Morea Ibrahimaj

RF Hacking Lab Development: HackRF One and Flipper Zero

Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Bachelor's Thesis

May 2024

Abstract

Author:	Morea Ibrahimaj
Title:	RF Hacking Lab Development: Hack RF One and Flipper Zero
Number of Pages:	50 pages + 1 appendix
Date:	May 2024
Degree:	Bachelor of Engineering
Degree Programme:	Information Technology
Professional Major:	Smart Devices and IoT
Supervisors:	Marko Uusitalo

This thesis project presents the development of hands-on laboratories for an Ethical Hacking course, designed to equip students with essential skills in the rapidly evolving field of Radio Frequency (RF) security. The labs utilize the HackRF One Software-Defined Radio (SDR) and the Flipper Zero, a specialized sub-GHz analysis tool, to provide a comprehensive exploration of RF fundamentals, signal analysis, protocol reverse engineering, and active attack techniques. Students engage in exercises such as intercepting and decoding Automatic Dependent Surveillance-Broadcast (ADS-B) transmissions and executing controlled replay attacks, gaining insight into the vulnerabilities of wireless systems. Ethical considerations are emphasized throughout, with labs conducted in controlled environments to promote responsible experimentation.

The project explores the strengths and trade-offs between general-purpose SDR platforms and specialized RF security tools, highlighting the importance of tool selection for effective analysis. These labs, along with recommendations for expansion to include topics like advanced attacks, defensive countermeasures, and emerging technologies, aim to create a strong foundation for future RF security education.

Ultimately, the research resulted in three-part lab tailored for students with no prior hacking experience.

Keywords: Ethical hacking, RF security, SDR

Contents

List of Abbreviations

ADC:	Analog-to-Digital Converter
ADS-B:	Automatic Dependent Surveillance-Broadcast
AM:	Amplitude Modulation
API:	Application Programming Interface
ASCII:	American Standard Code for Information Interchange
BLE:	Bluetooth Low Energy
BPSK:	Binary Phase Shift Keying
CIA:	Confidentiality, Integrity, and Availability
CSF:	Cybersecurity Framework
DSP:	Digital Signal Processing
EHF:	Extremely High Frequency
ELF:	Extremely Low Frequency
EM:	Electromagnetic
FM:	Frequency Modulation
FSK:	Frequency Shift Keying
FFT:	Fast Fourier Transform
GPS:	Global Positioning System

GPU:	Graphics Processing Unit
HF:	High Frequency
HTTP:	Hypertext Transfer Protocol
IR:	Infrared
ISMS:	Information Security Management System
ISO/IEC:	International Organization for Standardization / International Electrotechnical Commission
IT:	Information Technology
LF:	Low Frequency
LOS:	Line of Sight
MF:	Medium Frequency
NIST:	National Institute of Standards and Technology
NFC:	Near Field Communication
OFDM:	Orthogonal Frequency-Division Multiplexing
OOK:	On-Off Keying
OSSTMM:	Open Source Security Testing Methodology Manual
QAM:	Quadrature Amplitude Modulation
QPSK:	Quadrature Phase Shift Keying
RF:	Radio Frequency

RFID: Radio Frequency Identification

SD: Secure Digital

SDR: Software-Defined Radio

SHF: Super High Frequency

SLF: Super Low Frequency

SQL: Structured Query Language

SSH: Secure Shell

UHF: Ultra High Frequency

ULF: Ultra Low Frequency

USB: Universal Serial Bus

VHF: Very High Frequency

VLF: Very Low Frequency

Glossary of Terms

Amplitude Modulation (AM): A modulation technique where the amplitude (strength) of a radio carrier wave is varied in proportion to an information signal (e.g., voice).

Antenna: A device that converts electrical currents into electromagnetic waves for transmission, or conversely, converts incoming electromagnetic waves into electrical currents for reception.

Bandwidth: The range of frequencies occupied by a radio signal. It determines the amount of data that can be transmitted per second.

Carrier Wave: The basic radio wave upon which information is superimposed through modulation.

Decibel-milliwatts (dBm): A unit of power measurement commonly used in radio communications to express signal strength.

Digital Signal Processing (DSP): The use of mathematical algorithms to manipulate and analyze digitized signals, such as radio signals.

Directivity: A measure of how much an antenna concentrates its radiated power in a specific direction.

Electromagnetic (EM) Spectrum: The entire range of electromagnetic radiation, including radio waves, visible light, X-rays, and more.

Fast Fourier Transform (FFT): An algorithm that efficiently converts a signal from the time domain (voltage changes over time) into the frequency domain (showing the strength of different frequency components).

Frequency: The number of cycles of a wave that occur in one second, measured in Hertz (Hz).

Frequency Modulation (FM): A modulation technique where the frequency of a radio carrier wave is varied in proportion to an information signal.

Fuzzing: A software testing technique that involves automatically injecting malformed or random data into a program to uncover coding errors and security loopholes.

Gain (Antenna): A measure of how much an antenna amplifies a signal in a specific direction compared to a reference antenna.

Hertz (Hz): The unit of measurement for frequency. One Hertz equals one cycle per second.

Impedance: The opposition of an antenna or circuit to the flow of alternating current. For efficient power transfer, the impedance of the antenna must match that of the transmitter or receiver.

Modulation: The process of encoding information onto a radio carrier wave.

Polarization: The orientation of the electric field in an electromagnetic wave.

Power (Radio Transmission): The amount of energy transmitted by a radio transmitter, typically measured in watts (W) or milliwatts (mW).

Propagation: The way in which radio waves travel from a transmitter to a receiver, influenced by factors like frequency, terrain, and atmospheric conditions.

Radio Band: A specific range of frequencies within the radio spectrum allocated for particular uses.

Radio Frequency (RF): The portion of the electromagnetic spectrum used for radio communication, generally ranging from 3 kHz to 300 GHz.

Receiver: A device that converts radio waves into electrical signals, enabling the extraction of transmitted information.

Selectivity: The ability of a receiver to isolate a desired signal within a narrow frequency range while rejecting adjacent signals.

Sensitivity: The minimum signal strength that a receiver can detect and successfully demodulate, measured in decibel-milliwatts (dBm).

Software-Defined Radio (SDR): A radio system where traditional hardware components (mixers, filters, etc.) are replaced with software running on a powerful processor.

Transceiver: A device that combines a transmitter and receiver, allowing for both the transmission and reception of radio signals.

Transmitter: A device that generates radio waves and modulates them with information for transmission.

Wavelength: The distance between two consecutive peaks (or troughs) of a wave.

1 Introduction

In his book *“Lights out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath”*, Ted Koppel [1] paints a grim picture of the United States’ vulnerability to a devastating cyberattack. A power grid attack could cause cascading outages causing widespread disruption – from the loss of running water and working sewage systems, to no refrigeration or light, to no access to devices people have come to rely so heavily on. It would equate to an alarming societal breakdown. Yet, cyberattacks can have even more immediate and devastating consequences on individuals, as highlighted by the tragic death attributed to ransomware at a German hospital; the hospital’s IT system failure, which prevented a critically ill patient from receiving timely care, underscores the real-world risks in a landscape increasingly driven by interconnected devices. [2]

Smart devices, from wearables to home appliances, are deeply integrated into daily life. Yet, the very wireless technologies that offer such convenience also create new avenues for cyber-attacks; WiFi, Bluetooth, RFID, and various other RF technologies are all susceptible to being exploited by hackers. These risks aren’t just theoretical. Smart homes have been infiltrated through unsecured wireless protocols, and even medical devices like pacemakers and insulin pumps have proven susceptible to radio frequency hacking [3]. Such vulnerabilities highlight the importance of hands-on RF security education. Educational institutions are recognizing the demand for trained ethical hackers by adapting cybersecurity programs accordingly. These professionals play a crucial role in identifying weaknesses and strengthening defences by applying an adversarial mindset. Training programs are increasingly incorporating hands-on learning components within cybersecurity curricula, offering a powerful method for going beyond theoretical concepts, allowing learners to directly engage with vulnerabilities and develop the skills needed to address them.

This thesis project focuses on developing RF hacking labs that introduce hands-on ethical hacking concepts, using two accessible tools: the HackRF One and

the Flipper Zero. Targeting students with an IT background, the labs provide practical exposure to RF security concepts even for those who may lack prior RF knowledge. While focusing on the attacker's perspective, they aim to strengthen defensive skills within the broader context of RF security. By exploring these devices' capabilities, participants stand to gain valuable skills for safeguarding the wireless networks that support modern life.

This thesis presents the design of these RF hacking labs, equipping ethical hackers with the skills necessary to mitigate wireless vulnerabilities. It outlines the lab design methodology, reviews relevant literature, and details the labs themselves. Ultimately, this project aims to contribute to the training of cybersecurity professionals who understand the unique risks in wireless communications, the tools used to exploit them, and how to proactively design more resilient systems.

2 Methodology and Materials

This thesis project involved designing and developing laboratory exercises to introduce ethical hacking concepts, focusing specifically on radio frequency (RF) technologies. Students enrolled in the elective Ethical Hacking course at Metropolia University of Applied Sciences were the intended audience. The core assumption was that students would have basic IT knowledge, but no specialized background in RF or cybersecurity is required for the participation in the labs.

2.1 Materials

The labs centred around two primary devices: HackRF One and Flipper Zero. The devices, along with the supporting hardware required, were selected and provided by the thesis supervisor.

The HackRF One is a versatile SDR peripheral, capable of transmitting and receiving signals across a wide frequency spectrum. For the purposes of this thesis and lab development, the device was supplemented with the PortaPack

add-on, which allows for use of the HackRF One on-the-field, as opposed to having to connect it to a computer running an SDR application. The add-on also provides a hand-held user interface with a touchscreen. Additionally, several antennas, SD cards, microUSB cable, and a computer were necessary for interfacing with this device.

The other device, Flipper Zero, is a portable multi-tool designed for exploration and interaction with RF systems, particularly in the sub-GHz range. The sub-GHz transceiver allows it to communicate with common access control systems, radio remotes, gate openers, and the like. It is capable of capturing, decoding, replaying, and even generating custom signals.

As for the software, it included SDR applications for interfacing with the HackRF One (specifically, SDR++ and SDR#), and configuration tools like qFlipper or the Flipper Mobile App for Flipper Zero configuration. The devices came with default firmware installed. HackRF One was running Mayhem (version 1.8.8), which was later updated to its latest version (at the time of writing, version 1.9.1) for access to expanded features. The Flipper Zero's default firmware was replaced with Xtreme firmware (a fork of Unleashed firmware) which added further functionality required for the labs.

2.2 Scope and Limitations

The labs targeted RF hacking fundamentals as a specific domain within ethical hacking. Concepts covered included signal capture, analysis, Automatic Dependent Surveillance-Broadcast (ADS-B) decoding, and sub-GHz replay attacks. The project timeline allowed approximately 6-8 weeks for the lab development section, with the rest of the time allocated to preliminary research of the devices and software. This was sufficient for creating the initial set of exercises, but ongoing evaluation and refinement will be valuable for future iterations. To ensure accessibility to students without prior RF knowledge, the initial exercises included introductory tutorials on basic RF concepts and device usage.

Certain techniques, such as jamming attacks, were considered but excluded due to a combination of technical and legal factors. The availability of only one radio transceiver limited exploration of scenarios involving active transmission; due to the half-duplex nature of the HackRF One, it was not possible to test transmission tasks without an additional receiver. Furthermore, since the target audience is presumed to lack RF expertise, and the author did not possess a radio transmission license, it was important to prioritize lab activities that were unlikely to cause unintended interference or violate regulations.

2.3 Lab Design Methodology

The design process followed a loosely structured approach to accommodate the exploratory nature of learning about the HackRF One and Flipper Zero. Labs were designed as a blend of introductory device familiarization and more open-ended tasks encouraging comparison between the devices' capabilities. Emphasis was placed on accessibility – given the lack of prerequisites for the course, the focus was on clarity of instructions and a gradual increase in complexity.

To further establish the constructiveness of the labs, more formalized pre-lab and post-lab surveys with students are recommended. This would help quantify the efficacy of the labs in conveying concepts and building practical skills. Such data collection could be conducted at the onset of the course in Spring 2025 (for the pre-lab surveys) and at the conclusion of the course and labs (for the post-lab surveys), and findings would contribute to future refinements of the lab activities. Tentatively, surveys have already been prepared for this purpose ensuring readiness for implementation when the course is offered.

3 Literature Review

Seeing as the research goal of this thesis was to design RF hacking labs using the HackRF One and Flipper Zero for students of various IT backgrounds taking an Ethical Hacking course, three research fields are implicated and naturally stand out as the theoretical framework that informs this study. Because of the hacking element of the lab, the concepts surrounding ethical hacking must first be discussed and understood as part of the scholarship on cybersecurity. Furthermore, as the devices are RF devices, basic elements of RF theory, such as wave properties, antennas, and radio bands, must also be explored. Finally, the particularities of RF hacking are explored with discussions, among others, about core tools required, signal analysis, protocols, and active attacks.

These three fields became the natural focus of the literature review because of their direct connection to the project. Chapters 3.1 and 3.2 first discuss the scope and tools of cybersecurity and ethical hacking. Following those, chapter 3.3 gives an overview of RF theory, highlighting the most relevant concepts as they pertain to the devices used in the labs. Finally, chapter 3.4 focuses on RF hacking and the tools and protocols essential to this field.

While other concepts can be considered relevant to the topic at hand (e.g., pedagogical considerations of curricula design), they were deemed to be outside of the scope of this study and were thus not included in the literature review.

The literature review keeps the research on track by providing clear links between the literature and the research goals of the thesis and providing a structure for systematically organizing and using concepts. All these concepts are put together to produce a well-rounded lab design in chapter 4 and 5, discussing the HackRF One and Flipper Zero lab design, respectively.

