PMKID v EAPOL rámcích, tím nůžeme snížit kompatibilitu klientských zařízeních které PMKID využívají. PMKID je používáno pro rychlejší přihlašování již přihlášených klientů k AP bez provedení kompletní authentikace. Např.: při přesunu mezi více AP na stejné síti. Další volba „Management Protection:“ nám určuje jestli budeme vyžadovat zabezpečení řídících rámců, na výběr máme za tří možností a sice: „allowed“ (povoleno) , „disabled“ (zakázáno), „required“ (vyžadováno). Tato volba je nekompatibilní se zabezpečením řídících rámců ve standardním balíčku pro nastavení bezdrátové sítě, tzn. pokud nemáme nainstalován balíček „wifiwave2“. Tato volba je ve výchozím stavu nastavená dle možností authentikace kde u WPA není podporovaná a u WPA3 je vyžadovaná. V návaznosti na povolení zabezpečení řídících rámců, můžeme u dalšího nastavení „Management Encryption:“ zvolit typ šifrování které se použije pro zašifrování řídících rámců. Ve výchozím stavu se použije CMAC. Položkou „WPS:“ můžeme povolit nebo zakázat authentikaci klienta pomocí WPS tlačítka, kdy se klient po dobu 2 minut od zmáčknutí tlačítka na routeru může přihlásit k síti bez zadání hesla. Toto je ve výchozím stavu povoleno, avšak tato funkce prozatím nebyla implementována. Položku „DH Groups:“ můžeme použit pro specifikování skupiny ECC při použití WPA3 authentikace. Na výběr máme ze tří možností 19,20,21 pro délku pole 256, 384 a 521-bitů. Můžeme se tedy rozhodnou jaké skupiny šifrování bude náš router podporovat. Můžeme vybrat všechny tři a nebo nechat pole prázdné, v tom případě se automaticky bude používat skupina 19, která je u WPA3 povinná. U další volby „SAE Anti Clogging Threshold:“ můžeme specifikovat po jakém počtu probíhajících authentikací SAE, začne AP požadovat po klientské stanici zahrnutí „cookie“, svázanou s MAC adresou klientské stanice, do požadavku na

authentikaci. Nemělo by tak dojít k přetěžování CPU, protože se budou vyřizovat pouze platné požadavky na authentikaci. Pokud položku nezakážeme,nebo nezměníme tak se použije hodnota 5. Položkou „SAE Max Failure Rate:“ omezíme počet neúspěšných asociačních požadavků klientských stanic za minutu, kdy po dovršení tohoto čísla nebude AP přijímat žádné nové požadavky na asociaci. Ve výchozím stavu je tato hodnota nastavéná na 40. Poslední položkou „OWE Transition Interface:“ můžeme po vytvoření virtuálního wifi rozhraní provozovat nezabezpečenou síť na jednom AP. Kdy zařízení které podporují standard Enhanced Open by se měli připojit pomocí OWE a tak komunikovat šifrovaně kdežto zařízení tuto možnost nepodporující by měli komunikovat jako ve standardní nezabezpečené síti. Toto virtuální rozhraní tedy vybereme v této nabídce.

Na další záložce EAP, najdeme možnosti „EAP Methods“ kde můžeme zvolit podporovanou metodu authentikace. Dále zde máme položku „EAP Certificate Mode“ kde můžeme zvolit jakým způsobem se má zacházet s TLS certifikátem RADIUS serveru. Dále pak tu je „EAP TLS Certificate“ kdy vybíráme název nebo ID certifikátu zabezpečení v úložišti certifikátu na našem zařízení. Do položky „EAP username“ vyplňujeme jméno pro přihlášení. „EAP Anonymous Identity“ je volitelná položka kterou můžeme vyplnit pro vzdálenou authentifikaci. Do položky „EAP Password“ vyplňujeme heslo které se má použít pro přihlášení. A v poslední položce nastavujeme, jestli se mají poslat přihlašovací informace RADIUS serveru pro ověření uživatelů. [8]

