26

Excel@FIT 2017

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

Vysoké učení technické v Brně

University of Malta

Automatizace útoku MitM na Wi-Fi sítích

Martin Vondráček

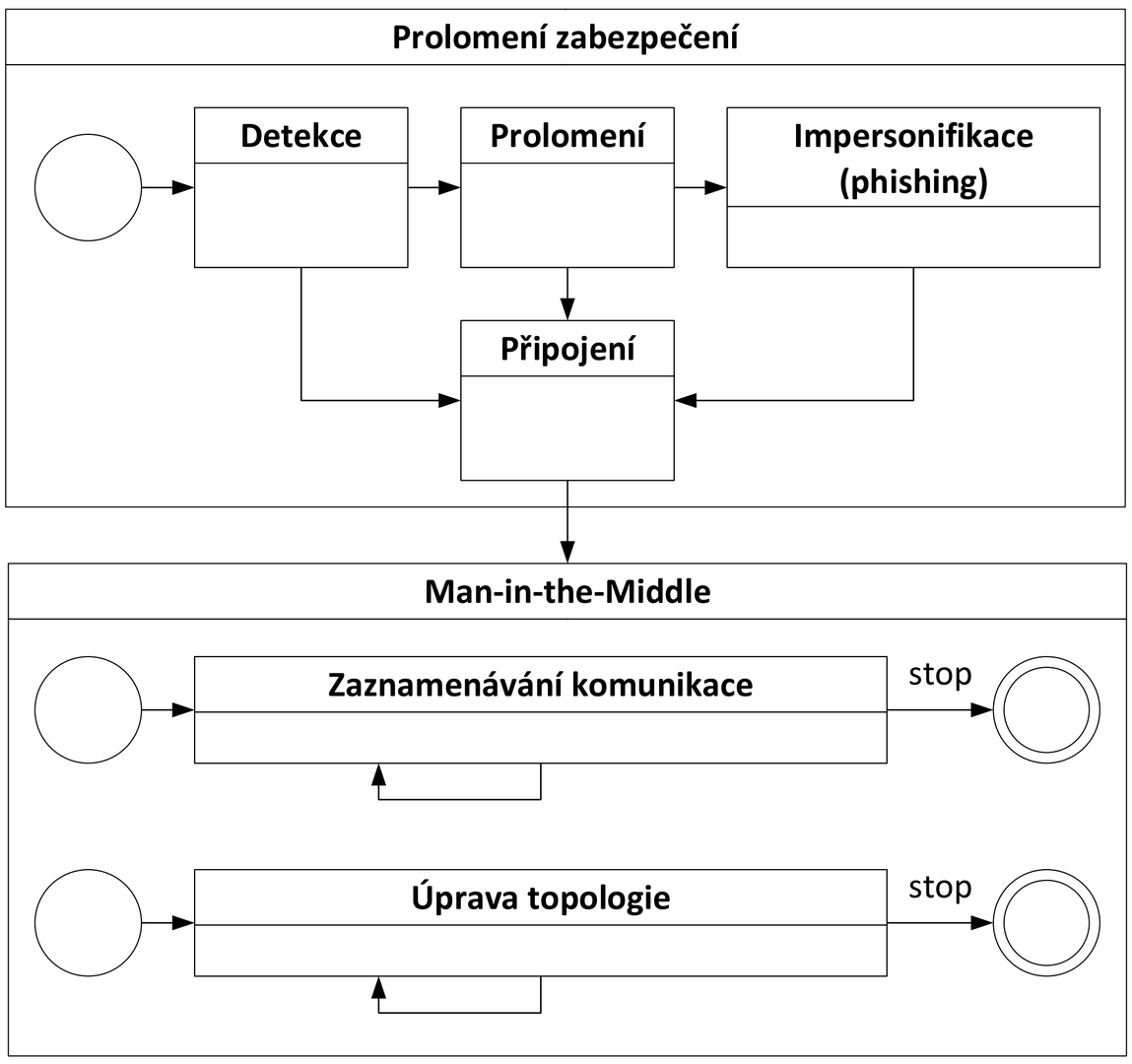
Je vaše síť bezpečná? Jak snadno vás lze odposlouchávat?