3.1 Cybersecurity Foundations and Frameworks for Ethical Practice

Cybersecurity's roots stretch back to the early days of computing, when concerns arose about safeguarding sensitive data stored on mainframes. As computer networks proliferated, so too did the potential for unauthorized access, data breaches, and malicious attacks. Today, cybersecurity is a multifaceted discipline that encompasses the strategies, technologies, and practices designed to protect networks, devices, and data from unauthorized access, theft, or sabotage. It is a dynamic field driven by the constant evolution of threats and the need to safeguard the confidentiality, integrity, and availability of digital assets. This concept is often referred to as the CIA triad, as illustrated in the figure below. [4]

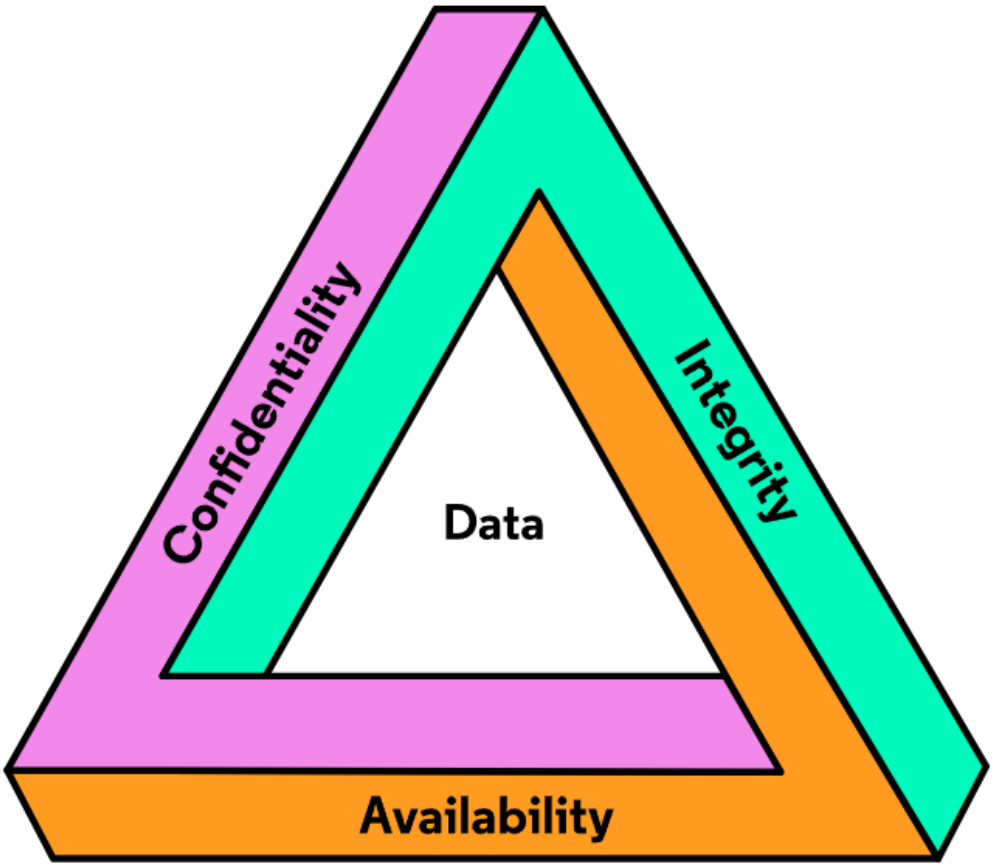

Figure 1 CIA Triad [4]

The CIA Triad is widely used model in cybersecurity, used to guide policies and measured for information security within an organization. The confidentiality

concept refers to the prevention of unauthorized access to sensitive information, ensuring that data is accessible exclusively to those with sufficient privileges. Various techniques, such as encryption, authentication, and access control are commonly employed to ensure data confidentiality. Integrity involves maintaining the accuracy and completeness of data in all its states (in storage, in process, and in transit). This means ensuring that information is not altered in unauthorized ways, whether by accident or malicious intent. Methods used to protect integrity of data include hashing, checksums, and maintenance of clear audit trails. Finally, data availability ensures that information is readily available to authorized users when needed. To support data availability, organizations are encouraged to maintain hardware, perform regular software updates, and implement robust disaster recovery plans to counteract service disruptions. [5]

Key elements within cybersecurity include [5]:

- **Risk Assessment:** The systematic identification and analysis of vulnerabilities, threats, and their potential impact on an organization's information systems.
- **Access Controls:** Mechanisms like authentication and authorization that regulate access to resources based on established policies and user permissions.
- **Encryption:** The process of disguising sensitive data to prevent unauthorized access, ensuring confidentiality even if data is intercepted.
- **Incident Response:** Processes and plans for detecting, mitigating, and recovering from security breaches in a timely manner.

Numerous frameworks exist to guide organizations in developing robust cybersecurity programs and fostering an ethical approach. These frameworks provide standards, best practices, and compliance guidelines. Notably:

- **NIST Cybersecurity Framework (CSF):** Widely adopted framework promoting a risk-based approach by prioritizing the most critical assets and threats. [6]

- **ISO/IEC 27001:** An international standard outlining requirements for an Information Security Management System (ISMS). [7]
- **OSSTMM:** The Open Source Security Testing Methodology Manual provides a standardized approach to penetration testing. [8]

These frameworks are particularly relevant to ethical hacking activities because they emphasize the importance of operating within a controlled environment, respecting data privacy, and prioritizing the overall security posture of an organization. Specific standards within these frameworks, such as those addressing penetration testing and vulnerability assessments, offer a roadmap for ethical hackers to conduct their work responsibly while contributing to the improvement of cybersecurity practices. [9]

Ethical considerations are paramount within cybersecurity, with ethical hacking playing a crucial role. The next section explores the specifics of ethical hacking, its techniques, and its significance within the broader cybersecurity landscape.

3.2 Ethical Hacking as a Subset of Cybersecurity

Within the dynamic landscape of cybersecurity, ethical hacking, also known as white hat hacking, distinguishes itself from malicious hacking by its intent and methodology. While malicious hackers exploit vulnerabilities for personal gain or destructive purposes, ethical hackers operate with the explicit consent of an organization to identify weaknesses in their systems before adversaries can exploit them. Ethical hackers adhere to a strict code of conduct, prioritizing transparency, confidentiality, and collaboration to strengthen the security defences of their targets.

3.2.1 Scope

The techniques and targets of ethical hacking mirror the rapidly evolving threat landscape. Ethical hackers analyze a wide range of technologies to identify

vulnerabilities that could be exploited by real-world attackers. Key areas include [5]:

- **Web Applications:** Testing the security of websites, APIs, and other web-facing interfaces to uncover vulnerabilities like SQL injection and cross-site scripting.
- **Networks:** Assessing network configurations, firewalls, and intrusion detection systems for potential misconfigurations or exploitable flaws.
- **Wireless Networks:** Analyzing wireless protocols like Wi-Fi and Bluetooth for vulnerabilities that attackers could leverage to gain unauthorized access or intercept communications.
- **IoT Devices:** Examining the security of the growing network of connected devices, such as smart home appliances and wearable technology, where RF protocols are often a prime target.
- **Social Engineering:** Testing human susceptibility to phishing attacks, impersonation, and other tactics aimed at manipulating individuals into divulging sensitive information or granting unauthorized access.

By strategically simulating attacks across these various technological fronts, ethical hackers provide organizations with a clear understanding of their vulnerabilities, allowing them to proactively implement security measures and strengthen their overall security posture against potential threats.

3.2.2 Tools

Ethical hackers employ a wide range of tools that closely resemble those used by malicious actors, enabling them to simulate real-world attacks in a safe environment. These tools fall into several key categories, each serving a specific purpose in the ethical hacker's process identifying vulnerabilities.

Network scanners, such as Nmap [10] and Nessus [11], are essential for

reconnaissance and mapping. They enable ethical hackers to identify active hosts on a network and enumerate open ports, which can provide clues about services running on those systems and potential entry points for exploitation. While both tools excel at network discovery, Nmap is known for its flexibility and customization options, whereas Nessus offers deeper vulnerability scanning capabilities and integrates with compliance reporting tools. [11]

Vulnerability assessment tools take the reconnaissance stage further by automating the process of identifying known vulnerabilities. Examples include OpenVAS [12] and the Metasploit Framework [13]. These tools typically maintain a database of known security flaws and correlate them with software versions detected during the scanning process. This helps ethical hackers pinpoint specific vulnerabilities that might be present on a system, allowing them to prioritize targets for exploitation. Metasploit Framework goes beyond mere vulnerability scanning and offers exploit modules, enabling ethical hackers to actively test if identified vulnerabilities can indeed be used to gain access or compromise systems [13].

Passwords remain a common point of weakness, and ethical hackers employ specialized tools for cracking them. John the Ripper [14], Hydra [15], and Hashcat [16] are popular choices, capable of brute force and dictionary attacks. Hashcat stands out with its support for GPU acceleration, significantly increasing the speed of cracking attempts, especially against modern hashing algorithms. [17] By deliberately attempting to break passwords, ethical hackers can identify weak user choices or poor password storage practices within organizations.

The wireless domain presents specialized challenges, and tools like Aircrack-ng [18] and Kismet [19] are tailored for this environment. Unlike wired networks, an attacker doesn’t need physical access to the network to intercept or inject traffic. Moreover, encryption protocols commonly used in wireless networks have historically been susceptible to various attacks. Tools like Aircrack-ng and Kismet are tailored for this environment, allowing ethical hackers to analyze wireless networks, capture packets for analysis, and test wireless protocols for

vulnerabilities that attackers could exploit to gain unauthorized access or intercept sensitive communications.

To gain a comprehensive understanding of a target network's security posture, an ethical hacker might follow an approach like this:

1. **Network Discovery and Reconnaissance (Nmap):** The process begins with network discovery using a tool like Nmap. The ethical hacker executes a scan to identify active devices (hosts) on the network and the services they offer. This initial scan might reveal open ports like port 22 (SSH) or port 80 (HTTP) indicating the presence of remote access and web server functionalities. [10]
2. **Vulnerability Assessment and Prioritization (OpenVAS):** With a network map in hand, the ethical hacker leverages a vulnerability assessment tool like OpenVAS to scan the identified hosts for known weaknesses. OpenVAS correlates the discovered services (e.g., SSH server) with its vulnerability database, pinpointing potential security flaws. The ethical hacker can then prioritize these vulnerabilities based on severity (critical, high, medium, low) and exploitability, focusing on those that could be easily leveraged by attackers.
3. **Exploit Testing and Privilege Escalation (Metasploit Framework):** If a high-risk vulnerability is identified, such as a known flaw in a specific SSH server version, the ethical hacker might utilize the Metasploit Framework. This tool offers exploit modules that can simulate an attacker's attempt to compromise the vulnerable system. A successful exploit test demonstrates the potential real-world impact of the vulnerability and might even reveal an initial foothold within the network. However, this initial access might be limited. Metasploit can also assist in identifying methods for privilege escalation, allowing the ethical hacker to potentially gain more control over the compromised system to further assess internal security measures.
4. **Password Strength Assessment (John the Ripper):** During the network reconnaissance stage, the ethical hacker might have noticed a web server

login page. To assess the strength of password protection for this service, they could employ a password cracking tool like John the Ripper. A dictionary attack using a list of common passwords could be attempted to determine if weak credentials are being used. If cracking is successful, it highlights the importance of enforcing strong password policies within the organization.

5. **Wireless Network Assessment (Kismet):** The ethical hacker might also consider the wireless network's security posture. A tool like Kismet can be used to detect nearby wireless access points and analyze their configurations. Weak encryption protocols or unsecured access points could be identified, posing a significant risk if left unaddressed.

The tools discussed here are merely a subset of the resources available to ethical hackers, who must remain up to date with the evolving threat landscape and continuously expand their toolset.

3.2.3 Educational Value

With the sophistication and prevalence of cyber threats on the rise, the importance of comprehensive cybersecurity preparedness has become paramount. Ethical hacking training holds significant value for students pursuing careers within the IT field. This approach emphasizes the necessity of understanding the attacker's mindset in order to design robust and resilient security systems. Furthermore, it underscores the importance of continuous learning and adaptation, as both attack techniques and defensive strategies constantly evolve.

Experiential learning plays a vital role in cybersecurity education, and ethical hacking is no exception. Hands-on labs provide a powerful way for students to grasp the practical implications of cyberattacks and develop the skills needed to defend against them. By simulating real-world scenarios in a controlled environment, students gain experience with the tools and techniques used by adversaries, building a deeper understanding of how to identify and mitigate

vulnerabilities. Furthermore, ethical hacking labs foster a proactive approach to security, encouraging students to think critically about potential weaknesses and develop solutions before they become exploited.

Beyond building technical proficiencies, ethical hacking labs serve as a crucial ethical training ground. Students learn the importance of operating within defined parameters and adhering to the highest ethical standards. They are confronted with the potential harm that could result from the misuse of cybersecurity skills, reinforcing responsible practices and emphasizing the importance of using their knowledge for the greater good.

3.2.4 Legal vs. Ethical Hacking

Understanding the distinction between legality and ethics is crucial within the field of ethical hacking. While ethical hacking seeks to strengthen defences by proactively identifying and mitigating vulnerabilities, it must always operate within the confines of the law. The legal landscape surrounding cybersecurity is complex and can vary significantly between jurisdictions.[1]

Even with the best of intentions, actions that might seem ethically justifiable from a technical standpoint can still carry legal ramifications. Conversely, there might be situations where a specific action is technically legal but raises ethical concerns. For example, an ethical hacker might be legally permitted to exploit a known vulnerability in an outdated software version if the organization has been warned of the risk but failed to take action. However, actively exploiting that

[1] While Finland has no specific legislation or legal framework that addresses cybercrime, as part of the EU, they adhere to the security regulation laid out by the union, namely the General Data Protection Regulation (GDPR), which govern the principles of data protection and privacy rights within the EU. [46]

vulnerability could cause service disruptions or data exposure, raising questions about the ethics of causing harm even in the pursuit of improving security.

