Vysoká škola polytechnická Jihlava

Aplikovaná informatika

**Demonstrační nástroj Man-in-the-middle útoků na Wi-Fi sítě**

Bakalářská práce

Autor práce: Jiří Karmasin

Vedoucí práce: Mgr. Antonín Přibyl

Jihlava 2023

**Vysoká škola polytechnická Jihlava**

Tolstého 16, 586 01 Jihlava

**ZADÁNÍ BAKALÁŘSKÉ PRÁCE**

Autor práce: **Jiří Karmasin**

Studijní program: Aplikovaná informatika

Obor: Aplikovaná informatika

Název práce: **Demonstrační nástroj Man-in-the-middle útoků na Wi-Fi sítě**

Cíl práce: Cílem práce je navrhnout a implementovat demonstrační nástroj k popisu a vysvětlení principu Man-in-the-middle (MITM) útoků na bezdrátové sítě. Tento nástroj poslouží k názorným ukázkám během školení kybernetické bezpečnosti především pro příslušníky Armády České republiky, proto musí být uživatelské rozhraní dostatečně intuitivní a přehledné. Součástí nástroje bude i popis relevantních protiopatření, které zvyšují imunitu proti MITM útokům. Nástroj bude implementován na platformě KALI Linux. Rovněž budou vytvořeny návodné a dokumentační nástroje (poster, brožura) pro cílové publikum pro zvýšení účinku školení s využitím tohoto nástroje.

Abstrakt

Vlastní text.

Klíčová slova

První klíčové slovo; druhé klíčové slovo; třetí klíčové slovo

Abstract

Vlastní text.

Keywords

První klíčové slovo; druhé klíčové slovo; třetí klíčové slovo

Prohlašuji, že předložená Zvolte položku. práce je původní a zpracoval/a jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem v práci neporušil/a autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, v platném znění, dále též „**AZ**“).

Byl/a jsem seznámen/a s tím, že na mou Zvolte položku. práci se plně vztahuje **AZ**, zejména § 60 (školní dílo).

Podle § 47b zákona o vysokých školách souhlasím se zveřejněním své práce podle směrnice prorektora pro studium č. 2/2020, a to bez ohledu na výsledek obhajoby.

Beru na vědomí, že VŠPJ má právo na uzavření licenční smlouvy o užití mé Zvolte položku. práce a prohlašuji, že **souhlasím** s případným užitím mé Zvolte položku. práce (prodej, zapůjčení apod.).

Jsem si vědom/a toho, že užít své Zvolte položku. práce či poskytnout licenci k jejímu využití mohu jen se souhlasem VŠPJ, která má právo ode mě požadovat přiměřený příspěvek na úhradu nákladů, vynaložených vysokou školou na vytvoření díla (až do jejich skutečné výše), z výdělku dosaženého v souvislosti s užitím díla či poskytnutím licence.

V Jihlavě dne Klikněte nebo klepněte sem a zadejte datum.

…………………………………….

Podpis studenta

Poděkování

*Na tomto místě můžete poděkovat všem, kteří si to podle vašeho úsudku zaslouží (např. vedoucí práce, konzultant, rodina atd.)*

*Vlastní text poděkování.*

Obsah

[Seznam obrázků 7](#_Toc151746691)

[Seznam tabulek 8](#_Toc151746692)

[Seznam zkratek 9](#_Toc151746693)

[Úvod 10](#_Toc151746694)

[1 Analýza síťových protokolů 11](#_Toc151746695)

[1.1 OSI model 11](#_Toc151746696)

[1.2 ARP 11](#_Toc151746697)

[1.3 Handshake 12](#_Toc151746698)

[1.4 WEP 12](#_Toc151746699)

[1.5 WPA, WPA2 12](#_Toc151746700)

[1.6 WPS 12](#_Toc151746701)

[1.7 SSL 12](#_Toc151746702)

[2 Analýza vektorů útoku 13](#_Toc151746703)

