Automatizovaná detekce vektorů útoku pomocí SDR (Software Defined Radio)

Bc. Ondrej Vavro

Diplomová práca
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Ondrej Vavro**
Osobní číslo:	**A21190**
Studijní program:	**N0613A140022 Informační technologie**
Specializace:	**Kybernetická bezpečnost**
Forma studia:	**Kombinovaná**
Téma práce:	**Automatizovaná detekce vektorů útoku pomocí SDR (Software Defined Radio)**
Téma práce anglicky:	**Automated Attack Vector Detection Using SDR (Software Defined Radio)**

Zásady pro vypracování

1. Specifikujte signály elektromagnetického spektra v rádiové oblasti, spadajících do signálů zpracováváných pomocí SDR (Software Defined Radio).
2. Popište nejčastejší útoky na bezdrátové technologie pomocí SDR.
3. Navrhněte přenosný systém pro detekci možných vektorů útoků s pomocí SDR.
4. Systém implementujte v testovacím prostředí.
5. Proveďte ověření funkcí navrženého systému a srovnejte jej s již dostupnými řešeními.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. COLLINS, Travis F., Robin GETZ, Di PU a Alexander M. WYGLINSKI. Software-defined radio for engineers: Artech House mobile communications series. Artech House, 2018. ISBN 978-1-63081-459-5.
2. EWING, Martin. ABCs of Software Defined Radio: Why Your Next Radio Will be SDR. Amer Radio Relay League, 2012. ISBN 978-0-87259-632-0.
3. POORE, Christopher. FISSURE: The RF Framework for Everyone. Proceedings of the GNU Radio Conference [online]. 2022, 7(1) [cit. 2022-11-30]. Dostupné z: [https://pubs.gnuradio.org/index.php/grcon/article/view/122/102](https://pubs.gnuradio.org/index.php/grcon/article/view/122/1 „https://pubs.gnuradio.org/index.php/grcon/article/view/122/102") .
4. PICOD, Jean-Michel, Arnaud LEBRUN a Jonathan-Christofer DEMAY. Bringing software defined radio to the penetration testing community. Black Hat USA Conference [online]. 2014 [cit. 2022-11-30]. Dostupné z: [https://www.blackhat.com/docs/us-14/materials/us-14-Picod-Bringing-Software-Defined-Radio-To-The-Penetration-Testing-Community-WP.pdf](https://www.blackhat.com/docs/us-14/materials/us-14-Picod-Bringing-Software-Defined-Radio-To-The-Penetration-Testing-Community-WP.pdf „https://www.blackhat.com/docs/us-14/materials/us-14-picod-bringing-software-defined-radio-to-the-penetration-testing-community-wp.pdf")
.
5. GRECO, Claudia, Giancarlo FORTINO, Bruno CRISPO a Kim-Kwang Raymond CHOO. AI-enabled IoT penetration testing: state-of-the-art and research challenges. ENTERPRISE INFORMATION SYSTEMS [online]. 2022 [cit. 2022-11-30]. ISSN 17517575. Dostupné z: doi:10.1080/17517575.2022.2130014 .
6. GUZMAN, Aaron a Aditya GUPTA. IoT Penetration Testing Cookbook: Identify vulnerabilities and secure your smart devices. 1. Packt Publishing, 2017. ISBN 9781787285170.
7. VEENS, Thomas. Automated 2G traffic interception and penetration testing. Eindhoven, 2018. Diplomová práce. Eindhoven University of Technology.

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **2. prosince 2022**
Termín odevzdání diplomové práce: **26. května 2023**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 7. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomové práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ....

podpis autora

ABSTRAKT

Práce rozebírá problematiku bezpečnostních útoků na téměř celé spektrum elektromagnetických frekvencí používaných ke komunikaci a přenosu dat, a to pomocí SDR. Využívá faktu, že některé frekvence jsou považovány za bezpečné pro přenos jen díky své rozdílné frekvenci od uživatelsky lehce dostupných. Práce popisuje návrh a provedení přenositelného zařízení, které je možné k tomuto účelu použít.

Kľúčové slová: bezpečnosť, frekvenčné spektrum, vektor útoku, SDR

ABSTRACT

Thesis analyzies security attacks on almost the entire range of electromagnetic frequencies used for communication and data transfer, with help of an SDR. It uses the fact that some frequencies are considered safe due to having different frequencies from the user frequencies, that are easily accessible. Thesis describes design, construction and implementation of a portable device useable to this end.