Ethical hacking goes beyond mere compliance with the law. It encompasses a deep commitment to responsible and transparent behaviour. Ethical hackers prioritize obtaining explicit consent, clearly documenting their actions, and adhering to strict reporting guidelines when disclosing vulnerabilities. They understand the potential harm that irresponsible actions can cause, both to the target organization and to the reputation of the cybersecurity field itself.

The line between legal and ethical hacking can often be nuanced. Ethical hackers operate in gray areas, pushing boundaries to uncover hidden vulnerabilities before malicious actors can exploit them. This underscores the importance of open communication and trust between ethical hackers and the organizations they serve.

3.3 Radio Frequency Theory

Since the labs are concerned with RF hacking, some basic understanding of radio theory is necessary. Thus, this chapter introduced radio, and discusses some of the more important concepts of radio theory, such as the properties of waves, propagation modes, radio bands, antennas, and SDR.

3.3.1 Wave Properties

The electromagnetic (EM) spectrum encompasses a wide range of radiation, with radio waves occupying a specific portion characterized by relatively long wavelengths and lower frequencies [20]. Understanding these wave properties is fundamental for successful RF hacking endeavours. EM waves (depicted in Figure 2), including radio waves, travel at the speed of light and exhibit properties such as frequency, wavelength, amplitude, and polarization.

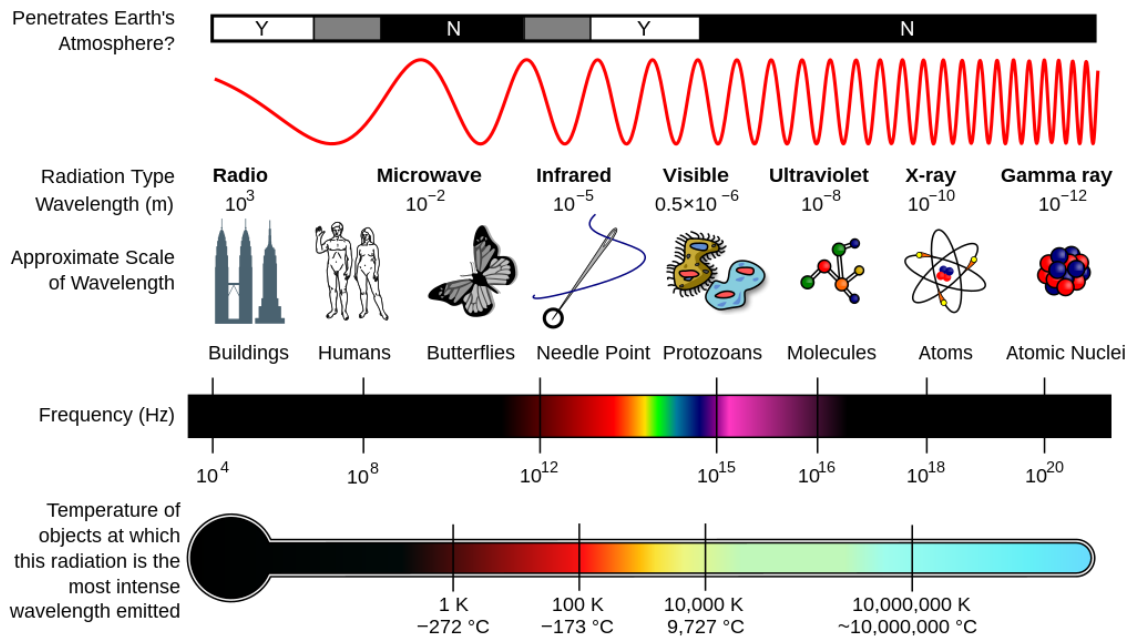

Figure 2 The electromagnetic spectrum and its properties [21]

The figure above illustrates several properties of EM waves, including the temperature, radiation type, wavelength, and frequency. The latter two are of particular interest in RF hacking. Measured in Hertz (Hz), frequency represents the number of wave cycles per second. It has an inverse relationship with wavelength, the distance between the two consecutive peaks of the wave. This means that higher frequency waves have shorter wavelengths, and vice versa. [22] Tuning a car radio to a specific station exemplifies this principle: selecting a station essentially changes the received frequency corresponding to a specific wavelength within the FM band. Understanding this relationship allows hackers to identify and target specific radio frequencies used in various systems. For example, knowing that Bluetooth operates in the 2.4GHz band allows a hacker to focus their efforts on this specific frequency range when searching for vulnerabilities in Bluetooth devices. Similarly, knowledge of the frequency range used in access control systems can guide hackers in their attempts to exploit these systems. Therefore, a grasp of these fundamental wave properties equips hackers with a crucial tool for identifying and manipulating radio frequency signals.

3.3.2 Propagation

Radio waves don’t simply travel in a straight line from a transmitter to a receiver. The journey of a radio wave, known as propagation, is influenced by its frequency and the environment it encounters. Propagation refers to the way in which a wave travels through a medium, influencing the range and reliability of communication. [20]

Rather than a simple beam, radio waves interact with various obstacles and can even bend due to atmospheric conditions. Lower-frequency signals, like those used in AM radio, tend to follow the curvature of the Earth (ground waves), enabling broadcast over long distances. Alternatively, some radio waves, particularly those in higher frequency ranges, bounce off the ionosphere (sky waves). This phenomenon allows communication across continents, but also introduces variability as the ionosphere shifts due to solar activity. [20]

Line-of-sight (LOS) propagation, particularly important for high-frequency signals like those used in WiFi and cellular communication, requires a clear path between the transmitter and the receiver. Obstructions like building or terrain can block or weaken the LOS signals. Sometimes, radio waves scatter by deflecting off objects and allowing them to reach receivers even when not in direct line-of-sight. This scattering makes eavesdropping possible even without being in the intended coverage area. [20]

By understanding the dynamics of radio wave propagation, hackers gain a strategic advantage. They can predict signal behaviour, identify potential interception points, and tailor attacks to exploit the unique characteristics of various wireless systems based on their frequencies and the intended operational environment.

3.3.3 Radio Bands

The vast radio frequency spectrum is divided into smaller segments known as radio bands. These bands are allocated by international organizations and regulatory bodies for specific uses like broadcasting, aviation, navigation, and scientific research. Each band exhibits distinct properties dictated by frequency range, influencing factors like propagation and signal reach, how readily they can penetrate obstacles, and the amount of data they carry. [20]

The table below provides an overview of key radio frequency bands. Each band has distinct characteristics that influence its use and potential vulnerabilities, as seen in the *RF Hacking Considerations* column. Understanding these characteristics is a powerful tool for an RF hacker, as it allows them to identify potential points of exploitation, have a good grasp of the attack surface, and lets them develop attack vectors tailored to the specific target system.

Table 1 Radio frequency bands and their respective ranges, common uses, and relevant considerations for RF hacking [23]

Frequency Band	*Range*	*Common Uses*	*RF Hacking Considerations*
Extremely Low Frequency (ELF)	3 Hz - 30 Hz	Submarine communication (one-way), geophysical research	Limited data transmission, penetration of ground and water
Super Low Frequency (SLF)	30 Hz - 300 Hz	Limited communication systems	Very long wavelengths, some penetration of ground and water
Ultra Low Frequency (ULF)	300 Hz - 3 kHz	Time signals, geophysical monitoring	Long-range, ground penetration capabilities
Very Low Frequency (VLF)	3 kHz - 30 kHz	Long-range navigation systems, time signals	Ground wave propagation, some atmospheric penetration

Low Frequency (LF)	30 kHz - 300 kHz	AM radio, maritime communication, navigation beacons	Long-distance communication via ground waves
Medium Frequency (MF)	300 kHz - 3 MHz	AM radio, amateur radio	Ground wave and some skywave propagation
High Frequency (HF)	3 MHz - 30 MHz	Shortwave broadcasting, long-range aviation and maritime communication, over-the-horizon radar	Skywave propagation for global reach but vulnerable to ionospheric disturbances
Very High Frequency (VHF)	30 MHz - 300 MHz	FM radio, television, two-way radios, aircraft communication	Primarily LOS propagation, some scattering
Ultra-High Frequency (UHF)	300 MHz - 3 GHz	Television, cellular networks, Wi-Fi, GPS, microwave links	Good mix of range and data capacity, LOS and some scattering
Super High Frequency (SHF)	3 GHz - 30 GHz	Satellite communication, radar, Wi-Fi, point-to-point links	Supports high data rates, susceptible to attenuation (rain fade)
Extremely High Frequency (EHF)	30 GHz - 300 GHz	High-speed wireless links, experimental research, millimeter-wave radar	Very short range, limited penetration, potential for secure communication

Table 1 highlights the interaction between frequency bands and the potential security risks they pose. For instance, the limited penetration of EHF signals implies that an attacker would need close physical proximity to compromise a system using this band, an exploit which would require a different approach than that of long-range ELF communication. Similarly, a hacker interested in disrupting

a wireless sensor network will try to leverage the UHF band's susceptibility to jamming and interference attacks. A good grasp of these differences between bands allows the ethical hacker to efficiently eliminate irrelevant attack vectors and prioritize the most vulnerable entry points with the highest likelihood of success.

3.3.4 Hardware

The foundation of RF systems lies in their hardware components. This chapter explores the core elements involved in wireless communication, primarily transmitters and receivers, and introduces hardware tools essential for RF hacking. Antennas, while radio-related hardware, are discussed in a dedicated chapter, as the information is quite dense.

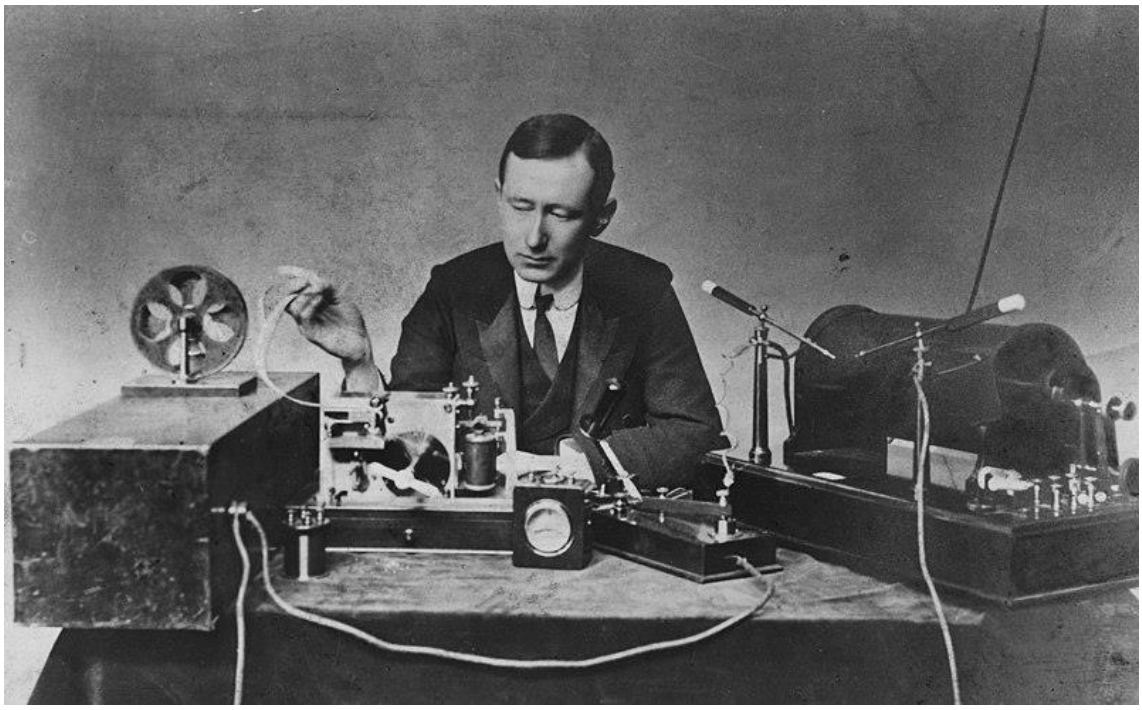

Figure 3 Guglielmo Marconi (the inventor of radio) with the spark-gap transmitter (right) and coherer receiver (left) [24]

At their core, transmitters transform electric signals into radio waves for broadcast, while receivers perform the reverse. Key features influencing the

capabilities of a transmitter include power output and modulation (i.e., the encoding of information onto a radio wave). [22]

The power output, measured in watts or milliwatts, significantly impacts the transmission range. Higher power allows signals to travel farther, but regulations often limit output to prevent interference with other users of the radio spectrum. Ethical considerations also come into play, as high-power transmissions can unintentionally disrupt nearby systems. [20]

Modulation, another crucial process, encodes information onto the carrier wave, that is, the invisible foundation of the radio wave. Common modulation schemes include Amplitude Modulation (AM) where the amplitude (strength) of the carrier wave varies according to the information signal, and Frequency Modulation (FM), where the carrier wave's frequency is varied. These two modes are applied to analogue information signals. [22] Digital modulation techniques, on the other hand, represent data as a series of pulses or symbols within the carrier wave[2]. [25] Understanding modulation is essential, as different schemes require specialized receivers for proper demodulation and retrieval of the original information.

