Radboud University Nijmegen

Faculty of Science

A Comprehensive Taxonomy of Wi-Fi Attacks

Master Thesis Cyber Security

Author:
Mark Vink
contact@markvink.com

Internal supervisor:
Dr.ir. Erik Poll
erikpoll@cs.ru.nl

External supervisor:
ing. Alex Verbiest
alex.verbiest@capgemini.com

October 2020

Abstract

Nowadays, Wi-Fi networks are commonly available everywhere, and we rely on Wi-Fi to maintain our productivity. Security protocols such as WEP, WPA, WPA2, and WPA3 make wireless networking more secure by providing authentication mechanisms and ensuring the transmitted data's confidentiality and integrity. Many papers have been published covering these security protocols' strengths and weaknesses, and researchers have found ways to exploit them. Our paper aims to provide an overview of the available research and create an in-depth taxonomy of attacks against Wi-Fi networks.

We started by defining the attack types covered in our taxonomy, namely; Man-in-the-Middle attacks, Key-recovery attacks, Traffic Decryption attacks, and Denial of Service attacks. While working on the taxonomy, we reconsidered the attack types a few times as we tried to fit in all attacks. We identified features that can be used to characterize and group Wi-Fi attacks, namely; the targeted security protocol, including the security mode, such as WPA-Personal. We examined whether the adversary interacts with network components, such as client devices. We also looked at whether tooling is available for the pentester. After this, we gathered information on around 30 different Wi-Fi attacks from research papers. We described the working of these attacks in our taxonomy, along with their countermeasures and available tooling.

We concluded that Evil Twin attacks and their variations are versatile, as an adversary can launch them against almost any network and security configuration. An adversary can use this kind of attack with a different goal, such as eavesdropping on traffic or collecting (Enterprise) credentials. Enterprise networks often deal with various client devices, and the adversary has to trick only one device to connect with their malicious network. For conclusions about all attack types, we refer to our taxonomy.

In the second part of our paper, we go over the gathered information on Wi-Fi attacks from a security professional's viewpoint, equipped with the task of auditing the security of a Wi-Fi network. We focused our guide on how to recover credentials and how to associate with the target network. We provide step-by-step flowcharts for the different security protocols that recommend attacks based on their effectiveness.

Furthermore, we discuss some of the most popular Wi-Fi auditing tools and their adoption of attacks. We can conclude that there is a lack of support for auditing WPA3 networks. None of the tools has full and official support. It would be especially interesting for tools that can launch Evil Twin attacks to adopt support, as cracking the exchanged handshakes is no longer feasible.

Contents

1 Introduction

Over the last two decades, Wi-Fi has played an integral role in keeping us connected at our homes, businesses, and public places. Nowadays, wireless networks are commonly available everywhere, and we rely on Wi-Fi to maintain our productivity. Various security protocols have been developed to protect Wi-Fi networks, including WEP, WPA, WPA2, and WPA3. These protocols make wireless networking more secure by providing authentication mechanisms and ensuring the data's confidentiality and integrity. Researchers have published various papers about the strengths and weaknesses of said protocols and discovered ways to exploit them.

Problem Statement

There is a lot of research available on individual Wi-Fi attacks or a group of similar vulnerabilities. However, to our knowledge, there is no paper with the goal of creating an in-depth overview of Wi-Fi attacks.

This paper aims to provide an overview of the available research and create an in-depth taxonomy of attacks against Wi-Fi networks. From the viewpoint of a security professional, we will be looking at what kind of attacks pose a threat to Wi-Fi networks, given the way it is protected. We describe the working of these attacks in our taxonomy, along with their countermeasures and available tooling. In the second part of our paper, we guide the pentester on exploiting a Wi-Fi network using the information gathered in the taxonomy. We compare some of the most popular Wi-Fi auditing tools and discuss their current state of support for auditing WPA3 networks.

Thesis Outline

In chapter 2. Background, we start by giving a background on how wireless networks work and their security requirements. We introduce security protocols that network administrators can use to protect their network. Within some of the security protocols, we can differentiate between Personal and Enterprise modes. In chapter 3. Taxonomy of Wi-Fi Attacks, we start by creating a list of types of Wi-Fi attacks and features that describe them. The types that we include in our taxonomy are Man-in-the-Middle attacks, Key Recovery attacks, Traffic Decryption attacks, and Denial of Service attacks. The features are used to group and compare the attacks within the taxonomy. Then we proceed with creating an overview of attacks against Wi-Fi networks, including countermeasures and references to tools to use by security professionals.

In chapter 4. Wi-Fi Pentester Framework, we go over the gathered information on Wi-Fi attacks from a security professional's viewpoint. We provide an overview of applicable attacks for different security protocols. Furthermore, we discuss the most popular Wi-Fi auditing tools and their adoption of attacks. In chapter 5. Future work, we discuss future work based on our findings. And in chapter 6. Conclusion, we discuss the process of writing our paper and list our conclusions.

2 Background

This chapter aims to provide background information to gain a better understanding of the involved technology. First, we introduce basic terminology associated with Wi-Fi networks and their security requirements (section 2.1). In section 2.1, we introduce management frames that are exchanged on a Wi-Fi network to maintain a connection between clients and access points. In section 2.3, we cover security protocols that are intended to keep Wi-Fi communications secure. Within some of the security protocols, we can differentiate between Personal and Enterprise modes (section 2.4). On top of Personal modes, an administrator may use techniques that make it easier to connect new devices with the network (section 2.5).

2.1 Wi-Fi Networks

Wi-Fi is a wireless technology, built upon the IEEE 802.11 set of standards that allows capable devices like laptops and mobile devices to create networks and exchange information without the need for actual wires. Internet connectivity occurs by connecting to a wireless router that allows the device to interface with the internet. Wi-Fi also provides access to a local network (WLAN) that allows you to send documents to a wireless printer, for example. Wireless networks offer several advantages over wired networks, such as the ease and speed of deployment of the network, and mobility and flexibility for its users [1]. Wireless devices must use a common Wi-Fi version, as defined in the IEEE 802.11 protocol standards, to be able to communicate with each other. The versions differ on the radio frequency they operate on, the available bandwidth, the maximum ranges, and other aspects.

A device within an 802.11 network is identified by its Media Access Control (MAC) address. A MAC address is a unique identifier assigned to the network adapter inside the Wi-Fi device. A collection of devices that communicate with each other within an 802.11 network is called the Basic Service Set (BSS). In infrastructure networks, the Basic Service Set Identifier (BSSID) is the MAC address used by the wireless interface of the access point. The Service Set Identifier (SSID), often referred to as the network name, is used by network administrators to assign an identifier to the network, such as "Office Network". When a Wi-Fi capable device is in range of a network, it can detect the network and attempt to connect to it. Wireless networks are vulnerable to a wide range of malicious attacks, including eavesdropping, Man-in-the-Middle (MitM), Denial of Service (DoS), spoofing, and frame injection [2].

The most critical security objectives for wireless networks are availability, authenticity, data confidentiality, and data integrity [1, 2, 3]. Availability is about ensuring the wireless network is available for authorized parties when needed. Authenticity concerns establishing trust about the identity of the involved parties. In terms of a wireless network, the objective is only to allow authorized clients to associate with the network. Data confidentiality concerns protecting data against unauthorized disclosure. In terms of a wireless network, the objective is to protect the transmitted data from eavesdropping by malicious actors, which can be achieved by using encryption. Data integrity concerns assuring that data is accurate, complete, and not altered by malicious actors during transmission. Security protocols, introduced in section 2.3, provide authentication mechanisms and protocols to ensure the confidentiality and integrity of transmitted data.

2.2 Wi-Fi Management Frames

There are three major classes of frames in 802.11 communication; management frames, control frames, and data frames. Wireless networks use several management frames to establish and maintain a connection between clients and access points, and provide roaming functionality. Control frames are used to acknowledge when data frames are received. Data frames contain the actual data that is transmitted [1, 4].

When a client connects to a wireless network, several management frames are exchanged (Figure 1) to establish the association. Broadcast and Probe Request/frames are used to make devices aware of the Wi-Fi network's availability. When the device is aware of the network, it first sends an Authentication Request. This frame was used to authenticate with WEP networks, however, it still exists to provide compatibility. On WPA and WPA2 networks, the actual authentication is optional taking place after association.

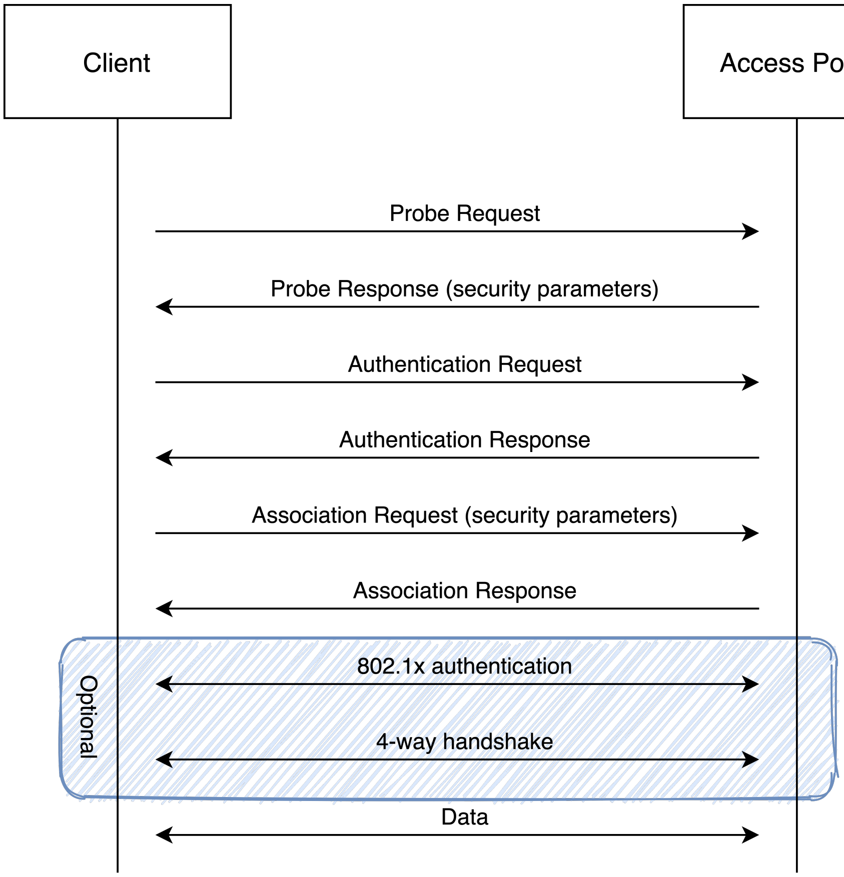

Figure 1: Wi-Fi connection phases

This section introduces the essential management frames, as they are important during the connection establishment. Some attacks we discuss later on rely on spoofing certain management frames.

Beacon

Bacon frames are broadcasted by the access point to announce the network's presence to nearby Wi-Fi-capable devices. They are transmitted at regular intervals and contain information about the network's capabilities and configuration, such as encryption details. When a device receives a Beacon frame, it can provide a list of nearby networks sorted by signal strength, allowing the user to choose the most optimal network to associate with.

Probe Request and Probe Response

Probe Requests are frames sent by a client to request information from either a specific network or all access points in the area. The broadcast destination address 'ff:ff:ff:ff:ff:ff' is used when the client is looking to receive responses from all nearby networks. The difference is that using Probe Requests to request information of nearby networks is considered an active scan, while only listening for Beacon frames is considered a passive scan.

The frame contains two fields; the SSID of the network the client is looking for and the rates that are supported by the client. Once the client sends the Probe Request, it waits for responses for a limited amount of time. If the client does not receive any answers, it moves to the next channel and repeats the discovery process.

Access Points that receive a Probe Request use the information in the frame to determine whether the client can join the network based on the SSID and the supported data rates. If the client is deemed to be compatible, the access point responds with a Probe Response containing the same information as a Beacon frame.

Authentication Request and Authentication Response

After receiving Probe Responses, a client may attempt to authenticate with a compatible network, for example, based on its security parameters. Originally, 802.11 authentication frames were designed for the WEP security protocol, which is proven to be insecure and therefore labeled as deprecated. On modern networks, using one of the WPA variations, the actual authentication may happen after the association phase.

Association Request and Association Response

After the client has determined which access point it wants to associate with, it sends an Association Request to that access point. The frame includes the chosen encryption types, if required. If the request matches the access point's capabilities, it responds with an Association Response stating it was successful.

Disassociation and Deauthentication

When a client wants to disconnect from the network, it needs to send a disassociation frame to the access point. Alternatively, if it wants to end the authentication relationship, it needs to send a Deauthentication frame. Both frames contain a single field, the reason for ending the relationship.

Protected Management Frames

In 2009, the Wi-Fi Alliance amended the IEEE 802.11w standard to increase the security of management frames [5]. Protected Management Frames (PMF) is a feature that offers data confidentiality, integrity, origin authenticity, and replay protection for management frames.

It is built upon the existing security mechanism, meaning that frames sent before transmission key establishment cannot be protected. This means, for example, that Beacons and Probe Requests/Responses cannot be protected. However, it enables protection for Disassociate and Deauthenticate frames, making it harder for an adversary to deauthenticate clients from a network.

The standard specifies that the feature must be implemented for 802.11 implementations that use TKIP or CCMP (in other words, WPA and WPA2). However, not all clients will support this feature; therefore, the usage is negotiated by the client and access point. WPA3 will make this security feature mandatory [6].

2.3 Wi-Fi Security Protocols

Any capable device within range of a wireless network can intercept packets sent by the access point and other clients, or try to send packets itself. Various security protocols have been developed to protect wireless communication between clients and the access point, including the various WPA protocols. The purpose of these protocols is to provide authentication and mechanisms to ensure the confidentiality and integrity of transmitted data. In this section, we provide some background information on these protocols. We will use their abbreviations when referring to the protocols later in our paper. Table 1 provides a comparison of the most important protocol features:

- Introduction: the year in which the protocol was introduced.
- Encryption: the algorithm that is used to encrypt packets providing data confidentiality.
- Key size: the size of the encryption key used by the encryption algorithm. This size includes the Initialization Vector (IV) that might be used as extra input for the encryption algorithm.
- Integrity: the mechanism that is used to provide data integrity.
- PMF: whether the protocol has support for Protected Management Frames (introduced in section 2.2).
- FS: whether the protocol provides Forward Secrecy.
- Deprecated: the year in which the protocol was deprecated, if that is the case.

	WEP	**WPA**	**WPA2**	**WPA3**
Introduction	1997	2003	2004	2018
Security modes	WEP-Open WEP-Shared	WPA-PSK WPA-Enterprise	WPA2-PSK WPA2-Enterprise	WPA3-Personal WPA3-Enterprise
Encryption	RC4	TKIP	AES-CCMP	AES-CCMP AES-GCMP
Key size	64-bit / 128-bit	128-bit	128-bit	128-bit / 256-bit
Integrity	CRC-32	64-bit MIC	CBC-MAC	SHA-2
PMF	Not available	Available but optional	Available but optional	Required
FS	No	No	No	Yes
Deprecated	Yes (2004)	Yes (2012)	No	No

Table 1: Comparison of security protocols

Distribution of Security Protocols

When a device's wireless capability is turned on, it is continuously scanning for available Wi-Fi networks. A probe request is sent by the smartphone to request information from either a specific access point or all access points in the area. When an access point receives a probe request, it sends out a probe response, letting nearby devices know it is available.

A technique called 'Wardriving' abuses this functionality by recording details and locations of wireless networks while driving around in a vehicle. The information may be uploaded to specific websites that create statistics and digital maps of the collected data. An example of a website that collects such information on Wi-Fi networks is wigle.net. At the time of writing, they have over 630 million networks listed in their database, including the security protocol that is being used by each access point.

