**OBOR**

**18-20-M/01 INFORMAČNÍ TECHNOLOGIE**

**ŠVP: Správa sítí a IT bezpečnost**

**MATURITNÍ PROJEKT**

TÉMA PRÁCE

**Bezpečnost v informačních technologiích**

2024/2025 Filip Struhár

**PROHLÁŠENÍ**

Prohlašuji, že jsem svou maturitní práci vypracoval samostatně a použil jsem pouze podklady (literaturu, projekty, SW, atd.) uvedené v seznamu.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne XX. X. 2025 ……………………………………

podpis

**PODĚKOVÁNÍ**

Text poděkování …. Běžně se děkuje rodinným příslušníkům za jejich morální podporu, vedoucí práce za její vedení, dalším konkrétním učitelům a konzultantům za věcné připomínky atd.

**ANOTACE**

|  |  |
| --- | --- |
| Jméno autora |  |
| Název maturitní práce | Musí se shodovat s oficiálním názvem práce v zadání |
| Rozsah práce | Počet stran práce ve formátu (např. 165 s. + 50 s. příloh) |
| Školní rok vyhotovení | 2024/2025 |
| Škola | Střední průmyslová škola na Proseku |
| Vedoucí práce |  |
| Využití práce | Zde popište použití práce, např. výukové účely v oboru Telekomunikace v předmětu tom a tom |
| Abstrakt | Např. Práce je zaměřena na návrh webové aplikace pro evidenci … |
| Klíčová slova | Zde uveďte klíčová slova práce, tj. slova, která definují její obsah, např. webové stránky, skriptovací jazyky, syntaxe,… |

**ANNOTATION**

|  |  |
| --- | --- |
| Autor |  |
| Title of graduation work |  |
| Extend | Např. 165 p. + 50 p. of appendices |
| Academic year | 2024/2025 |
| School | Střední průmyslová škola na Proseku |
| Supervisor |  |
| Application |  |
| Abstrakt |  |
| Key words |  |
|  |  |

**Obsah**

[1 ÚVOD 8](#_Toc190632184)

[2 Zabezpečení wifi 9](#_Toc190632185)

[2.1 Jak funguje wifi? 9](#_Toc190632186)

[2.2 Šifrovací metody 10](#_Toc190632187)

[2.2.1 WEP (Wired Equivalent Privacy) 10](#_Toc190632188)

[2.2.2 WPA (Wi-Fi Protected Access) 11](#_Toc190632189)

[2.2.3 WPA2 12](#_Toc190632190)

[2.2.4 WPA3 12](#_Toc190632191)

[2.3 Enterprise autentizace 13](#_Toc190632192)

[2.3.1 RADIUS server 13](#_Toc190632193)

[2.4 Zjednodušená autentizace ve WiFi sítích 13](#_Toc190632194)

[2.4.1 WPS (Wi-Fi Protected Setup) 14](#_Toc190632195)

[2.4.2 DPP (Device Provisioning Protocol) 14](#_Toc190632196)

[2.5 Segmentace sítě 15](#_Toc190632197)

[3 Bezpečnostní slabiny WiFi 16](#_Toc190632198)

[3.1 WEP 16](#_Toc190632199)

[3.2 Prolomení 4-Way handshake 17](#_Toc190632200)

[3.2.1 Vyjednání šifrovacích klíčů 17](#_Toc190632201)

[3.2.2 Brute force na handshake 18](#_Toc190632202)

[3.3 WPS 19](#_Toc190632203)

[3.3.1 Brute force 19](#_Toc190632204)

[3.3.2 Pixie dust 19](#_Toc190632205)

[3.4 PMKID 20](#_Toc190632206)

[3.5 Mann In The Middle 21](#_Toc190632207)

[3.5.1 Evil Twin 21](#_Toc190632208)

[3.6 Rogue AP 22](#_Toc190632209)

[3.7 Wifi jamming 22](#_Toc190632210)

[4 Specifikace systémových komponent 23](#_Toc190632211)

[4.1 Systémové specifikace 23](#_Toc190632212)

[4.2 Bezdrátové síťové karty 24](#_Toc190632213)

[4.2.1 Tenda U10 C650 24](#_Toc190632214)

[4.2.2 Mediatek MT7922 24](#_Toc190632215)

[5 Přístupové body 25](#_Toc190632216)

[5.1 Mikrotik RB941-2nDs 25](#_Toc190632217)

[5.2 TP-Link AX23 26](#_Toc190632218)

[SEZNAM OBRÁZKŮ 30](#_Toc190632219)

# ÚVOD

Text

# Zabezpečení wifi

Wifi je bezdrátová síťová technologie, která umožňuje mnoha zařízením komunikovat mezi sebou a internetem bez nutnosti zdlouhavého a složitého pokládání kabelů. Narozdíl od ethernetového řešení ale zdaleka nedosahuje tak vysokých přenosových rychlostí a spolehlivosti. Tato technologie je definována standardem IEEE 802.11.

## Jak funguje wifi?

Pro nasazení této technologie se používají wifi routery, repeatery a access pointy. K přenosu dat jsou používány rádiové vlny, které jsou vysílány na určitém frekvenčním pásmu. Obvykle se k přenosu využívají pásma 2,4GHz a 5GHz, kde 2,4GHz díky jeho delší vlnové délce poskytuje větší pokrytí a dosah, zatímco 5GHz vyšších přenosových rychlosti. U některých bezdrátových routerů s vyšší cenou se můžeme v dnešní době setkat s pásmem 6GHz. Dalšími důležitými pojmy jsou šířka pásma (20, 40 a 80MHz) a čísla kanálů, která se odvíjejí od frekvenčního pásma. Kanály umožňují vysílačům eliminovat jejich vzájemné rušení. Šířka pásma definuje množství dat, které může být v jednom čase přenášeno. Platí ale pravidlo, že čím vyšší je šířka pásma tím větší šíři kanálů vysílač “zabírá” a ruší. Wifi se dále dělí na různé standardy (Wifi 1 - 802.11b, Wifi 2 - 802.11a, …), které vnímáme jako generace obohacující technologii o vyšší přenosové rychlosti, funkce a pokročilejší bezpečnostní techniky.