On the receiving end, the radio waves need to be translated back into usable electrical signals. Radio receivers perform this critical function[3]. The two most important factors in successful reception of signals are the sensitivity and selectivity of a radio receiver. The former is measured in decibel-milliwatts (dBm) and represents the minimum signal strength a receiver can detect and successfully demodulate. High sensitivity allows for receiving weak signals, often crucial for long-range communication or for capturing faint transmissions in

[2] Other examples of modulation methods include Frequency-Shift Keying (FSK) and Orthogonal Frequency-Division Multiplexing (OFDM), both of which are digital modulation methods.
[3] A device that allows for both transmission and receiving of radio waves is called a transceiver.

crowded RF environment. Conversely, low-sensitivity receivers might be required in strong signal environments to avoid overload when only nearby, powerful transmissions are of interest. [26]

Selectivity, on the other hand, describes the receiver's ability to isolate a specific signal within a narrow bandwidth while rejecting unwanted signals on adjacent frequencies. Filters play a vital role in achieving selectivity, allowing the receiver to focus on the targeted signal and minimize interference from other transmissions. [27]

Additionally, the architecture of a receiver plays a role in its sensitivity and selectivity. The specific design choices within an architecture, such as the type and quality of filters, can significantly impact these performance aspects. The majority of radio receivers apply the superheterodyne architecture (commonly referred to as *superhet*) which offers a good balance between performance and cost, while providing good selectivity and sensitivity. [27] However, other examples include direct conversion receivers [27], known for their simplicity, and SDRs, which offer exceptional flexibility through software-driven signal processing. Traditional receivers (such as the superhet) rely heavily on fixed analogue hardware circuits (i.e., mixers, filters, amplifiers). These define their operating frequency, selectivity, and overall performance. In SDRs, however, much of the traditional hardware is replaced by software running on a processor. The initial analogue RF signal is digitized early on in the process using an analogue-to-digital converter (ADC), allowing for demodulation, filtering, and any other signal processing tasks to be implemented in software. This software-centric approach gives SDRs unparalleled flexibility. They can be configured for vastly different frequencies, bandwidths, and modulation schemes with simple software changes rather than hardware modifications. This flexibility does come with some trade-offs in their reliance on high-speed digital processors. Regardless, they are increasingly popular tools for both legitimate and malicious RF exploration due to their adaptability. [20]

3.3.5 Software

Software plays an increasingly important role in modern RF systems. From controlling traditional radio hardware to enabling flexible SDR architectures and advances signal analysis, RF software offers a powerful toolkit. This chapter primarily explores SDR concepts and tools, along with a brief look at how digital signal processing and simulation software are transforming RF exploration and analysis.

In SDR, many functions traditionally performed by hardware are moved into the software realm. Instead of fixed analogue circuits, an initial RF signal is quickly digitized, enabling tasks like demodulation, filtering, and analysis to be implemented using powerful processors and malleable software. This offers unparalleled adaptability, allowing SDRs to be configured for a vast range of frequencies, bandwidths, and modulation schemes through simple software modifications. Popular SDR platforms like HackRF One [28], LimeSDR [29], and BladeRF [30] have transformed RF exploration for hobbyists and professionals alike. At the heart of SDR's flexibility lies Digital Signal Processing (DSP). Algorithms manipulate signals mathematically, enabling core tasks like filtering, the Fast Fourier Transform (FFT)[4], and demodulation of diverse signals. [31] Ethical hackers can leverage their understanding of DSP to analyze RF signals in greater depth, identifying potential vulnerabilities and even crafting software-based attacks.

Beyond SDR, various open-source RF analysis tools offer insights into wireless communication. GNU Radio's graphical flowcharts enable the creation of custom signal processing whether used on SDR-captured signals or those generated

[4] This algorithm is a cornerstone of RF analysis, as it converts signals from the time domain (voltage changes over time) into the frequency domain (showing strengths of different frequency components).

from other sources, spectrum analyzers visualize RF activity across a range of frequencies, and dedicated tools exist for analysing specific protocols like WiFi or Bluetooth [32]. While powerful simulation platforms like MATLAB and Simulink exist for advanced RF system design, accessible open-source tools play a significant role in RF experimentation and ethical hacking. Understanding the theoretical basis of such simulators (even without using them directly) can aid in identifying potential weak points in complex RF systems.

3.3.6 Antenna Theory

Antennas act as the gateways between the realm of electrical signals and the invisible world of electromagnetic waves. They form the critical link enabling wireless communication, both in the transmission and reception of radio signals. To understand the behaviour of RF systems fully, a grasp of the fundamental principles of antenna operation is essential.

At their core, antennas function by converting electrical currents into electromagnetic waves for radiation into space, or conversely, capturing incoming electromagnetic waves and inducing corresponding electrical currents. Key antenna properties dictate their performance and suitability for different applications [20]:

- **Directivity/Gain:** Describes how an antenna focuses its radiated energy in specific directions. High-gain antennas concentrate their power, increasing range.
- **Polarization:** Refers to the orientation of the electromagnetic wave's electric field. For optimal reception, transmit and receive antennas should have matching polarizations.
- **Bandwidth:** Refers to the range of frequencies that an antenna can transmit – or receive – radiation energy to.

Various antenna designs exist, each offering different radiation patterns, gains, and physical sizes [20]. Some common examples include:

- **Dipoles:** Simple and versatile antennas, often used as a reference point
- **Yagi-Uda:** Highly directional antennas, popular for long-range applications
- **Loop Antennas:** Known for their directional properties, often used for radio direction finding.

The figure below shows the radiation patterns of dipole and Yagi-Uda antennas.

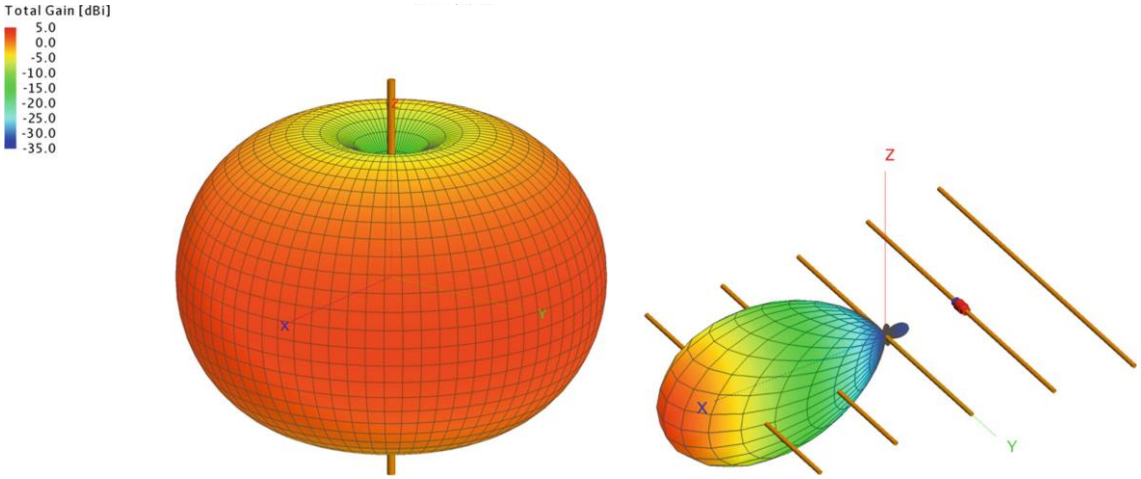

Figure 4 Dipole radiation pattern model (left) and Yagi radiation pattern model (right) [20]

The radiation patterns depicted in Figure 4 can be constructed with the use of computer-aided design programs by plotting the antennas' gain on a 3D plane. The figure informs that dipoles emit most of their radiation along their length, and the least radiation near the top and bottom of the pole. On the other hand, the Yagi-Uda radiation is more directional than that of the dipole.

Selecting the optimal antenna for a specific task involves considering the desired frequency range, space constraints, and the need for directional or omnidirectional coverage. Environmental factors also play a role, as antennas

must be constructed from materials suitable for their intended operational environment.

While the design and optimization of antennas can involve complex electromagnetic simulations, even a basic understanding of antenna theory provides valuable insights for ethical hackers. Knowledge of radiation patterns, polarization, and impedance matching helps anticipate the potential range and effectiveness of both legitimate wireless systems and those targeted for analysis and potential exploitation.

3.4 RF Hacking and Tools

As discussed in the previous chapters, RF signals surround us invisibly, carrying the data that powers the wireless world. From WiFi and Bluetooth to keyless car fobs and garage door openers, RF technology shapes the daily lives of most. For hackers and security enthusiasts, understanding and manipulating these signals opens up a realm of fascinating possibilities.

RF hacking involves the study, analysis, and potential exploitation of radio-based communications. Using specialized tools, attackers can intercept, replay, jam, or even spoof RF signals to gain unauthorized access, disrupt systems, or carry out a range of malicious activities. While this knowledge can be misused, RF hacking can also be a force for good. Ethical hackers seek to understand vulnerabilities in wireless systems so as to strengthen their security, develop protective countermeasures, and explore the field responsibly for the advancement of knowledge [9]. This chapter introduces the fundamental concepts behind RF hacking and explores the range of tools available for working with radio frequencies.

RF hacking centers around a few fundamental concepts. At its core are radio frequencies, the electromagnetic waves that carry the data that powers the wireless realm. These frequencies occupy designated ranges within the electromagnetic spectrum, similar to how lanes on a highway are reserved for

specific types of traffic. Devices communicate using protocols, which define the rules and structures of radio communications, and function as a pre-defined language that governs how devices interact. [33] To transmit information across these frequencies, devices use modulation, a technique for embedding data onto a radio carrier wave. The specific modulation technique employed depends on the type of data being transmitted and the desired characteristics of the signal. For instance, FM radio uses frequency modulation, where the audio signal is encoded by subtly changing the frequency of the radio wave. In contrast, many digital wireless devices use complex modulation schemes that efficiently pack large amounts of data onto the carrier wave for high-speed communication.

Traditional radio hardware is typically designed for specific purposes, like listening to FM radio or receiving WiFi signals. They are “tuned” to a particular frequency range and often limited to understanding a single protocol. In the realm of RF hacking, where the target signal might be unknown or utilize a proprietary protocol, traditional radios become limiting. This is where SDRs come in. SDRs are a game changer for RF hacking due to their flexibility. [25] Unlike traditional radios that are locked to specific frequencies and protocols, SDRs are controlled by software, allowing them to adapt to a wide range of frequencies and protocols. This versatility makes them ideal for research and exploration in the realm of RF hacking. SDRs, other relevant RF hacking tools, and their applications, are further discussed in the chapters below.

3.4.1 Core RF Hacking Tools

To explore the world of RF hacking, a specialized toolkit is essential. At the heart of this toolkit lies the SDR, the cornerstone of flexibility. An SDR can be thought of as a multi-purpose tool on the workbench of an RF hacker; where a traditional radio might be specialized for certain tasks, an SDR can reconfigured on the fly. This allows for the analysis on unknown signals, experimentation with different protocols, and even the development of custom wireless solutions, all from a single piece of hardware. In essence, SDRs become powerful tools for not only exploration, but also manipulation within the world of RF hacking, offering a level

of flexibility that traditional hardware simply cannot match. Popular SDR platforms include HackRF One, BladeRF, and LimeSDR, each offering its own strengths. HackRF One (depicted in Figure 5) is a highly accessible and versatile choice, covering a substantial frequency range and is well-suited for experimentation with RF, which makes it particularly useful for hands-on labs [28]. BladeRF, on the other hand, is better suited for applications demanding higher bandwidth and greater precision [30]. LimeSDR strikes a balance between performance and affordability while featuring multiple input and output channels for advanced techniques [29].

Figure 5 The HackRF One [28]

The figure above shows the HackRF One peripheral without the PortaPack add-on.

Another indispensable tool for the RF hacker is the spectrum analyzer. This device allows users to visualize the strength of signals across a range of frequencies. It is invaluable for identifying active transmissions, analysing the characteristics of unknown signals, and mapping out the overall RF activity of a given environment. [22] Additionally, signal generators complement spectrum analyzers by providing a controlled way to test and analyze wireless devices or systems. With a signal generator, a hacker can create a specific type of signal and inject it into a device. The spectrum analyzer can then be used to observe

how the device reacts to that signal, providing insights into its behaviour and potential vulnerabilities. This functionality opens doors to security testing techniques like replay attacks (where recorded signals are replicated to test device responses) and exploring the principles of intentional jamming (although it is crucial to understand and respect the regulations surrounding signal disruption).

The RF hacking landscape extends beyond these foundational tools to include those designed for close-range wireless systems; RFID and NFC are technologies found in access cards, contactless payment systems, and more. Tools dedicated to these protocols allow for the analysis, interaction, and potential manipulation of these systems. Devices like the Flipper Zero highlight the importance of security testing and exploration within the realm of short-range wireless technologies. The Flipper Zero stands out as a particularly versatile tool for analysing, interacting with, and even manipulating RFID and NFC systems. Its ability to read, emulate, and replay signals across a range of frequencies offers a hands-on way to understand these technologies and explore their potential vulnerabilities. [34] While other NFC/RFID-specialized tools like the Proxmark3 [35] and ChameleonMini [36] exist, the Flipper Zero's accessibility and multi-functionality make it a compelling choice for labs and security research.

Since the focus of this thesis are the HackRF One and Flipper Zero, these two devices’ functionalities and technical capabilities are discussed in more detail in the chapters concerning lab design. Additionally, a comparative analysis of the two is laid out in chapter 6.

3.4.2 Signal Analysis and Reverse Engineering

The analysis of radio frequency communications forms the bedrock of RF hacking. From deciphering wartime transmissions to uncovering the hidden language of wireless devices, signal analysis has played a pivotal role in shaping our technological landscape. This subchapter explores the methods used to dissect these unseen signals, revealing the modulation techniques used to

embed information, the data they carry, and ultimately, the protocols that govern wireless device interactions. Mastery of signal analysis unlocks the understanding of proprietary systems and even the development of custom wireless solutions.

Building upon the foundation laid in the Radio Theory chapter, a revisiting of the fundamental concept of modulation is useful. Modulation is the process of encoding information onto a radio carrier wave. Common techniques include Amplitude Modulation (AM), Frequency Modulation (FM), and various digital schemes. To unlock this information hidden within these modulations, RF hackers employ various tools, such as the SDR and the spectrum analyzer. This subchapter delves into the process of decoding modulations, where SDRs and spectrum analyzers take centre stage.