Keywords: security, frequency spectrum, attack vector, SDR

Chci poděkovat mému vedoucímu práce, panu Ing. Davidu Malaníkovi, PhD., za jeho cenné poznatky v oblasti bezpečnosti, které mi poskytl, určování směru a formy práce, aby odpovídala vědeckému standardu, a za jeho pečlivost při kontrole obsahu práce a trpělivost při její korektůře.
Také chci poděkovat celému obsazení fakulty, a zejména jeho vedení, za to, že mi umožnilo věnovat se tomuto studijnímu oboru a snad tak přispět k zvýšení bezpečnosti v moderním IT světě.
V neposlední řadě děkuji svým rodičům, sourozencům a blízkým za jejich trpělivost, kolegům za jejich ochotu dělit se o studijní informace a za diskuzi k studijním problémům.

OBSAH

ÚVOD

Prešlo viac ako 120 rokov od Herzovho objavu rádiových vĺn a ich využitia Marconim k prenosu kódovanej informácie. Za toto obdobie bolo ľudstvo schopné pokoročiť vo využívaní rádiovej komunikácie na takú úroveň, že dnes je len málo miest na Zemi, ktoré by neboli pokryté pozemnou rádiovou komunikáciou a takmer žiadne, ktoré by odolali dosahu satelitnej rádiovej komunikácie.

Táto skutočnosť viedla k tomu, že dnes je možné takmer z každého miesta na Zemi odpočúvať nejakú komunikáciu, či už je podstatná alebo nepodstatná. Táto skutočnosť v minulosti nebola postatná, keďže pre zachytenie rádiovej komunikácie bolo potreba buď univerzálnu a komplexnú, ťažko prenositeľnú techniku alebo špeciálne zariadenie nastavené od výroby na jediný účel (a na relatívne úzke frekvenčné pásmo). V dôsledku toho nebola potreba ochrany komunikácie na prvom mieste, ak vôbec bola braná v potaz.

Vývoj však ženie kupredu i techniku v tejto oblasti, a to míľovými krokmi. To čo bolo kedysi možné len s objemným a drahým hardwarom je dnes dosiahnuteľné s ľahko prenositeľným zariadením, ktoré sa vojde doslova do dlane. Už nie je potreba veľmi citlivých prímačov a amplifikáciu a filtrovanie signálu, ktorý kvôli vysokému šumu ani nebolo možné dekódovať. Stačí sa dostaviť do rozumnej vzdialenosti, a ani konfigurovateľná filtrácia "za behu" nerobí modernej technike problémy.

A čo viac, komplexná a rýchla komunikácia, vyžadujúca logiku stavových automatov na čipe, je dnes nahraditeľná rýchlymi procesormi a ich výpočetnou kapacitou či vhodnými, na mieste reprogramovateľnými, čipmi. Je tak skutočne možné dekódovať takmer akúkoľvek komunikáciu a teda i na ňu útočiť, čo otvára mnohé otázky ohľadom zabezpečenia rádiovej komunikácie v našej spoločnosti.

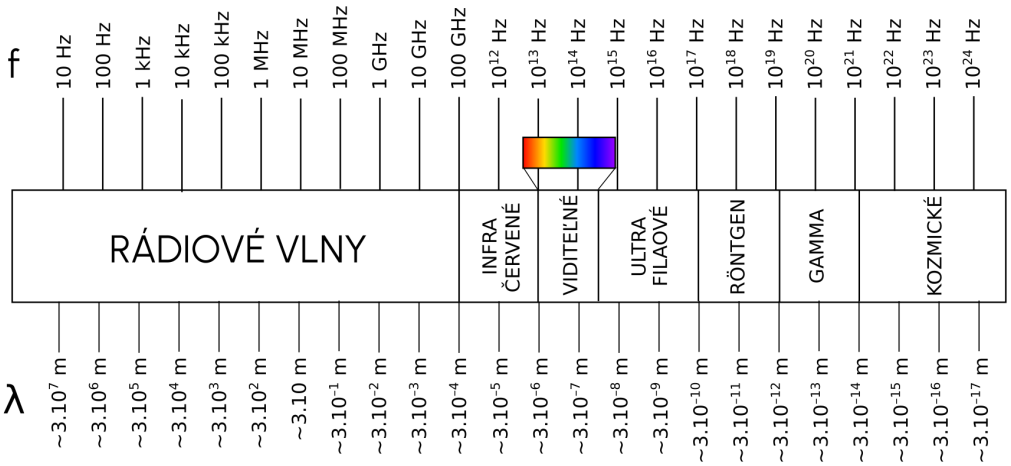
Táto práca sa zaoberá problematikou vyhľadávania slabých miest spôsobených nedostatočným zabezpečením alebo designovou chybou v návrhu komunikačných prvkov. V Sekcii 1 a 2 rozoberá fyzikálne princípy a základy rádiovej komunikácie, Sekcia 3 sa venuje univerzálnemu zariadeniu využívajúcemu software pre rádiovú komunikáciu – Software Defined Radio (SDR). Sekcia 4 ďalej skúma bezpečnosť v danej oblasti a Sekcia 5 prezentuje využiteľný software a nástroje pre analýzu a spracovanie zachytenej komunikácie. Nasledujúce sekcie prezentujú návrh a zostavenie zariadenia umožňujúceho skúmať bezpečnosť v teréne, a to na základe existujúcich komponentov (Sekcia 6), tak i novo vytvorených (Sekcia 7). Posledná Sekcia 8 skúma možnosti takéhoto zariadenia – v testovacom i reálnom prostredí.