Authentication Types – (může být povoleno současně)	WPA PSK	WPA2 PSK	WPA EAP	WPA2 EAP	WPA3 PSK	OWE	WPA3 EAP	WPA3 EAP 192
WPA PSK	1	A	A	A	X	X	X	X
WPA2 PSK	A	1	A	A	A	X	X	X
WPA EAP	A	A	1	A	X	X	X	X
WPA2 EAP	A	A	A	1	A	X	A	X
WPA3 PSK	X	A	X	A	1	X	X	X
OWE	X	X	X	X	X	1	X	X
WPA3 EAP	X	X	X	A	X	X	1	X
WPA3 EAP 192	X	X	X	X	X	X	X	1
Encryption (MikrotikKlient)								
CCMP		A			A	A		
CCMP 256		A			A	A		
GCMP		A			A	A		
GCMP 256		A			A	A		
TKIP	N	N	N	N	X	X	X	X
Encryption (AX210-W10), (Intel AC9560-W11) – připojí se A/N X-nelze								
CCMP		A			A	A		
CCMP 256		N			N	N		
GCMP		N			N	N		
GCMP 256		N			N	N		
TKIP	N	N	N	N	X	X	X	X
Encryption (Nokia7.2-Android_11 1.10.2022) – připojí se A/N X-nelze								
CCMP		A			A	A		
CCMP 256		N			N	N		
GCMP		N			N	N		
GCMP 256		A			A	A		
TKIP	N	N	N	N	X	X	X	X
Group Encryption (Jde konfigurovat)								
CCMP	A	A	A	A	A	A	A	X
CCMP 256	X	A	X	A	A	A	A	A
GCMP	X	A	X	A	A	A	A	X
GCMP 256	X	A	X	A	A	A	A	A
TKIP	A	A	A	A	X	X	X	X

Obrázek 3: kompatibilita metod zabezpečení a možnost připojení některých zařízení

V tabulce níže je kompatibilita jednotlivých možností nastavení ověřovacích metod mezi sebou:

4 Útoky na WPA3

4.1 Downgrade

Největším bezpečnostním rizikem při použití WPA3 je když je AP nakonfigurováno aby bylo zpětně kompatibilní pro klienty kteří WPA3 nepodporují. To znamená když je použito WPA3 zabezpečení v tranzitním režimu, který je zpětně kompatibilní s WPA2. V takovém případě je možnost použití downgrade útoku buď způsobem MiTM, kdy můžeme zachytit beacon rámec vysílaný AP a pozměnit jeho část kde AP dává klientské stanici vědět jaké funkce podporuje, kde odstraníme informaci o tom že AP podporuje WPA3 a budeme takto upravené beacon rámce vysílat a tím máme možnost že klientská stanice zachytí námi modifikovaný beacon rámec,a i když sama o sobě bude podporovat WPA3, tak jí tak donutíme aby použila starší zabezpečení

WPA2 a 4-way handshake. Pokud stanice ale WPA3 nepodporují tak můžeme zachytit 4-way handshake i tak.

Stejným typem tohoto útoku také může být, pokud známe název Wifi sítě SSID, vytvořit vlastní AP, podporující pouze WPA2, se stejným názvem.

Dalším typem downgrade útoku může být pozměnění zpráv při vyjednávání pomocí SAE handshaku, kdy můžeme odstranit informace o podpoře kryptografie eliptických křivek a donutit tak AP k použití jiného typu křivky, což je méně bezpečné. [19]

4.2 Side-channel leaks

Dalším typem útoku může být cache-based side-channel útok, kdy klient využije aplikaci se škodlivým kódem nebo JavaScript běžící v prohlížeči, který zjistí jaká část v algoritmu Dragonfly byla použita při generování hesla. A společně s timing-based side-channel útokem, který je založený na měření času potřebného k zakódování hesla během Dragonfly handshaku, můžeme odvodit kolik iterací bylo zapotřebí. Tyto informace pak mohou pomoci k prolomení hesla hrubou silou.[19]

4.3 FragAttacks: Fragmentation & Aggregation Attacks

FragAttack je nástroj, který umožňuje testovat AP a WiFi klienty jestli jsou zranitelní vůči fragmentačním a agregačním útokům. Tyto zranitelnosti mohou postihovat všechny chráněné WiFi sítě. Tyto typy útoků jsou použitelné jak proti WPA2 tak WPA3, protože oba dva protokoly využívají CCMP nebo GCMP šifrovací protokoly.