Spectrum analyzers provide a visual representation of signals across a range of frequencies. By studying the characteristics of a signal on a spectrum analyzer, RF hackers can start to identify the modulation type in use. For example, a signal with a narrow bandwidth that shifts in frequency likely indicates Frequency Modulation (FM), while variations in the signal's amplitude suggest Amplitude Modulation (AM). While spectrum analyzers provide visual clues, SDRs are the workhorses of modulation decoding. SDRs capture raw radio frequency data, which can then be processed by software designed for demodulation. Popular software tools, such as GNU Radio [32] or Universal Radio Hacker [37], provide a wide array of demodulators for various modulation schemes. By experimenting with different demodulators and observing the output, RF hackers can confirm the modulation type and begin extracting the embedded information.

This process can be illustrated with a basic example. If a spectrum analyzer reveals a signal with a constant carrier frequency and variations in its amplitude, this indicates the likely presence of Amplitude Modulation. To confirm this, an RF hacker would employ an SDR to capture a segment of this signal. This captured signal is then fed into an AM demodulator within their chosen software. If the output from the demodulator produces intelligible audio, both the presence of AM

modulation is confirmed and the original audio data that was transmitted is revealed. Of course, real-world signals are often more complex. Digital modulation schemes introduce a layer of encoding where the data is represented as symbols or binary sequences. Specialized demodulators are required to interpret these digital modulations, and additional analysis might be needed to uncover the underlying data structures and meanings.

Figure 6 depicts the difference between FM and AM.

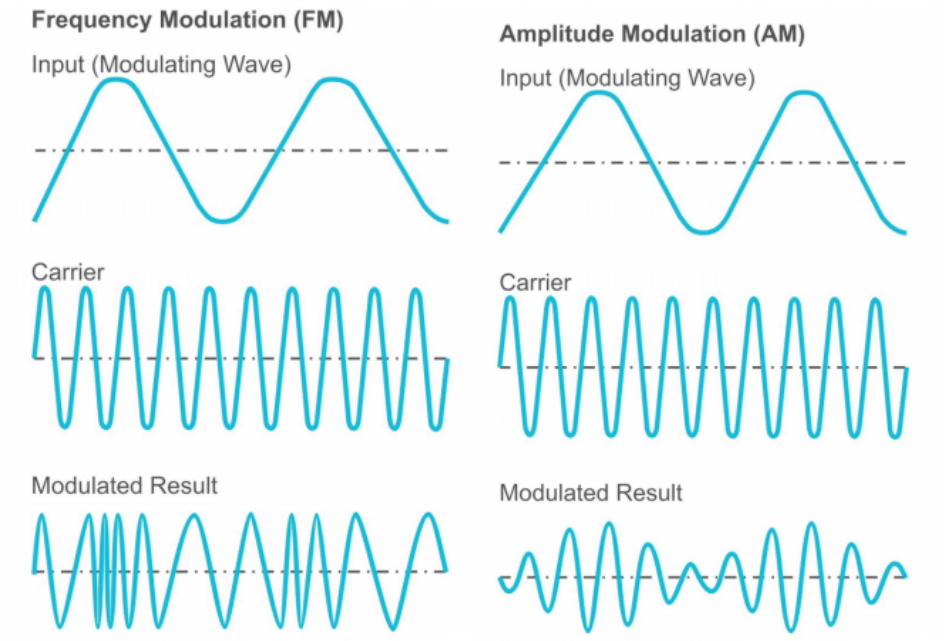

Figure 6 The difference between FM and AM [38]

In contrast to analogue methods like AM and FM, digital modulation schemes represent data as discrete symbols or changes in the carrier wave's characteristics. A simple example is On-Off Keying (OOK), where the information that is to be transmitted is converted into a series of binary 1s and 0s. [39] Then, this digital data is mapped to the presence or absence of the carrier wave. For modulation, the carrier wave is "turned on" for a set period to represent a binary 1 and "turned off" for another set period to represent a binary 0, essentially encoding the digital information onto the carrier wave. For demodulation, an SDR receives the modulated signal and decodes the binary 1s and 0s by analysing the presence or absence of the carrier wave at specific intervals, thus recovering

the original digital information. The OOK process is analogous to using a flashlight to transmit Morse code by repeatedly turning it on and off again at intervals. This particular scheme is amongst the simplest ones; there are other more complex methods, such as Binary Phase-Shift Keying (BPSK), where these binary 1 is represented by keeping the carrier wave in its normal phase, and a binary 0 is represented by inverting or shifting the phase of the carrier wave by 180 degrees (much like flipping the sine wave upside down). Other examples include Quadrature Phase-Shift Keying (QPSK) which uses four different phase shifts to represent two bits of data per symbol, further improving efficiency, or Quadrature Amplitude Modulation (QAM) which combines phase shifts with amplitude changes, allowing even more data to be transmitted within the same bandwidth. [27] While digital modulations vary in complexity, they all share a common theme: instead of embedding data continuously onto the carrier wave like analogue modulation, they represent data through discrete changes (shifts, amplitude variations, or a combination of the two) in the carrier wave's characteristics that can be detected and decoded by an SDR. This concept is illustrated in the figure below.

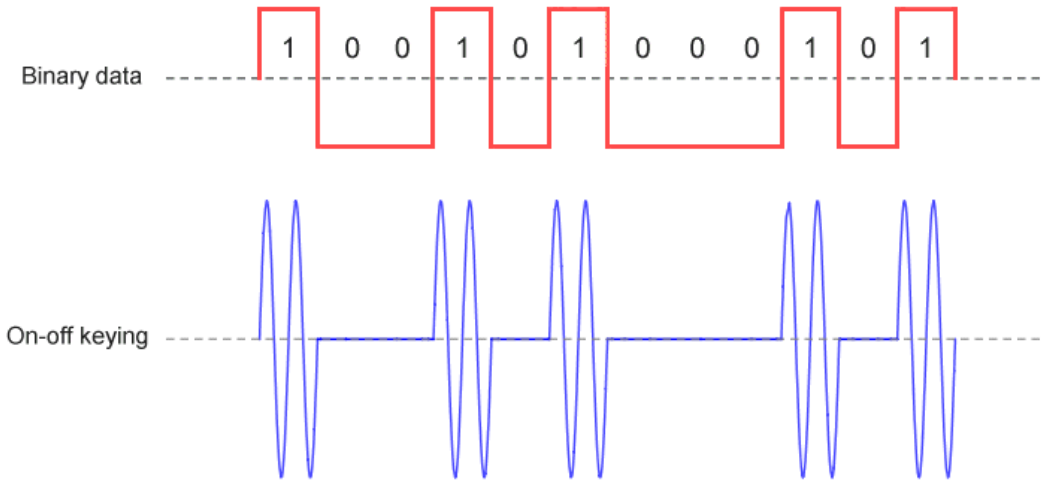

Figure 7 Digital modulation example [40]

Digital modulations often offer advantages in terms of noise immunity and the ability to transmit more complex data. However, they typically require more sophisticated demodulation techniques within an SDR environment.

The act of demodulation reveals the raw data embedded within the signal, but it is important to understand that this raw data does not always translate directly into readily understandable information. Further analysis and decoding are required to translate this data into meaningful formats. The data extracted could be simple binary sequences, standard ASCII text or more complex proprietary data structures designed for a specific device or protocol. The methods employed for data extraction depend heavily on the type of modulation and the suspected data format. For standard data types like binary or ASCII, existing tools and libraries often provide the necessary decoding functionality. Software designed for signal analysis (similar to those used for demodulation) typically includes tools for interpreting common data formats. For instance, Wireshark, a widely used network analysis tool, can effectively interpret and present captured data when it matches known protocols. However, when working with proprietary protocols, simple tools might not suffice. In such cases, custom analysis is often necessary. This might involve the use of programming languages like Python to manipulate the extracted data, search for patterns, and hypothesize about the structure of the data. This process can be time-consuming and iterative, as researchers experiment with different decoding strategies.

The ability to successfully extract and decipher the data flowing over the radio frequencies paves the way for the next crucial step in RF hacking: reverse engineering the underlying protocols. Understanding the protocols that govern the interaction between wireless devices is the key to both uncovering their functionalities and to finding potential vulnerabilities. A protocol within this context can be considered to be a set of rules and conventions that dictate the structure, sequencing, and meaning of messages exchanged between devices. Even after successfully extracting and decoding the data, reverse engineering of the protocol remains crucial for several reasons:

- **Gaining control:** Deciphering data alone only allows for passive observation, whereas reverse engineering the protocol enables the

hacker to craft custom messages that conform to the protocol, providing a level of control over the target's device's actions.

- **Developing compatibility:** Understanding a proprietary protocol is the first step towards creating compatible devices or software, even in the absence of official documentation.
- **Vulnerability discovery:** In-depth protocol analysis often reveals design flaws, insecure implementations, or hidden commands that could lead to security vulnerabilities and potential exploits.

The process of protocol reverse engineering is often methodical yet investigative. It starts with capturing multiple transmissions between wireless devices using tools like SDRs. The next step involves a careful examination of captured data, searching for patterns, recurring elements, or any structural clues within the transmissions. These observations become the basis for forming hypotheses about how the protocol functions. For example, a researcher might notice that a remote control for a garage door sends a command to open or close a door, but the command is always preceded by a specific byte sequence. They could hypothesize that this sequence serves as a header, potentially containing an identifier for the remote control or even a security code. Hypotheses about the protocol's structure are then tested, often through carefully crafted transmissions created using an SDR. By sending these transmissions to the garage door receiver and observing the responses, deductions can be confirmed or refined. This iterative proves of analysis, hypothesis formation, testing, and refinement gradually reveals the inner workings of the protocol.

The combination of modulation, data extraction and decoding, and protocol reverse engineering empowers RF hackers to not only understand the invisible communication channels, but also manipulate them. This understanding serves as the foundation for further exploration into active attack techniques, ultimately contributing to the development of more robust security measures for wireless devices.

3.4.3 Active Attacks

The previous subchapter focused on understanding the components of wireless communication, providing tools to analyze modulations, extract data, and dissect protocols. This subchapter, however, shifts focus on the active manipulation of RF systems, moving beyond passive observation. Active attacks involve the intentional targeting of wireless devices for specific purposes.

These techniques demand increased caution due to their potential for disruption. Understanding such attacks is essential for the ethical development of secure RF systems. It is crucial to execute these tactics responsibly within controlled environments and with explicit permission, respecting both legal regulations and the need to avoid unintended consequences.

This exploration of active attacks begins with the replay attack. By capturing and retransmitting legitimate signals, this technique can be used to exploit systems that rely on predictable communications. A replay attack rests on the fact that many wireless devices, especially older ones, or those prioritizing simplicity over security, may not implement robust authentication or protection against the repletion of commands. Tools like the HackRF One and the Flipper Zero are instrumental in executing replay attacks. Their ability to capture and retransmit radio signals provides the core functionality necessary. A simple example to illustrate the concept involves a remote control for a garage door opener. If this device uses a static code (one that does not change with each transmission) and lacks any form of encryption, it could be vulnerable to a replay attack. An attacker could use an SDR to record the signal transmitted when the legitimate user presses the open button. With this recording, the attacker can then use their SDR or Flipper Zero to rebroadcast the captured signal at will, effectively allowing them to open the garage door. [41]

This scenario demonstrates a basic version of a replay attack. In more complex cases, attacks might target encrypted systems where the attacker aims to elicit specific responses based on protocol manipulation rather than a direct replay of

raw data. [42]

Vulnerabilities susceptible to replay attacks are often rooted in the lack of the following:

- **Rolling codes:** Systems that employ codes that change with each use, offering protection against simple replay, as depicted in Figure 8.
- **Encryption:** Encryption obscured the content of the signal, preventing the raw data from being replayed successfully.
- **Timestamping:** Incorporating timestamps into transmission can help devices identify and reject old, replayed commands.

Figure 8 Visualization of the difference between static (left) and rolling (right) codes of key fobs [43]

A different, yet related, form of active RF manipulation focuses on jamming and interference attacks, seeking to disrupt wireless communications entirely. Jamming involves intentionally transmitting signals with the aim of overwhelming or obscuring legitimate communications within a targeted frequency range. It is helpful to distinguish between targeted jamming, which aims to disrupt a specific

channel or frequency, and wideband jamming, which attempts to degrade communication across a broader spectrum. [44]

SDRs enable the generation of jamming signals with customizable parameters. An attacker might tune their SDR to a specific frequency used by a target wireless system and then transmit either noise or a structured signal to disrupt transmissions within that channel. The consequences of jamming can be significant, ranging from temporary service disruption to the complete denial of communication between wireless devices.

Regulations surrounding jamming activities are stringent in most jurisdictions due to the potential for widespread disruption. Jamming can interfere with critical communications systems, including emergency services or aviation channels. For this reason, it is essential to highlight the ethical implications of jamming attacks, stressing the need for responsible use confined to controlled testing environments.

Protocol-specific attacks represent another key category of active RF manipulation strategies, often requiring a deeper understanding of wireless protocols. These attacks leverage the knowledge gained through the type of protocol reverse engineering techniques discussed in the previous chapter. By identifying weaknesses or vulnerabilities in a specific protocol’s authentication mechanisms, encryption, or message structure, an attacker can craft custom transmissions to manipulate the behaviour of wireless devices. [45]

The execution of protocol-specific attacks can vary in complexity. Here are some examples to illustrate potential scenarios:

- **Exploiting weaknesses in RFID/NFC systems:** Tools like the Flipper Zero, with their RFID and NFC capabilities, can sometimes be used to compromise systems with poor authentication or outdated encryption protocols.

- **Fuzzing wireless protocols:** The process of “fuzzing” involves sending intentionally malformed or random data within a specific protocol to identify unexpected or exploitable behaviour in the target device.
- **Attacks on IoT protocols:** Low-power wireless protocols used in the vast network of IoT devices (such as Zigbee, or LoRaWAN) can be targeted through protocol-specific exploits discovered through research and analysis.