[2.1 Aplikace MITM 13](#_Toc151746704)

[2.2 ARP poisoning + (MAC flooding) 13](#_Toc151746705)

[2.3 SSLsplit 13](#_Toc151746706)

[2.4 Analýza existujících nástrojů 13](#_Toc151746707)

[3 Návrh implementace 14](#_Toc151746708)

[3.1 Zdůvodnění použitého jazyka implementace 14](#_Toc151746709)

[3.2 Návrh funkcionalit konzolového back-endu 14](#_Toc151746710)

[3.3 Návrh GUI 14](#_Toc151746711)

[4 Implementace 15](#_Toc151746712)

[4.1 Implementace konzolového back-endu 15](#_Toc151746713)

[4.2 Implementace GUI 15](#_Toc151746714)

[5 Testování 16](#_Toc151746715)

[5.1 Testy funkčnosti 16](#_Toc151746716)

[5.2 Testy výkonosti 16](#_Toc151746717)

[Závěr 17](#_Toc151746718)

[Seznam použité literatury 18](#_Toc151746719)

[Přílohy 19](#_Toc151746720)

# Seznam obrázků

# Seznam tabulek

# Seznam zkratek

AČR Armáda České republiky

NATO North Atlantic Treaty Organization (Severoatlantická aliance)

NÚKIB Nádorní úřad pro kybernetickou a informační bezpečnost

MITM Man-in-the-middle

MAC Medium Access Control

IP Internet protocol

TCP Transmission Control Protocol

UDP User datagram protocol

EAPOL Extensible authentication protocol over LAN

LAN Local area network

SSID Service Set Identifier

# Úvod

Dnešní svět se stále více digitalizovaný. To s sebou nese mnoho pozitivních jevů jako je zvýšení produktivity téměř všech lidských činností, rychlost komunikace mezi lidmi a možnost mít všechny myslitelné informace doslova na dlani kdykoliv si člověk přeje. Mimoto však s sebou přináší i mnoho bezpečnostních hrozeb a zranitelností, které před příchodem digitálního věku neexistovaly.

Kybernetická bezpečnost se tedy stává jedním z nejnaléhavějších problémů, kterým čelíme v této době. Jedním z hlavních způsobů, kterým zvyšovat bezpečnost v kyberprostoru, je dle vyjádření NÚKIB školení a osvěta v oblasti kybernetické bezpečnosti a chování v digitálním prostoru. Školení jsou klíčová pro posilování odolnosti organizací vůči kybernetickým útokům.

Jako specialista kybernetické bezpečnosti sloužící v Armádě České republiky je mojí povinností takováto školení provádět. Z mých letitých zkušeností je zřejmé, že teoretický výklad na povinných školeních nemá zdaleka takový dopad jako praktická ukázka probírané látky. A právě proto se moje bakalářská práce zaměřuje na návrh a implementaci demonstračního nástroje, který má za cíl poskytnout názorné ukázky útoku man-in-the-middle (MITM) a tím pomoci školitelům a studentům lépe porozumět této kybernetické hrozbě.

MITM útoky patří mezi nebezpečné techniky, při kterých útočník vstupuje mezi komunikující strany a může odposlouchávat a modifikovat datový tok. Tato zranitelnost Wi-Fi sítí je známá a často zneužívaná, což pro příslušníky resortu Ministerstva obrany představuje hrozbu při využívání Wi-Fi připojení k internetu.

Cílovým publikem bude široká škála posluchačů při školení od neznalých uživatelů koncových zařízení (smartphonů) až po IT techniky a síťové administrátory. Každému posluchači by při tom měla demonstrační ukázka přinést nový poznatek. Výsledný nástroj by tedy měl být přehledný, a přitom měl mít možnost poskytovat hlubší a komplexnější informace o fázích útoku, pokud by to o měl posluchač zájem.

Práce bude dále diskutovat o klíčových aspektech man-in-the-middle útoků, jejich důsledcích, a především ochranných opatřeních proti nim. Kromě toho popíše proces vývoje demonstračního nástroje.