Obrázek 1 - Wifi standardy

## Šifrovací metody

Díky tomu, že wifi nevyužívá žádné kabely a signály obsahující data vysílá volně do prostoru, není možné fyzicky zamezit tomu, aby si jakýkoliv náhodný útočník přenášená data zachytil a zpracoval. Kvůli této problematice postupem času začaly vznikat způsoby a techniky, jak uchovat přenášená data po wifi síti v bezpečí.

Šifrovací metody wifi slouží k ochraně přenášených dat před jejich odposlechem, autentifikaci klientů a kontroly integrity dat po přenosu po wifi. V dnešní době jsou známy tyto šifrovací protokoly: WEP, WPA, WPA2, WPA3. Šifrovací protokol WEP je považován za zastaralý a již by se z pohledu bezpečnosti neměl nacházet na žádné wifi síti. Nejbezpečnějším řešením v dnešním době je WPA3 nabízející nejpokročilejší šifrovací algoritmy a zabezpečovací funkce, ale není podporován všemi access pointy. V takovém případě je používán jeho předchůdce WPA2, který je stále široce využíván a je považován za bezpečný.

### WEP (Wired Equivalent Privacy)

První vyvinutou šifrovací metodou pro wifi. K šifrování dat používá RC4 64/128/256bitový klíč, který je sdílený mezi všemi zařízeními v síti, jedná se tedy o statický klíč. Skládá se ze dvou částí - sdíleného klíče (40, 104 nebo 232bitový) a inicializačního vektoru IV (24 bitů).

Inicializační vektor sdíleného klíče je připojen na začátek každého klíče a je vysílán nešifrovaně. Jeho účelem je diverzifikace klíče pro různé datové rámce, bohužel kvůli jeho délce dochází k opakování klíčů při delším používání.

Pro zajištění integrity dat WEP využívá CRC-32 kontrolní součet. Před odesláním dat je stejným RC4 klíčem šifrován takzvaný kontrolní součet (32bitový hash postaven z dat před odesláním), který je u přijímače po dešifrování zkontrolován, zda je totožný a nebyl cestou změněn. Autentizace u tohoto protokolu je pouze jednosměrná a je ověřován pouze klient. Existují dvě metody autentizace, a to „Open system“ autentizace, při které klient žádnou autentizací neprovádí nebo „Shared Key“ autentizace, při které se používá WEP klíč, který může být následně útočníkem z úvodního handshaku snadno získán.

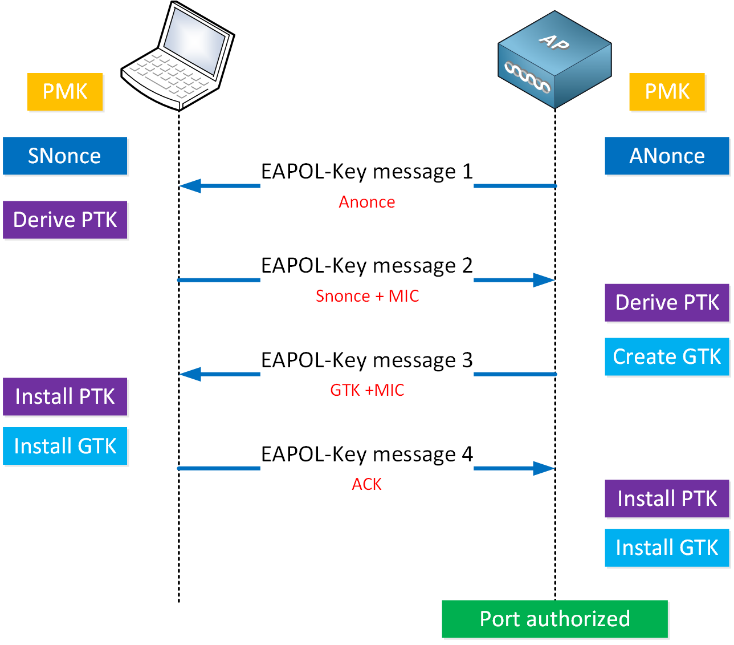
### WPA (Wi-Fi Protected Access)

Využívá k šifrování dat TKIP, který stále používá šifrovací algoritmus RC4 jako jeho základ, ale oproti WEP jsou klíče dynamické, to znamená, že pro každý paket je generován nový 128bitový klíč a v průběhu komunikace je klíč nadále měněn. Což zamezuje, aby byl útočník schopen případně získaným klíčem dešifrovat veškerou komunikaci.

Inicializační vektor je zde 48bitový. Pro kontrolu dat je využíván MIC, který je považován za bezpečnější než CRC-32 u WEP.

WPA umožnuje dva módy autentizace – Enterprise (802.11X) a PSK (Personal). Personal používá předem sdílené klíče, které jsou poskytnuty uživatelům autorizovaným pomocí hesla. Je často využíván v domácích sítích, zatímco Enterprise, jak už z názvu vypovídá, se zaměřuje více na firemní nebo podnikové řešení, kdy je k autentizaci potřeba autentizační server.

WPA také přišlo s metodou vyjednání šifrovacích klíčů pomocí 4way handshake, tyto PTK klíče používá klient a AP k šifrování své komunikace.



Obrázek 2 - 4-Way handshake

### WPA2

Velice populární a dodnes aktuální šifrovací metoda. Kombinuje funkcionality WPA, oproti TKIP využívá CCMP, který zajišťuje integritu dat na síti a jako šifrovací algoritmus používá AES, který je dodnes dostačující.

WPA2 zajišťuje implementaci a vyhovění všech požadavků standardu 802.11i, který vylepšuje autentizaci a šifrovaní pro sítě wifi.

### WPA3

WPA3 Personal již neautentizuje pomocí PSK klíčů a nahrazuje jej pomocí PAKE a šifrovacího algoritmu SAE, který zajišťuje bezpečnou výměnu klíčů i v případě slabšího hesla. WPA3 Enterprise nabízí šifrování 256bitovými klíči, takovéto opatření přináší větší odolnost vůči útokům s moderním hardwarem a splňuje normu CNSA, která je doporučena pro vysoce citlivé aplikace.