I. TEORETICKÁ ČASŤ

1 Elektromagnetické spektrum

Elektromagnetická sila je jednou zo štyroch základných síl, ktoré boli fyzici schopní objaviť a dopodrobna matematicky popísať. Niet preto divu, že využitie tejto sily nás sprevádza každý deň.

Už James Clerk Maxwell v klasickej teórii elektromagnetizmu, ktorá vznikla najmä z jeho práce, prepovedal vznik elektromagnetických vĺn, ktoré sa šíria priestorom [3]. V tej dobe predstava zahrňovala hlavne svetlo, ale matematicky dávali zmysel i iné frekvencie.



Obr. 1.1 Rozdelenie elektromagnetického spektra, **f** predstavuje frekcencie a **λ** vlnové dĺžky [1].

Z dnešného hľadiska môžeme elektromagnetické spektrum rozdeliť do nasledujúcich kategórií (viď Obr. 1.1):

- pásmo rádiových frekvencií
- infračervené pásmo
- viditeľné svetlo
- ultrafialové pásmo
- rontgenové pásmo
- pásmo gamma
- pásmo kozmického žiarenia

Frekcencie nad ultrafialovým žiarením (vrátene jeho časti) radíme do kategórie ıi-onizujúceho žiarenia, pretože ich vplyvom dochádza k zmene genetickej informácie a

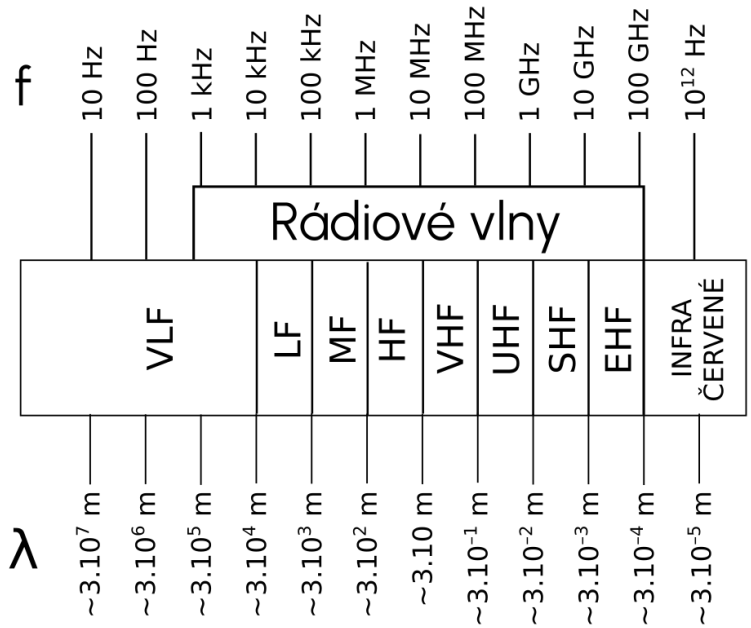
rozpadu bunečného života. Tieto frekvencie na Zemi filtrujú vrstvy atmosféry a umožňujú tak život na našej planéte.

Nižšie frekvencie okolo seba vidíme každý deň. Ich vplyv na život je minimálny, prevážne sa premieňajú na teplo. Špeciálne rádiové frekvencie majú schopnosť do istej miery prenikať predmetmi a práve z tohoto dôvodu sú vhodné pre komunikáciu na väčšie vzdialenosti. Ďalšie detaily v tomto smere poskytne nasledujúca kapitola.