Cílem práce je tedy nejen vytvořit funkční nástroj pro demonstrace, ale také přispět k zvýšení povědomí o MITM útocích a zlepšení schopností obrany proti nim. Věřím, že vypracovaný projekt má potenciál přispět k bezpečnosti digitálního prostoru a k lepší přípravě jednotlivců na výzvy, které s sebou nese kybernetická éra.

# Man-in-the-middle útok

Kybernetický útok Man-in-the-middle, který by se dal přeložit také jako Muž-uprostřed, je typ útoku na bezdrátovou komunikaci dvou zařízení. Zneužívá nepopiratelného faktu, že na rozdíl od metalického ethernetového nebo optického síťového spojení, je bezdrátová komunikace zajišťována pomocí vysílání elektromagnetických vln, které se šíří všesměrově do okolí. U například ethernetového spojení pomocí UTP kabelu je jednoznačné, odkud a kam signál drátem prochází a elektromagnetické vyzařování samotného kabelu je zanedbatelné. U bezdrátových technologií, jako je Wi-Fi, je však nejednoznačné, ze kterého zařízení přijatý signál vychází.

Útočník může pomocí zachytávání komunikace ostatních zařízení, nedokonalostem v používaných protokolech a vysíláním specifických rámců zapříčinit, že se vměstná do komunikace mezi zařízení oběti a přípojný bod. Veškerou komunikaci potom může monitorovat anebo pozměnit, čímž kompromituje integritu a důvěrnost dat, což jsou dva ze tří pilířů kybernetické bezpečnosti.

Obecná posloupnost MITM útoku na bezdrátové sítě vypadá následovně.

1. *Počáteční stav*.

Klient je připojen k AP (Access Pointu), tedy přístupovému bodu k internetu pomocí hesla a šifrovaně komunikuje.

Obsah obrázku skica, kresba, kreslené, klipart

Popis byl vytvořen automaticky

Obrázek 1: Počáteční stav

*(Zdroj: vlastní)*

1. *Fáze útoku – Rekognoskace, deautentifikace, lámání hesla*.

Útočník pomocí svého Wi-Fi adaptéru zachytává v okolí se šířící rámce a z nich extrahuje potřebné informace o AP a zařízení oběti. Jakmile má potřebné znalosti, začne vysílat deautentifikační rámce a zároveň zachytává pokus o opětovné připojení k síti odpojené oběti. Po jejich zachycení má potřebné zdroje k pokoušení se o prolomení hesla ze zašifrovaných zpráv. Lámání helsa probíhá například offlinovým slovníkovým útokem a bude popsán v pozdějších kapitolách.

1. *Fáze útoku – útočník je v síti a provádí Man-in-the-middle*.

Se získaným heslem se útočník připojuje k síti a jako další zařízení a pomocí techniky APR poisoningu zapříčiňuje, že komunikace oběti nejde napřímo k AP, ale jde přes útočníkovo zařízení. Tím se útočník stává „mužem uprostřed“.

1. *Fáze útoku – výkonná fáze.*

Dosavadní činnost útočníka žádným způsobem negativně neovlivňuje komunikaci oběti. V této fázi útoku ale nastává samotné zneužití provedeného MITM například odposloucháváním komunikace (zachytávání DNS dotazů), přesměrování na falešný web (DNS spoofing), nebo čtení obsahu samotné komunikace po prolomení SSL zabezpečení například pomocí SSLsplitu.

Obsah obrázku skica, kresba, kreslené, klipart

Popis byl vytvořen automaticky

Obrázek 2: Po úspěšném MITM útoku

*(Zdroj: vlastní)*

1. *Fáze útoku – Exfiltrace.*

Úspěšný útok je takový, o kterém oběť ani neví, že se stal. V poslední fázi tedy útočník reverzně vrazí pozměněné ARP záznamy na původní hodnoty a odpojuje se od sítě.