WPA3 také přidává metodu zabezpečení komunikace na otevřených wifi sítích pomocí standardu zvaného OWE. Ten šifruje komunikaci klientů s AP napříč tomu, že nevyžaduje heslo. Každý klient používá pro šifrovanou komunikaci vlastní unikátní klíč.

Dalším novým mechanismem je DPP označovaný jako Wi-Fi Easy Connect, který je bezpečným nástupcem WPS. Byl navržen pro snazší a pohodlnější připojení zařízení bez obrazovek (typicky IoT) do wifi sítí. Namísto slabého pinu DPP využívá QR kódy nebo NFC technologii k připojení zařízení. Easy Connect byl následně také rozšířen do WPA2.

## Enterprise autentizace

Tento mechanismus je podporován pouze u WPA2/WPA3, je označován jako standard 802.11X a je dále také využíván u ethernetových sítí.

Nepoužívá PSK klíče k autentifikaci jako Personal. K ověřování využívá univerzální autentizační framework EAP, který se dále dělí. EAP-TLS ověřuje na základě certifikátů na obou stranách. Dále se potkáme s PEAP, který nevyžaduje klientský certifikát a ověřuje klienta přihlašovacími údaji z AD. Používaný je také EAP-FAST (Cisco).

### RADIUS server

RADIUS je autorizační protokol, který ověřuje uživatele a spravuje jejich přístupy na síti.

Klienty může autentifikovat pomocí certifikátů nebo uživatelských údajů. Výhodou formy ověřování certifikáty je, že je síťový administrátor nasadí na uživatelská zařízení pomocí MDM nebo group policy a uživatelé pak již nemusí dále řešit hesla k wifi. Současně to také eliminuje možnost použití slabého hesla uživatelem. Na druhou stranu ověřování pomocí uživatelských údajů je pohodlné pro nasazení do již zavedeného prostředí AD.

RADIUS server můžeme mít externí, cloudový, ale může také být zabudovaný přímo v access pointu. Je také schopný pomocí funkce „Per-User VLAN Tagging“ automaticky dle certifikátu či přihlašovacích údajů rozřazovat uživatele do různých VLAN.

## Zjednodušená autentizace ve WiFi sítích

S příchodem IoT se velice zpopularizovalo používání chytrých zařízení jako jsou IP kamery, termostaty, chytré zámky a mnoho dalšího i v běžné domácnosti. Tento okruh zařízení obohacující chod domácnosti nazýváme “chytrá domácnost”. Tyto zařízení potřebují být k možnosti komunikace a nastavení vzájemně propojení. I přesto že existují řešení pro IoT jako je ZigBee, tak stále veliká část těchto prvků využívá nejčastěji síť wifi. Pro usnadnění připojení k wifi IoT zařízení, které mají většinou omezené možnosti uživatelského rozhraní, byla vyvinuta technologie WPS. Ta se ale později prohlásila za nebezpečnou kvůli útokům využívajících slabin této technologie. S příchodem Wifi 6 bylo vyvinuto bezpečné DPP splňující dnešní standardy pro běžné použití.

### WPS (Wi-Fi Protected Setup)

Tato technologie umožňuje zařízením alternativní možnost připojení k wifi síti, a to více způsoby. Prvním je, že určitou dobu po zmáčknutí WPS tlačítka na routeru, lze připojit jakékoliv zařízení podporující wifi bez nutnosti zadání hesla. Při tomto scénáři AP klientovi pomocí navázaného spojení handshakem předává heslo k síti. Klient si heslo ukládá a má tak k dispozici přístup k síti i po uplynutí časové lhůty, kdy je WPS aktivní po stisku. Některá klientská zařízení mohou mít tlačítko WPS také, v takovémto případě se pro autentizaci spínají obě tlačítka. Druhá forma zjednodušené autentizace funguje na bázi 8číselného PINu, který funguje jako alternativa pro přihlašování heslem. Tento PIN je náhodně vygenerován při zapnutí funkce WPS na routeru a je možné ho manuálně zvolit. K autentizaci musí klient vyplnit 8číselný PIN místo hesla a router následně klienta autentifikuje právě pomocí zadaného PINu.



Obrázek 3 - Detail WPS tlačítka

### DPP (Device Provisioning Protocol)

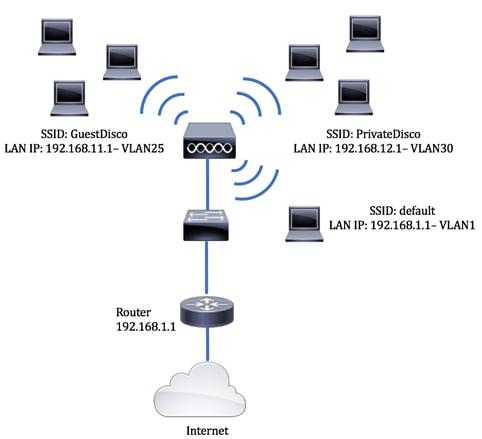
DPP neboli The Device Provisioning Protocol je technologie nahrazující zaostalé WPS. Bývá také marketingově označován jako Wifi Easy Connect. K šifrování hesla přenášeného mezi klientem a AP je využíván ECDH.

Prvky využívající DPP se rozdělují na Enrollee - klient, který se chce připojit k wifi pomocí DPP, Configurator - zařízení, které je již autentizováno a připojeno k wifi a poskytuje šifrování heslo enrollee zařízení. Poslední je Connector, to je speciální handshake, který je odpovědný za bezpečné předání.

V případě, že se enrollee chce připojit do sítě, configurator vygeneruje DPP URI sítě, která obsahuje veřejný bootstrapping klíč zařízení. Připojované zařízení má dva způsoby, jakým URI dostat – pomocí QR kódu nebo bezdrátových technologií jako je bluetooth nebo NFC. Po obdržení DPP URI naváží zařízení zabezpečené spojení pomocí ECDH. Dalo by se to nazvat privátním tunelem, ve kterém využívají své veřejné klíče k šifrování své komunikace. Přes takovýto šifrovaný tunel je následně konfigurátorem přeposíláno heslo, není ale přenášeno v plain textové podobě, ale ve formě již zmiňovaného connectoru, který umí dešifrovat pouze konkrétní zařízení.