These examples highlight the ongoing need to prioritize security throughout all stages of RF device and protocol development. It is a reminder that even as wireless solutions evolve, the potential for attacks persists, making continuous vulnerability assessment and the implementation of mitigation strategies essential. To address these threats, the next section discusses defensive countermeasures designed to mitigate the risk of active attacks.

3.4.4 Securing Wireless Devices

As demonstrated throughout this exploration of RF hacking methodologies, wireless devices are susceptible to a range of attacks, including replay attacks, jamming, and protocol-specific exploits. From simple garage door openers to systems controlling critical infrastructure, the growing reliance on RF technology underscores the paramount importance of robust security measures. The concepts of cryptography, authentication, and secure protocol design form the cornerstones of proactive defence.

Encryption stands as the first line of defence, transforming readable data into seemingly random ciphertext. Strong encryption algorithms are vital, balancing security with the computational overhead they introduce, particularly in resource-constrained devices. Authentication mechanisms verify the identity of devices before they communicate, preventing impersonation and unauthorized access. Crucially, secure key management is needed for encryption and authentication. This includes protected storage of keys, robust distribution methods, and a

process for periodic key rotation to minimize the impact of potential compromises. Additionally, protocols themselves must be designed with resilience in mind. The ability to gracefully handle unexpected or malformed inputs lessens the likelihood of crashes or exploitable behaviour uncovered through fuzzing attacks. [5]

Beyond preventative design, ongoing vigilance is crucial. Intrusion detection systems designed for RF environments can monitor for anomalous activity indicative of attacks. Spectrum analyzers play a vital role in detecting unauthorized transmissions or the presence of jamming signals. The discovery of vulnerabilities underscores the importance of firmware updates. These updates often patch weaknesses, closing avenues of exploitation. Even with robust technical safeguards, physical security should not be overlooked. Limiting physical access to sensitive RF devices adds another layer of protection. [5]

It is important to recognize that security is an ongoing process rather than a static state. As attackers find new methods and technologies evolve, continuous assessment, adaptation, and re-evaluation of security practices are essential. Ethical hacking plays a crucial role in this process. By understanding the techniques and thought processes of malicious actors, vulnerabilities can be proactively identified and mitigated. Through a combination of secure design, defensive tools, and a commitment to vigilance, the risks inherent in wireless communication can be managed, paving the way for a more secure and resilient wireless future. [33]

4 HackRF One Lab Design

HackRF One, a remarkably versatile SDR peripheral developed by Great Scott Gadgets, is a transceiver capable of sending and receiving signals across a wide frequency spectrum. It provides a platform for exploration, analysis, and manipulation of wireless technologies. This chapter details the development of hands-on labs centred on the HackRF One, designed to equip students with technical skills in RF hacking while upholding the principles of ethical conduct.

The PortaPack module is an add-on that attaches to the HackRF One device and augments the system with a touchscreen interface and allows it to function independently of SDR software, at least to a certain extent. While the PortaPack is very practical in providing a portable device with a user-friendly interface, SDR software is still required for tasks that require more advanced signal processing capabilities.

Before discussing the development process of the lab, it is important to get familliar with its hardware and interface. The figure below gives an overview of the external part of the hardware and a brief explanation of their functionalities.

4.1 Functionality and Technical Capabilities

The HackRF One offer a suite of core functions essential for exploring the world of wireless communications. Firstly, it acts as a wideband radio receiver, capable of intercepting signals across a vast frequency range spanning from 1MHz to 6GHz. This enables students to analyze diverse wireless protocols used in various consumer, commercial, and industrial applications. Secondly, the device’s transmission capabilities allow it to generate and transmit radio signals. This transmission capability is crucial replicating wireless signals, testing the resilience of devices, and – under strict ethical guidelines – executing controlled attack scenarios.

The PortaPack add-on augments the HackRF One’s capabilities in numerous ways. Its touchscreen interface, built-in controls, and battery power streamline field operations and provide basic signal reception and replay functionality without the need for a connected computer. Additionally, the PortaPack includes some signal visualization tools, which can be helpful for identifying signal patterns and activities. However, for true spectrum analysis with features like frequency sweeping and detailed measurements, the HackRF One would still need to be connected to a computer with dedicated SDR software.

4.2 Lab development

The RF hacking lab is designed with a progressive structure, guiding students from foundational concepts to more advanced RF manipulation techniques. It begins with a comprehensive introduction to the HackRF One and Flipper Zero, including setup and configuration instructions. The lab then goes into wireless signal fundamentals, covering RF properties, modulation schemes, and the principles behind common wireless protocols. This lays the groundwork for understanding how radio signals work and how wireless devices communicate.

Building upon this foundation, students can explore RF analysis techniques, learning to capture, analyze, and decode various wireless transmissions. A specific focus is placed on Automatic Dependent Surveillance-Broadcast (ADS-B), where students intercept and decode real-time flight data, comparing it with online flight trackers to deepen their understanding of wireless protocol structures.

The lab also incorporates active RF experimentation, with an emphasis on ethical considerations. Students learn signal replay and manipulation techniques, focusing on a 433 MHz key fob system. Both the HackRF One PortaPack and the Flipper Zero are used, allowing students to directly compare the devices' functionalities, strengths, weaknesses, and ease of use in RF hacking scenarios.

Throughout the lab, students are required to produce detailed reports documenting their findings, analyses, reflections, and answers to specific questions. Visual evidence, such as screenshots and other relevant images, further substantiates their results. A dedicated device comparison report allows students to critically evaluate the suitability of the HackRF One and Flipper Zero for various real-world RF tasks, drawing from their hands-on lab experiences.

4.3 Implementation

To successfully complete this lab, students are required the following devices: a HackRF One + PortaPack, and a Flipper Zero. Additionally, students need an SDR application suitable for their operating system and either the qFlipper or Flipper Mobile App for managing the Flipper Zero. A telescopic antenna can be utilized for all the HackRF One based exercises, however other antennas are also available for use or experimentation.

Importantly, the HackRF One PortaPack was updated to its latest firmware (nightly Mayhem update) to ensure optimal functionality and compatibility with the lab exercises. A microSD card is essential for the PortaPack, as it enables the saving of captured signal data for replay attacks and houses necessary data files for ADS-B reception (i.e., *airlines.db*, *icao24.db*, and *world_map.jpg*). These files may need to be added to the SD card separately, as they can be obtained from the Mayhem GitHub repository.

The lab consists of a series of hands-on exercises designed to provide practical experience with RF analysis and manipulation. Students begin by configuring both the HackRF One (with SDR software) and the PortaPack to receive and analyze FM radio signals. This exercise focuses on identifying different radio stations and exploring the properties of the signal. Next, students use the HackRF One PortaPack to capture and decode ADS-B signals from aircraft. They extract flight data such as altitude and aircraft ID, comparing their findings against online flight trackers and discussing potential sources of discrepancies.

The lab then goes into replay attacks, where students use the HackRF One PortaPack and the Flipper Zero to record and replay signals from a 433 MHz wireless key fob, simulating the opening of a controlled device such as a garage door. An optional bonus exercise guides students through the process of pairing the Flipper Zero with the 433 MHz receiver without the need for the original key fob, demonstrating how to manually add and configure a new remote. For the full lab manual, refer to Appendix 1.

Detailed instructions for each task are provided in the lab manual, including software configuration, device setup, signal analysis steps, and visual aids such as screenshots and diagrams. A dedicated section emphasizes the crucial importance of adhering to local laws and regulations regarding RF experimentation. Students are explicitly instructed to perform replay attacks only on controlled systems, with permission, and within a safe, isolated testing environment.

4.4 Future Recommendations

The lab provides a solid foundation in RF security concepts and techniques using the HackRF One. Here are recommendations for further enhancements and expansions:

- **Exploration of Additional Protocols:** the lab can be expanded to analyze other wireless protocols commonly used in consumer and industrial applications, such as WiFi, Bluetooth, or Zigbee.
- **Advanced RF Manipulation:** more complex RF manipulation techniques can be introduced, including signal jamming (within a controlled environment), creating custom signal modulation schemes, or fuzzing wireless protocols to discover vulnerabilities.
- **Hardware Add-ons:** additional hardware could enhance the lab experience, such as RF signal amplifiers or logic analyzers to examine digital components of wireless devices.
- **Tool development:** students with software development skills can be encouraged to create custom scripts or tools to automate common RF analysis tasks or extend the functionality of the HackRF One and Flipper Zero.

All future experimentation should adhere to strict ethical guidelines and local regulations surrounding wireless communications. Students should always obtain permission before interacting with systems they do not own and operate within safe and legal boundaries.

5 Flipper Zero Lab Design

Building on the HackRF One's broad-spectrum analysis capabilities, this chapter introduces the Flipper Zero. Its focus on the sub-GHz frequency range enables exploration of wireless protocols commonly used in access control systems, garage doors, car key fobs, and other devices communicating below 1 GHz. Students can analyze and interact with these systems, broadening their RF security understanding.

5.1 Tool Setup and Configuration

Before discussing the Flipper Zero-based labs, it is important to consider firmware selection and device configuration. These choices significantly impact the device's functionality and adherence to legal and ethical guidelines within RF security experimentation.

The standard Flipper Zero firmware offers a solid foundation, but custom firmware options like Unleashed and Xtreme provide extended capabilities. For this lab, Xtreme firmware was chosen due to its wider range of supported protocols and features, despite potential stability trade-offs compared to Unleashed or the default firmware. Certain firmware functionality, however, may have legal restrictions in different jurisdictions, emphasizing the importance of responsible use.

Within the Xtreme firmware, the menu settings were adjusted to display all available options. This customization enhances the user experience and provides access to the full range of Flipper Zero tools relevant for RF analysis and manipulation. Furthermore, the device allows for the creation of a custom sub-GHz remote. This feature allows for the configuration of a dedicated remote interface for the specific device under analysis (e.g., the garage door key fob), making interaction much more intuitive than navigating through saved signal files.

5.2 Lab Development

The purpose of the Flipper Zero was to serve as a complementary tool to the HackRF One, showcasing its strengths in the sub-GHz range.

While both Unleashed and Xtreme firmware should theoretically support these labs, Xtreme firmware was used during development for its wider feature set. The QFlipper desktop application (or the iOS/Android mobile app) is also required for device configuration, firmware management, and file management.

To ensure a successful lab, the students are provided with detailed instructions. The expected deliverables include short reports summarizing their findings and discussing the processes involved in both lab sections, as well as screenshots/videos documenting the successful replay.

The third part of the lab manual leverages the Flipper Zero's strengths in analysing and interacting with wireless devices within the sub-GHz range. Students begin by using the Flipper Zero to decode a common 433 MHz key fob signal. They can observe how the device often automatically recognizes the protocol, providing valuable insights into the signal's structure – a task that might require more in-depth analysis with the HackRF One.

Building upon this knowledge, students then execute a replay attack to open a garage door using the decoded key fob signal. The lab manual guides them through comparing the streamlined process on the Flipper Zero with the steps involved using the HackRF One PortaPack. This comparison highlights the Flipper Zero's ease of use in this specific scenario.

The lab goes further by encouraging students to explore the Flipper Zero's ability to emulate the key fob's pairing signal. Pairing typically involves an initial exchange between the key fob and the receiver where the receiver authenticates the key fob and grants it access. By capturing this initial communication sequence using the Flipper Zero, students can then analyze the data packets being exchanged. With this information, they can attempt to replicate the pairing process using the Flipper Zero itself. If successful, the Flipper Zero would be able to communicate with the receiver and potentially gain access, bypassing the need for the original key fob altogether. This advanced task demonstrates the Flipper Zero's ability to not only decode and replay signals, but also manipulate them to achieve specific goals. Refer to Appendix 1 for the lab manual.

5.3 Future Recommendations

The Flipper Zero's extensive capabilities offer numerous avenues for future lab development. Building upon the foundation of these labs, students could experiment with exploring interactions with iButtons (commonly used in access control systems), analysing and emulating NFC tags and cards, or manipulating IR remote controls. Additionally, under strict controls and with explicit permissions, labs could be designed to experiment with Bluetooth Low Energy (BLE) attacks or the disruption of wireless devices in the sub-GHz range. Such expansions would provide students with an even broader understanding of the various attack surfaces in the modern wireless landscape and the tools used to explore them. Moreover, exploring tools that specifically complement the Flipper Zero's functionality could expand its reach. Examples might include specialized RF signal analyzers for in-depth protocol investigation or logic analyzers to examine communications within digital components.

6 Comparative Analysis

Previous chapters explored the use of the HackRF One and the Flipper Zero in analysing and manipulating RF signals. Building upon this foundation, this chapter presents a direct comparison of the two devices. The analysis considers their respective strengths, weaknesses, and optimal use cases within the field of RF security. This comparative approach aims to illuminate the importance of tool selection, empowering informed decision-making when approaching RF security tasks.

6.1 Device Comparison

The HackRF One's strength lies in its role as a versatile SDR. It provides a broad-spectrum analysis window, enabling users to explore a vast range of frequencies. The flexibility of SDR allows for deep customization of signal processing and analysis techniques, making it adaptable to diverse research scenarios.

However, this versatility can also introduce a steeper learning curve, particularly for those unfamiliar with SDR principles and the intricacies of raw signal analysis.

The Flipper Zero, in contrast, thrives in its sub-GHz specialization. Automatic protocol identification and a streamlined interface dramatically simplify tasks such as decoding common wireless signals used in garage door openers, car key fobs, and other sub-GHz devices. This user-friendliness allows rapid experimentation and interaction. However, this targeted focus means the Flipper Zero may encounter limitations when faced with protocols outside its primary areas of sub-GHz or its other specifically supported functionalities.