	Unencrypted	**Unknown**	**WEP**	**WPA**	**WPA2**	**WPA3**
2010	33.70%	15.94%	45.05%	2.83%	2.46%	0.00%
2011	27.11%	18.68%	38.65%	6.53%	8.98%	0.00%
2012	21.76%	18.00%	30.31%	10.04%	19.80%	0.00%
2013	18.51%	14.51%	24.34%	11.68%	30.92%	0.00%
2014	14.33%	14.44%	19.56%	11.64%	39.99%	0.00%
2015	10.78%	17.16%	15.23%	10.40%	46.41%	0.00%
2016	8.30%	18.96%	12.08%	9.13%	51.68%	0.00%
2017	6.47%	19.73%	9.64%	7.88%	56.42%	0.00%
2018	5.07%	19.77%	7.77%	6.78%	60.71%	0.00%
2019	4.08%	19.36%	6.42%	5.87%	64.34%	0.00%
2020	3.55%	19.16%	5.53%	5.23%	66.59%	0.00%

Table 2: Distribution of different security protocols, data collected from wigle.net

Each row of Table 2 represents the distribution of security protocols between observed networks as of the first of January. As of the beginning of 2020, 3.55% of the networks observed by wigle.net do not use any encryption, 5.53% use WEP, 5.23% use WPA, 66.59% use WPA2, and only around 20 observed networks are using WPA3. These statistics show that most of the networks are currently secured by WPA2, meaning that a vulnerability in WPA2 could lead to a higher number of potential targets than the other protocols. However, there still exist legacy systems that only support WEP or WPA.

2.3.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) was the first security protocol developed for 802.11 networks to prevent eavesdropping on wireless data transmitted between clients and access points. As the name implies, the protocol's goal was to provide an equivalent security level as wired networks. The RC4 encryption algorithm, known as a stream cipher, is used to ensure confidentiality. It was marked deprecated with the introduction of WPA2 in 2004 [7].

Stream ciphers allow an adversary to perform several statistical attacks to obtain (parts of) the key or the plaintext. Examples are the reused key attack, bit-flipping attack, and the chosen-IV attack. WEP tries to guard against these kinds of attacks by augmenting the key with the IV so that a different key is used for each packet. Initially, WEP was using 64-bit encryption (40-bit key and 24-bit initialization vector) because of export restrictions in the USA. After the limitation was lifted, it was increased to 128-bits (104-bit key and 24-bit IV) [1]. Also, to ensure integrity, WEP uses a CRC-32 checksum.

Authentication

WEP offers two methods for authenticating with the network: Open System authentication and Shared Key authentication. With the first method, the client does not provide its credentials to the access point during the authentication phase. Any client can send an authentication request containing its MAC address, and the access point will accept the client regardless of whether the client knows the WEP key or not. Using WEP Open does not mean any client can just use the network, since they still need the WEP key to decrypt the traffic from the access point.

Shared Key authentication provides an extra layer of protection, since the client and access point perform a so-called 'handshake' before the client is associated. During this so-called 'handshake', the client proves that it knows the correct WEP key before it is allowed to associate with the network. The challenge-response handshake (Figure 2) goes as follows:

1. The client starts by sending an authentication request to the access point.
2. The access point responds with a challenge.
3. The client encrypts the challenge with the WEP key and sends the result back to the access point.
4. The access point verifies the request by the client and responds with a success message.

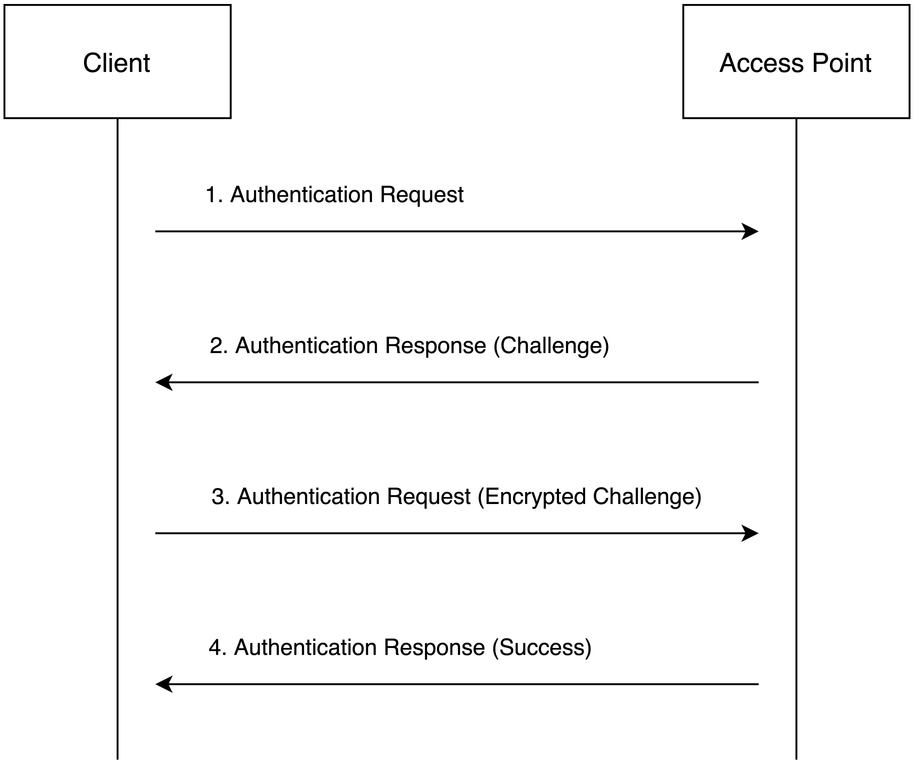
Client
Access Point
1. Authentication Request
2. Authentication Response (Challenge)
3. Authentication Request (Encrypted Challenge)
4. Authentication Response (Success)

Figure 2: Challenge-response protocol for WEP Shared Key authentication

Data integrity and confidentiality

The encryption algorithm works as follows [8, 9]: a secret key k is shared between clients of a network. When one client wants to communicate message M, it calculates the integrity checksum $c(M)$ and appends it to the message; this gives him $M.c(M)$. This combination is then encrypted using the RC4 stream cipher. The RC4 stream is generated by key k and an initialization vector (IV) v, denoted as RC4(v, k). The sender then transmits the encrypted message along with v. The receiver, who has a copy of key k, can decrypt the ciphertext by performing an XOR operation between the encrypted message and RC4(v, k).

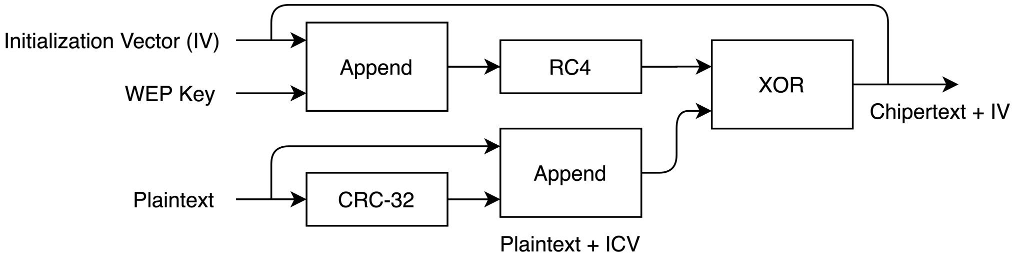

Figure 3: WEP RC4 encryption algorithm

2.3.2 Wi-Fi Protected Access (WPA)

In 2003, Wi-Fi Protected Access (WPA) was introduced, intended as a temporary measure to provide a higher level of security while awaiting the availability of the more complex WPA2 protocol. WPA could be rolled out as a firmware update on existing hardware that was designed for WEP. The main reason for WPA was to overcome some of the cryptography issues that exist in WEP. The WPA protocol was deprecated in 2012 [10].

It uses TKIP for data encryption, which generates a different key for every packet. Furthermore, it also uses a 64-bit MIC for a higher level of security to maintain integrity [3]. Most WPA protected networks use a pre-shared key (PSK), referred to as WPA-Personal, while WPA-Enterprise uses an authentication server for providing keys and certificates. Table 3 provides an overview of the keys used in WPA and WPA2 networks.

Key	**Use**	**Origin**
Pre-shared Key (PSK)	Authentication	Configured
Pairwise Master Key (PMK)	Long-term key to derive other keys	EAP negotiation
Pairwise Transient Key (PTK)	Encrypt unicast communication	Derived from PMK or PSK
Group Transient Key (GTK)	Encrypt multicast communication	Derived from PMK or PSK

Table 3: WPA/WPA2 key management

Authentication

802.11i-2004 is an amendment to the 802.11 standards to offer two new mechanisms: the four-way handshake and the group key handshake, replacing the broken WEP protocol. WPA implemented a subset of this amendment while still using the RC4 stream cipher. While WPA2 is referred to as the full implementation of 802.11i-2004, using the AES cipher.

The 4-way handshake (Figure 4) is a mechanism that allows the client and access point to prove to each other that they both know the PMK without sending the key. The PMK is constructed using the PBKDF2 algorithm with the passphrase as the key, and the SSID as the salt. After that, the previous HMAC output is used as input until 4096 rounds is reached. The passphrase can be a pre-shared key on a WPA-Personal network or the output of 802.1x authentication on a WPA-Enterprise. Furthermore, the 4-way handshake negotiates a fresh session key (Pairwise Transient Key), and installs the encryption and integrity keys.

1. The access point starts by sending a nonce (ANonce) to the client and a replay counter. A nonce is a random or semi-random number that is generated for specific one-time use in cryptographic communications.

2. The client generates its nonce (SNonce) and calculates a MIC over the nonce received from the access point. Then, the client proceeds by sending the SNonce, MIC, and the same replay counter to the access point.

3. Upon receiving the second frame, the access point verifies the MIC over ANonce. If correct, the access point constructs the GTK and calculates a MIC over the client's SNonce. Then, the access point proceeds by sending the GTK, MIC, and the incremented replay counter to the client.

4. Upon receiving the third frame, the client verified the MIC over SNonce. If correct, the client sends a confirmation frame to the access point, and both parties proceed by installing the encryption and integrity keys.

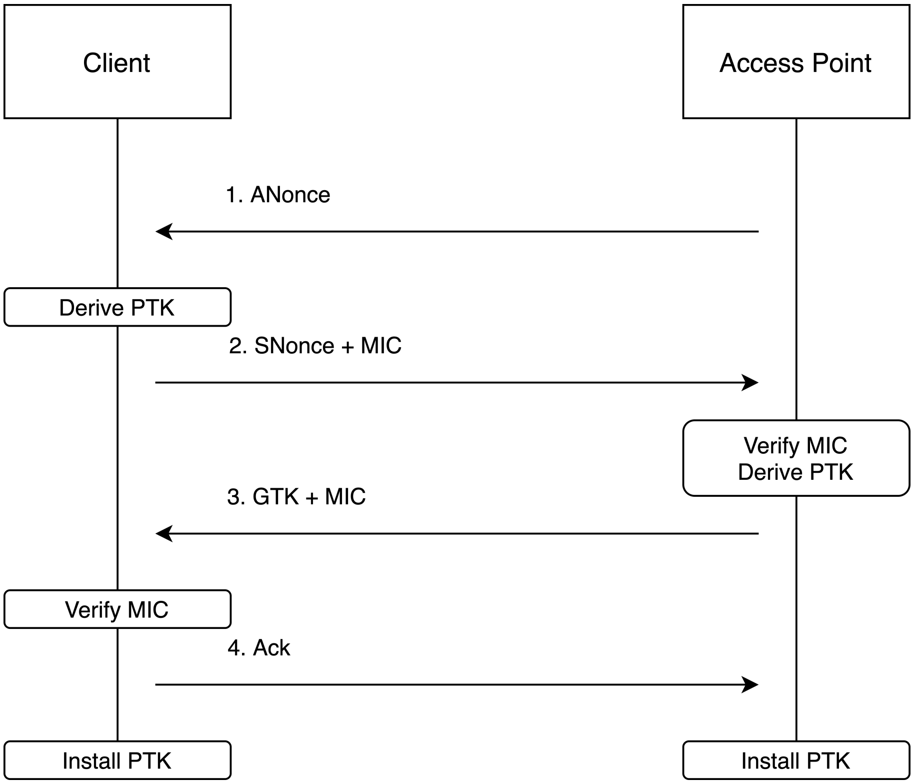

Figure 4: Simplified 4-way handshake

Data integrity and confidentiality

Temporal Key Integrity Protocol (TKIP) (Figure 5) is the encryption protocol used in WPA, which replaced the broken WEP. It still uses the RC4 cipher for data encryption, as WPA was intended to be rolled out on existing hardware as a temporary solution until the release of WPA2 a year later. There are four improvements in the comparison between TKIP and WEP [11, 12]:

1. TKIP introduces a new MIC called 'Michael' to protect the integrity of messages. It has a 64-bit length compared to a 32-bit CRC that WEP uses.
2. TKIP reuses the WEP IV field as a packet sequence number to be able to detect replay attacks. When the receiver notices a packet with the same or a smaller sequence number for the same encryption key, it is considered to be out-of-sequence.
3. TKIP uses a per-packet key mixing function. It eliminates the same key to be used by different clients or access points by taking into account the local MAC address (phase 1). Furthermore, it de-correlates the IVs and the per-packet key (phase 2).
4. It has a re-keying mechanism to provide fresh encryption and integrity keys.

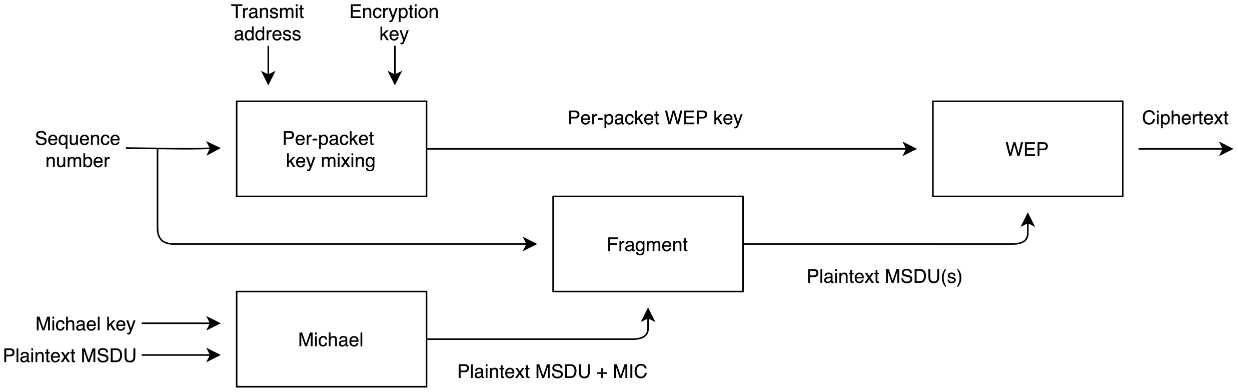

Figure 5: Temporal Key Integrity Protocol diagram

2.3.3 Wi-Fi Protected Access II (WPA2)

Wi-Fi Protected Access II (WPA2) was introduced in 2004 as a replacement for WEP [7] and the temporary WPA. In 2006, the Wi-Fi Alliance required all newly certified devices to support WPA2, ensuring that modern hardware offers the latest security protocols. WPA2 uses CCMP-AES for data encryption, but it can also support TKIP for backward compatibility with legacy devices. It employs a 128-bit key and a 48-bit IV to minimalize vulnerability to a replay attack.

Authentication

WPA2 implements the same 4-way handshake as was introduced in WPA.

Data integrity and confidentiality

Counter Mode CBC-MAC Protocol (CCMP) (figure 5) is the encryption protocol used in WPA2, which replaced TKIP. It used the same key-establishment process as WPA; however, there is no separate key for encrypting the data and constructing the MIC. In comparison with TKIP, CCMP provides a superior level of security by using AES encryption, which is stronger than RC4 and gives better integrity protection than MICHAEL [13].