## Segmentace sítě

Tato praktika, která se využívá nejen u wifi. Pomáhá zvyšovat bezpečnost a efektivitu správy sítě tím, že rozděluje velkou síť na menší, oddělené části nebo segmenty dle struktury filmy např.: vedení, zaměstnanci. Každý segment může mít své vlastní bezpečnostní politiky a monitoring. To umožnuje správcům efektivněji spravovat a řídit menší segmenty sítě než jednu velkou síť. Segmentaci sítě nejčastěji zajišťuje VLAN. Ta u access pointu funguje tak, že zobrazuje pro každou VLAN vlastní SSID a klientovi rámce jsou následně tagovány příslušným VLAN tagem pro danou virtuální síť. Zařízení pak mohou komunikovat pouze v rámci své virtuální sítě. Ke komunikaci mezi sítěmi VLAN je pak potřeba správně nakonfigurovaný směrovač.



Obrázek 4 - Schéma wifi VLAN

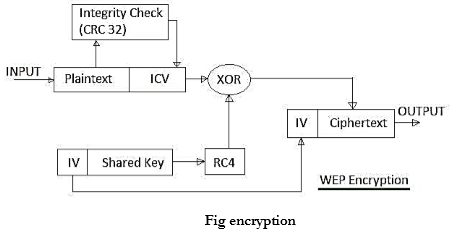
# Bezpečnostní slabiny WiFi

Bezpečnostní slabiny WiFi jsou v dnešní době velice častým cílem útoků díky hojné popularitě této technologie. Mezi nejčastější bezpečnostní rizika patří odposlouchávání či neoprávněný přístup do sítě, což jsou praktiky, proti kterým je potřeba se bránit.

## WEP

Oproti ostatním standardům má WEP hned několik slabin. První je jeho zranitelností je jeho fixní 64bitový nebo 128bitový klíč, který pro tuto dobu již považovaný za nedostatečný. I přesto, že byl v budoucnu obohacen o 256bitový klíč není tento standard považován za bezpečný. Jeho největší slabinou totiž není jeho délka klíče, ale způsob, jakým je klíč tvořen. WEP k šifrování používá statické klíče. To v praxi znamená, že každé zařízení na síti používá identický klíč. Proto je k tomuto klíči pro každý paket přidáván náhodné 24bitové číslo neboli inicializační vektor. Ten má zajistit různorodost klíče a je nešifrovaně obsáhnut v poslaném paketu, jelikož ho následně příjemce používá k dešifrování. Iniciační vektor se díky jeho nízkému počtu kombinací ve větší síti rychle začne opakovat.

Tohoto útočník dokáže snadno využít. Prvně začne tím, že zachytí velké množství paketů například pomocí nástroje wireshark. Z těchto paketů získá různé variace inicializačních vektorů, které se v síti objevují. Čím více tím větší šance, že bude klíč prolomen. Pak pomocí FMS nebo KoreK matematických algoritmů využívajících statistické vzorce je útočník schopen odvodit sdílený klíč neboli heslo k síti bez nutnosti slovníkového útoku. Tento zastaralý standard by tedy již z bezpečnostních důvodů neměl být využíván.



Obrázek 5 - Šifrování WEP

## Prolomení 4-Way handshake

Tímto typem útoku může útočník získat potřebný klíč pro dešifrovaní komunikace mezi access pointem a supplicantem neboli klientem nebo může kombinací s útokem hrubou silou získat heslo k wifi síti. Tento útok funguje na wifi sítě zabezpečené pomocí WPA nebo WPA2 autentizovaný pomocí pre-shared klíče PSK. To znamená, že náchylnými jsou šifrovací metody WPA Personal a WPA2 Personal. Doporučenou obranou proti tomuto typu útoku je nastavení silného hesla (ideálně 12místné se speciálními znaky a čísli) nebo přechod na IEEE 802.11X neboli Enterprise, který k autentizaci nepoužívá PSK, ale EAP/PEAP.

### Vyjednání šifrovacích klíčů

Průběh vyjednávání šifrovacích klíčů PTK a GTK je následující: AP i klient mají svůj PMK derivovaný z PSK a SSID. První EAPOL zpráva je poslána klientovi nazývá se Anonce. Pomocí Anonce, Snonce, PMK a MAC adres klienta a Access pointu klient odvodí svůj PTK. V druhé EAPOL zprávě posílá klient access pointu Snonce a MIC, kterým si druhá strana ověří kontrolu integrity dat. Tím je zajištěno, že data nebyla po cestě změněna. Access point obdobným způsobem odvodí svůj PTK. V případě že klient zadal špatný PSK (heslo na wifi), by access point v teto chvíli ukončil process vyjednávání klíčů a na další dva kroky by již nedošlo. V případě, že zadal klient správný PSK je poslána třetí EAPOL message klientovi se zašifrovaným GTK společně s MIC. Klíč GTK si klient ukládá a posílá čtvrtou a poslední EAPOL message oznamující access pointu, že má oba potřebné klíče a je připraven na šifrovanou komunikaci. Tento process probíhá při každé autentizaci nového zařízení do sítě.

Obsah obrázku text, snímek obrazovky, diagram, Písmo

Popis byl vytvořen automaticky

Obrázek 6 - Vyjednání šifrovacích klíčů

### Brute force na handshake

Cílem útočníka je zachytit EAPOL zprávy posílané mezi klientem a access pointem v rámci 4-Way handshake. K dosažení tohoto může buďto vyslat na access point deautentifikační paket, který vynutí konkrétnímu nebo všem klientům na síti znovu provést autentizaci nebo jednoduše vyčká na příchod nového zařízení do sítě. V případě, že zachytí handshake a získá všechny potřebné hodnoty k vygenerování PTK, může útočník zkoušet různé kombinace hesel a konstruovat pomocí nich vlastní PTK. Pokud útočníkem zkonstruovaný PTK odpovídá zachycenému PTK, heslo do sítě je prolomeno.