Celý tento postup bude v následujících částech práce podrobněji popsán a ve výsledném nástroji bude možné jej krok po kroku demonstrovat s náležitým komentářem a vysvětlivkami.

# Analýza síťových protokolů

K úspěšnému provedení MITM útoku je nutné znát alespoň základní protokoly, které se využívají při bezdrátové Wi-Fi komunikaci. Právě nedokonalosti a funkcionalita těchto protokolů umožňují útok provést.

Bezdrátovou komunikaci, jejíž napadení bude práce demonstrovat je Wi-Fi. Wi-Fi připojení koncových zařízení k internetu využívá sadu standardizovaných protokolů IEEE 802.11 (IEEE Standard for Information technology, 2016), díky kterým je vůbec možné samotnou komunikaci navázat a provozovat. V první části práce popíšu a analyzuji základní sadu protokolů. Na tuto analýzu navážu v následující kapitole, kde se zaměřím na slabá místa jednotlivých aspektů komunikace. Dobře znát princip těchto protokolů je tedy zásadní pro pozdější zneužití jejich zranitelností.

## OSI model

Útok MITM probíhá na 2. spojové (neboli linkové) vrstvě referenčního ISO/OSI modelu. Pracuje tedy s tzv. rámci. Po úspěšném přesměrování rámců na zařízení útočníka pak může probíhat následné využití MITM na vyšších vrstvách. Při SSLsplitu je to šifrování, které se řadí do 5. relační vrstvy (Wu, 2020). Při práci s DNS dotazy se pak pracuje na nejvyšší, aplikační vrstvě (Rymond, 2022).

Obsah obrázku text, snímek obrazovky, Písmo

Popis byl vytvořen automaticky

Obrázek 3: ISO/OSI referenční model

*(Zdroj: wikipedia.org)*

## Inicializace připojení k Wi-Fi

Samotné připojení bezdrátového zařízení k Wi-Fi probíhá v několika krocích s využitím různých rámců (frames). Zde uvádím výčet těch nejdůležitějších:

* Beacon frame – tento rámec je v pravidelných intervalech vysílán AP, pokud je Wi-Fi síť nastavená jako viditelná. Obsahuje mimo jiné SSID, tedy název sítě, a informace o zabezpečení. Účelem je oznamovat do okolí dostupnost sítě.
* Probe request – rámec vysílají koncová zařízení, když aktivně hledají požadovanou síť, která není nastavená jako veřejná. Obsahuje SSID hledané sítě.
* Probe response – odpověď AP na probe request s informacemi jako v beacon framu.
* Authentication request frame – rámec zasílající klient k přístupovému bodu, v němž ho žádá o ověření. Toto ověření může být být buď otevřené (pak není spojení šifrování), nebo pomocí hesla (shared key authentication). Toto spojení je bezpečnější.
* Authentication response frame – odpověď AP směrem ke koncovému zařízení. Spojení buďto potvrzuje, nebo zamítá při otevřením spojení. U spojení s ověřovacím klíčem si vyžaduje heslem zašifrovaný řetězec (challenge text). Při jeho úspěšném dešifrování přístupovým bodem, je klientské zařízení ověřeno a připojeno.
* Association request/response frame – klíčový prvek v procesu připojování. Po úspěšném ověření v předcházejícím kroku dochází k samotnému připojení. V association response rámci je klientovi zaslána jeho nově přiřazená IP adresa.

## Proces autentizace

Samotná autentizace z předcházející části pak může probíhat několika způsoby. Ty jsou časem přidávány s tím, jak předešlé ztrácejí na bezpečnosti kvůli jejich nedokonalostem a prolomení.