The choice between these two devices often hinges on the trade-off between broad-spectrum analysis with greater complexity versus targeted workflows simplified interactions. This trade-off is evident when replicating a 433 MHz garage door remote signal, as is the case with the lab task. The Flipper Zero's sub-GHz specialization and support for common protocols often allow for automatic signal detection. Moreover, its user-friendly interface guides the user through capturing, saving, and replaying the necessary signal. While the HackRF One PortaPack simplifies the process compared to the raw HackRF One configuration, it still involves setting capture parameters such as the sample rate, bandwidth, and gain to optimize signal reception. Utilizing HackRF One without the PortaPack add-on for such a task would introduce further complexity.

This contrast between the two devices highlights a fundamental difference in their approaches. For deeper analysis of unknown signals, especially those outside the sub-GHz range, the HackRF One provides greater flexibility. By providing access to the raw signal characteristics, the HackRF One empowers users to investigate the intricacies of custom or proprietary wireless protocols, dissecting their modulation schemes and data encoding mechanisms.

6.2 Importance of Tool Selection

The preceding analysis highlights the importance of choosing the appropriate tool for the task when exploring the world of RF security. The HackRF One excels in its versatility due to its SDR nature. This flexibility empowers investigations across a wide range of frequencies and protocols. Conversely, the Flipper Zero shines in its targeted functionality. Its focus on sub-GHz analysis and streamlined interface makes it ideal for rapid interaction with common wireless devices.

Choosing the right tool involves several considerations:

- **Task Complexity:** For in-depth signal analysis, protocol reverse engineering, or exploration beyond common sub-GHz bands, the HackRF One's SDR capabilities provide the necessary control and adaptability.
- **User Expertise:** The Flipper Zero's simplified workflows lower the barrier to entry for RF security experimentation, particularly for those less familiar with SDR concepts.
- **Target Specificity:** If the task involves a known sub-GHz protocol supported by the Flipper Zero, its specialized interface can significantly speed up the process.
- **Device Availability:** Both cost and supply chain constraints might factor into the decision if multiple tools could potentially be suitable.

RF security practitioners benefit from a diverse toolkit. Understanding the strengths, limitations, and appropriate use cases for both general-purpose SDR solutions and specialized devices is crucial for success in this field.

6.3 Key Takeaways

The combined exploration of radio frequencies using both the HackRF One and Flipper Zero provides valuable RF security insights. The HackRF One lab introduced core concepts such as:

- **Spectrum Analysis:** Understanding how to visualize and scan different radio frequencies.
- **Signal Manipulation:** Basic techniques for capturing, potentially modifying, and retransmitting signals.
- **SDR Fundamentals:** The principles of Software Defined Radio and how it enables flexible signal analysis.

The Flipper Zero labs then build upon this knowledge by demonstrating:

- **Sub-GHz Protocol Interaction:** The ease with which common sub-GHz devices can be analyzed and controlled, highlighting the potential vulnerabilities in everyday wireless systems.
- **Streamlined Workflows:** The power of specialized interfaces in simplifying RF security tasks, lowering the barrier to entry for researchers.
- **Device-Specific Attacks:** Techniques like replay attacks and potentially pairing manipulation, which are particularly relevant to the sub-GHz domain.

These labs collectively equip students with a diverse toolkit for RF exploration. They underscore the importance of selecting the right tool for the job, whether that demands the broad analysis capabilities of an SDR solution or the targeted functionality of a specialized device like the Flipper Zero.

7 Conclusion and Recommendations

This thesis project focused on the development of practical labs for an Ethical Hacking course, utilizing the HackRF One and Flipper Zero as core tools for Radio Frequency (RF) security exploration. Building upon a foundation of RF theory, including concepts like frequency, propagation, modulation, and antennas, these labs fostered hands-on skills in signal analysis, protocol reverse engineering, and the execution of controlled active attacks. Students gained experience intercepting and decoding diverse wireless transmissions, including Automatic Dependent Surveillance-Broadcast (ADS-B) from aircraft. Exercises such as replay attacks further demonstrated the potential consequences of RF vulnerabilities.

The HackRF One, with its Software-Defined Radio (SDR) capabilities, provided a versatile platform for deep signal analysis and experimentation across a wide range of frequencies. In contrast, the Flipper Zero streamlined interactions with common sub-GHz wireless devices, illustrating the power of specialized tools for targeted RF security tasks. Throughout the labs, a strong emphasis was placed on ethical considerations and responsible experimentation within controlled environments, underscoring the importance of responsible behaviour when investigating RF systems.

The labs developed in this thesis aimed to provide students with the knowledge and experience to navigate the complex landscape of RF security. Dynamic and rapidly evolving, the field of RF security offers numerous opportunities for further research and lab development. Potential avenues for curriculum expansion include:

- **Advanced RF Attacks:** The introduction of sophisticated attack techniques, such as controlled signal jamming, protocol fuzzing, and the analysis of complex wireless systems would enhance students' understanding of the potential attack vectors.

- **Defensive Countermeasures:** Incorporation of intrusion detection techniques, robust security protocols, and spectrum monitoring would provide a well-rounded approach to RF security.
- **Emerging Technologies:** Analysing cutting-edge protocols like Bluetooth Low Energy, Zigbee, and others would prepare students for emerging security challenges.
- **Community Engagement:** Fostering participation in online communities dedicated to RF exploration and security would promote knowledge sharing and collaboration, fuelling innovation within the field.

By emphasizing hands-on learning, ethical principles, and the use of both specialized and versatile tools, this thesis project has contributed to the development of the Ethical Hacking course, with a particular focus on RF hacking. The labs and lessons learned can serve as a foundation for future educational initiatives, empowering students to become responsible and skilled practitioners in this critical domain.

References

1. Koppel T. Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath: Crown; 2015.
2. Associated Press. AP News. [Online].; 2020 [cited 2024 March]. Available from: https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94.
3. United Press International. UPI. [Online].; 2022 [cited 2024 March]. Available from: https://www.upi.com/Health_News/2022/06/01/medical-devices-pacemakers-cybersecurity/7041653656330/#:~:text=Concerns%20have%20existed%20for%20quite,it%20was%20known%20as%20St.
4. Codecademy. Codecademy. [Online]. [cited 2024 March]. Available from: https://www.codecademy.com/learn/introduction-to-cybersecurity/modules/intro-cybersecurity-what-is-cybersecurity/cheatsheet.
5. Cisco Learning Network. [Online Course: Cybersecurity Essentials]. [cited 2024 March]. Available from: https://skillsforall.com/launch?id=cf383adf-262f-496f-aee7-0084d36dd60f&tab=curriculum&view=92b090ad-8809-52f7-afd3-281e65999c1e.
6. National Institute of Standards and Technology. NIST. [Online].; 2024 [cited 2024 March]. Available from: https://www.nist.gov/cyberframework.
7. ISO/IEC. ISO. [Online]. [cited 2024 March]. Available from: https://www.iso.org/standard/27001.
8. Open Worldwide Application Security Project. OWASP. [Online]. [cited 2024 March]. Available from: https://owasp.org/www-project-web-security-testing-guide/v41/3-The_OWASP_Testing_Framework/1-Penetration_Testing_Methodologies.
9. CompTIA. CompTIA. [Online]. [cited 2024 March]. Available from: https://www.comptia.org/content/articles/what-is-ethical-hacking.

10. Nmap. Nmap. [Online]. [cited 2024 March]. Available from: https://nmap.org/book/man.html.
11. Tenable Inc. Tenable. [Online].; 2024 [cited 2024 March]. Available from: https://docs.tenable.com/nessus/Content/GettingStarted.htm.
12. Greenbone OpenVAS. OpenVAS. [Online]. [cited 2024 March]. Available from: https://www.openvas.org/.
13. Metasploit. Metasploit. [Online]. [cited 2024 March]. Available from: https://www.metasploit.com/.
14. Openwall. Openwall. [Online]. [cited 2024 March]. Available from: https://www.openwall.com/john/.
15. FreeCodeCamp. FreeCodeCamp. [Online].; 2022 [cited 2024 March]. Available from: https://www.freecodecamp.org/news/how-to-use-hydra-pentesting-tutorial/.
16. Hashcat. Hashcat. [Online]. [cited 2024 March]. Available from: https://hashcat.net/hashcat/.
17. Haschat. Haschat. [Online]. [cited 2024 March]. Available from: https://hashcat.net/wiki/doku.php?id=frequently_asked_questions#how_many_gpu_can_hashcat_handle.
18. Aircrack-ng. Aircrack-ng. [Online]. [cited 2024 March]. Available from: https://www.aircrack-ng.org/.
19. Kismet. Kismet Wireless. [Online]. [cited 2024 March]. Available from: https://www.kismetwireless.net/.
20. Wulff A. Beginning Radio Communications: Radio Projects and Theory Cambridge: Standard Apress; 2019.
21. Inductiveload. [Digital picture].; 2007 [cited 2024 April]. Available from: https://upload.wikimedia.org/wikipedia/commons/c/cf/EM_Spectrum_Properties_edit.svg.
22. Silver HW. Ham Radio For Dummies. 4th ed. Hoboken: John Wiley & Sons Inc.; 2021.

23. Cadence PCB Solutions. Cadence. [Online]. [cited 2024 April]. Available from: https://resources.pcb.cadence.com/blog/2022-an-overview-of-frequency-bands-and-their-applications.
24. Time Inc. [Google Image].; 2008 [cited 2024 April]. Available from: https://images.google.com/hosted/life/4a204d82f07524bd.html.
25. Donat W. Explore Software Defined Radio: Pragmatic Bookshelf; 2021.
26. Vinod Joseph SM. Network Convergence: Ethernet Applications and Next Generation Packet Transport Architectures: Elsevier Inc.; 2014.
27. Les Besser RG. Practical RF Circuit Design for Modern Wireless Systems: Passive Circuits and Systems: Artech House; 2002.
28. Great Scott Gadgets. Great Scott Gadgets. [Online]. [cited 2024 March]. Available from: https://greatscottgadgets.com/hackrf/one/.
29. Lime Microsystems. Lime Micro. [Online]. [cited 2024 March]. Available from: https://limemicro.com/products/boards/limesdr/.
30. Nuand. Nuand. [Online]. [cited 2024 March. Available from: https://www.nuand.com/bladerf-1/.
31. Lyons RG. Understanding Digital Signal Processing. 3rd ed.: Pearson; 2010.
32. GNU Radio. GNU Radio. [Online].; 2024 [cited 2024 April]. Available from: https://www.gnuradio.org/about/.
33. Davies G. Networking Fundamentals: Packt Publishing; 2019.
34. Flipper Zero. Flipper Zero. [Online]. [cited 2024 April]. Available from: https://flipperzero.one/.
35. Proxmark. Proxmark. [Online]. [cited 2024 April]. Available from: https://proxmark.com/proxmark-3-hardware/proxmark-3-evo.
36. ProxGrind. Chameleon Tiny. [Online]. [cited 2024 April]. Available from: https://chameleontiny.com/.
37. Pohl J. MajorGeeks. [Online].; 2024 [cited 2024 April]. Available from: https://www.majorgeeks.com/files/details/universal_radio_hacker.html.

38. TAIT Radio Academy. TAIT Radio Academy. [Online]. [cited 2024 April]. Available from: https://www.taitradioacademy.com/topic/how-does-modulation-work-1-1/.
39. National Instruments. NI. [Online].; 2023 [cited 2024 April]. Available from: https://www.ni.com/docs/en-US/bundle/pxi-pxie-5650-5651-5652-features/page/ook.html#:~:text=OOK%20is%20a%20modulation%20scheme,defined%20bit%2Dstream%20or%20PRBS.
40. Technology UK. Technology UK. [Online]. [cited 2024 April]. Available from: https://www.technologyuk.net/telecommunications/telecom-principles/digital-modulation-part-one.shtml.
41. Thompson KM. Bauen Solutions. [Online]. [cited 2024 March]. Available from: https://bauensolutions.com/2020/10/15/the-invisible-threat-rf-based-attacks/.
42. Olha Mykhaylova ASTNTFVS. Resistance to Replay Attacks of Remote Control Protocols. Kyiv: Cybersecurity Providing in Information and Telecommunication Systems; 2024.
43. Pavel Zhovner AZRN. Flipper Blog. [Online].; 2024 [cited 2024 April]. Available from: https://blog.flipper.net/response-to-canadian-government/.
44. Krutitsky E. ResearchGate. [Online].; 2022 [cited 2024 April]. Available from: https://www.researchgate.net/publication/359700399_Cybersecurity_-_Introduction_to_Jamming.
45. Allen Harper, Ryan Linn et al. Gray Hat Hacking: The Ethical Hacker's Handbook. 6th ed.: McGraw-Hill; 2022.
46. Wolford B. GDPR.eu. [Online]. [cited 2024 April]. Available from: https://gdpr.eu/what-is-gdpr/.

Exploring Wireless Communications

This lab is designed to provide you with a foundational understanding of radio frequencies and how wireless communication works, using the versatile capabilities of the HackRF One. Additionally, you will also have the opportunity to use Flipper Zero, in order to compare the functionalities of the two devices. They're both powerful tools that allow users to send and receive radio signals across a wide range of frequencies. In this lab, you'll first have the opportunity to familiarize yourself with radio signals with a relatively simple exercise. As you progress through it, you will explore more advanced aspects of RF hacking.

> **Note**: Remember the importance of responsible and ethical use of RF technology. Always adhere to local laws and regulations and respect the privacy and security of wireless communications.

Setting up your HackRF One and SDR

HackRF One operates as a transceiver, meaning it can both send and receive radio signals ranging from 1MHz to 6GHz. The PortaPack module is an add-on that attaches to the HackRF One device and augments the system with a touchscreen interface, which allows it to function independently of SDR software, at least to a certain extent. While the PortaPack is very practical in providing a portable device with a user-friendly interface, SDR software is still required for tasks that require more advanced signal processing capabilities.

Before working with the HackRF One PortaPack device, it is important to familiarize yourself with its hardware and interface. The figure below gives an overview of the external part of the hardware and a brief explanation of their functionalities.