Nástroj byl vydán Mathym Vanhoefem z KU Leuven výzkumné skupiny a centrem pro kybernetickou bezpečnost NYU Abu Dhabi.*[27]*

4.3.1 Použití nástroje

Nástroj lze stáhnout ze stránek projektu na GitHubu.*[28]* Nástroj byl nainstalován dle pokynů se všemi doporučenými ovladači. Jako operační systém byl tedy použit Ubuntu 20.04 s dodatečně nainstalovaným kernelem 5.8. Pro testování byl použit notebook DELL Latitude 3480 s procesorem i3-7100 a 8GB RAM, jako síťová karta byl použit USB síťový adaptér TP-Link TL-WN722N v1 s atheros chipsetem. Router zvolený pro otestování byl použit MikroTik HAP AX2 s továrním firmwarem RouterOS 7.6 následně upgradovaný na 7.7 a 7.8. Z důvodu kompatibility síťové karty byly testy prováděny pouze na 2,4Ghz pásmu. A budu testovat pouze WPA3 Personal.

4.3.2 Provedení Testování

Pro provedení testu na zranitelnosti musíme nejdříve upravit konfigurační soubor ve složce „fragattacks/research“ s názvem „client.conf“, kde najdeme popisek „ WPA3 home network“ pod který musíme zadat SSID a heslo naší WiFi sítě. Poté následně byly provedeny jednotlivé příkazy, s tím že pokud nějaký test projde, je tedy tím myšleno že zařízení je zranitelné.

Níže vidíme tabulku ve které jsou popsány typy útoků, řádky které jsou zabarveny modře, vyžadují kontrolu na druhém PC pomocí nástroje Wireshark a nebo tcpdump.

4.3.2.1 Výsledky

Vysledky Testovani Fragattacks			
Test	**ROS 7.6**	**ROS 7.7**	**ROS 7.8**
Kontrola funkčnosti			
klasický ping	úspěšný	úspěšný	úspěšný
fragmentovaný ping	úspěšný	úspěšný	úspěšný
základní zkouška zařízení			
fragmentovaný ping se spožděním mezi fragmenty	úspěšný	úspěšný	úspěšný
fragmentovaný ping proložený jiným rámcem			
frtagmenovaný ping proložený jiným rámcem s kontrolou číslování rámců	úspěšný	úspěšný	úspěšný
Útok A-MSDU			
ping zabalený do klasického A-MSDU rámce	úspěšný	úspěšný	úspěšný
poslaání A-MSDU rámce s LLC/SNAP hlavičkou	neúspěšný	neúspěšný	neúspěšný
poslání A-MSDU rámce s LLC/SNAP hlavičkou – chybný	neúspěšný	neúspěšný	neúspěšný
Kombinovaný klíč			
Pošle 2 fragmenty s jiným klíčem relace	neúspěšný	neúspěšný	neúspěšný
Pošle 2 fragmenty s jiným klíčem relace (funkční i když cíl podporuje pouze pakety jdoucí po sobě)	neúspěšný	neúspěšný	neúspěšný
útok na cache			
pošle fragment,následně zkusí vynutit reassociaci a poté pošle 2. fragment	neúspěšný	neúspěšný	neúspěšný
pošle fragment,následně zkusí vynutit reassociaci a poté pošle 2. fragment akorát s větším odstupem	neúspěšný	neúspěšný	neúspěšný
pošle fragment, následně se odpojí a znovu připojí a poté pošle 2. fragment	neúspěšný	neúspěšný	neúspěšný
pošle fragment, následně se odpojí a znovu připojí a poté pošle 2. fragment s delším odstupem	neúspěšný	neúspěšný	neúspěšný
Pakety nejdou po sobě			
fragmentovaný ping, aby pakety nešli po sobě	neúspěšný	neúspěšný	neúspěšný
kombinovaný útok s šifrovanými a nešifrovanými rámci			
Pošle 1. fragment šifrovaný a 2. v plantextu	neúspěšný	neúspěšný	neúspěšný
Pošle 1. fragment v plantextu a 2. šifrovaný	neúspěšný	neúspěšný	neúspěšný
pošle ping v plantextu	neúspěšný	neúspěšný	neúspěšný
fragmentovaný ping s fragmenty v plantextu	neúspěšný	neúspěšný	neúspěšný
mixovaný fragmentovaný ping plaintext/encrypted pro linux	neúspěšný	neúspěšný	neúspěšný
broadcast fragment attack			
pošle unicastový ping v plaintextu s 2. fragmentem jako broadcast	neúspěšný	neúspěšný	neúspěšný
pošle unicastový ping v plaintextu s 2. fragmentem jako broadcast. Behem handshake	neúspěšný	neúspěšný	neúspěšný
A-MSDU EAPOL útok			
pošle A-MSDU rámec obsahující ping označený jako EAPOOL	neúspěšný	neúspěšný	neúspěšný
pošle A-MSDU rámec obsahující ping označený jako EAPOOL poslaný během handshake	neúspěšný	neúspěšný	neúspěšný
pošle poškozený A-MSDU rámec obsahující ping označený jako EAPOOL	neúspěšný	neúspěšný	neúspěšný
pošle poškozený A-MSDU rámec obsahující ping označený jako EAPOOL poslaný během připojování	neúspěšný	neúspěšný	neúspěšný