## WPS

První zřejmou slabinou WPS je, že každý, kdo má fyzický přístup k routeru má možnost zmáčknout WPS tlačítko a dostat se jak do sítě bez nutnosti znát jakékoliv heslo či PIN. Dále je WPS náchylné na další komplexnější útoky, které autor rozebere níže. Oproti prolomení handshake u WPA je u tohoto protokolu jedinou možností efektivní ochrany protokol kompletně vypnout a přejít na novější a bezpečnější DPP.

### Brute force

Tento útok probíhá „online” a útočník se při něm zkouší různé PIN kódy oproti routeru dokud není úspěšný. Jedná se o méně efektivní útok a díky 100 miliardám kombinacím PINu je na slabších zařízeních neproveditelný. Router může mít proti tomuto typu útoku implementovaný obranný mechanismus, který je schopen dočasně vypínat WPS po zaznamenání více neúspěšných pokusů o autentizaci.

### Pixie dust

Oproti brute force útoku na WPS se jedná o „online” útok, který je mnohonásobněji efektivnější. Využívá totiž bezpečnostního nedostatku designu autentizačního PINu WPS - 8místný kód se totiž skládá ze dvou klíčů (4místného a 3místneho) a posledním číslem je kontrolní součet. WPS používá k autentizaci tuto sekvenci:

Obsah obrázku text, snímek obrazovky, software, diagram

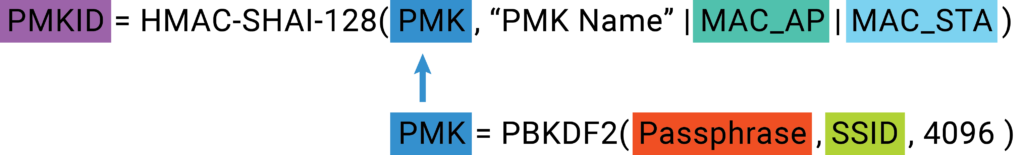
Popis byl vytvořen automaticky

Obrázek 7 - Autentizační sekvence WPS

Zachycením této sekvence získá hashované výstupy obou PINů a potřebné hodnoty k replikovaní algoritmu generujícího tyto hashované výstupy. Tímto způsobem následně útočník offline slovníkovým útokem jednotlivé klíče prolamuje každý zvlášť, což snižuje počet kombinací na 10 000 u prvního klíče a 1000 u klíče druhého. Jedná se o tak málo kombinací, že jsou tuto šifru schopni prolomit i slabší zařízení.

## PMKID

Útok na PMKID se zaměřuje na sítě využívající access point roaming definován ve standardu IEEE 802.11r. Tento mechanismus zajišťuje plynulé přepojování a přesouvaní klientů v síti z jednoho AP na druhé. Zařízení se automaticky přepojuje vždy k nejbližšímu access pointu jemu dostupnému a jeho aktivní síťové relace jsou bez přerušení přenášeny mezi AP spolu s ním. Tento standard potřebuje efektivní a rychlý způsob autentizačního procesu klienta pro plynulý přechod bez odezvy či ztráty spojení mezi access pointy. Z tohoto důvodu místo opakovaného provádění 4-Way handshake access pointy využívají funkcionalitu PMK caching, která právě pracuje s PMKID. Ten je hashem generovaným access pointem při procesu autentizace, který obsahuje PMK.



Obrázek 8 - Detail PMKID

Nebezpečnost útoku spočívá v tom, že utočník při jeho provedení nepotřebuje deautentizovat klienty jako tomu bylo u handshake prolomení, ale stačí mu jednoduše PMKID od AP vyžádat.

V případě že útočník zná SSID, MAC AP, MAC klienta a PMK, což jsou potřebné hodnoty k vygenerování PMK a následného vygenerování PMKID, může slovníkovým útokem zkoušet hesla, dokud zachycený PMKID nebude s útočníkovým vygenerovaným PMKID identický. V takové chvíli je heslo uhodnuto. Obranou proti tomuto útoku je úplné vypnutí access point roamingu v případě, že není používán či použití silného hesla wifi.

## Mann In The Middle

Skupina útoků týkajících se nejen wifi, ale mnoha dalších komunikačních technologií, kde se dává důraz na jejich bezpečnost. Primárním cílem MITM útoku je dostat odposlouchávající zařízení mezi zařízení komunikující mezi sebou aniž by o tom věděli. Výsledkem je poté únik či manipulace s daty. To může hrát klíčovou roli pro provedení dalších útoků jako je krádež identity či přihlašovacích údajů. S tímto útokem se můžeme potkat nejčastěji ve veřejných prostorech jako jsou kavárny, restaurace a bary.

### Evil Twin

Často se snaží uživatele oklamat tím, že je nakonfigurován s obdobnými parametry jako má skutečný access point například v nějaké kavárně. Často se útočník snaží nabídnout svým klientům vyšší sílu připojení, aby se jim jeho access point zobrazoval výše ve wifi nabídce než originální access point. Může se také stát, že útočník skutečný access point vyřadí rušením.



Obrázek 9 - Evil Twin

Tento typ útoku se dělí na pasivní odposlech, při kterém útočník procházející komunikaci může pouze číst a na aktivní odposlech, při kterém může útočník data upravovat a manipulovat. Zatímco pasivní odposlech útočníkovi umožní například získat citlivé údaje a hesla oběti, aktivní odposlech může vést například ke scénaři kdy útočník poslanou transakci po síti přesměruje na svůj bankovní účet.

Efektivní prevencí proti takovému útoku je opatrnost, HTTPS protokol, či využití VPN.