Shrnutí

Tato práce se zaměřuje na výzkum v oblasti bezpečnosti bezdrátových sítí. Analyzované technologie a způsoby zabezpečení trpí slabinami, které mohou být zneužity k provedení útoku MitM. Práce zahrnuje přehled dostupných nástrojů zaměřených na využití jednotlivých slabin. Výsledkem této práce je balíček wifimitm a CLI nástro wifimitmcli, oba implementované v jazyce Python. Balíček poskytuje funkcionalitu pro automatizovaný útok MitM a může být použit jako součást dalšího software. Nástroj wifimitmcli je schopen úspěšného provedení plně automatizovaného útoku bez jakéhokoli zásahu útočící osoby. Tento výzkum nachází využití v oblasti automatizovaných penetračních testů a forenzního vyšetřování. Projekt byl zveřejněn jako softwarový produkt v rámci výzkumné skupiny NES@FIT a jako bakalářská práce v květnu 2016, později toho roku autor obdržel cenu děkana VUT FIT a cenu rektora VUT v Brně.

Poděkování

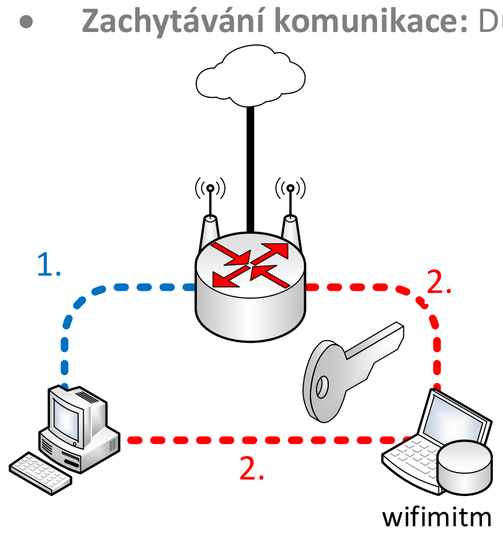
Autor by chtěl vyjádřit poděkování vedoucímu bakalářské práce Ing. Janu Pluskalovi a zahraničnímu vedoucímu bakalářské práce v rámci programu Erasmus+ Dr Johannu A. Briffovi za jejich cenné rady, ochotu a možnost práce pod jejich vedením. Dále autor děkuje Ing. Pluskalovi za řadu přínosných připomínek při přípravě článku.



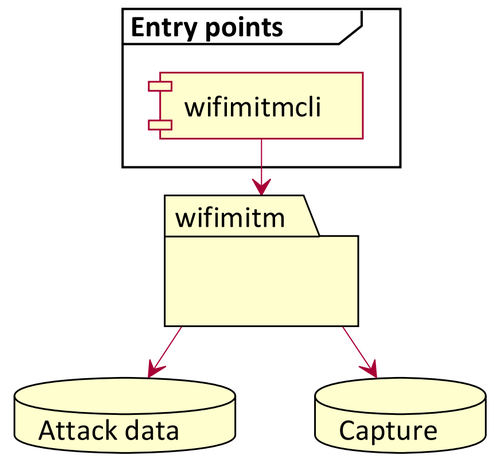
*Obrázek 1: Přehled jednotlivých fází útoku MitM na Wi-Fi síti. V rámci prolomení zabezpečení je možný útok na **WEP** OSA, **WEP** SKA, **WPA** PSK, **WPA2** PSK. V případě slovníkového útoku na zařízení od UPC je **slovník personalizován** implicitními hesly. Při dobře zabezpečené síti se přechází k **impersonifikaci**, kdy se útočník maskuje za pravou síť. Modifikace síťové topologie využívá podvržení ARP komunikace (**ARP Spoofing**). Následně je možné veškerou komunikaci oběti zachytávat, případně podvrhávat.*

Začleněné nástroje

- **Přístup do sítě:** airmon-ng, airodump-ng, aircrack-ng, aireplay-ng, upc_keys, wifiphisher, wpaclean, netctl
- **Modifikace topologie:** Framework for Man-In-The-Middle attacks
- **Zachytávání komunikace:** Dumpcap

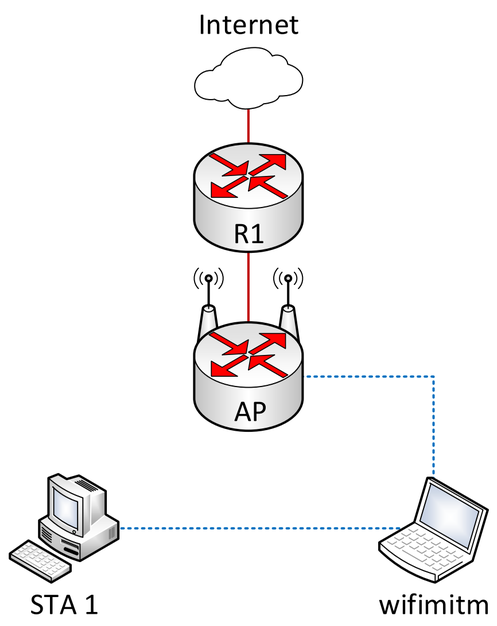


Obrázek 2: Schéma útoku MitM na bezdrátových sítích.