Figure 9 External hardware

Figure 2 User interface

1. Antenna Connector: Allows for the connection of different types of antennas to receive and transmit signals over various frequency ranges.
2. Rx/Tx LEDs: Indicators for receive (Rx) and transmit (Tx) operations. Only one will light up at a time due to the half-duplex nature of the device.
3. Other Status LEDs: Indicators for the 1.8V power rail, RF power, and USB connectivity.
4. DFU Mode Button: Used to put the device into Device Firmware Upgrade mode for firmware updates.
5. 3.3V Rail Status LED: Indicates the status of the 3.3V power supply rail.
6. Reset Button: Used to reset the HackRF One.
7. Encoder Thumb Wheel: A navigation tool to scroll through options. Pressing the wheel acts as a center push button.
8. Directional Push Buttons: For navigating the menu and selections, with an Enter/ON/OFF button in the center.
9. CLKIN: Input for an external clock source to synchronize the HackRF One to other equipment.
10. CLKOUT: Output to provide a clock signal from the HackRF One to external devices.
11. MicroUSB Port: For connecting the HackRF One to a computer or power source.
12. Headset/Mic Jack: For connecting a headset or external microphone for audio-based applications.

Pressing the wheel turns the device on; pressing it twice turns it off. Once the device is turned on, the *Main Menu* will be visible on the screen. This menu allows you to access the various functions of the PortaPack firmware.

While the PortaPack add-on allows for HackRF operations without an SDR application, it is important to also know how to operate HackRF One without the PortaPack's user interface. For that, you need to install an SDR application on your computer. There are many options available for download online (e.g., SDR#, SDR++, GRC…), each catering to different levels of expertise, operating systems, and other specific requirements. Select one that's suitable for you and install it before getting started with the lab.

Setting up your Flipper Zero

In some ways similar to the HackRF One, the Flipper Zero is a versatile multi-tool built for exploring and interacting with various RF systems. It can analyze, capture, and replay signals across a wide range of frequencies commonly used for garage doors, gates, car key fobs, and access control systems. Unlike HackRF One, Flipper Zero also works with near-field communication (NFC), low-frequency/high-frequency radio-frequency identification (RFID) tags and cards, allowing for tag interactions such as reading, emulation, and manipulation. It can also capture, store, and transmit infrared (IR) codes, enabling control of TVs, air conditioners, and other IR-enabled devices. It excels in wireless device interaction in the sub-GHz range, making it suitable for doorbells, weather sensors, and other smart home technologies. Beyond its core functions, the Flipper Zero includes tools for working with iButtons, BadUSB payloads, and even has some simple built-in games for moments of downtime.

Before diving into the practical exercises, it is important to become acquainted with the Flipper Zero's hardware and user interface; it has a compact, portable design, making it highly convenient for field use.

Its main hardware components consist of the Display, Directional Pad, GPIO pins, and a microSD card slot.

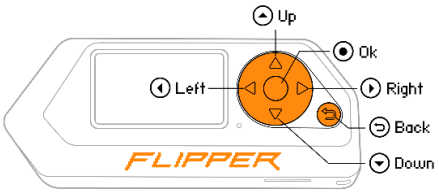

Figure 3 Controls

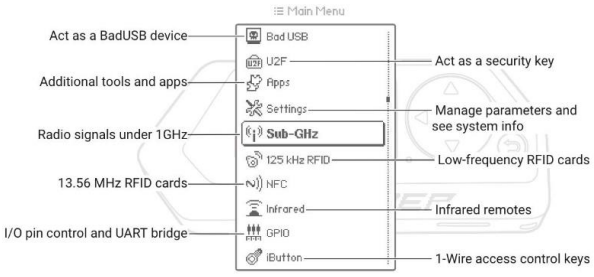

Figure 4 Main Menu

Pressing and holding the *Back* button turns the device on and off (you can only turn off the device from the *Desktop* view). Once the device is on, the *Desktop* view shows the time and battery percentage of the device. To go to the *Main Menu*, press the OK button, which allows you to access the various functions of Flipper Zero. Moreover, you can customize the Left and Right buttons to offer a shortcut to a particular function. Refer to figure below for more information.

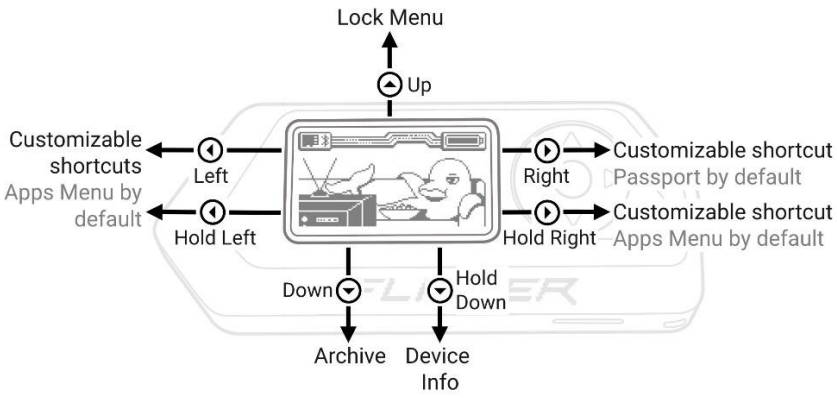

Figure 5 Button controls from Desktop view

Note: The figures above depict the original (default) firmware of Flipper Zero. For the purposes of this lab, the firmware of your device has been changed to Xtreme (version *XFW-0053_02022024*). You may want to update the firmware (you can check the latest update on their GitHub), or even switch to a different one, however Xtreme or Unleashed are recommended, since these add some extra functionality to the device.

In order to get the most out of Flipper Zero, it is recommended to install its supplementary app, either on your computer (*qFlipper*) or on your iOS/Android phone (*Flipper Mobile App*). These applications allow the user to update the device's firmware and databases, manage files on the microSD card, repair corrupted firmware, and even control the device remotely.

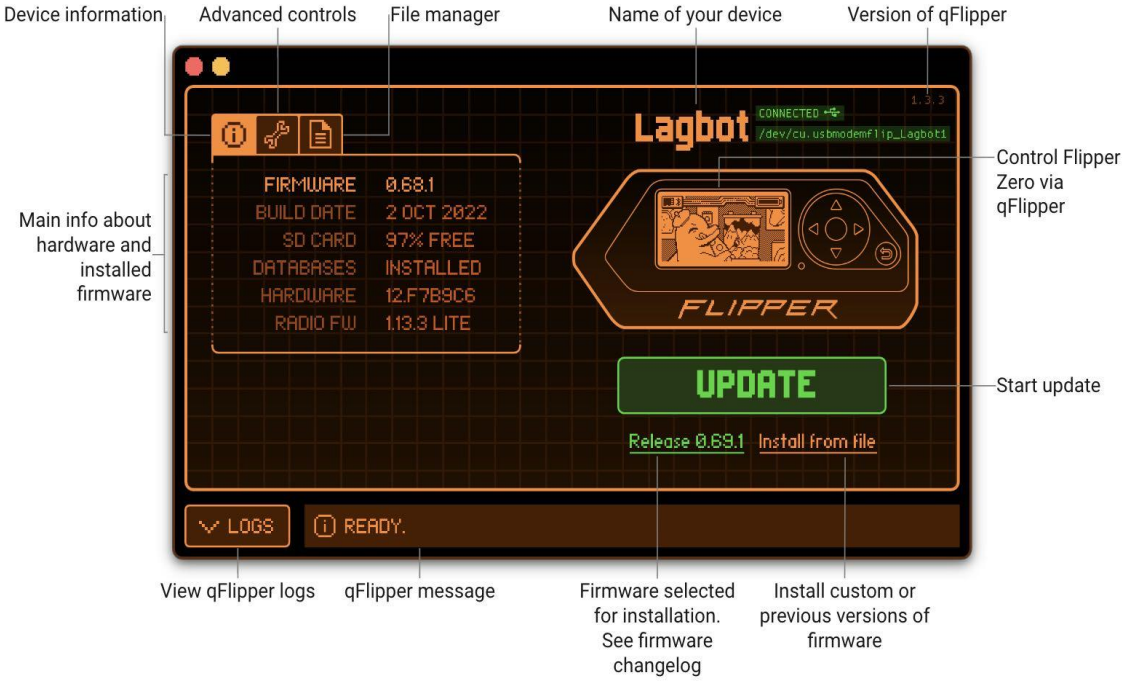

Figure 6 qFlipper interface

The *qFlipper* application can be downloaded from the Flipper Zero website. Moreover, the website has extensive documentation regarding the device as well as the supplementary applications, which you can refer to throughout the lab assignments if you need additional information.

Part I: Basic Signal Receiver (1p)

Objective: Learn to set up and use HackRF One to analyze common RF-signals.

Setup for HackRF One (SDR Mode):

1. Connect the device to the computer using a USB cable

> **Note:** If using a HackRF One PortaPack device, put your device in HackRF One mode by toggling to "HackRF" on the main screen. Now the device can be set up using the SDR.

2. Attach the appropriate antenna to the to the antenna port (labeled "ANT")
3. Open the SDR software on your computer and select HackRF One as the input device
4. Adjust the gain to optimize signal clarity and set the sample rate to define how frequently the signal is sampled
5. Tune into the FM radio band (88 – 108 MHz) and press *Play* to start receiving

Setup for PortaPack:

1. Turn on device and go to Receive
2. Go to Audio and toggle to WFM
3. Set an appropriate bandwidth and scan through the frequencies to tune into various local radio channels[5]

Task: Write a short report (of up to 300 words) describing the process:

- Discuss the differences between capturing signals using SDR software in HackRF One mode and utilizing the PortaPack UI for the same purpose.
- List some of the radio channels you were able to tune into.
- Feel free to add any other information that you found relevant to the report

---

Part II: ADS-B (2p)

Objective: Capture and analyze Automatic Dependent Surveillance-Broadcast (ADS-B) signals from aircraft.

Setup:

1. Connect to the HackRF One PortaPack an antenna that can receive ADS-B signals[6]
2. Toggle to the *ADS-B Receiver*
3. Tune into the frequency for ADS-B.

---

[5] The Finnish Transport and Communication Agency maintains a list of Finnish radio channels and their frequencies.
[6] Look up the appropriate frequency for capturing ADS-B signals.

Task: Write a short report (of up to 400 words) describing the process:

- List the flights you were able to capture information about and explain what data you gathered about them (e.g., altitude, aircraft ID etc.).
- Compare this data with real-time information available on online flight tracking platforms for the same flight.
- Report on any anomalies or discrepancies found between the ADS-B captured data and the online tracking information. Discuss potential reasons for anomalies if any are detected.
- Provide a screenshot displaying the map overview of flights as seen on the HackRF One PortaPack interface, along with a screenshot showcasing specific flight data such as altitude, speed, and aircraft ID, as examples of the information being tracked.
- Feel free to add any other information that you found relevant to the report

---

Part III: Replay attack with 433Mhz key fob

Objective: Unlock the garage door using HackRF One PortaPack and Flipper Zero instead of key fobs

Setup for HackRF One PortaPack (2p):

1. Pair the key fob to the receiver (if it isn't already paired) following the instructions in the documentation[7]
2. Insert a mini-SD card into the HackRF One PortaPack if it doesn't have one
3. Attach an appropriate antenna to the device
4. Navigate to *Record* and tune into the frequency specified in the documentation.
5. After pressing *REC*, press the key fob button to transmit the signal to the receiver, then press *REC* again to stop recording
6. Repeat the process for both buttons A and B
7. Now that your signals are stored on the device (i.e., the SD card), replay the signal to unlock the garage using only the HackRF One PortaPack transmission

Setup for Flipper Zero (2p):

1. Assuming that the receiver has already been paired with the key fob, navigate to *SubGHz/Read/Config*
2. Set the appropriate frequency for the Flipper Zero to read.
3. Press Read to capture the signal (the protocol name will be listed)
4. Click on the signal to see more information.
5. Press Save and name the signal
6. Repeat the process for both buttons A and B
7. Now that your signals are saved, replay the signal to unlock the garage using only the Flipper Zero

---

[7] To find the receiver's documentation, search for "*Qiachip KR2402A DC6-30V 2 Channel Receiver*"

Bonus (3p):

1. Reset the receiver following the instructions in the documentation, so no key fobs are paired to it (you can test that the key fobs have been unpaired by pressing the buttons after resetting the receiver; it should ignore the button presses)
2. Pair the receiver without using the key fob but using only the Flipper Zero's *Add Manually* function from the *SubGHz* menu
3. Read the receiver's documentation to find out how to pair a new key fob (for both *Momentary* and *Toggle* mode)
4. On the Flipper Zero, navigate to *SubGHz/Add Manually* to bypass the need for a key fob and select the appropriate protocol[8] when prompted
5. Pair the receiver (following the instructions on the receiver's documentation) to Flipper Zero without the use of the key fob.

Task: Write a report (of up to 500 words) to describe the process.

For the HackRF One PortaPack part:

- Provide a screenshot (using PortaPack's functionality) of the HackRF One PortaPack interface while the Replay attack is in progress

For the Flipper Zero part:

- Provide a screenshot (using *qFlipper* or the *Flipper Mobile App*) of the saved signal information
- If you completed the **Bonus** part, explain how you did it in detail and the results it yielded

Finally, discuss the differences between the two devices in your experience:

- Which device had a more user-friendly interface?
- Did any device offer more advanced functions or flexibility?
- Which device did you prefer for this type of task and why?
- Feel free to add any other information that you found relevant to the report.

Note: Most modern key fobs (e.g., car key fobs) do not allow for replay attacks as they have what's called "rolling code", meaning the code transmitted in the signal will change every time the button is pressed. However, in our case, we have basic/fixed signals, meaning the code will be the same once the button has been paired with the receiver, and can thus be easily replicated by any Rx/Tx device.

[8] Hint: It was listed when you captured the key fob signal with the Flipper Zero.