Obrázek 4: fragattacks-normal

Rozšířený test zranitelností			
A-MSDU útok			
kontrola jestli je ignorovaný A-MSDU rámec	neúspěšný	neúspěšný	neúspěšný
ověří jestli je A-MSDU rámec ověřen a až poté ignorován	neúspěšný	neúspěšný	neúspěšný
Mixed key attack			
Pokud je nový klíč aplikován pozdě	neúspěšný	neúspěšný	neúspěšný
pokud je přijmut datový rámec během handshaku výměny klíčů	neúspěšný	neúspěšný	neúspěšný
pokud zařízení provede handshake během výmeny klíčů v plaintextu	neúspěšný	neúspěšný	neúspěšný
pokud zařízení provede handshake během výmeny klíčů v plaintextu s aktivním vyžádáním změny klíče	neúspěšný	neúspěšný	neúspěšný
pokus aplikovat nový klíč po odeslání 3.zprávy během 4-cestného handshaku	neúspěšný	neúspěšný	neúspěšný
stejné jako předchozí 4 testy, akorát s delší prodlevou před posláním 2. fragmentu	neúspěšný	neúspěšný	neúspěšný
cache attack			
test útoku na cache, kdy 2. fragment je poslán v plaintextu	neúspěšný	neúspěšný	neúspěšný
mixed plain/encrypt útok			
poslání klasického pingu jako fragmentovaný A-MSDU rámec	neúspěšný	neúspěšný	neúspěšný
fragmentovaný ping s 1. a 3. rámcem šifrovaným a 2. v plaintextu	neúspěšný	neúspěšný	neúspěšný
kontrola broadcastu			
ping v plaintextu jako broadcast po 4-cestném handshaku	neúspěšný	neúspěšný	neúspěšný
ping v plaintextu jako broadcast během 4-cestném handshaku	neúspěšný	neúspěšný	neúspěšný
ping v plaintextu během 4-cestného handshaku	neúspěšný	neúspěšný	neúspěšný
pošle broadcastem fragment	neúspěšný	neúspěšný	neúspěšný
A-MSDU EAPOOL útok			
plaintext A-MSDU rámec obshující ping poslaný během handshake(proti AP)	neúspěšný	neúspěšný	neúspěšný
AP forwards EAPOL attack (§6.6)			
test jestli AP přepošle EAPOL rámec	neúspěšný	neúspěšný	neúspěšný
test jestli AP přepošle fragmentovaný EAPOL rámec	neúspěšný	neúspěšný	neúspěšný
Test podpory fragmentace			
pošle ping v zašifrovaném 2. fragmentu, bez odeslání 1. fragmentu	neúspěšný	neúspěšný	neúspěšný
pošle ping v zašifrovaném 1. fragmentu bez odeslání 2. fragmentu	neúspěšný	neúspěšný	neúspěšný

Obrázek 5: fragattacks-extended

Výše vidíme dvě tabulky které nám říkají úspěšnost testu, Všechny červené položky jsou testy proti zranitelnostem, které se neprojevily. Modře zabarvené řádky nám ukazují testy,

které pro ověření je nutné zkontrolovat na druhém PC Připojeném na stejnou Wifi. Výsledky jsem kontroloval na PC s Windows 10, ve Wiresharku.