## Rogue AP

Jedná se o neautorizovaný access point nainstalovaný v síti bez souhlasu vlastníka. Nejčastěji se s ním potkáme ve firemních prostředích. V některých případech může být vytvořen například zaměstnancem neumýslně. I v takovémto případě se jedná o nelegalní činnost. Oproti Evil Twin je cílem otevřít backdoor do sítě a umožnit tak další útoky jako je MITM, sniffing, monitoring, phishing a další…

Obsah obrázku text, snímek obrazovky, Písmo, symbol

Popis byl vytvořen automaticky

Obrázek 10 - Rogue AP

## Wifi jamming

Tento útok využívá deautentizační rámce. To je typ management rámce, který vynutí konkrétnímu klientovi na základě MAC adresy či všem klientům na síti použítím broadcastové MAC adresy ukončit jejich spojení s access pointem. Tyto zařízení se následně do sítě dostanou opakovanou autentizací. Útok spočívá v tom, že se útočník vydává za access point (AP spoofing) a opakovaně zaplavuje síť či klienta těmito rámci. Tím docílí, že cílová zařízení opakovaně ukončují své spojení s reálným AP a tím dočasně vyřadí klienta či síť z provozu. K tomuto útoku stačí znát pouze BSSID sítě a případně MAC adresu klienta, což jsou jednoduše sniffovatelné informace. Zařízení samotná nemají žádnou možnost, jak zjistit, že se jedná o činnost útočníka nikoliv reálného AP, proto jim slepě věří. Jako prevence slouží mechanismus PMF, který nabizí pouze některé access pointy. Tento mechanismus umožňuje access pointům detekovat tyto podvržené rámce a dostatečně brzy o tom informovat své klienty. PMF je zakomponován do standardu WPA3. Na WPA3 zabezpečených sítích se tedy takového útoku není třeba bát.

# Specifikace systémových komponent

V této kapitole si popíšeme systémové parametry a použitý hardware, který byl pro vývoj nástroje používán.

## Systémové specifikace

Nástroj byl vyvíjen a testován na počítači s operačním systémem Linux, konkrétně na distribuci openSUSE Tumbleweed. Zde jsou parametry a informace o platformě, získané nástrojem „neofetch“, který zobrazuje obecné informace o systému, a nástrojem „uname“, zobrazujícím verzi kernelu neboli linuxového jádra:

Obsah obrázku text, snímek obrazovky, menu

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 11 - Informace o systému

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 12 - Verze linuxového jádra

## Bezdrátové síťové karty

Wifi karty jsou důležitou součásti pro penetrační testování wifi sítí. Tyto zařízení umožňují bezdrátovou komunikaci počítačů s přístupovými body využitím protokolu 802.11 neboli wifi.

### Tenda U10 C650

Prvním využívaným adaptérem je externí wifi adaptér Tenda U10 C650.

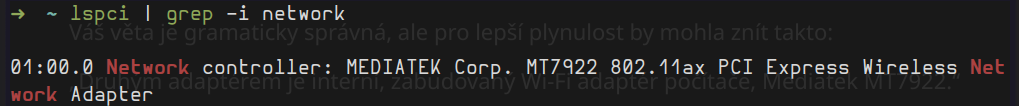
Obsah obrázku text, zeď, router, interiér

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 13 - Wifi adaptér Tenda U10

### Mediatek MT7922

Druhým adaptérem je interní, zabudovaný wifi modul počítače, Mediatek MT7922.



Obrázek 14 - Wifi modul Mediatek MT7922

# Přístupové body

Zde si popíšeme jednotlivé přístupové body použité k připojení zařízení do testovaných wifi sítí.

## Mikrotik RB941-2nDs

První přístupový bod je Mikrotik RB941-2nD s operačním systémem RouterOS 6. Na tomto zařízení bude testováno zachycení a následné prolomení PMKID řetězce.

Obsah obrázku text, router, computer, elektronika

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 15 - Snímek Mikrotik RB941-2nDs

Obsah obrázku text, elektronika, snímek obrazovky, číslo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 16 - Systémové informace Mikrotik RB941-2nDs

## TP-Link AX23

Přístupový bod od firmy TP-Link, běžně užívaný v současných domácnostech, poslouží k testování útoků na WPA2, wifi jammingu a Evil Twin útoku.

Obsah obrázku router, interiér, elektronika, zeď

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 17 - Snímek TP-Link AX23

Obsah obrázku text, snímek obrazovky, Písmo, design

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 18 - Verze firmware TP-Link AX23

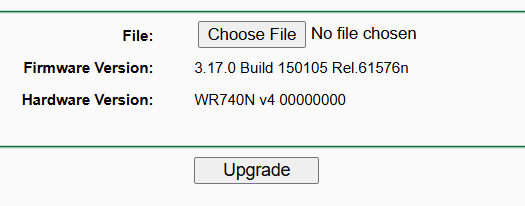
# TP-Link WR740N

Posledním využitým routerem je TP-Link starší generace, konkrétně se jedná o model WR740N. Tento router poslouží pro další testování provedených útoků na starším hardwaru.

Obsah obrázku router, interiér

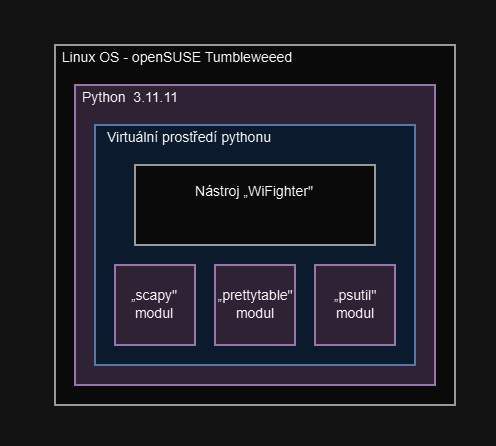
Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 19 - Snímek TP-Link WR740N



Obrázek 20 - Verze firmware TP-Link WR740N

# Konfigurace vývojového prostředí

Nástroj je napsán v jazyku python kvůli jeho rozšiřitelnosti. Ke spuštění využívá virtuální prostředí pythonu, které slouží jako samostatný izolovaný prostor pro balíčky nezbytné k chodu nástroje. To předchází konfliktním situacím a špatnému verzování v případě, že má uživatel více python projektů na jednom systému. Toto prostředí obsahuje potřebné doinstalované moduly neboli balíčky, rozšiřující základní python o další funkce. Toto prostředí si dále popíšeme v této kapitole.