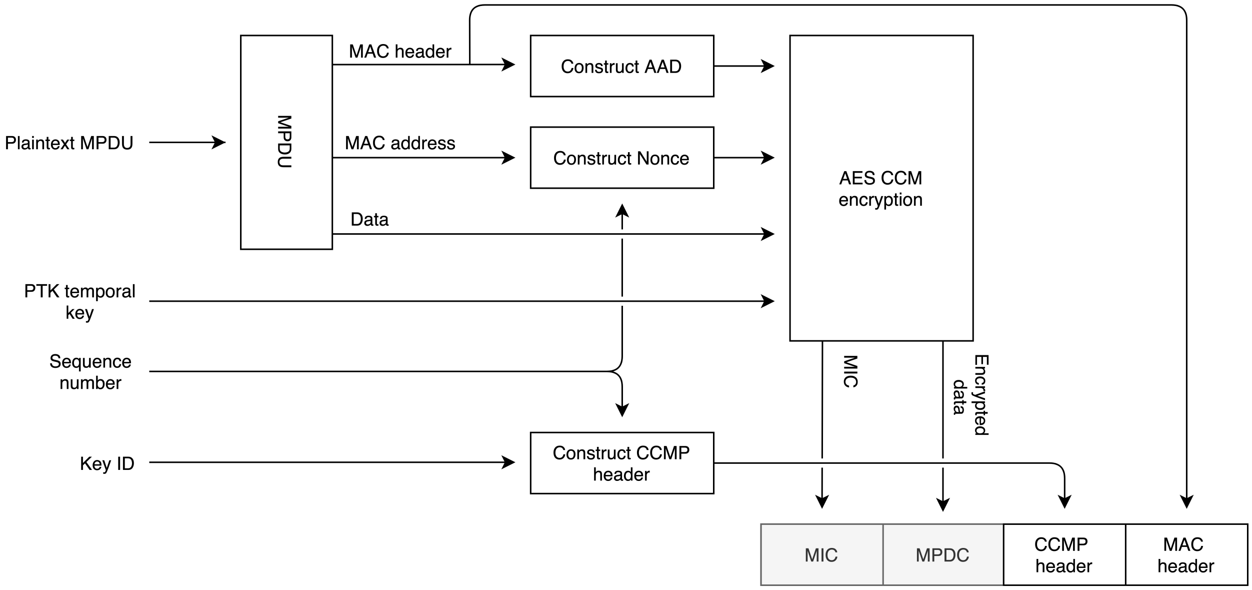

Figure 6: Counter Mode CBC-MAC Protocol diagram

2.3.4 Wi-Fi Protected Access III (WPA3)

Released in 2018, Wi-Fi Protected Access II (WPA3) is the latest security protocol, increasing the level of security and solving several weaknesses of the previous WPA versions. WPA3-Personal replaces the WPA2 PSK authentication with Simultaneous Authentication of Equals (SAE), which is resistant to offline dictionary attacks [14]. A new feature in WPA3 is Opportunistic Wireless Encryption (OWE) that replaces open authentication used in public networks. The encryption key is different for each client, so none of the connected devices can decrypt traffic meant for other clients.

Authentication

WPA3-Personal introduced Simultaneous Authentication of Equals (SAE), which replaced the 4-way handshake with a zero-knowledge proof. The focus of SAE is to authenticate clients upon connecting with the network properly while protecting against malicious actors trying to guess the password. After the client and access point successfully performed SAE, they each created a cryptographically strong key that is used to derive the session key.

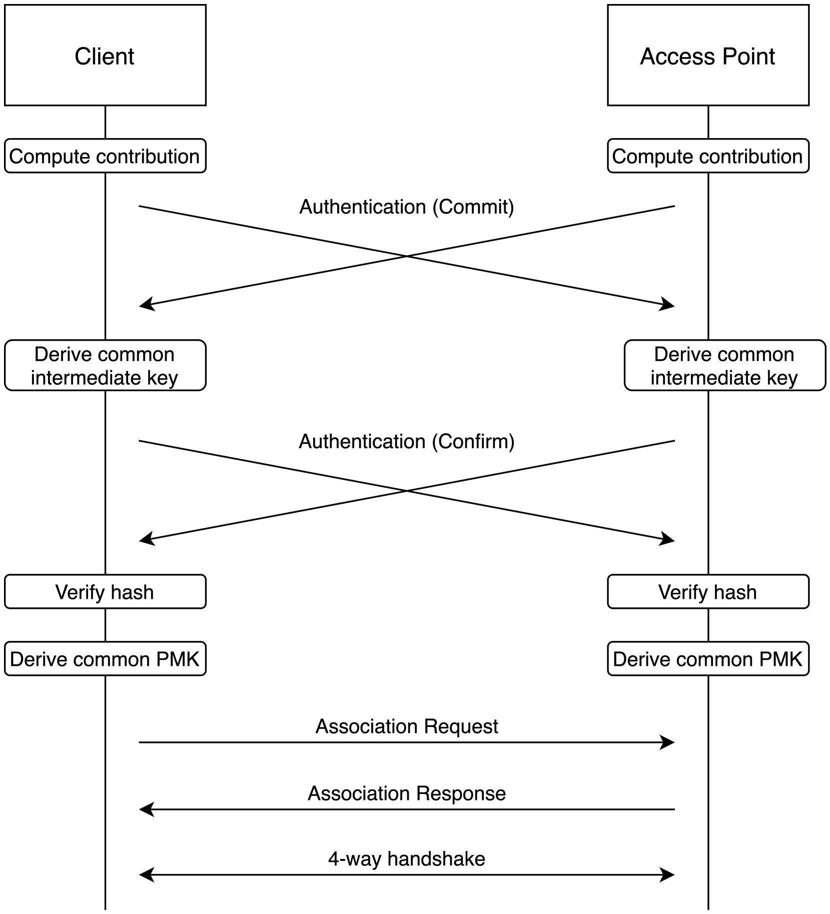

Figure 7: Simplified SAE handshake

Data integrity and confidentiality

Galois/Counter Mode Protocol (GCMP) is the encryption protocol used in WPA3, which is a more secure and efficient protocol than CCMP. This protocol uses AES encryption with a 256-bit key size, which is double the size of that CCMP is using. Additionally, the SHA384 algorithm of the SHA2 family is used to safeguard the data's integrity.

2.4 Wi-Fi Security Modes

Within the different WPA security protocols developed by the Wi-Fi Alliance, we differentiate between Personal and Enterprise modes. Both security modes use the same encryption method (TKIP or CCMP) to preserve the confidentiality and integrity of transmitted data. The main difference between these security modes is how clients authenticate towards the network. Personal networks are designed for home networks and use a pre-shared key (PSK) for authentication. Enterprise networks use the IEEE 802.1X standard, which provides authentication mechanisms that relay the authentication towards an authentication server (RADIUS).

2.4.1 Personal

Personal (also known as PSK) is commonly used to secure wireless networks for households and small businesses. Clients authenticate with the network using a pre-shared key or passphrase without the need for an authentication server. It is important to note that the pre-shared key cannot be managed for individual clients and is the same for everyone who uses it. If the network administrator decides to change the key, all clients needs to be informed and update the key separately.

On Personal networks, the pre-shared key is used as the Pairwise Master Key (PMK) for the 4-way handshake between the client and the access point. If an adversary captures this handshake, it can attempt to perform an offline brute-force attack to recover the pre-shared key. If the adversary succeeds in recovering the pre-shared key, he can decrypt the encrypted traffic between the client and the access point. Open networks are extra vulnerable, since the key is already known to the adversary, so all that's required is to capture the handshake. WPA3-PSK offers greater protection against (offline) brute-force attacks and protecting traffic on open networks.

2.4.2 Enterprise

The major difference from a Personal network is that Enterprise networks use an authentication server (RADIUS) for centralized control over access to the wireless network. Users who try to connect with the network are identified based on the provided credentials or certificates. The access point acts as a broker between the client and the authentication server (Figure 8).The authentication server verifies whether the supplied credentials match an existing user allowed to authenticate to the wireless network, and grants the user access to the network. Until successful authentication, the client is not provided with network activity and is only communicating with the access point.

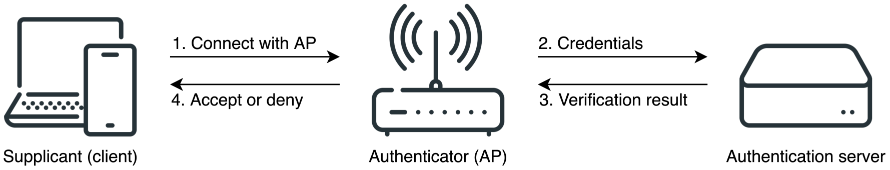

Figure 8: Components of an Enterprise network

Extensible Authentication Protocol (EAP) is an authentication framework used in Enterprise networks to check the client's credentials with an authentication server. The EAP protocol can be configured to accept credentials using different authentication types (EAP-TTLS/PAP and PEAP-MSCHAPv2) and certificates (EAP-TLS) as a method for authentication. When a client requests access, the access point opens a secure tunnel with the authentication server. When the authentication server has verified the client, it provides the access point with a pairwise master key (PMK) to derive the keys for the current session.

2.5 Wi-Fi Connection Protocols

In a standard Personal network setup, a client cannot connect with the wireless network without knowing the SSID and corresponding pre-shared key. The Wi-Fi Alliance has set up two different certification programs that are designed to make it faster and easier for network administrators to connect new devices to the network. These connection methods are built on top of the existing security protocols WPA2 and WPA3.

2.5.1 Wi-Fi Protected Setup (WPS)

The Wi-Fi Protected Setup (WPS) feature of WPA2 makes it easier to connect new devices to a wireless network. WPS is not targeted for use in Enterprise networks, where separate authentication servers are used to control network access. It is an optional feature that you can configure on most modern routers; however, it might be enabled by default on some models. Products that offer WPS allow administrators at least one of three easy methods to connect new devices; Personal Identification Number (PIN), Push-Button Configuration (PBC), or Near Field Communication (NFC) [15, 16].

- Personal Identification Number: using the PIN method, a device is added to the network by entering an 8-digits identifying number. This number is used to ensure that the right device is added, preventing malicious attempts to add unauthorized devices. The number can be printed on a label or dynamically generated and shown on a display of the device.
- Push-Button Configuration: using the PBC method, a device is added to the network by pushing a button on the access point and the client device.
- Near Field Communication: using the NFC method, an NFC-capable device is added to the network by tapping it with another NFC-tag or device.

2.5.2 Device Provisioning Protocol (DPP)

The Wi-Fi Device Provisioning Protocol (DPP) is a new connection protocol for WPA2 and WPA3 that replaces WPS. It is an optional feature offered by Easy Connect certified devices. With Wi-Fi Easy Connect, a configurator is responsible for enrolling other devices on the network by simply scanning a QR-code (Figure 9). This configurator can be a smartphone or tablet that is previously connected with the network.

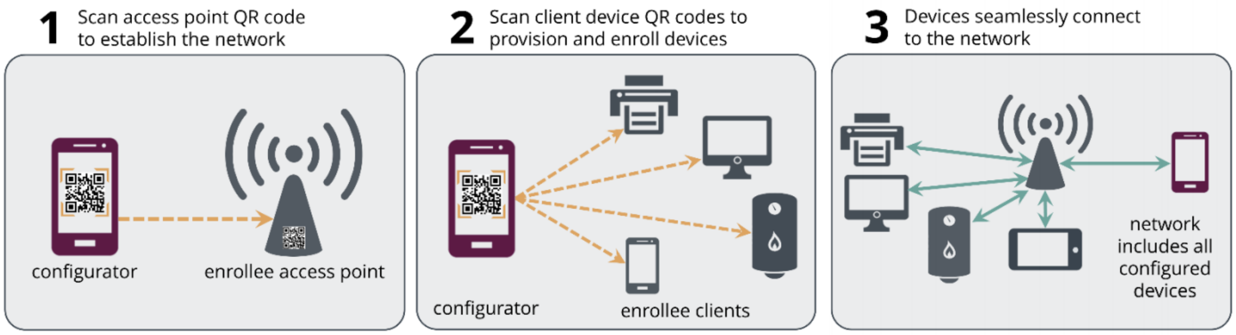
1 Scan access point QR code to establish the network
configurator
enrollee access point
2 Scan client device QR codes to provision and enroll devices
configurator
enrollee clients
3 Devices seamlessly connect to the network
network includes all configured devices

Figure 9: Wi-Fi Easy Connect - figure by the Wi-Fi Alliance

3 Taxonomy of Wi-Fi Attacks

In the previous chapter, we introduced the basics of Wi-Fi networks, security protocols (section 2.3), and common types of attacks (section 3.1). In this chapter, we construct a comprehensive overview of attacks targeting Wi-Fi networks. First, we describe what features can distinguish Wi-Fi attacks and tell them apart from each other. For the overview itself, we will use the type of attacks to group them. Later on, we discuss attacks that fit in the taxonomy and point the security auditor to tools that he can use for auditing and common countermeasures.

Related work on taxonomies

In the past, researchers have published papers covering Wi-Fi attacks. In this section, we discuss some of the papers that create a (partial) overview of Wi-Fi attacks. However, to our knowledge, there is no paper with the goal of creating an in-depth overview of attacks, listing their features, and providing the security auditor with tools and common countermeasures. Most of the papers we were able to find are several years old and focus on attacks that target the WEP security protocol. Our paper aims to examine attacks from a broader perspective, including multiple types of attacks and various security protocols.

- In 2007, Tews published his Diploma thesis [17] covering the WEP security protocol and known attacks against it. In his paper, the author distinguished between attacks exploiting weaknesses of the RC4 cipher and attacks that are not related to RC4. The author describes the mathematical background of the attacks, provides examples, and describes countermeasures that can be implemented when applicable. Given that the paper is several years old, it only covers attacks related to the WEP protocol. Also, the paper focuses on encryption cracking to recover the key or plaintext.

- As basis for their research in 2008, Beck and Tews [18] started with describing Key-recovery attacks against WEP that have been published before, including FMS, KoreK, PTW, and ChopChop. For each of these attacks, they provided the theoretical basis and the success rate of each attack, given that the adversary captures a certain number of packets. Later, they improved the performance of the PTW attack by looking at the correlations found by KoreK. After this, they concluded in their paper that the TKIP protocol used by WPA is a slightly modified version of WEP, allowing them to modify ChopChop to work for WPA. Their research is useful to get a better understanding of the published Key-recovery attacks against WEP and their efficiency.

- In 2010, Caneill and Gilis [8] took a similar approach by first covering existing Key-recovery attacks on WEP, followed by proposing two new attack concepts. Furthermore, they go briefly over some WPA attacks in their paper, which is useful to get a better understanding of WEP/WPA attacks.

3.1 Types of Wi-Fi Attacks

There are several types of attacks that an adversary can use to compromise a Wi-Fi network's security. An adversary may attempt to breach a Wi-Fi network's security objectives, such as breaking confidentiality by eavesdropping on traffic from legitimate users. We focus on Man-in-the-Middle attacks, Key-recovery attacks, Traffic Decryption attacks, and Denial of Service attacks in the taxonomy.

- **Man-in-the-Middle**: A Man-in-the-Middle (MitM) attack is a type of attack where the adversary secretly relays communication between two parties breaching the mutual authentication. In a wireless network, the adversary relays packets between the access point and a client, allowing him to eavesdrop on traffic, and replay, modify, and block packets from reaching their destination. Eavesdropping and altering traffic allows the adversary to obtain credentials, display incorrect information, use services on behalf of the victim, and perform many more malicious actions [19].

  The adversary may attack individual clients by launching a rogue access point that appears legitimate to the victim or its device. We speak of an Evil Twin attack, when the malicious network uses the same MAC, BSSID, and SSID as the target network. The adversary can provide internet access when expected from the target network, making it harder for a user to notice that it is connected to a malicious network. However, the adversary has now placed himself in a Man-in-the-Middle position and can eavesdrop on traffic. According to Norton's survey, 54% of consumers cannot tell the difference between a secure and an insecure public network [20]. An Evil Twin is interesting for both adversaries and security auditors as it is adopted by a large number of well-known auditing tools.