Pro semi automatické testování byl vyvinut script. Viz. Příloha4

4.4 Dragonblood

Je sada nástrojů pro testování zranitelností WPA3 a SAE handshaku nazývaného též Dragonfly, a zároveň soupis objevených zranitelností profesorem Mathy Vanhoefem a Eyal Ronenem, kteří o těchto zranitelnotech publikovali dokument „Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd“*[22][23][25][25]*

V sadě nástrojů jsou obsaženy tyto:

- Dragonslayer – Provádí útok proti EAP-PWD klientům a serveru, má za cíl obejít autentizaci při znalosti pouze jména. Já jsem se zaměřil pouze na SAE handshake poskytovaný pouze routerem, bez využití externího authentikačního serveru.
- Dragondrain – nástroj zaměřený proti SAE handshaku k ověření jestli je AP odolný vůči útoku typu DoS.
- Dragontime – Experimentální nástroj proti SAE handshaku kdy jsou použity MODP skupiny 22, 23 nebo 24. Většina implementací tyto skupiny nepodporuje. Já jsem pomocí tohoto nástroje netestoval, jelikož RouterOS od MikroTik, nemá tyto skupiny implementované.
- Dragonforce – experimentální nástroj, který pomocí informací získaných díky timing a cache-based útokům, provádí password partitioning útok, který je podobný slovníkovým útokům. Tento nástroj jsem vynechal, protože je značně složitý.*[26]*

4.4.1 Dragondrain-and-time

Nástroj poskytuje možnost provedení útoku typu DoS (Denial of service). Tento útok je založený na principu, kdy AP je nuceno výpočty ověřovat jestli daný klient je oprávněný připojit se k síti. Tím že je zatíženo vyřizováním požadavků od klientů, dojde k zahlcení výpočetních zdrojů vedoucí buď k nemožnosti připojení legitimních klientů a nebo k odpojení již připojených. V nejhorším případě může vést až k restartování zařízení. Je v podstatě zacílen proti anti-clogging mechanismu pro ochranu před větším počtem souběžně vyřizovaných žádostí o připojení.

4.4.1.1 Provedení útoku

Pro provedení útoku byl použit notebook DELL Latitude 3480 s CPU i3-7100, 8GB RAM s nainstalovaným OS Kali Linux 2022.3 s připojeným USB WiFi adaptérem TP-Link TL-WN722N v1 podporující monitorovací a injektující režim. Nástroj byl nainstalován dle návodu na stránkách projektu.[24]

Jako testovaný router byl použit Router MikroTik HaP ax2 s oficiální podporou WPA3 za použití zabezpečení WPA3-PSK (SAE) Only, s vypnutou podporou WPA2. Router měl jako tovární firmware RouterOS 7.6, tudíž byly postupně otestovány verze RouterOS 7.6, 7.7 a 7.8 protože MikroTik routery nepodporují downgrade na verze nižší než tovární.

Testování probíhalo spouštěním příkazu:

dragondrain -d wlan1 -a XX:XX:XX:XX:XX:XX -c 6 -b 54 -n 1 -r 200

s pozměněnými parametry viz níže.

Tento příkaz slouží k ověření jestli je možné obejít anti-clogging mechanismus. Následně byli měněny parametry příkazu, a sledováno jestli se v závislosti na změně nějakého parametru výrazně liší účinnost útoku. Pro možnost porovnání, bylo uděláno od verze příkazu 3 pokusy. (verzí příkazu rozumíme s různými parametry) Zjišťování zda-li je prováděný útok účinný bylo prováděno na jiném PC, který byl připojen k testovanému routeru prostřednictvím hostitelské lokální sítě z WAN strany testovaného routeru. Pomocí programu WinBox, byla sledována na záložce „System/Resources“ položka „CPU Load“, pro detekci jestli nějakým větším způsobem dochází k zatěžování systému. A na kartě „Wireless“, na záložce „Registration“, byli sledováni připojení klienti. Při provádění testů byli připojeni 2 zařízení. Při spuštění útoku se spustila časomíra a byli sledováni připojení klienti, zda-li dojde k jejich odpojení. V případě že došlo k odpojení klientů, tak byl zaznamenán čas a přerušen útok. Časomíra zůstala spuštěná do doby, dokud nedošlo znovu k poklesu vytížení procesoru. Během této doby byly prováděny nahodilé pokusy o znovupřipojení klientů. Aby pokud možno nemohlo dojít ke zkreslení výsledků pokusu, byl po každém provedeném pokusu router restartován. Pokud nedocházelo k odpojení připojených klientů a zároveň bylo nízké vytížení procesoru, byl test po 5-ti minutách přerušen a označen za neúspěšný. V případě neúspěšného pokusu byl pokus opakován ještě jednou. Takto byl test proveden postupně pro 3 verze RouterOS. Díky tomu že bylo zjištěno že jednotlivé pokusy se stejnými parametry se zásadně neliší, tak pokusy pro následující RouterOS byly provedeny už jenom jednou.