Obrázek 21 - Schéma vývojového prostředí

## Využívané systémové balíčky

WiFighter využívá několik nástrojů ke svému fungování a instalaci. Tyto nástroje jsou součástí takzvaných balíčků. Tyto balíčky jsou dostupné pouze pro distribuce openSUSE a jsou instalovány pomocí správce balíčků „zypper“, který je součástí openSUSE distribucí. Na jiných linuxových distribucích se mohou nástroje nacházet v jiných balíčcích nebo se jmenovat jinak.

Obsah obrázku text, Písmo, snímek obrazovky

Obsah vygenerovaný umělou inteligencí může být nesprávný. Potřebné balíčky se instalují následujícím příkazem v terminálu:

Obrázek 22 - Instalace potřebných systémových balíčků

Jednotlivé balíčky si nyní představíme a popíšeme…

### Make

Nástroj make je využíván pro automatizaci kompilace a instalace potřebných nástrojů v instalačním skriptu na základě takzvané „makefile“.

### Gawk

Tento balíček obsahuje potřebný nástroj zvaný „awk“. Ten je používaný k filtraci dat z textových řetězců.

### Sed

Nástroj pro textové úpravy souborů. V instalačním skriptu je pomocí něj nastavován interpretační řádek python skriptu, specifikující, jaký interpretační program má být použít k jeho spuštění.

### Iputils

Sada nástrojů pro práci se sítěmi. Jeho součástí je potřebný nástroj „ping“, který testuje dostupnost a latenci komunikace mezi síťovými zařízeními.

### Iproute2

Sada nástrojů pro správu síťových rozhraní nahrazující balíček „net-tools“. Potřebným nástrojem z této sady je „ip“, který ulehčuje správu síťových rozhraní.

### Iw

Nástroj „iw“ umožňuje zobrazení informací a správu bezdrátových síťových rozhraní. Také je pomocí něj možné získat informace o okolních dostupných přístupových bodech.

### Python311

Python 3 balíček pro OpenSUSE distribuce.

### Aircrack-ng

Sada nástrojů pro penetrační testování wifi sítí. Využívána k deautentifikaci klientů přístupového bodu, zachytávání komunikace při navazování spojení klientů s přístupovým bodem a útokům na hesla.

### Hashcat

Výkonný nástroj pro prolamování hashovaných řetězců. Podporuje různé hashovací algoritmy. Umožňuje hardwarovou akceleraci, rozdělení zátěže mezi grafickou kartu a procesor a paralelní zpracovaní procesů.

### Pocl

Implementace OpenCL (standard pro paralelní programování), která umožňuje spuštění OpenCL programů na různých platformách. Tento balíček je potřeba pro funkčnost nástroje hashcat.

### Hostapd

Software umožňující vytvoření vlastní bezdrátové sítě na linuxovém zařízení.

### Dhcp-server

Tento software umožňuje nakonfigurovat a spustit vlastní server pro dynamické přidělování IP adres.

### Iptables

Nástroj pro správu firewallových pravidel zařízení.

## Využívané „Hcxtools“

Hcxtools je sada nástrojů kam patří vyžadované nástroje „hcxdumptool“ verze 6.2.6 a „hcxpcapngtool“. Tyto nástroje nejsou v základu dostupné v openSUSE repozitáři balíčků. Tudíž je potřeba nainstalovat nástroje manuálně z GitHubu, což je webová platforma pro hostování a správu kódu, kde vývojáři sdílejí své projekty a spolupracují na nich. Hcxdumptool je WiFighterem využíván pro vyžádaní a zachycení PMKID řetězce od přístupového bodu, v případě, že je oběť na tento typ útoku náchylná. Hcxpcapngtool je poté následně použit pro konverzi záznamu zachycené komunikace (obsahující PMKID) do hash formátu, který je čitelný pro nástroj hashcat.

Postup instalace těchto nástrojů je následující:

Obsah obrázku text, snímek obrazovky, Písmo

Obsah vygenerovaný umělou inteligencí může být nesprávný.

Obrázek 23 - Instalace Hcxtools

Obsah obrázku text, snímek obrazovky, Písmo, Grafika

Obsah vygenerovaný umělou inteligencí může být nesprávný.Instalaci nástrojů ověříme spuštěním následujících příkazů:

Obrázek 24 - Test instalace Hcxtools

ZDROJE

1. **Vyas, Radhika.** What is WEP Security? *securew2.* [Online] [Citace: 15. říjen 2024.] https://www.securew2.com/blog/what-is-wep-security.

2. **teamques10.** Explain WEP in detail. *ques10.com.* [Online] [Citace: 3. 12 2024.] https://www.ques10.com/p/14141/explain-wep-in-detail/.

3. **Stepanov, Mykhailo.** hackenproof.com. *[Part 2] How to Hack Into Wi-Fi – WPS Pixie Dust.* [Online] [Citace: 3. 12 2024.] https://hackenproof.com/blog/for-hackers/how-to-hack-wifi-wps-pixie-dust.

4. —. [Part 2] How to Hack Into Wi-Fi – WPS Pixie Dust. *hackenproof.* [Online] [Citace: 4. listopad 2024.] https://hackenproof.com/blog/for-hackers/how-to-hack-wifi-wps-pixie-dust.

5. **Kinzer, Kelsey.** How Does RADIUS Improve WiFi Security? *jumpcloud.* [Online] [Citace: 16. říjen 2024.] https://jumpcloud.com/blog/radius-improve-wifi-security.

6. **Ikechukwu, Linda.** Everything You Should Know About Wi-Fi Security. *smallstep.* [Online] [Citace: 15. Říjen 2024.] https://smallstep.com/blog/everything-wifi-security/.

7. **Charlie Bromberg, Joker2a.** WPS. *thehacker.* [Online] [Citace: 4. listopad 2024.] https://www.thehacker.recipes/radio/wi-fi/wps/.

8. **Chandel, Raj.** Wireless Penetration Testing: PMKID Attack. *hackingarticles.* [Online] [Citace: 4. listopad 2024.] https://www.hackingarticles.in/wireless-penetration-testing-pmkid-attack/.