  As concluded in section 3.3.8, Man-in-the-Middle attacks are versatile and powerful as an adversary can target almost any network and security configuration. The adversary can also have different goals in mind, such as eavesdropping on traffic or collecting Wi-Fi credentials of Enterprise networks.

- **Key-recovery**: A Key-recovery attack is a type of attack where the adversary attempts to recover the pre-shared key used to associate with a network. Recovering this key provides the adversary with new capabilities, such as launching an Evil Twin attack or associating with the network as a client and performing other attacks, such as ARP spoofing [14].

  An adversary may attempt to exploit potential weaknesses in the authentication protocol that is executed between a client and the access point. For example, the adversary could capture the 4-way handshake of a client associating with the network and perform an offline Dictionary attack (section 3.4.5). WPA3 offers greater protection against these offline brute-force attacks due of the new handshake that derives a common PMK.

  Another technique the adversary may use is recovering the key by performing statistical analysis on encrypted traffic. Networks secured with WEP are the most susceptible, as they can be cracked within a couple of minutes using freely available tools [21]. As concluded in section 3.4.10, starting from WPA, the pre-shared key is no longer used to encrypt traffic directly, therefore making statistical analysis infeasible.

- **Traffic Decryption**: A Traffic Decryption attack is a type of attack where the adversary attempts to crack the encryption of a packet exchanged on a network. Breaking the encryption usually means that the adversary learns the plaintext of a packet, which breaches data confidentiality. Along with other attacks, the adversary may recover encryption keys used for data integrity, allowing the adversary to spoof packets.

  As concluded in section 3.5.8, most of the attacks propose a scheme to recover the plaintext of one packet, such as altering packets and having the access point forward them to the adversary. The proposed schemes are somewhat complicated. There is no tooling available; therefore, attempting to decrypt traffic from modern networks seems complicated for an adversary or a pentester compared to other attack types.

- **Denial of Service**: A Denial of Service (DoS) attack is a type of attack that aims to affect the availability of system resources to legitimate users [22]. An adversary may attempt to overload a system with many requests, so there are insufficient resources to handle the requests. Also, software vulnerabilities may lead to denial of service; for example, an adversary may include special characters in its request that the application cannot handle, causing the software to crash.

  In a wireless network, an adversary can take different approaches, targeting multiple layers of the OSI model layer. As wireless communication happens over a shared medium where data is broadcasted via radio waves, an adversary can intentionally interfere with these radio signals. These kinds of attacks on the Physical layer are known as radio frequency jamming. Denial of Service attacks on the Data Link layer are perpetrated by spoofing packets to a client or access point. For example, an adversary can spoof deauthentication packets (section 3.6.2), causing legitimate clients to be de-associated from the network.

  As concluded in section 3.6.5, launching a Denial-of-Service attack can be interesting for an adversary with the intent to disrupt Wi-Fi communication. Some of the attacks, such as the one targeting TKIP, can be achieved by transmitting a low number of packets.

3.2 Features of Wi-Fi Attacks

To be able to group and compare Wi-Fi attacks in our taxonomy, we identified 5 features. The most important feature is the type of attack, for example, Evil Twin attacks, Key-recovery attacks, and Denial of Service attacks. Furthermore, we consider the protocol that the attack targets, whether the adversary interacts with the network components, the efficiency of the attack, and whether tools are available for the security auditor. These features are used in Table 4 to provide an overview of the attacks we discuss in the taxonomy. See Appendix C for more context on the features that are included in the table.

- **Type**: The most important feature is the type of attack, correlated with the adversary's objective. For example, the adversary may set up a malicious access point to place himself in a Man-in-the-Middle position (type) or perform a Key-recovery attack (type) to obtain the encryption key. In our taxonomy, we consider the following types: Man-in-the-Middle attacks, Key-recovery attacks, Traffic Decryption attacks, and Denial of Service attacks. See section 3.1 for a detailed description of each attack type.

- **Protocol**: Most attacks exploit a weakness that comes with the configuration of the network. For example, when the adversary wants to perform a Key-recovery attack, the possible attacks depend on the network's security protocol. In our taxonomy, we consider the following protocols: WEP, WPA, WPA2, and WPA3. For some attacks, it may also depend on whether the network is using Personal or Enterprise mode. In the table, we display WPA-Personal as WPA-PSK and WPA-Enterprise as WPA-EAP.

- **Interaction**: Another feature that we can compare is whether the adversary needs to interact with the network components to make its attack succeed. When the adversary does not interact with the network, it is considered a passive attack. For example, an adversary may listen to encrypted traffic and attempt to recover the encryption key by performing an offline Dictionary attack. On the other hand, the adversary may perform an active attack where the adversary interacts with the access point or clients. Some attack types may be active or passive by their nature, while other attack types may be possible either actively or passively.

In our taxonomy, we consider the following interaction values: passive, active (client), active (access point), and active (MitM). Which component the adversary is interacting with is placed between parentheses. Man-in-the-middle means that the adversary is relaying packets between the access point and a client.

- **Tools**: Another relevant feature is whether tools are available for a security auditor to test if a network is vulnerable to an attack. In our taxonomy, we consider the following values: None (there are no tools available), - (there is a proof-of-concept available), + (there is a tool available for testing), ++ (there are multiple tools available, or it is part of a multi-purpose suite).

- **Efficiency**: Another feature that can be used to compare attacks is the efficiency of the attack, although this might not be relevant for all attack types. For statistical Key-recovery attacks, the efficiency can be expressed in the number of packets that need to be collected to reach a certain success probability. In other cases, efficiency might be expressed in the amount of time the adversary needs to perform its attack. This feature is only displayed in the table per attack type/protocol when it is relevant.

Type	Protocol	Name	Interaction	Tools	Year
Man-in-the-Middle	*-*	Evil Twin Attack 3.3.1	Active (client)	++	2001
	-	KARMA Attack 3.3.3	Active (client)	++	2004
	WPA-EAP WPA2-EAP	EAP-PEAP Relay Attack 3.3.2	Active (MitM)	++	2003
	-	MANA Attack 3.3.4	Active (client)	++	2004
	WPA-* WPA2-*	Hole196 Vulnerability 3.3.5	Active (MitM)	None	2010
	WPA-Open WPA2-Open	Lure10 Attack 3.3.6	Active (client)	+	2017
	WPA-Open WPA2-Open WPA3-Open	Known Beacon Attack 3.3.7	Active (client)	+	2018
Key-recovery	WEP	FMS Attack 3.4.1	Passive	++	2001
	WPA-PSK WPA2-PSK	Dictionary Attack 3.4.5	Passive Active(client)	++	2003
	WEP	KoreK Attack 3.4.2	Passive	++	2004
	WEP	PTW Attack 3.4.3	Active (access point)	++	2007
	WPA-PSK WPA2-PSK	WPS Brute-force Attack 3.4.4	Active (access-point)	++	2011
	WPA-EAP WPA2-EAP WPA3-EAP	EAP-GTC Downgrade Attack 3.4.6	Active (client)	++	2013
	WPA-PSK WPA2-PSK	WPS Pixie Dust Attack 3.4.8	Active (access point)	++	2014
	WPA-PSK WPA2-PSK	PMKID Hash Dictionary Attack 3.4.7	Active (access point)	++	2018
	WPA3-PSK	Downgrade Attack against WPA3-Transition 3.4.9.1	Active (client)	None	2019
	WPA3-PSK	Downgrade Attack against Security Group 3.4.9.2	Active (MitM)	None	2019
	WPA3-PSK	Timing-Based Side-Channel Attack 3.4.9.3	Active (access point)	-	2019
	WPA3-PSK	Cache-Based Side-Channel Attack 3.4.9.4	Active (client)	-	2019
Traffic Decryption	WEP	ChopChop Attack 3.5.1	Active (access point)	++	2004
	WPA-*	Beck-Tews Attack 3.5.2	Active (client)	-	2008
	WPA-*	Ohigashi-Morii Attack 3.5.3	Active (MitM)	None	2009
	WPA-*	Michael Reset Attack 3.5.4	Active (client)	None	2010
	WPA-*	Vanhoef–Piessens Attack 3.5.5	Active (client)	None	2013
	WPA-*	NOMORE Attack 3.5.6	Active (client)	None	2015
	WPA-* WPA2-*	KRACK Attack 3.5.7	Active (MitM)	-	2017
Denial of Service	*-*	Resource Exhaustion Attack 3.6.1	Active (access point)	++	-
	WEP WPA-* WPA2-*	Deauthentication Flooding Attack 3.6.2	Active (access point)	++	-
	WPA-*	TKIP Michael MIC failure 3.6.3	Active (access point)	++	2013
	WPA3-*	Dragonfly Resource Exhaustion Attack 3.6.4	Active (access point)	+	2018

Table 4: Overview of Wi-Fi attacks

3.3 Man-in-the-Middle

A Man-in-the-Middle (MitM) attack is a type of attack where the adversary secretly relays communication between two parties breaching the mutual authentication. In a wireless network, the adversary relays packets between the access point and a client, allowing him to eavesdrop on on traffic, and replay, modify, and block packets from reaching their destination. Eavesdropping and altering traffic allows the adversary to obtain credentials, display wrong information, use services on behalf of the victim, and perform many more malicious actions [19].

Protocol	Name	Interaction	Tools	Year
-	Evil Twin Attack 3.3.1	Active (client)	++	2001
WPA-EAP WPA2-EAP	EAP-PEAP Relay Attack 3.3.2	Active (MitM)	++	2003
-	KARMA Attack 3.3.3	Active (client)	++	2004
-	MANA Attack 3.3.4	Active (client)	++	2004
WPA-* WPA2-*	Hole196 Vulnerability 3.3.5	Active (MitM)	None	2010
WPA-Open WPA2-Open	Lure10 Attack 3.3.6	Active (client)	+	2017
WPA-Open WPA2-Open WPA3-Open	Known Beacon Attack 3.3.7	Active (client)	+	2018

Table 5: Overview of Man-in-the-Middle attacks

3.3.1 Evil Twin Attack

An Evil Twin attack is a network set up by an adversary, trying to trick users or devices into connecting with the network. The access point appears to be legitimate by using the same MAC, BSSID, and SSID as the target network. When a device connects to the Evil Twin's network, the adversary can eavesdrop on all (unencrypted) traffic [14]. It is hard to pinpoint the exact date on which the Evil Twin attack was discovered; however, the oldest whitepaper[1] we were able to find dates from 2001.

When looking at Evil Twin attacks, the implementation and impact depend on how the target network is secured [19]. We differentiate between networks that are open to the public and networks that require a form of authentication before clients are allowed to connect to the network. When the target network is secured, and the pre-shared key is unknown, the adversary can attempt to trick the user by launching a captive portal-style Evil Twin attack.

Later in the taxonomy, we discuss some variations in which the adversary launches a malicious access point similar to an Evil Twin attack. For example, with the KARMA (section 3.3.3) attack, the adversary reaches the same capabilities without the need of being in the range of a specific target network. Attacks like MANA (section 3.3.4), Lure10 (section 3.3.6), and Known Beacon (section 3.3.7) are similar, as the adversary is not required to be located near the target network. These kinds of attacks do not always try to

[1] http://www.packetnexus.com/docs/wireless_LAN_security.pdf

obtain credentials for a specific target network, but sometimes are used to target users or their devices.

Open networks

Open Wi-Fi networks are commonly available; for example, many stores, hotels, airports, and other public places provide free access to the internet to their visitors. Most of these networks are open to the public and do not require users to know a pre-shared key to authorize with the network. In other cases, a pre-shared key might be required, but is publicly available information. For example, restaurants or hotels that hand out the password to their customers.

Open networks form the perfect target for an Evil Twin attack as they lack authentication. All that is required for an adversary is setting up a network using the same SSID and providing a stronger signal than the legitimate target network.

Captive portal-style Evil Twin Attack

When the target network's pre-shared key is unknown to the adversary, he can attempt to use social engineering to obtain credentials by setting up a captive portal-style Evil Twin attack. This type of attack does not exploit one particular security protocol and can be launched against different kinds of secured networks.

In a captive portal-style Evil Twin attack, the adversary sets up an open network with the same SSID as the secure network. The adversary may flood deauthentication packets to keep clients from connecting to the legitimate network. When users notice that they cannot connect with the legitimate network, they might choose to connect to the malicious network.

A captive portal is something a client will see when connecting to an open network that asks the user to provide information (like the room number at a hotel) before providing access to the internet. Upon connecting with the Evil Twin network, the user is shown a portal asking him to provide their credentials. For example, the adversary can display a web page pretending to be the router, informing the user that their credentials are needed to install some update on the router before internet access is granted.

Countermeasures When considering countermeasures for Evil Twin attacks, we can approach it from different perspectives, which all contribute to an overall more complete solution. From a client perspective, there are several best practices that can be configured for the client to be less vulnerable. For example, simply disabling wireless interfaces when the device is not actively connected to a network [23], disabling auto-connection, or forgetting networks after connecting with them. This helps prevent the device from connecting with an Evil Twin impersonating a network.

There are other steps a user of a network can take to minimalize the risks when dealing with a potential Man-in-the-Middle attack. For example, by routing traffic through a Virtual Private Network (VPN), it is harder for an adversary to inspect traffic while sitting in a Man-in-the-Middle position, since only the encrypted traffic from the tunnel with the VPN is observable. Also, browser plugins such as HTTPS Everywhere[2] help to prevent the adversary from forcing the browser to use an insecure HTTP connection.

Researchers have developed several different techniques and tools that can detect an Evil Twin attack. These approaches may run on the client-side, or the server-side inspecting the network [24, 23]. Organizations

[2] `https://www.eff.org/https-everywhere`

can deploy a Wireless Intrusion Detection System (WIDS) to monitor the wireless spectrum and detect rogue access points.

Security protocols before the introduction of WPA3 do not specify how the client should know the SSID that identifies the authentication server. Furthermore, a device can be configured to accept any certificate from the authentication server without validating the certificate. Standards of WPA3 Enterprise specify that a client may only send authentication material when the user explicitly accepts trust in the certificate provided by the authentication server. Client configuration that skips validation of the certificate or puts trust in any presented certificate is not allowed. Secondly, with WPA3 Enterprise, it is possible for network administrators to constrain how clients may obtain the certificate [25].

Tools The tool Airbase-ng from the suite Aircrack-ng (section 4.2.1) is aimed at attacking clients by setting up a (malicious) access point. This setup is often completed with other tools such as Dnsmasq to provide clients with internet access, and SSLStrip to hijack HTTP traffic.

The toolkit Airgeddon (section 4.2.2) is capable of launching a complete Evil Twin attack by integrating with various tools. It is able to automate the whole process, from selecting the target, deauthentication of clients, capturing handshakes, setting up the access point, providing a captive portal, and eavesdropping on traffic.

The toolkit Eaphammer (section 4.2.3) is designed to perform directed Evil Twin attacks against WPA2-Enterprise networks and has also integrated with various other tools to automate the process. It is capable of capturing RADIUS credentials and launching hostile/captive portal attacks

3.3.2 EAP-PEAP Relay Attack

Extensible Authentication Protocol (EAP) is an authentication framework used in Enterprise networks to check the client's credentials with an authentication server (section 2.4). Protected EAP (PEAP) encapsulates EAP inside an SSL wrapper to create an encrypted and authenticated tunnel. In 2002, researchers from Nokia described Man-in-the-Middle attacks against tunneled authentication protocols [26], including PEAP.

An adversary acts as a middleman in a relay attack and mediates an authentication attempt (usually challenge-response) between two parties. The first step for the adversary is to trick a device into connecting with a malicious access point. Then, the adversary relays the authentication attempt to a legitimate access point (Figure 10). If successful, the legitimate RADIUS server allows the adversary to connect to the targeted network. The attack works when there is no channel binding between the client connecting with the access point and the RADIUS server.