Používané parametry při spuštění příkazu jsou následující:

-d – vybraná síťová karta

-a – MAC adresa bezdrátového rozhraní na routeru vůči kterému vedeme útok

-c – WiFi kanál na kterém router vysílá

-b – bitrate

-n – počet podvrhovaných MAC adres

-r – počet podvržených handshaků za vteřinu

-g – specifikace DH skupiny pro výpočet eliptické křivky

4.4.1.2 Výsledky útoku

V tabulce DRAGONDRAIN viz příloha1, vidíme jednotlivé výsledky.

RouterOS 7.6

z tabulky jde vyčíst, že příkazem kterým se provádí útok:

„dragondrain -d wlan1 -a 48:A9:8A:30:30:C4 -c 6 -b 54 -n 2 -r 200“ pro -n (1-4)

jde obejít anti-clogging mechanismus. Během provádění příkazu se nejde připojit k wifi síti, ale již připojení klienti zůstávají připojeni a funguje jim i internet. Shodně u všech variant příkazu pro -n = 1-4, dojde po zhruba 4 - 4,5 minutách k odpojení klientů od wifi. Zároveň s tím přeruším útok. Následně trvá ještě přibližně 2,5 minuty, než přestane být vytížen procesor routeru a umožní připojení klientů. Po celou tuto dobu se k routeru nelze připojit, dokonce ani když se snažíme připojit pomocí 5Ghz rozhraní a CPU je vytížen na 25%.

Pro -n >= 5 nedojde k takovému vytížení CPU a nedojde k odpojení již připojených klientů, ale nejde se připojit k wifi během provádění útoku. Po ukončení útoku se jde hned normálně připojit.

Dále lze z měření vyčíst že pokud se pro útok použije DH skupina 20 a 21 nastavovaná parametrem „-g“ dochází po ukončení útoku k prodlužování doby kdy se nejde k wifi připojit. V případě DH skupiny 20, v průměru skoro na 13,5 minuty a u skupiny 21 dokonce až 33 minut. Po tomto zjištění byl zkušebně změněn parametr „-r“ udávající počet poslaných COMMIT rámců, na hodnotu 25, s předpokladem že by mohlo dojít ke snížení času nedostupnosti wifi, díky menšímu zahlcení COMMIT rámci. Ovšem tato domněnka se nepotvrdila.

RouterOS 7.7

Oproti předchozí verzi systému, pro parametr „-n“ 1-4, i navzdory vytížení CPU na 25%, nedojde k odpojení již připojených klientů a po přerušení útoku se ještě nelze přihlásit k WiFi cca 3-3,5 minuty. Při překročení „-n“ >= 5 zafunguje anti-clogging mechanismus, takže vytížení CPU je nízké, ale během útoku se nelze připojit k wifi. Ihned po přerušení útoku se k WiFi lze opět připojit. Obdobně jako v předchozí verzi systému se u „-g“ 20 a 21 výrazně prodlužuje doba po kterou se nelze připojit k Wifi po přerušení útoku. DH skupiny 20 na 19,5 minuty a u skupiny 21 dokonce až na 1 hodinu.