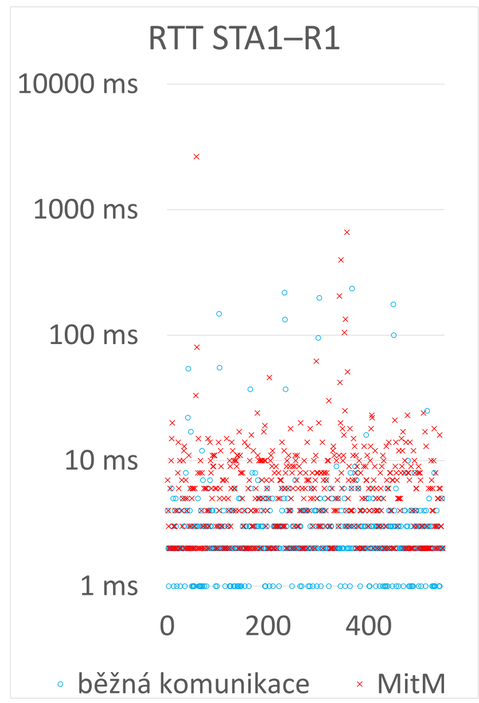


Obrázek 3: Schéma balíčku wifimitm a nástroje wifimitmcli.

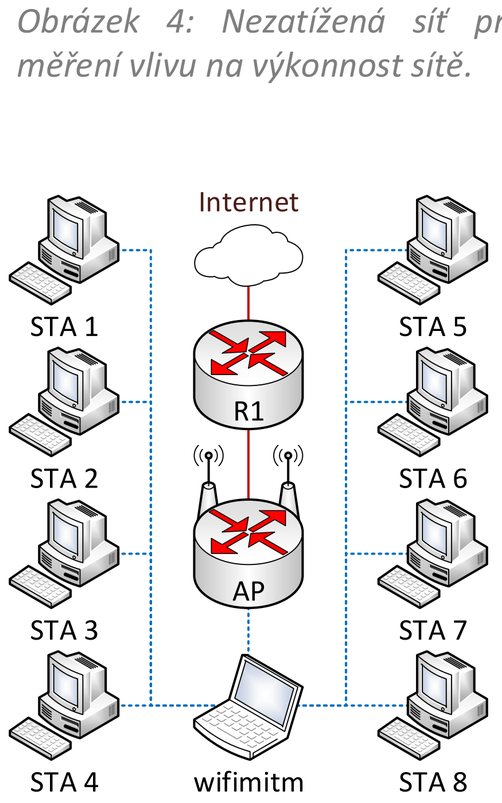
Experimenty



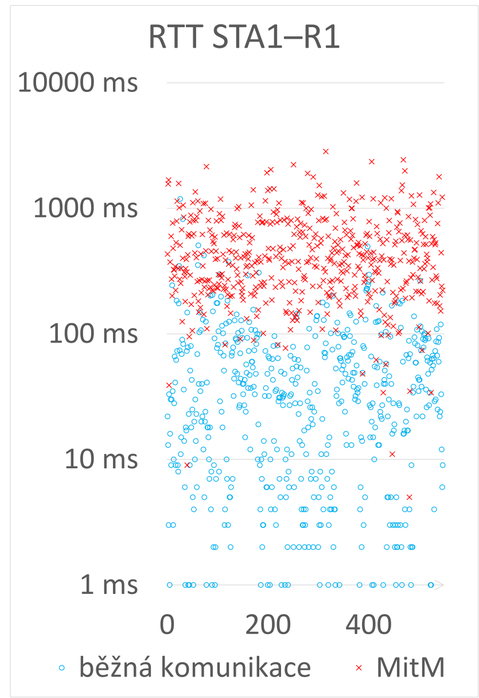
Obrázek 4: Nezatížená síť pro měření vlivu na výkonnost sítě.



Obrázek 5: Odezva v nezatížené síti při běžné komunikaci a při probíhajícím útoku .



Obrázek 6: Zatížená síť pro měření vlivu na výkonnost sítě.



Obrázek 7: Odezva v zatížené síti při běžné komunikaci a při probíhajícím útoku.