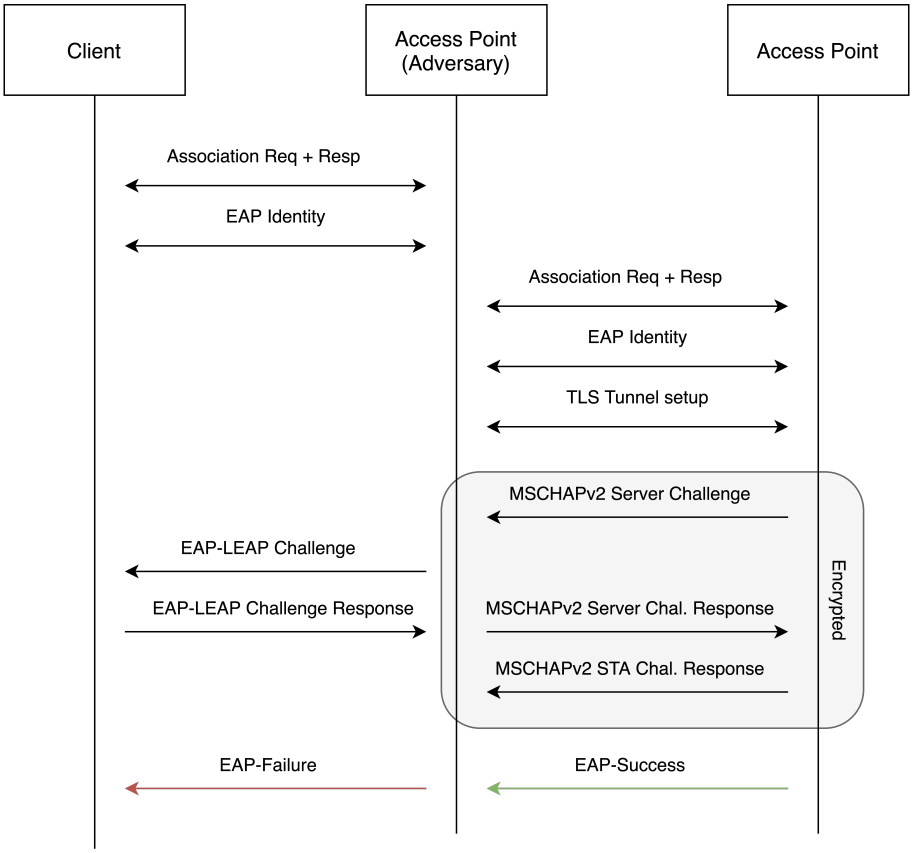

Figure 10: Flow diagram for the EAP-PEAP Relay attack

Countermeasures There exist several methods to mitigate the EAP-PEAP Relay attack [26, 27]. First, by using client certificates to authenticate client devices, the TLS tunnel would fail to set up. Using client certificates is an effective countermeasure, however, it will require additional administrative effort. Secondly, PEAP version 2 introduces an optional feature called cryptographic binding to address Man-in-the-Middle attacks. This binding ensures that the client authenticating towards the RADIUS server is the same client that created the tunnel with the access point.

Tools The patch Hostapd-mana (section 4.2.5) has support for the EAP-PEAP Relay attack.

3.3.3 KARMA Attack

For a classic Evil Twin attack (section 3.3.1) to work, the adversary needs to be in the range of the target network. In some cases, the adversary might not be interested in targeting clients of a specific network, but targeting individual clients instead, regardless of the network they are connected to.

Wi-Fi-enabled devices broadcast probe-request frames (section 2.2) containing information on networks that are known to the device, and that it is looking for. A Karma[3] attack abuses this information by listening for direct probe-requests and respond to any request it observes [28]. This mechanism even works for networks with hidden SSID, as clients still send probe-requests for those kinds of networks.

[3] `http://theta44.org/karma/`

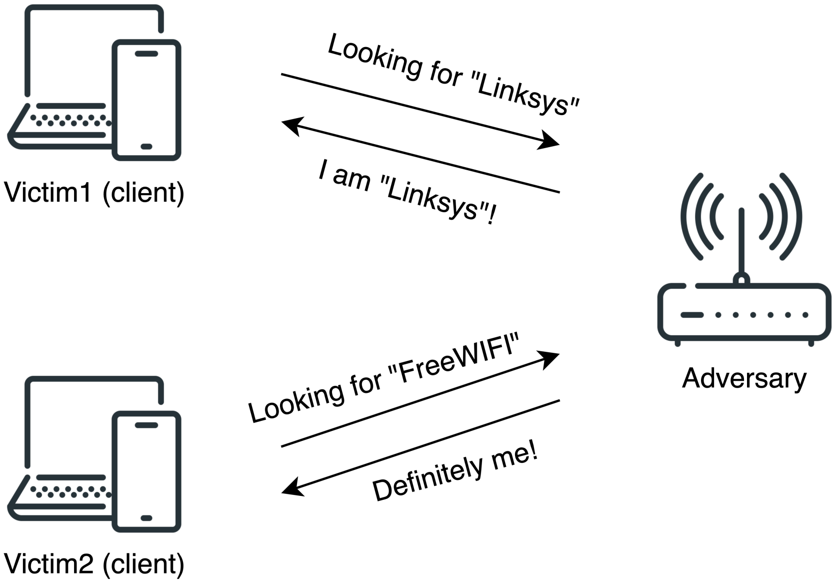

Figure 11: Flow diagram for the KARMA attack

Countermeasures Vendors have tried to address KARMA by limiting active probing or relying solely on passive scanning. However, new attack variations like MANA (section 3.3.4) and Known Beacon (section 3.3.7) have risen to bypass these countermeasures.

Another mitigating measure can be to restrict stored networks in the PNL to a specific MAC address. This measure might be effective if the network is unknown to the adversary, so it cannot spoof its MAC address. However, this solution will not solve the problem entirely, as some networks operate on multiple access points using different MAC addresses, and are still subject to spoofing.

Tools Simple Karma Attack[4] is a tool intended to launch a simple and fast KARMA attack. It is capable of capturing probe-requests to select the target network, and it integrates with various other tools to set up the access point and host a captive portal.

3.3.4 MANA Attack

Modern devices have changed the way they handle probe-responses as a countermeasure against the original KARMA attack (section 3.3.3): if a known network does not respond to a broadcast probe first, the device will know the network is not available and ignore directed probe-responses.

To overcome the countermeasure, the adversary must know the networks a client is looking for and respond to broadcasts first. MANA[5] implemented this behavior by storing the Preferred Network List (PNL) for devices it sees. Then, when the adversary observes a broadcast from one of the devices, a directed probe-response frame is sent for all of the stored networks.

The load MANA attack is a variant in which the adversary responds to broadcasts by sending probe-response frames for the union of all stored PNLs of all devices it knows, regardless of the device that is

[4] `https://github.com/Leviathan36/SKA`

[5] `https://sensepost.com/blog/2015/improvements-in-rogue-ap-attacks-mana-1%2F2/`

sending the broadcast.

Countermeasures The MANA attack is a new attack variation that counters limited probing. However, the same mitigating measure as for the KARMA attack (section 3.3.3) applies. By restricting the stored networks in the PNL to a specific MAC address, the adversary must know the MAC address of the network.

Tools The toolkit Eaphammer (section 4.2.3) is designed to perform directed Evil Twin attacks. However, it is interesting to note that it supports the MANA attack and the Known Beacon attack.

3.3.5 Hole196 Vulnerability

The Hole 196 vulnerability [29] does not involve the cracking of encryption keys; however, it still allows the adversary to learn about plaintext data sent by other clients. For this attack to work, the adversary needs to be connected to the same network as its victims.

Networks secured with WPA or WPA2 use two different encryption keys: the Pairwise Transient Key (PTK), used to secure the traffic between a particular client and the access point, and the the Group Temporal Key (GTK), used for encrypting broadcast packets. Since all clients share the same GTK, it allows the adversary to send spoofed ARP request packets directly to other clients. In this request, the adversary specifies its own MAC address as the gateway.

1. The adversary constructs a fake ARP request packet and sends it directly to other clients on the network. The adversary specifies its own MAC address as the gateway. The packet is encrypted using the GTK, which is known to the adversary.

2. The Victim sends traffic encrypted with its PTK to the access point, with the MAC address of the adversary as the gateway. The adversary cannot reveal the plaintext, as the PTK is shared between the client and the access point.

3. However, since the MAC address of the adversary is set as the gateway, the traffic will be forwarded to the adversary by the access point. The access point decrypts the traffic and encrypts it with the PTK shared with the adversary.

4. After learning the plaintext, the adversary delivers the packet to the access point, so that the communication of the victim continues as normal.

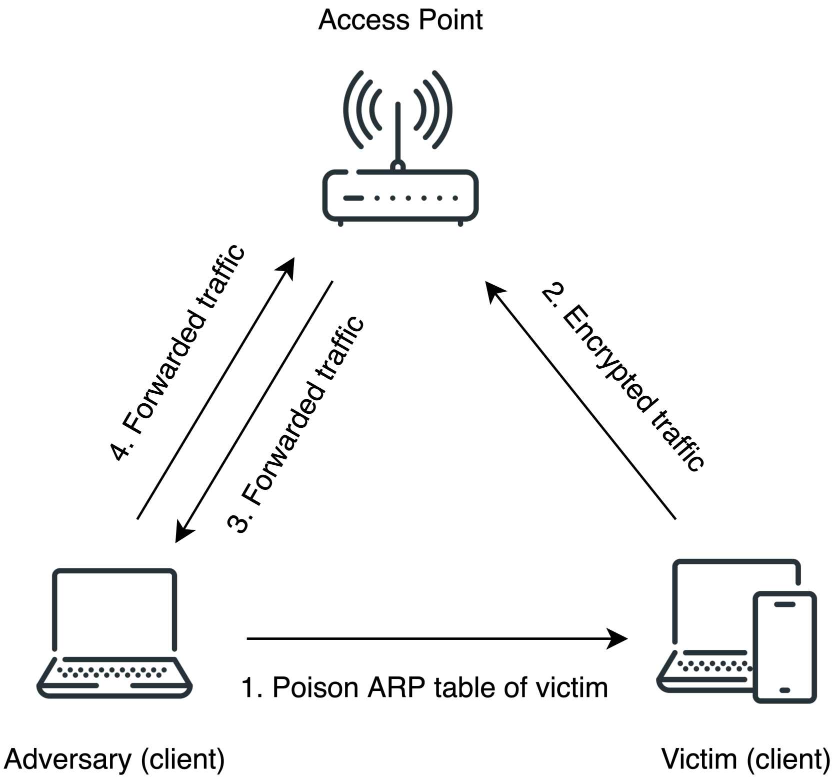

Figure 12: Flow diagram for the Hole196 vulnerability

The difference with a classic ARP poison attack is that the adversary sends spoofed packets directly to the victim encrypted with the GTK. This reduces the footprint of the attack, as the spoofed packet does not reach the access point and does not travel over the wire. This makes it harder for an intrusion detection system to detect the attack.

Countermeasures Network administrators may use client isolation to restrict data communication between two clients connected with the same access point. An adversary authenticated to the network may still send spoofed ARP packets, but he will no longer receive traffic from a victim. Another layer of defense is the use of a wireless intrusion prevention system (WIPS) that can detect spoofed packets.

Tools There does not seem to be a tool that implements the Hole196 attack directly. Of course, tools such as Aircrack-ng includes tools for spoofing and transmitting packets. Therefore, it might be possible with Aircrack-ng; however, it is not marketed as such. Tools like Ettercap[6] and Bettercap[7] are designed to perform Man-in-the-Middle attacks; however, they target wired networks.

3.3.6 Lure10 Attack

Windows version 10 offered the feature Wi-Fi Sense to suggest open networks known as a good quality hotspot. If the device is in range of one of the networks on the list, Wi-Fi Sense automatically accepts the terms of the hotspot and connects the devices to it.

[6] `https://www.ettercap-project.org/`

[7] `https://www.bettercap.org/`

The Lure10[8] attack abuses this behavior of Wi-Fi Sense by tricking the device into 'thinking' it is located in the area of a hotspot trusted by the service, followed by mimicking the network. Since Wi-Fi Sense is designed to automatically connect with known hotspots, the device will connect with the Evil Twin network. As a result, in 2017, Microsoft turned off Wi-Fi Sense's ability to automatically connect with open hotspots by default.

Countermeasures From a client perspective, the same practices as for the Evil Twin attack (section 3.3.1) help to prevent the Lure10. These practices include disabling wireless interfaces when a Wi-Fi connection is not needed and disabling auto-connection with known networks. When users apply these practices, their devices will not connect with the malicious Wi-Fi network under control of the adversary.

Tools Wifiphisher (section 4.2.4) is a rogue access point framework capable of targeting devices with limited or without active probing. It has support for the Lure10 attack and the Known Beacon attack.

3.3.7 Known Beacon Attack

Devices with limited active probing or without direct probing are still vulnerable when the adversary knows what open networks a device may be looking for. The Known Beacon attack[9] begins by constructing a large list of known open networks. For example, common networks like "iPhone" and hotspots that exist in hotels, airports and other public locations. The adversary transmits probe-response frames for all the networks in its lists, tricking devices looking for a known network into connecting with the Evil Twin network.

Countermeasures From a client perspective, the same practices used against the Evil Twin attack (section 3.3.1) help to prevent the Known Beacon attack. These practices include disabling wireless interfaces when a Wi-Fi connection is not needed and disabling auto-connection with known networks. When users apply these practices, their devices will not connect with the malicious Wi-Fi network under control of the adversary.

Tools The toolkit Eaphammer (section 4.2.3) is designed to perform directed Evil Twin attacks against Enterprise networks. It can load a wordlist containing ESSID's that will be used to broadcast beacon frames for the rogue access point.

3.3.8 Conclusion

Man-in-the-Middle (MitM) is a type of attack where the adversary secretly relays communication between two parties, breaching the mutual authentication, and in some cases, the integrity and confidentiality of transmitted data. A Man-in-the-Middle position allows the adversary to eavesdrop on (encrypted) traffic, and replay, modify, and block packets from reaching their destination.

Examples of this attack type include an Evil Twin attack (section 3.3.1) and an ARP poisoning attack (section 3.3.5), in both of which the adversary attempts to eavesdrop on traffic. The Evil Twin attack and its variants are versatile, as the adversary can launch it against almost any network and security configuration. Large enterprise networks often deal with various types of client devices with different implementations and

[8] `https://census-labs.com/news/2017/05/11/lure10-exploiting-windows-automatic-association-algorithm/`

[9] `https://census-labs.com/news/2018/02/01/known-beacons-attack-34c3/`

security settings. The adversary has to trick only one of the devices to connect with its malicious network and expose credentials.

Open networks are the perfect target for an Evil Twin attack, as they lack authentication. All that is required for an adversary is to provide a stronger signal than the target network. Users often use these open networks on the go, such as in airports, hotels, and while visiting stores. Several practices could help users protect their devices, such as disabling wireless interfaces when not connected to a Wi-Fi network, disabling auto-connection, and forgetting networks after connecting with them.

Manufacturers of client devices must be aware that their users are not necessarily aware of the risks, and should implement the countermeasures by default. WPA3 offers greater protection for open networks by implementing a new feature called Opportunistic Wireless Encryption (OWE). As soon as the adoption of WPA3 becomes more common, administrators are encouraged to migrate to offer connected devices greater protection.

When considering protected networks, the adversary can use different styles of Evil Twin attacks. For example, an adversary can attempt to relay challenge-responses (section 3.3.2) between the real authentication server to authenticate himself instead of the legitimate client. Also, the adversary can launch a Captive portal-style Evil Twin attack (section 3.3.1) in which he uses social engineering to trick the victim in giving up his credentials. Another thing to consider is the broad availability of well-known auditing tools capable of launching Evil Twin attacks and their variations.

WPA3 is supposed to offer greater protection for Enterprise networks, as the standards dictate that the user must explicitly accept trust in the authentication server's certificate. However, different manufacturers will likely display the check differently, allowing auditors to find clever ways of tricking the users into accepting trust in their bogus certificate.