2 Rádiový prenos dát

2.1 Využívané frekvencie a legislatíva

Po úvodnom objave existencie a možnostiach využitia elektromagnetických vĺn, špeciálne v rádiovej oblasti, nastal veľký boom v ich využívaní, ktorý viedol až k zavedeniu noriem ich používania a prideľovana frekvenčných pásiem pre isté spôsoby ich využitia.



Obr. 2.1 Rozdelenie rádového spektra podľa ITU, **f** predstavuje frekcencie a **λ** vlnové dĺžky [1].

Rádiové spektrum tvoria vlny so širokým rozpätím frekvencií približne do 100 GHz (viď Obr. 2.1) a môžeme ich rozdeliť do nasledujúcich kategórií [2]:

- pásmo veľmi nízkych frekvencií (VLF) – využitie v komunikácii s ponorkami, v komunikácii v podzemních baniach
- pásmo nízkych frekvencií (LF) – využitie v navigácii, synchronizácii časových signálov, pre amatérske rádio a identifikáciu na rádiovej frekvencii(RFID)
- pásmo stredných frekvencií (MF) – využitie pre vysielanie rádia v oblasti amplitúdovej modulácie (AM), lavínové záchranné vysielače„ pre amatérske rádio
- pásmo vysokých frekvencií (HF) – využitie pre vbezkontaktné platby a komunikáciu blízkeho poľa (NFC), leteckú komunikáciu "za horizont", komunikáciu na mori, bezdrôtové domáce telefóny

- pásmo veľmi vysokých frekvencií (VHF) – využitie pre vysielanie rádia v oblasti frekvenčnej modulácie (FM), televízne prenosy, amatérske rádio, bezpečnostné zložky (polícia, hasiči, a pod.), komunikáciu informácií o počasí z meteorologických staníc
- pásma ultra (UHF) a super (SHF) vysokých frekvencií – mikrovlnná komunikácia – bezdrôtovú lokálnu sieť (WiFi), BlueTooth, ZigBee, LoRa, a pod., mikrovlnný ohrev jedla, satelitnú navigáciu (GPS, Galileo, Glonass, Beidou), satelitná telefónna komunikácia, satelitné vysielanie, a pod.
- pásmo extra vysokých frekvencií (EHF) – rádio astronómia, mikrovlnné zbrane, a pod.

Z uvedených pásiem sa táto práca bude prevažne orientovať na rozmedzie od vysokých frekvencií (HF) až po super vysoké frekvencie (SHF).

2.2 Štandardné komponenty

2.3 Abstraktné vrstvy a protokoly

2.4 Rádiové a bezdrôtové systémy

3 Software Defined Radio (SDR)

3.1 História SDR

3.2 Komponenty SDR

3.3 Súčasný stav SDR

4 Bezpečnosť rádiových systémov

4.1 Analýza bezpečnosti rádiových systémov

4.2 Silné, slabé miesta a problémy prevedenia útoku

4.3 Kategórie útokov

4.4 Využitie SDR pri útokoch

5 Software a nástroje

5.1 Analýza frekvenčného spektra

5.2 Detekcia typu komunikácie a použitých protokolov

5.3 Tvorba packetov

5.4 Tvorba sledu komunikácie

II. PRAKTICKÁ ČASŤ

6 Návrh systému s SDR

6.1 Analýza požiadavkov pre návrh systému

6.2 Výber hardware komponentov

6.3 Výber software komponentov

6.4 Zostavenie systému a nastavenie software

7 Návrh detekcie možných vektorov útoku

7.1 Automatická analýza rádiovej komunikácie

7.2 Detekcia vybraných protokolov a zachytávanie komunikácie

7.3 Zostavenie možných útokov na základe komunikácie

7.4 Prevedenie útoku

8 Testovanie systému

8.1 Testovanie komponent systému

8.2 Testovanie systému imitáciou reálneho cieľa

8.3 Nasadenie systému v reálnej prevádzke

ZÁVER

ZOZNAM POUŽITEJ LITERATÚRY

[1] NASA: Radio Spectrum. [online] [cit. 6. februára 2023]. Dostupné z WWW: <https://www.nasa.gov/directorates/heo/scan/spectrum/radio_spectrum>.

[2] Article 2: Nomenclature. In *Radio Regulations*, Ženeva: International Telecommunication Union, první vydání, 2020, ISBN 978-92-61-30301-3, s. 25–26.

[3] GRIFFITHS, D. J.: *Introduction to Electrodynamics*. Cambridge: Cambridge University Press, Čtvrté vydání, 2013, ISBN 978-1-10842-041-9.