### WEP

[*Šifrování*](https://cs.wikipedia.org/wiki/Kryptografie) *komunikace pomocí statických* [*WEP*](https://cs.wikipedia.org/wiki/Wired_Equivalent_Privacy) *klíčů (Wired Equivalent Privacy)* [*symetrické šifry*](https://cs.wikipedia.org/wiki/Symetrick%C3%A1_kryptografie)*, které jsou ručně nastaveny na obou stranách bezdrátového spojení. Kvůli nedostatkům v protokolu lze zachycením specifických rámců a jejich analýzou lze klíč relativně snadno získat (programem* [*Aircrack-ng*](https://cs.wikipedia.org/wiki/Aircrack-ng)*). Autentizace přístupu do WPA sítě je prováděno pomocí PSK ([Pre-shared key](https://cs.wikipedia.org/wiki/Pre-shared_key" \o "Pre-shared key) – obě strany používají stejnou dostatečně dlouhou* [*heslovou frázi*](https://cs.wikipedia.org/wiki/Heslo)*),* [*RADIUS*](https://cs.wikipedia.org/wiki/RADIUS) *serverem (ověřování přihlašovacím jménem a heslem) nebo dalšími variantami* [*EAP*](https://cs.wikipedia.org/wiki/Extensible_Authentication_Protocol) *protokolu.*

### WPA, WPA2, WPA3

*Kvůli zpětné kompatibilitě využívá* [*WPA*](https://cs.wikipedia.org/wiki/Wi-Fi_Protected_Access) *(Wi-Fi Protected Access) WEP klíče, které jsou ale často dynamicky bezpečným způsobem měněny (protokoly TKIP, CCMP). Pro průběžnou změnu klíčů slouží speciální doprovodný program, který nazýváme prosebník (suplikant). Z tohoto důvodu bylo možné doplnit WPA i do staršího hardware a výrobci nemuseli uvádět na trh úplně nová zařízení. PSK klíč lze zjistit pouze slovníkovou metodou (tj. zkoušením různých hesel proti odposlechnuté variantě úspěšné autentizace).*

*Novější* [*WPA2*](https://cs.wikipedia.org/wiki/IEEE_802.11i) *přináší kvalitnější šifrování (šifra AES), která však vyžaduje větší výpočetní výkon, a proto nelze WPA2 používat na starších zařízeních.*

### WPS

*Pro snadnější připojení do bezdrátové sítě je možné se připojit pomocí* [*WPS*](https://cs.wikipedia.org/wiki/Wi-Fi_Protected_Setup)*. Na zařízení může být WPS tlačítko, kdy po jeho zmáčknutí lze se po omezený čas do bezdrátové sítě připojit bez autentizace. Místo tlačítka může být zadán osmimístný PIN (oba způsoby lze kombinovat). Číselný kód však lze v poměrně krátké době uhádnout zkoušením různých variant. Novější zařízení proto obsahují omezení počtu pokusů o připojení, případně lze WPS úplně vypnout.*

## ARP

ARP je zkratka „adress resolution protocol“. Jeho účelem je převod fyzické MAC adresy na síťovou IP adresu. Aby mohlo zařízení připojené do sítě komunikovat s okolními zařízeními v lokální síti, musí znát jejich i svoji MAC adresu. K tomu slouží dva hlavní rámce:

* ARP request – tímto rámcem se zařízení dotazuje na broadcastové adrese (FF:FF:FF:FF:FF:FF) na MAC adresu zařízení se známou IP adresou.
* ARP response – zařízení, které rozpoznalo svoji IP adresu v ARP requestu odpovídá na MAC adresu odesílatele rámec se svojí MAC adresou.

Tím je dokončen proces připojení a koncové zařízení je plně funkční ve Wi-Fi síti.

# Analýza vektorů útoku

Základní charakteristikou, která odlišuje bezdrátové připojení od Ethernetového je všesměrové elektromagnetické vysílání komunikujících stran. Tyto rámce tedy mohou být zachyceny a zpracovány kýmkoliv v dosahu signálu.