3.4 Key-recovery

A Key-recovery attack is a type of attack where the adversary attempts to recover the pre-shared key used to associate with a network. Recovering this key provides the adversary with new capabilities such as launching an Evil Twin attack or associating with the network as a client and perform other attacks such as ARP spoofing [14].

Protocol	**Name**	**Interaction**	**Tools**	**Year**
WEP	FMS Attack 3.4.1	Passive	++	2001
WPA-PSK WPA2-PSK	Dictionary Attack 3.4.5	Passive Active(client)	++	2003
WEP	KoreK Attack 3.4.2	Passive	++	2004
WEP	PTW Attack 3.4.3	Active (access point)	++	2007
WPA-PSK WPA2-PSK	WPS Brute-force Attack 3.4.4	Active (access point)	++	2011
WPA-EAP WPA2-EAP WPA3-EAP	EAP-GTC Downgrade Attack 3.4.6	Active (client)	++	2013
WPA-PSK WPA2-PSK	WPS Pixie Dust Attack 3.4.8	Active (access point)	++	2014
WPA-PSK WPA2-PSK	PMKID Hash Dictionary Attack 3.4.7	Active (access point)	++	2018
WPA3-PSK	Downgrade Attack against WPA3-Transition 3.4.9.1	Active (client)	-	2019
WPA3-PSK	Downgrade Attack against Security Group 3.4.9.2	Active (MitM)	-	2019
WPA3-PSK	Timing-Based Side-Channel Attack 3.4.9.3	Active (access point)	-	2019
WPA3-PSK	Cache-Based Side-Channel Attack 3.4.9.4	Active (client)	-	2019

Table 6: Overview of Key-recovery attacks

3.4.1 FMS Attack

The FMS attack [30] is a statistical attack on WEP exploiting weaknesses in the RC4 stream cipher. The attack allows the recovery of the encryption key after observing a large number of encrypted packets which also include the corresponding initialization vector. The IV and the WEP key are used as input for the scheduling algorithm (KSA) to generate a matrix, from which RC4 generates its keystream. The root of the attack is a statistical anomaly in KSA that allows a small portion of the matrix to end up in the keystream to be more likely than other values.

The paper describes several "weak" IVs - in those packets encrypted with a weaker key structure, there is a 5% chance that one byte of the key will be leaked. Knowledge of the plaintext, such as headers in certain packets, is used to leak the byte of the plaintext. After observing around 4-6 million packets, the adversary has a success probability of 50% of recovering the full WEP key [18].

Countermeasures The attack abuses the fact that WEP uses the pre-shared key as input for the RC4 encryption algorithm. Researchers found weaknesses in the RC4 cipher that allows the recovery of the encryption key. Since WEP has been deprecated since 2004, our only advice would be to migrate to a more modern security protocol.

Tools The tool WEPCrack[10] was the first implementation of the attack, allowing network administrators to test if their network is vulnerable for the attack.

Popular toolkits like Aircrack-ng (section 4.2.1) and Airgeddon (section 4.2.2) have built-in support for performing the FMS attack.

3.4.2 KoreK Attack

An anonymous user of NetStumbler with the pseudonym KoreK published code that implements different attacks on WEP. The attack was based on the original FMS attack; however, the author managed to find new correlations between the RC4 key and the generated keystream, allowing the new tool to recover the key faster and reduce the keyspace.

KoreK did not publish any theoretical analysis of the correlations that he found; however, a different researcher published a paper covering the theoretical basis [31]. Using the work of KoreK, an adversary can recover the WEP with a probability of 50% after observing 700.000 packets [18].

Countermeasures The attack abuses the fact that WEP uses the pre-shared key as input for the RC4 encryption algorithm. Researchers found weaknesses in the RC4 cipher that allow the recovery of the encryption key. Since WEP has been deprecated since 2004, our only advice would be to migrate to a more modern security protocol.

Tools The tool Aircrack-ng (section 4.2.1) can recover the WEP key once enough encrypted packets have been captured. It offers support for different Key-recovery attacks, including the correlations found by Korek.

3.4.3 PTW Attack

The Key-recovery attack PTW is an extension of Klein's attack on RC4, applied to the WEP protocol. The attack allows determining bytes of the key independently from each other, reducing the time needed to brute-force the remaining key bytes [32].

To perform the attack, the adversary needs to capture a set of packets and recover their keystream. Given the first 3 bytes of all per-packet keys, the adversary can attempt to calculate and test the root key. If the test fails, the adversary continues with testing other probable keys [8].

After collecting between 35.000 to 40.000 packets, the adversary has a success probability of 50% of recovering the full WEP key, which can be collected within 60 seconds on a fast network. To achieve a success rate of 95%, the adversary needs to collect 85.000 packets [32].

Countermeasures The attack abuses the fact that WEP uses the pre-shared key as input for the RC4 encryption algorithm. Researchers found weaknesses in the RC4 cipher that allow the recovery of the encryption key. Since WEP has been deprecated since 2004, our only advice would be to migrate to a more modern security protocol.

Tools The tool Aircrack-ng (section 4.2.1) can recover the WEP key once enough encrypted packets have been captured. It offers support for different Key-recovery attacks, and PTW is used as the default option.

[10] `http://wepcrack.sourceforge.net/`

3.4.4 WPS Brute-force Attack

On networks that have WPS enabled, devices can join the network by entering an eight-digit number. In 2011, Viehböck [33] described a design flaw in the communication between the client and the access point, making a brute-force attack feasible for an adversary. Once the adversary succeeds in recovering the PIN, the PSK will be sent in the communication, resulting in the adversary to learn the WPA/WPA2 pre-shared key.

The first design flaw is that when entering the static 8-digit PIN printed on the label of your router on to the device you are connecting, there is no other form of authentication, which is potentially vulnerable to brute-force attacks. Since the PIN is made up of 8-digits, there are 10^8 (=100.000.000) possible combinations, potentially taking months to years to guess.

However, Viehböck found a second design flaw that allows the adversary to determine whether parts of the PIN are correct. The client splits the PIN into two halves and verifies these with the access point. This allows an adversary to verify the 4-digits and the last 4-digits independently. Since the last digit is used as a checksum, the possible PIN combinations are reduced to $10^4 + 10^3$ (=11.000).

Experiments by the author showed that one PIN guess usually takes between 0.5 and 3 seconds to complete. Some manufacturers of access points did not implement any mechanism that prevented an unlimited number of guesses. These design flaws allow an adversary to try all combinations in less than four hours, thus recovering the WPA/WPA2 pre-shared key.

Countermeasures The combination of both design flaws makes a brute-force attack feasible for an adversary. Manufacturers should address the vulnerability by implementing a lock-down period after a few incorrect attempts. However, since access points are often running for a long time, a determined adversary may still succeed in recovering the PIN. The advice for affected network administrators is to disable WPS, as it is deemed insecure and replaced by a newer standard.

Tools The most popular tools that implement a brute-force attack against WPS are Bully[11] and Reaver[12].

3.4.5 Dictionary Attack

When a network uses WPA-Personal or WPA2-Personal, the pre-shared key is used as the Pairwise Master Key (PMK) for the 4-way handshake between the client and the access point. The pre-shared key can be a 256-bit number or a passphrase between 8 and 63 bytes long. During the handshake, the Pairwise Transient Key (PTK) key is created to encrypt traffic, making it impossible for the adversary to derive the PMK from cracking encrypted data packets sent between the client and the access point.

Passive

In 2003, Moskowitz published an online article [34] describing an offline attack against the 4-way handshake itself. In order to perform the attack, the adversary needs to be close to the network and capture one 4-way handshake between a client and the access point. The adversary can wait for new clients to associate with the network or send deauthentication packets (3.6.2) to force clients to reconnect.

[11] `https://github.com/aanarchyy/bully`

[12] `https://github.com/t6x/reaver-wps-fork-t6x`

During the handshake, the client and the access point both sent each other a plaintext nonce, and later a MIC over that nonce, to prove they know the PMK. An adversary can abuse this plaintext nonce and MIC to see if he can guess the pre-shared key. In 2015, researchers analyzed real-world handshakes and concluded that 68% of the handshakes in their experiment were crackable using passwords candidate rules like numbers, phone numbers, and birthday formats [35].

Active (client)

When the adversary is not near the access point or cannot intercept the handshake from connected clients, he can attempt to launch an active attack against a client. The adversary starts by launching a malicious Evil Twin network that appears to be the target network. Upon connecting, the client device attempts to authenticate, using the 4-way handshake. Since the adversary does not know the pre-shared key, it is unable to complete the handshake. However, collecting half of the handshake, as provided by the connecting client, is enough to perform an offline brute-force attack against the pre-shared key [36, 37].

Countermeasures Since the Dictionary attack relies on the pre-shared key's complexity, the stronger the passphrase, the more secure the network will be. The 802.11i standard recommends a passphrase of at least 20 characters to make it unpractical for an adversary to recover the plaintext.

WPA3-Personal uses a new handshake called Simultaneous Authentication of Equals (SAE), which derives a common PMK between the client and the access point. Since the common PMK is not based on the pre-shared key, it is resistant to offline dictionary attacks [14].

Tools Several auditing tools, such as Aircrack-ng (section 4.2.1) and Airgeddon (section 4.2.2), are capable of capturing the 4-way handshake. Once the handshake is captured, the auditor can attempt to recover the pre-shared key. If the auditor has access to accelerated hardware, we recommend using the open-source tool Hashcat[13], as it is designed for recovering passwords offline. If the auditor does not have access to hardware, he could upload the captured handshake to one of the online cracking services to attempt to recover it. However, there is a risk that the cracked key is leaked to the public by using third party services.

3.4.6 EAP-GTC Downgrade Attack

Hoover and Snodgrass first announced the EAP-GTC Downgrade attack during their talk BYO-Disaster at Defcon [38]. This attack can recover Enterprise credentials by targeting client devices that support EAP Generic Token Card (EAP-GTC) as an authentication method. It is a variation of a general EAP downgrade attack in which the adversary tries to downgrade the authentication method to EAP-GTC as their first choice during the EAP negotiation process. EAP-GTC is an authentication method that supports the use of hardware tokens and one-time passwords with EAP-PEAP. The implementation is similar to PEAPv0/EAP-MSCHAPv2; however, it does not have a peer challenge.

For this attack, the adversary sets up an Evil Twin network for a known Enterprise network. Then, the adversary proceeds by suggesting EAP-GTC during the EAP negotiation with every client that attempts to connect with the network. Often wireless profile configuration on client devices does not specify the type of password authentication used; therefore, one can be suggested from the server-side. If the client

[13] https://hashcat.net/hashcat/

accepts the suggested authentication method, it will either prompt the user to provide a one-time password or transmit the plaintext password automatically. Since many clients do not specify the kind of password that is required, users might believe they are prompted for their network credentials. Since the method is intended for one-time passwords, the network credentials are then sent in plaintext to the adversary.

Countermeasures The attack relies on clients that support EAP-GTC; therefore, to mitigate this downgrade attack, users should disable weak EAP authentication methods on their devices. Within a corporate setting, administrators should disable EAP-GTC consistently across all devices in a centralized way. Suppose an organization still needs to use hardware tokens and one-time passwords to authenticate towards the Wi-Fi network. In that case, its users should be aware that their device asks for a token instead of their Enterprise credentials.

Tools The toolkit Eaphammer (section 4.2.3) is designed to perform directed Evil Twin attacks against Enterprise networks. It has support for downgrade attacks, including EAP-GTC, allowing the adversary to collect plaintext credentials.

3.4.7 PMKID Hash Dictionary Attack

Previously, we looked at the traditional Dictionary attack (section 3.4.5) that affects WPA and WPA2. Upon connecting with the network, a 4-way handshake is executed between the client and the access point. When an adversary is close to the network and can capture one of those handshakes, it can attempt to brute-force the captured MIC and recover the pre-shared key.

However, when there are no connected clients, the adversary is not able to capture the handshake. In 2018, Steube (author Hashcat) revealed a new attack method [39] that does not need the handshake to brute-force the pre-shared key. For the PMKID attack, the adversary still needs to be nearby the network; however, he can obtain the required material by communicating with the access point.

The attack exploits the Robust Security Network (RSN) information that is part of the first EAPoL frame. This frame is received during the authentication phase, right before the 4-way handshake [14]. Most modern routers with roaming functions enabled append an optional field at the end of this frame containing the PMKID, an identifier used by the access point to keep track of the PMK used for one client. The PMKID is derived by taking a hash from the PMK, a static value, and the client's MAC address, and the access point's MAC address.

Since the static value and the involved MAC addresses are known to the adversary, he can abuse the PMKID hash to perform a brute-force attack against the PMK. The advantage of capturing the PMKID instead of the handshake is that the attack is faster; no need to wait for clients, and stealthier; no need to deauthenticate clients. Countermeasures include the same as for the Dictionary attack against a captured handshake: make sure to use a strong and complex passphrase.

Countermeasures The attack relies on an optional field that may or may not be present on an access point. However, network administrators should be aware that adversaries can obtain hashed key-material by capturing the 4-way handshake or the RSN IE field. Since the adversaries need to recover the pre-shared key using brute-force, the stronger the passphrase, the more secure the network will be. The 802.11i standard recommends a passphrase of at least 20 characters to make it unpractical for an adversary to recover the plaintext.

WPA3-Personal uses a new handshake called Simultaneous Authentication of Equals (SAE), which derives a common PMK between the client and the access point. Since the common PMK is not based on the pre-shared key, it is resistant to offline dictionary attacks [14].

Tools The tool Bettercap has the capabilities to discover networks and capture 4-way handshakes/PMKID hashes. After the hash is captured, the open open-source tool Hashcat can be used to perform a brute-force attack.

3.4.8 WPS Pixie Dust Attack

On networks that have WPS enabled, devices can join the network by entering an eight-digit number. In 2011, Viehböck described a design flaw in the communication between the client and the access point, making a brute-force attack feasible for an adversary (section 3.4.4). Most manufacturers of routers and access points have implemented protection against these kinds of brute-force attacks by locking requests after too many incorrect attempts.

In 2014, Bongard [40] described an offline brute-force attack against WPS that allows an adversary to crack the PIN in seconds. The author discovered that some access points use a weak method to generate the nonces that are supposed to be secret. To prove that the access point knows the PIN, it sends two hashes to the client during the exchange process, one for each part of the PIN. The hash's input is half of the PIN, a nonce, and the involved public keys. The client can obtain all the information that it needs by performing the protocol until the third message; now, it has possession of the hashes and the relevant public information. If the adversary can guess the nonces, it can also compute the PIN. And by recovering the PIN, the adversary can obtain the WPA/WPA2 pre-shared key of the network.

The ability to guess the nonces relies on the chipset that is used by the access point. Some chipsets use a static nonce or a weak random number generator. There is a spreadsheet[14] to determine whether a certain access point model used a chipset that is vulnerable for this attack. We should mention that this spreadsheet is not complete, and vulnerable access point models might be missing.

Countermeasures Manufacturers should address the vulnerability by using chipsets that use strong random number generators. The advice for affected network administrators is to disable WPS, as it is deemed insecure and replaced by a more modern standard.

Tools The most popular tools that implement a brute-force attack against WPS are Bully and Reaver. Both tools support the Pixie Dust attack by utilizing Pixiewps[15], which is an implementation of the attack.

3.4.9 Dragonblood Vulnerabilities

One of the supposed improvements of WPA3 over its predecessors is that it should be nearly impossible to crack the network's password. In April 2019, the researchers Vanhoef and Ronen analyzed [37] the Dragonfly

[14] `https://docs.google.com/spreadsheets/d/1tSlbqVQ59kGn8hgmwcPTHUECQ3o9YhXR91A_p7Nnj5Y/edit`

[15] `https://github.com/wiire-a/pixiewps`

handshake as used by WPA3, and discovered a group of vulnerabilities referred to as Dragonblood. Initially, they discovered five vulnerabilities; two downgrade attacks, two side-channel information leaks, and one denial of service attack. In August 2019[16], the researchers found two new vulnerabilities; one side-channel information leak and an information leak in the EAP-pwd protocol. In a downgrade attack, the adversary tried to force the client or access point into abandoning a more secure operation in favor of an older, less secure option that is typically offered to provide backward compatibility. After the adversary succeeds in getting the target to use the lesser secure method, it can abuse older flaws, potentially allowing the adversary to recover the password.