RouterOS 7.8

Zatím nejaktuálnější systém, oproti oboum předchozím verzím, nedochází k výraznému zatížení CPU pro „-n“ 1-5 a nedojde ani k odpojení již připojených klientů a během provádění útoku se lze s menšími potížemi připojit k WiFi. Po přerušení útoku se lze okamžitě připojit. Pro „-n“ 10 dojde k zatížení CPU na 0-12%, ale taktéž nedojde k odpojení klientů a po přerušení útoku se lze ihned normálně připojit. Dokonce pro DH skupiny 20 a 21, taktéž nedojde k odpojení připojených klientů a dokonce ihned po skončení útoku se lze připojit. Jediné slabší místo je pro vysoký parametr „-n“ v tomto případě 100, kdy se během útoku nelze připojit a pravděpodobně kvůli anti-clogging mechanismu, i když není CPU extrémně vytížen, se nešlo připojit více než 12 minut po přerušení útoku. Díky tomuto jsem zkusil následně tento mechanismus vypnout a následně se bylo možné po přerušení útoku ihned připojit.

Pro Možnosti testování byl vyvinut script Dragondrain.script.sh viz Příloha2

5 Doporučení

Na základě zjištěných skutečností bych doporučil, aby v případě nasazení WiFi routeru MikroTik s podporou WPA3, byl na routeru nainstalován nejnovější operační systém RouterOS, nyní RouterOS 7.8. V nastavení WiFi aby pokud možno bylo pouze zabezpečení WPA3-PSK a aby byl deaktivovaný mechanismus anti-clogging, hlavně z důvodu rychlejšího zotavení v případě DoS útoku.

Slovník pojmů

OID - Object Identifier, PMF - Protected Management Frame, PSK - Preshared key, RSN - Robust Security Network, RSNE - RSN element, SAE - Simultaneous Authentication of Equals, SAE-PK - SAE Public Key, SSID - Service set identifier, WPA3 - Wi-Fi Protected Access® 3, CPU – procesor, DH – Diffie-Hellman, EAP – Extensible authentication protocol, OWE - Opportunistic Wireless Encryption,

Seznam literatury

[1] Wikipedia contributors. "Simultaneous Authentication of Equals." Wikipedia, The Free Encyclopedia. Available: https://en.wikipedia.org/wiki/Simultaneous_Authentication_of_Equals. [Accessed: April 13, 2023].

[2] Graham, M. "Dragon Fly - Zero Knowledge Proof." asecuritysite.com. Available: https://asecuritysite.com/encryption/dragon. [Accessed: April 13, 2023].

[3] Suresh, A. "WPA3-SAE Mode." mrn-cciew. Available: https://mrncciew.com/2019/11/29/wpa3-sae-mode/. [Accessed: April 13, 2023].

[4] PlanetMath.org. (n.d.). Elliptic Curve Cryptography [Webpage]. Retrieved from https://planetmath.org/ellipticcurvecryptography

[5] Praneeth. "WPA3 Authentication – PART 1." Praneeth's Blog. Available: https://praneethwifi.in/2021/02/04/wpa3-authentication-part-1/.

[6] "WPA3 Dragonfly Handshake." hu-berlin.de. Available: https://sarwiki.informatik.hu-berlin.de/WPA3_Dragonfly_Handshake.

[7] Weisstein, E.W. "Elliptic Curve Cryptography." From MathWorld--A Wolfram Web Resource. Available: https://mathworld.wolfram.com/EllipticCurveCryptography.html. [Accessed: April 13, 2023].

[8] "WifiWave2." RouterOS - MikroTik Documentation. Available: https://help.mikrotik.com/docs/display/ROS/WifiWave2. [Accessed: April 13, 2023].

[9] Wi-Fi Alliance. (2018). WPA3 Specification v3.1 [PDF file]. Retrieved from https://www.wi-fi.org/download.php?file=/sites/default/files/private/WPA3%20Specification%20v3.1.pdf

[10] Wi-Fi Alliance. "Wi-Fi CERTIFIED WPA3™ December 2020 update brings new protections against active attacks: SAE Public Key and Transition Disable." Wi-Fi Alliance. Available: https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security. [Accessed: April 13, 2023].

[11] Wi-Fi Alliance. "WPA3 Specification." wi-fi.org. Available: https://www.wi-fi.org/download.php?file=/sites/default/files/private/Wi-Fi_Protected_Access_3.pdf. [Accessed: April 13, 2023].