## Aplikace MITM

### Lámání WEP2 hesla

## ARP poisoning + (MAC flooding)

## SSLsplit

## Analýza existujících nástrojů

# Návrh implementace

27

## Zdůvodnění použitého jazyka implementace

## Návrh funkcionalit konzolového back-endu

## Návrh GUI

# Implementace

## Implementace konzolového back-endu

### EvilTwin Wi-Fi

### ARPspoof

## Implementace GUI

# Testování

## Testy funkčnosti

## Testy výkonosti

# Závěr

# Seznam použité literatury

<https://cs.wikipedia.org/wiki/Wi-Fi>

<file:///D:/1_HACK/CYBER%20BOOKS/ethical_hacking_and_penetration_testing_guide.pdf>

<https://prabhjeetlearning.medium.com/capturing-a-wi-fi-handshake-the-key-to-network-security-testing-d7aad39b3fdf>

"IEEE Standard for Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," in IEEE Std 802.11-2016 (Revision of IEEE Std 802.11-2012), vol., no., pp.1-3534, 14 Dec. 2016, doi: 10.1109/IEEESTD.2016.7786995.

RAYMOND, Serena. *What is the DNS Layer and How Do I Secure It?* [online]. 2022 [cit. 2023-11-22]. Dostupné z: https://www.dnsfilter.com/blog/dns-layer-how-to-secure

FREIER, A, KARLTON, P. *The Secure Sockets Layer (SSL) Protocol Version 3.0*. 2011. https://datatracker.ietf.org/doc/html/rfc6101

Wu, Wentz. *What OSI Layer does TLS Operate and Why?* 2020. <https://wentzwu.com/2020/08/21/what-osi-layer-does-tls-operate-and-why/>

MARUŠIC, Marek. Automatizace MitM útoku pro dešifrování SSL/TLS. Brno, 2016. Ba-

kalářská práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí

práce Pluskal Jan.

SYNTAXE:

BIERNÁTOVÁ, Olga a Jan SKŮPA. *Bibliografické odkazy a citace dokumentů dle ČSN ISO 690 (01 0197)* *platné od 1. dubna 2011* [online]. Brno, 2011 [cit. 2020-12-09]. Dostupné z: <http://www.citace.com/soubory/csniso690-interpretace.pdf>

*Citace.com* [online]. [cit. 2020-12-01]. Dostupné z: citace.com

ČMEJRKOVÁ, Světla, Jindra SVĚTLÁ a František DANEŠ. *Jak napsat odborný text*. Praha: Leda, 1999. ISBN 80-85927-69-1.

ČSN ISO 690 (01 0197) *Informace a dokumentace - Pravidla pro bibliografické odkazy a citace informačních zdrojů*. 3. vyd. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Česká technická norma.

ECO, Umberto. *Jak napsat diplomovou práci*. Olomouc: Votobia, 1997. Velká řada (Votobia). ISBN 80-7198-173-7.

FIŠER, Zbyněk. *Tvůrčí psaní: malá učebnice technik tvůrčího psaní*. Brno: Paido, 2001. Edice pedagogické literatury. ISBN 80-85931-99-0.

*Internetová jazyková příručka* [online]. Praha: Ústav pro jazyk český, © 2008–2020 [cit. 2020-12-09]. Dostupné z: https://prirucka.ujc.cas.cz/

KERSLAGER, Milan. Typografická pravidla. *SPŠE a VOŠ Liberec* [online]. 2016 [cit. 2020-12-01]. Dostupné z: https://www.pslib.cz/milan.kerslager/Typografick%C3%A1\_pravidla

KOČIČKA, Pavel a Filip BLAŽEK. *Praktická typografie*. Praha: Computer Press, c2000. DTP & grafika. ISBN 80-7226-385-4.

MEŠKO, Dušan, Dušan KATUŠČÁK a Ján FINDRA. *Akademická příručka*. České, upr. vyd. Martin: Osveta, 2006. ISBN 80-8063-219-7.

*Nová citační norma ČSN ISO 690:2011 – Bibliografické citace.* [online]. Dostupné z: https://www.iso690.zcu.cz

# Přílohy