In a side-channel information leak attack, the adversary can trick the client or access point into using a weaker algorithm, which allows the adversary to obtain information about the key. By repeating this attack, the adversary may recover the full password. In this section, we will look at the attacks that can be used to recover the pre-shared key used to secure the wireless network.

Attack	**Objective**	**Interaction**
Downgrade Attack against WPA3-Transition 3.4.9.1	Partial 4-way handshake	Active (client)
Downgrade Attack against Security Group 3.4.9.2	Usage of weak security group	Active (MitM)
Timing-Based Side-Channel Attack 3.4.9.3	Eliminating password candidates	Active (access point)
Cache-Based Side-Channel Attack 3.4.9.4	Eliminating password candidates	Active (client)

Table 7: Overview of Dragonblood vulnerabilities in regarding to key-recovering

3.4.9.1 Downgrade Attack against WPA3-Transition

The WPA3 specifications describe a transition mode in which the network supports both WPA3-SAE supported clients, and WPA2-PSK supported clients to connect with the network using an identical password. This mode will allow older clients to use the network while gradually moving over to newer devices that are WPA3-capable. Not that this transition mode is only applicable for Personal networks, as WPA3-SAE replaces WPA2-PSK.

The adversary can exploit this feature by setting up an Evil Twin network and announcing its existence by sending out Beacon frames informing clients that the network only supports WPA2-PSK. When clients connect with the network, the adversary will collect the partial 4-way handshake, which gives him enough information to perform a Dictionary attack (section 3.4.5) and potentially recover the pre-shared key of the network.

[16] `https://wpa3.mathyvanhoef.com/`

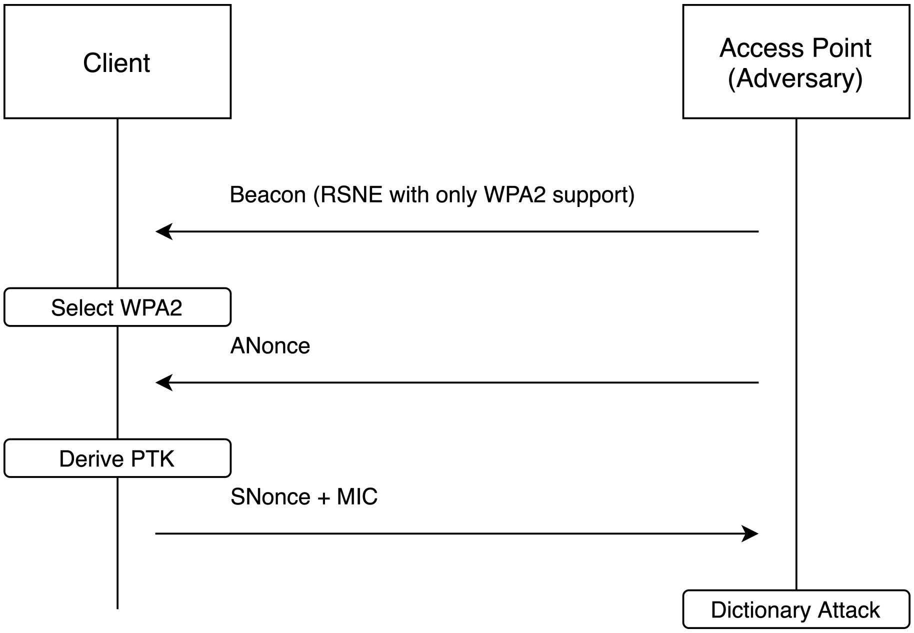

Figure 13: Dragonblood Downgrade attack against WPA3-Transition

The client can detect this downgrade attack during the handshake; however, it is already too late at that point; the adversary has collected enough material to use for an offline Dictionary attack (section 3.4.5). The research showed that some client implementation allow the client to connect with the WPA2 rogue access point, while the target network supports WPA3 only.

Countermeasures Since this attack does not exploit WPA3-SAE itself but relies on a transition mode, the most straightforward countermeasure for network administrators would be not to enable this mode. If an organization wants to transition to WPA3 gradually, it could choose to deploy two separate WPA2/WPA3 networks with a different pre-shared key. A measure that clients should implement is to store whether a known network supports WPA3, and if that is the case, do not allow a downgrade to WPA2.

3.4.9.2 Downgrade Attack against Security Group

The SAE handshake that is used for WPA3 supports different security groups, and the client and access point can negotiate the group to use. The client who starts the handshake sends a frame that includes the security group it wants to use. The access point will respond with a decline message if it does not support the specified group. The negotiation continues until the client and access point has found a security group they both supports.

However, an adversary can force the client and access point to use the weakest security group that they support by relaying messages between them (Man-in-the-Middle). The adversary blocks the Auth-Commit packets sent by the client from reaching the access point, and sends a response himself, denying the chosen security group until the adversary is satisfied with the weaker security group.

3.4.9.3 Timing-Based Side-Channel Attack

The researchers discovered that the time it takes for an access point to respond to commit frames might leak information about the pre-shared key. When the access point uses certain multiplicative groups (22, 23, or 24), the algorithm that encodes the pre-shared key takes on a variable number of iterations. The amount of iterations depends on the pre-shared key and the MAC address of the client and the access point. An adversary can try to determine the number of iterations by measuring the amount of time it took for the access point to respond. After that, the adversary can simulate how long it would take to process a password candidate and eliminate candidates until a Dictionary attack (section 3.4.5) becomes feasible.

3.4.9.4 Cache-Based Side-Channel Attack

The researchers demonstrated that one open-source implementation of SAE is vulnerable to a side-channel attack. In this exploit, the adversary runs code on the machine of the victim that is observing the memory during the handshake. This vulnerability allows the adversary to learn the number of loops in the algorithm that was required to find the secret point. Using the information, the adversary can rule out possible passwords, and after eliminating enough candidates, a Dictionary attack (section 3.4.5) becomes feasible. Since this attack exploits a specific implementation that has been patched already and requires code running on the client, we do not believe there are countermeasures the security auditor should take.

Tools The authors of the Dragonblood analysis made their tools available so that other researchers can replicate the results. However, the provided tools seem to be experimental and are missing documentation, making them not field-ready to be used by security auditors.

3.4.10 Conclusion

A Key-recovery attack is a type of attack where the adversary attempts to recover the pre-shared key or Enterprise credentials used to associate with a network. With the pre-shared key, the adversary can potentially decrypt traffic, launch an Evil Twin attack, and associate with the network.

Name	**Interaction**	**Efficiency**	**Year**
FMS Attack 3.4.1	Passive	4-6M packets →50%	2001
KoreK Attack 3.4.2	Passive	700k packets →50%	2004
PTW Attack 3.4.3	Active (access point)	35-40k packets →50% 85k packets →95%	2007

Table 8: Efficiency of the Key-recovery attacks against the WEP protocol

When looking at Table 6, we can see a shift in the technique used by these attacks over time. WEP uses the RC4 stream cipher, which exposes vulnerabilities that allow an adversary to recover the key. At first, the attacks were passive from nature, collecting encrypted packets, and applying statistical analysis. Later, researchers found that injection attacks can increase the amount of (encrypted) traffic transmitted by the access point, allowing a faster collection of packets for analysis. The efficiency column in Table 8 tells us how many packets an adversary needs to collect on average to reach a certain success probability of recovering the WEP key. Starting from WPA, the pre-shared key is no longer used to encrypt traffic directly, therefore making statistical analysis infeasible.

Most of the Key-recovery attacks, such as those against the WEP protocol, WPS, and the Dictionary attacks, aim to recover the pre-shared key of a Personal network. Since there are more modern replacements for WEP, WPA, and WPS, we can only recommend users not to use it in their network setup. The brute-force attacks against WPA/WPA2 (section 3.4.5 and 3.4.7) are powerful from the adversaries perspective, as they are executed offline after intercepting a few packets. However, since both attacks rely on the pre-shared key's complexity, we can only recommend administrators to configure a strong passphrase. WPA3-Personal uses a new handshake called Simultaneous Authentication of Equals (SAE), which derives a common PMK between the client and the access point. Since the common PMK is not based on the pre-shared key, it is resistant to offline Dictionary attacks.

Since most organizations use Enterprise networks, the EAP-GTC Downgrade attack (section 3.4.6) has the most potential for an adversary. If successful, it is a powerful attack, as it tries to trick devices into giving up plaintext credentials. The authors did not mention whether WPA3 would be vulnerable as the attack was discovered in 2013 already. However, it is apparent that EAP downgrade attacks still work when exploitable authentication methods, such as hardware tokens and one-time passwords, are not disabled on devices and suggested by the adversary. As for the Dragonblood attacks against WPA3 (section 3.4.9), we believe the downgrade attack has the most potential as it allows the adversary to apply some of the older WPA2 attacks. The side-channel attacks seem to be implementation-specific and can be solved by software updates.

3.5 Traffic Decryption

A Traffic Decryption attack is a type of attack where the adversary attempts to crack the encryption of a packet exchanged on a network. Breaking the encryption usually means that the adversary learns the plaintext of a packet, which breaches data confidentiality. While with other attacks, the adversary may recover encryption keys used for data integrity, allowing the adversary to spoof packets.

Protocol	Name	Interaction	Tools	Year
WEP	ChopChop Attack 3.5.1	Active (access point)	++	2004
WPA-*	Beck-Tews Attack 3.5.2	Active (client)	-	2008
WPA-*	Ohigashi-Morii Attack 3.5.3	Active (MitM)	None	2009
WPA-*	Michael Reset Attack 3.5.4	Active (client)	None	2010
WPA-*	Vanhoef–Piessens Attack 3.5.5	Active (client)	None	2013
WPA-*	NOMORE Attack 3.5.6	Active (client)	None	2015
WPA-* WPA2-*	KRACK Attack 3.5.7	Active (MitM)	-	2017

Table 9: Overview of Traffic Decryption attacks

3.5.1 ChopChop Attack

The ChopChop attack is implemented by another tool published by the anonymous user with the pseudonym KoreK. The attack exploits a weakness of the CRC32 checksum and the lack of protection against replaying messages. A successful attack does not recover the WEP key itself, but allows an adversary to reveal the plaintext without knowing the key [8].

Before a packet is encrypted, a CRC32 checksum is appended to the data of the packet. The adversary starts by listening for traffic and selects an encrypted packet he wants to decrypt. He truncates one byte from the end of the packet, resulting in that the message no longer passes the integrity checksum. Now, the adversary can attempt to brute-force the value of the truncated byte by reconstructing the message, and send it to the access point with a multicast destination address. Upon receiving, the access point decrypts the packet and verifies the integrity check. If the check passes, the message is broadcasted by the access point, allowing the adversary to learn if the guess was correct [41]. After recovering the last byte of the plaintext, the adversary continues this mechanism until he recovers the full plaintext.

Countermeasures The ChopChop attack exploits a weakness in the CRC32 checksum of the WEP security protocol. As WEP is longer considered secure, and deprecated since 2004, it should not be used anymore to protect a Wi-Fi network.

Tools The tool Aireplay-ng from the suite Aircrack-ng (section 4.2.1) is aimed at generating traffic that can be used by Aircrack-ng to recover WEP keys. The tool offers an implementation for the ChopChop attack. Another popular tool, Airgeddon (section 4.2.2), tries to automate the process of recovering WEP keys, and has built-in support for the ChopChop attack.

3.5.2 Beck-Tews Attack

Previously, we introduced the security protocol WPA (section 2.3.2), which used the TKIP protocol. This protocol offers a more sophisticated key-mixing function in comparison to WEP. This measure makes it harder for an adversary to find a correlation between the plaintext (which might be partially known), the ciphertext, and the encryption key. However, the researchers Back and Tews [18] discovered that, under the right circumstances, it is still possible to perform a ChopChop-like attack against WPA. After successfully performing the attack, the adversary has the MIC-key and a keystream for the access point to client communication. Recovering this material will allow the adversary to forge 3-7 packets to the client [42].

For this attack to work, the adversary needs to be able to capture packets exchanged between the access point and the client. Furthermore, the network must support the Quality of Service (QoS) enhancement and have a longer re-keying interval of at least 12 minutes.

The adversary starts with capturing an encrypted ARP request or response. Most parts of the plaintext are known to the adversary, except for the source and destination IP address, 8-byte MIC, and 4-byte ICV checksum. We assume that the adversary can guess most of the (local) IP addresses, and use a modified Chop-Chop attack to recover the MIC and ICV. If a guess was incorrect for the last byte, the packet is dropped by the client. However, when the last byte is correct, the client sends a MIC failure report frame to the access point. The adversary now has to wait 1 minute to prevent countermeasures by the access point, meaning that it will take around 12-15 minutes to recover the full 12-bit MIC and ICV [18, 42].

Countermeasures The authors discovered that it is still possible to perform a ChopChop-like attack against the WPA security protocol. As WPA and TKIP are no longer considered secure, and both deprecated since 2012, it should not be used anymore to protect a Wi-Fi network. If using a modern security protocol is not an option, then a short re-keying interval should be configured to prevent this attack. For example, in 2 minutes, an adversary can only decrypt 2 of the 12-bytes. Another option would be to disable MIC failure report frames, as the adversary would no longer be able to detect when its guess was successful.

Tools One of the authors, Martin Beck, is part of the team behind Aircrack-ng (section 4.2.1). He released a proof-of-concept implementation of their attack called Tkiptun-ng[17]

3.5.3 Ohigashi-Morii Attack

The Beck-Tews attack (section 3.5.2) has the requirement that the networks must support the Quality of Service (QoS) enhancement. The reason for this requirement is that the adversary needs to obtain an encrypted packet with an IV larger than the TSC value. In 2009, Ohigashi and Morii [43] improved the attack by applying it to a Man-in-the-Middle attack that works around this requirement.

The Ohigashi-Morii attack requires the adversary to sit between the client and the access point, allowing the replaying of packets. The adversary is receiving the packets as first, obtaining with it a higher IV value than the TSC value. The adversary proceeds by performing the ChopChop (section 3.5.1) attack before delivering the packet to ensure the TSC value is not yet increased by the receiver. Furthermore, the authors describe methods to lower the execution time of the attack to 1-4 minutes compared to 12 minutes for the original Beck-Tews attack.

Countermeasures The Ohigashi-Morii attack is an improvement on the Beck-Tews attack against WPA. Therefore, the same general advice applies: As WPA is no longer considered secure and has been deprecated since 2012, it should not be used anymore to protect a Wi-Fi network. If using WPA is required, then disabling the Quality of Service (QoS) enhancement helps to prevent this attack.

Tools The authors of the paper did not provide a demonstration of their attack or any tools that could help to implement the proposed scheme. Also, since the attack is targeted at an older security protocol, and relies on a specific enhancement, and an adversary needs to have Man-in-the-Middle capabilities, we do not foresee a high demand for this attack, especially since there exist more advanced attacks and tools when the adversary has Man-in-the-Middle capabilities.

3.5.4 Michael Reset Attack

In 2008, Beck and Tews found a way to reverse the Michael algorithm, allowing them to perform a ChopChop attack against WPA (section 3.5.2). In 2010, Beck found [44] a flaw in the Michael algorithm itself, allowing new packets to be created with a valid MIC. Based on the flaw, the author presents a scheme to decrypt all traffic sent to the client.

If the Michael algorithm reaches a point where the two internal key words have the same value as at the beginning when the Key was set, then the remaining bytes of the plaintext will have no influence on the calculated MIC value. An adversary would be able to inject plaintext in a packet, trigger a reset of the algorithm, and end up with the same correct MIC as before.