9. **Howdle, Dan.** Securing your Wi-Fi router: Protect your home network. *cable.co.uk.* [Online] [Citace: 3. 12 2024.] https://www.cable.co.uk/broadband/guides/router-security/.

10. **Hoorvitch, Ido.** Cracking WiFi at Scale with One Simple Trick. *cyberark.* [Online] [Citace: 4. listopad 2024.] https://www.cyberark.com/resources/threat-research-blog/cracking-wifi-at-scale-with-one-simple-trick.

11. **Gillis, Alexander S.** Wi-Fi Protected Access (WPA). *techtarget.* [Online] [Citace: 15. říjen 2024.] https://www.techtarget.com/searchmobilecomputing/definition/Wi-Fi-Protected-Access.

12. **Gargan, Richard.** Network Access With DPP (Device Provisioning Protocol). *netmaker.* [Online] [Citace: 16. říjen 2024.] https://www.netmaker.io/resources/device-provisioning-protocol-dpp.

13. **Garakh, Iliya.** WPS – What is it, and how does it work? *passwork.* [Online] [Citace: 16. říjen 2024.] https://passwork.pro/blog/what-is-wps/.

14. **Bouška, Petr.** Cisco WiFi - základní principy a protokoly. *samuraj-cz.* [Online] [Citace: 14. Říjen 2024.] https://www.samuraj-cz.com/clanek/cisco-wifi-zakladni-principy-a-protokoly/.

15. **ayusharma0698.** geeksforgeeks. *Wifi Protected Access (WPA).* [Online] [Citace: 14. říjen 2024.] https://www.geeksforgeeks.org/wifi-protected-access-wpa/.

16. **Agapidis, Lazarus.** WPA and WPA2 4-Way Handshake. *networklessons.* [Online] [Citace: 3. listopad 2024.] https://networklessons.com/cisco/ccnp-encor-350-401/wpa-and-wpa2-4-way-handshake.

17. **Accessagility.** Rogue Access Points. *accessagility.com .* [Online] [Citace: 3. 12 2024.] https://www.accessagility.com/rogue-wifi-wireless-access-point-ap.

18. **Academy, Khan.** Rogue access points. *khanacademy.org.* [Online] [Citace: 3. 12 2024.] https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks.

19. **Cybersecura.** WPA/WPA2 cracking, PMKID, Evil Twin... Overview of attacks and threats to Wi-Fi in 2022. *cybersecura.* [Online] Cybersecura. [Citace: 3. listopad 2024.] https://www.cybersecura.com/en/post/overview-of-attacks-and-threats-to-wifi-in-2022.

20. **Networklessons.** WPA and WPA2 4-Way Handshake. *networklessons.com.* [Online] Networklessons. [Citace: 3. 12 2024.] https://networklessons.com/cisco/ccnp-encor-350-401/wpa-and-wpa2-4-way-handshake.

21. **Nextcomp.** Jak vybrat wifi router? *nextcomp.cz.* [Online] [Citace: 3. 12 2024.] https://www.nextcomp.cz/articles/105620.

22. **PODA.** Jak funguje domácí Wi-Fi. *https://www.poda.cz/.* [Online] PODA. [Citace: 14. Říjen 2024.] https://www.poda.cz/novinky/jak-funguje-domaci-wi-fi/.

23. **Cyberark.** cyberark.com. *Cracking WiFi at Scale with One Simple Trick .* [Online] Cyberark. [Citace: 3. 12 2024.] https://www.cyberark.com/resources/threat-research-blog/cracking-wifi-at-scale-with-one-simple-trick.

24. **Cisco.** Configure Multiple SSIDs on a Network. *cisco.com.* [Online] Cisco. [Citace: 3. 12 2024.] https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5652-configure-multiple-ssids-on-a-network.html.

25. **WiFi Professionals.** 4-Way Handshake. *wifi-professionals.com.* [Online] WiFi Professionals. [Citace: 3. 12 2024.] https://www.wifi-professionals.com/2019/01/4-way-handshake.

SEZNAM OBRÁZKŮ

[Obrázek 1 - Wifi standardy 9](#_Toc190717303)

[Obrázek 2 - 4-Way handshake 11](#_Toc190717304)

[Obrázek 3 - Detail WPS tlačítka 14](#_Toc190717305)

[Obrázek 4 - Schéma wifi VLAN 15](#_Toc190717306)

[Obrázek 5 - Šifrování WEP 16](#_Toc190717307)

[Obrázek 6 - Vyjednání šifrovacích klíčů 18](#_Toc190717308)

[Obrázek 7 - Autentizační sekvence WPS 19](#_Toc190717309)

[Obrázek 8 - Detail PMKID 20](#_Toc190717310)

[Obrázek 9 - Evil Twin 21](#_Toc190717311)

[Obrázek 10 - Rogue AP 22](#_Toc190717312)

[Obrázek 11 - Informace o systému 23](#_Toc190717313)

[Obrázek 12 - Verze linuxového jádra 23](#_Toc190717314)

[Obrázek 13 - Wifi adaptér Tenda U10 24](#_Toc190717315)

[Obrázek 14 - Wifi modul Mediatek MT7922 24](#_Toc190717316)

[Obrázek 15 - Snímek Mikrotik RB941-2nDs 25](#_Toc190717317)

[Obrázek 16 - Systémové informace Mikrotik RB941-2nDs 25](#_Toc190717318)

[Obrázek 17 - Snímek TP-Link AX23 26](#_Toc190717319)

[Obrázek 18 - Verze firmware TP-Link AX23 26](#_Toc190717320)

[Obrázek 19 - Snímek TP-Link WR740N 27](#_Toc190717321)

[Obrázek 20 - Verze firmware TP-Link WR740N 27](#_Toc190717322)

[Obrázek 21 - Schéma vývojového prostředí 28](#_Toc190717323)

[Obrázek 22 - Instalace potřebných systémových balíčků 29](#_Toc190717324)

[Obrázek 23 - Instalace hcxtools 31](#_Toc190717325)