[12] Engel, C. "Microsoft PowerPoint - WLPC 55-Min Talk - WPA3 - final." d2cpnw0u24fjm4.cloudfront.net. Available: https://d2cpnw0u24fjm4.cloudfront.net/wp-content/uploads/2018/06/13201254/WLPC_55-Min_Talk_WPA3_final.pdf. [Accessed: April 13, 2023].

[13] Wikipedia contributors. Diffie-Hellman key exchange. In Wikipedia, The Free Encyclopedia [Webpage]. Retrieved from https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange

[14] Jager, T., Kohlweiss, M., Schäge, S., Schwenk, J., & Tredoux, C. (2019). On the Security of TLS 1.3 and QUIC Against Weaknesses in PKCS# 1 v1. 5 Encryption. In Advances in Cryptology – CRYPTO 2019 (pp. 733-762). Springer International Publishing.

[15] Password-authenticated key agreement - Wikipedia

[16] [802.11] NXP Community. (2020, June 10). 802.11 Wi-Fi Security Concepts [Webpage]. Retrieved from https://community.nxp.com/t5/Wireless-Connectivity-Knowledge/802-11-Wi-Fi-Security-Concepts/ta-p/1163551

[17] Meraki. (n.d.). WPA3 Encryption and Configuration Guide [Webpage]. Retrieved from https://documentation.meraki.com/MR/Wi-Fi_Basics_and_Best_Practices/WPA3_Encryption_and_Configuration_Guide

[18] Sectigo Store. (2020, June 09). ECDSA vs RSA: Everything You Need to Know [Webpage]. Retrieved from https://sectigostore.com/blog/ecdsa-vs-rsa-everything-you-need-to-know/

[19] Goodin, D. (2019, November 04). Serious flaws leave WPA3 vulnerable to hacks that steal Wi-Fi passwords. Ars Technica. Retrieved from https://arstechnica.com/information-technology/2019/04/serious-flaws-leave-wpa3-vulnerable-to-hacks-that-steal-wi-fi-passwords/

[20] Forum post. (2020, September 8). Retrieved from https://forum.mikrotik.com/viewtopic.php?t=180831#p894496

[21] MikroTik. (n.d.). RouterOS Changelog. Retrieved from https://mikrotik.com/download/changelogs#show-tab-tree_2-id-7cd31cf6820896d838535a73cafb15ca

[22] Mathy Vanhoef. About. Retrieved from https://www.mathyvanhoef.com/p/about.html

[23] Vanhoef, M. (n.d.). WPA3: Simultaneous Authentication of Equals. Retrieved from https://wpa3.mathyvanhoef.com/

[24] Vanhoef, M. (n.d.). Dragonblood and Time Attacks against WPA3 and EAP-pwd. Retrieved from https://github.com/vanhoefm/dragondrain-and-time

[25] Vanhoef, M., & Piessens, F. (2020). Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2020(3), 142-166.

[26] Vanhoef, M. (n.d.). WPA3 Tools. Retrieved from https://wpa3.mathyvanhoef.com/#tools
[27] FragAttacks. (n.d.). Retrieved from https://www.fragattacks.com/

[28] Vanhoef, M. (n.d.). fragattacks. Retrieved from https://github.com/vanhoefm/fragattacks
[29] Tan, H., Jia, X., Liu, S., Zhou, W., Lin, J., & Yang, X. (2021). A survey on the security of WiFi networks. Journal of Network and Computer Applications, 183, 103032. [30] Wi-Fi Alliance. (2020, December 7). Wi-Fi CERTIFIED WPA3™ December 2020 update brings new

protections against active attacks: SAE Public Key and Transition Disable. Retrieved from https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

[31]Vanhoef, M., & Ronen, E. (2019). Dragonblood: A Security Analysis of WPA3's SAE Handshake. Retrieved from https://www.semanticscholar.org/paper/Dragonblood%3A-A-Security-Analysis-of-WPA3's-SAE-Vanhoef-Ronen/8ff38f0627217ebcc7add9ad2a69bb28cd3dd6cf/figure/0

[32]TechTarget. (n.d.). WPA3 protocol: Should enterprises implement the changes? Retrieved from https://www.techtarget.com/searchsecurity/answer/WPA3-protocol-Should-enterprises-implement-the-changes.

Tabulka obrázků

Seznam Příloh