[17] `https://www.aircrack-ng.org/doku.php?id=tkiptun-ng`

The author proceeds with describing a scheme where the adversary first captures a packet and changes the content to be an IP/ICMP echo-request packet. The adversary set the destination address of the packet towards its own remote address. When the client responds to the echo, it will carry the same padding as that sent to the client, allowing the adversary to receive the packet's plaintext as meant for the client.

Countermeasures The requirements for this attack are tighter than the Beck-Tews attack, and the scheme seems rather complex. First, the network needs to support QoS and a longer re-keying interval. Second, the client must be connected with the internet and respond to ICMP requests, so that the adversary can receive the responses. The same countermeasures as for the original attack apply; configuring the re-keying time to a low value, such as two minutes.

Tools The author did not provide a demonstration of the attack in its paper. The proposed scheme has tight requirements and is rather complex to decrypt one single packet. There exist more effective methods for an adversary to obtain plaintext traffic, such as easy to execute Man-in-the-Middle attacks. Therefore, it seems only logical that none of the Wi-Fi auditing tools have implemented this attack.

3.5.5 Vanhoef–Piessens Attack

In 2010, Beck presented a scheme to decrypt traffic sent by the access point to one client (section 3.5.4). The adversary starts with capturing a packet, then abusing a flaw in the Michael algorithm to construct a new packet with a valid MIC. However, this packet is constructed as an ICMP request so that the victim will ping the adversary. The resulting frame is sent to the adversary, allowing the recovery of the plaintext.

In 2013, Vanhoef and Piessen [42] concluded that Becks' suggestion to use ICMP requests might not be successful, as it included a checksum over the header and data section. Since the full packet's plaintext is unknown to the adversary, he cannot calculate the correct checksum. The authors suggest constructing a UDP prefix, as specifying a checksum for this packet is optional. When a UDP packet is received on a closed port, the receiver sends an ICMP destination unreachable reply. On Windows, Linux, and Android, this reply contains a copy of the full UDP packet, allowing the adversary to recover the full plaintext. The attack can be prevented with the same countermeasures as the Beck-Tews attack (section 3.5.2).

Countermeasures As WPA and TKIP are no longer considered secure, and both deprecated since 2012, it should not be used anymore to protect a Wi-Fi network. Network administrators are advised to migrate to a more modern security protocol. The attack can be prevented with the same countermeasures as the Beck-Tews attack (section 3.5.2): configuring a short re-keying interval so that the adversary does not have enough time to decrypt the full 12-bytes key.

Tools In the paper, the authors claim to have created a proof of concept tool which demonstrates their attack. Once a vulnerable packet has been captured, the tool can construct the UDP prefix and apply the Michael reset attack. However, the authors do not seem to have released their tool to the public.

3.5.6 NOMORE Attack

In 2015, researchers from KU Leaven published a paper [45] describing new attacks against RC4 in TLS and WPA-TKIP. The attack against TKIP relies on its weak MIC and per-packet key construction, allowing the adversary to decrypt arbitrary packets.

The authors used statistical hypothesis tests to find new biases in the RC4 keystream. These biases allow an adversary to decrypt a complete packet and derive the MIC key within an hour. By injecting TCP packets and decrypting them, the success probability of recovering the MIC key increases significantly.

Countermeasures The authors describe how to exploit weaknesses in the RC4 encryption algorithm in both TKIP and TLS. In general, any protocol that uses the RC4 algorithm should be considered vulnerable to their attack. As WPA and TKIP are no longer considered secure, and both deprecated since 2012, it should not be used anymore to protect a Wi-Fi network. Network administrators are advised to migrate to a more modern security protocol.

Tools The authors did not release any tools that can be used to test for their attack. However, any protocol that uses the RC4 algorithm should be considered vulnerable.

3.5.7 KRACK Attack

Vanhoef and Piessens discovered KRACK (an acronym for Key Reinstallation Attack) in 2017. In their paper [46], they present a design flaw in the IEEE 802.11i 4-way handshake (see 2.3.2). This handshake is executed between the client and the access point upon connecting with a WPA or WPA2 network. During the handshake, both the client and the access point prove that they know the PMK and negotiate a fresh session key.

After receiving the third message of the handshake, the client will install the PTK and GTK. After the key is installed, it is used to encrypt packets using TKIP or CCMP, depending on the WPA version. However, since packets may be lost, the access point will retransmit the third message when it does not receive an appropriate response from the client. This means that a client may receive the third message multiple times, and with each time, it will reinstall the same key. When the key is reinstalled, the nonce and replay counter used by the data-confidentiality protocol is reset.

An adversary can abuse this behavior by acting as a Man-in-the-Middle and blocking the response from the client (fourth message), resulting in the access point to retransmit and the client to reinstall the keys. The impact of the attack depends on the data-confidentiality protocol that is used by the network. With both TKIP and CCMP, packets towards the client can be replayed, and packets sent by the client can be decrypted. In the case when TKIP is used, the MIC can be recovered, allowing the adversary to forge packets from the client.

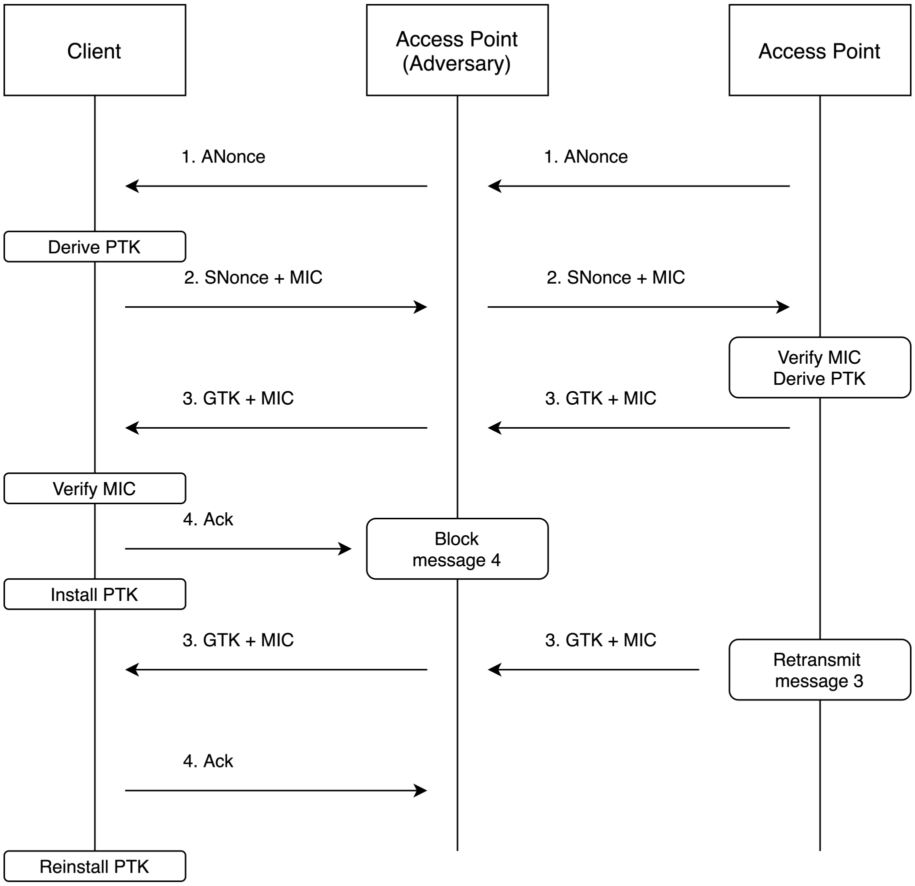

Figure 14: KRACK replay attack

Countermeasures Countermeasures against this attack include the client not resetting the nonce and replay counter when reinstalling a key and for the access point not resending Message 3. Luckily, implementations can often be patched by the manufacturer via a software update. That being said, administrators should ensure that clients on their network and the access points run the latest software version.

In their follow-up paper [47], Vanhoef explains that WPA3 uses the 4-way handshake, and therefore, implementations might be vulnerable to a key reinstallation attack. However, the Wi-Fi Alliance requires testing for this vulnerability during their certification process.

Tools The researcher published scripts[18] that can be used to test if a client or access point is affected by the KRACK attack. They also implemented a proof-of-concept that exploits the vulnerability for demonstration purposes, which is going to be released at a later moment.

3.5.8 Conclusion

A Traffic Decryption attack is a type of attack where the adversary attempts to crack the encryption of a packet exchanged on a Wi-Fi network. Breaking the encryption means that the adversary learns the plaintext of a packet, which breaches data confidentiality.

[18] `https://github.com/vanhoefm/krackattacks-scripts`

Almost all of the attacks against WPA with TKIP are based on two discoveries; the first is that the MIC key can be recovered, and the second is that a new packet can be constructed that passes the MIC verification. The combination of both discoveries leads to the capability of injecting traffic back into the Wi-Fi communication.

Some papers propose a scheme in which they use the traffic injection capability to recover a packet's plaintext. For example, the Michael attack (section 3.5.4 and the Vanhoef–Piessens attack (section 3.5.5) propose that the adversary prepend the packet in some way that it is relayed by the router back to the adversary in an unencrypted form. However, these proposed schemes are relatively complex to execute and inefficient, as each packet needs to be attacked individually.

3.6 Denial of Service

A Denial of Service (DoS) attack is a type of attack that aims to affect the availability of system resources to legitimate clients [22]. An adversary can take different approaches, targeting different layers of the OSI model. Since Wi-Fi communication relies on radio signals, an adversary can intentionally interfere with these radio signals (Physical layer). The adversary can also target the Data Link layer by transmitting spoofed packets to the access point. In our taxonomy, we focus on the second method because jamming a signal is a low-level attack. It would be more interesting to look over attacks that prevent or delay other clients from connecting with the access point.

Protocol	**Name**	**Interaction**	**Tools**	**Year**
-	Resource Exhaustion Attack 3.6.1	Active (access point)	++	-
WEP WPA-* WPA2-*	Deauthentication Flooding Attack 3.6.2	Active (access point)	++	-
WPA-*	TKIP Michael MIC failure 3.6.3	Active (access point)	++	2013
WPA3-*	Dragonfly Resource Exhaustion Attack 3.6.4	Active (access point)	+	2018

Table 10: Overview of Denial of Service attacks

3.6.1 Resource Exhaustion Attack

One method of making a system unavailable is by trying to consume as many resources as possible, exhausting the memory and processor capacity, making the access point unavailable to respond to requests from legitimate clients. The adversary can try to achieve such Denial of Service by flooding the access point with Probe requests, Authentication requests, and Association requests [48]. The access point will respond to those requests, as it may believe these packets originate from legitimate clients, causing an increase in processor and memory usage. If the adversary successfully exhausts all available resources, legitimate clients can no longer be served. In general, 250 frames per second is sufficient to make the access point stop servicing active TCP connections [49].

Countermeasures The researchers Singh and Sharma published a paper [49] listing different techniques that can detect or prevent Denial of Service attacks against Wi-Fi networks. Since the adversary is not abusing any flaw, but rather is spoofing packets as they appear to be originating from different clients, we should be looking at spoof detection. Most of the listed techniques, such as Radio Frequency Fingerprinting and introducing Sequence number based schema, are not interested in network administrators, as it is not something they can simply enable to protect their network. Organizations can deploy a Wireless Intrusion Detection System (WIDS) with capabilities to detect spoofed packets.

Tools Almost all well-known Wi-Fi auditing tools such as Aircrack-ng (section 4.2.1) and Airgeddon (section 4.2.2) have Denial of Service capabilities.

3.6.2 Deauthentication Flooding Attack

In 2000, Bidou published a paper [50] covering the history of and different in Denial of Service attacks and the various involved techniques. One of the methods described in the paper is the abuse of management frames spoofed by the adversary to disrupt Wi-Fi service for clients. We are not sure if this is the oldest paper describing this technique; however, it is one of the earliest to be published.

As introduced in section 2.2, management frames are used to establish and maintain a connection between clients and access points. As part of the authentication process, a client can request to de-authenticate from the network by sending the appropriate frame. Upon receiving, the access point terminates the session with the client, freeing up resources for other clients.

The fact that these management frames lack any form of authentication makes it suitable to perform a denial of service attack. The only requirement is that adversary is in the range of the access point the client is communicating with. The adversary proceeds by crafting a Deauthentication frame with the client's MAC address as the sender, and the MAC address of the access point as the receiver. After this, the adversary keeps sending this packet to the access point, resulting in the client being disconnected [50, 48].

Countermeasures Upon receiving a management frame, access points do not have a method to verify the sender's authenticity. In 2009, the Wi-Fi Alliance amended the IEEE 802.11w standard addressing this issue by introducing Protected Management Frames (PMF). This feature offers data confidentiality, integrity, origin authenticity, and replay protection for management frames. Our advice for network administrators is to enable this feature when supported by the access point. Also, network administrators are encouraged to migrate to the WPA3 security protocol, which requires this feature by default.

Tools Almost all well-known Wi-Fi auditing tools, such as Aircrack-ng (section 4.2.1) and Airgeddon (section 4.2.2) have Denial of Service capabilities.

3.6.3 TKIP Michael MIC failure

As introduced in section 3.5.2, the researchers Beck and Tews discovered that it is still possible to perform a ChopChop-like attack against WPA. For their attack to work, the adversary needs to wait 1 minute after a failed guess to prevent countermeasures. This precaution is necessary to prevent the access point from detecting the spoofed packets and deploying countermeasures. These countermeasures include the access point to force re-keying or deauthenticating the client. This countermeasure opens a Denial of Service vulnerability, as an adversary can easily send unsuccessful forgery attempts, shutting down the connection. All that is required for the adversary is to intercept a valid TKIP sequence counter, modify the MIC value, and transmit it every two minutes [49]. The researchers Vanhoef and Pierssen discovered that the same countermeasure could be triggered by abusing the Quality of Service (QoS) enhancements [42]. The MIC value calculated by the client seems to depend on the priority of the MSDU. An adversary could intercept one valid packet and retransmit it with a different priority, resulting in the MIC verification's failure.

Countermeasures In a presentation by Harkins, he argues that TKIP's countermeasure should be re-evaluated, since it is unnecessary to cease communication with all connected clients. Instead, he recommends that only the association under attack should be subject to a short delay and re-keying [51, 52]. However, this is not something network administrators can configure themselves, and should be implemented in the standard. Since WPA and TKIP have been deprecated, we would advise network administrators to migrate to a more modern security protocol.

Tools The Wi-Fi auditing tool Airgeddon integrates with MDK4 to offer Denial of Service attack capabilities. One of the included modes allows the auditor to trigger the MIC verification countermeasures on TKIP access points.

3.6.4 Dragonfly Resource Exhaustion Attack

The Dragonfly handshake starts with one party sending a commit frame to the other. It is computationally expensive to generate a response for this frame due to the defenses against side-channel attacks. During the hash-to-curve method, at least 40 iterations are performed to mitigate timing attacks. If Dragonfly with Brainpool curves are used, then at least 80 iterations are performed. An adversary can overload an access point by transmitting as little as 16 commit frames per seconds [37]. This may slow down the functionality of the access point and prevent or delay other clients from connecting with the access point using WPA3.

Countermeasures As a remedy for draining resources, the authors suggest using a more efficient hash-to-curve method such as Icart, SWU, or S-SWU. Another countermeasure could be implementing a low-priority background thread for processing commit frames to ensure that it will not affect the overall performance.

Tools The authors of Dragonblood published a tool called Dragondrain[19], which can be used to verify whether an access point is vulnerable to their discovered Denial of Service attack.

3.6.5 Conclusion

A Denial of Service (DoS) attack is a type of attack that aims to affect the availability of system resources to legitimate users. An adversary can take different approaches when performing a Denial of Service attack, targeting a separate layer of the OSI model. The adversary may target the Physical layer by jamming the radio frequencies or targeting the Data Link layer by spoofing packets. In the taxonomy, we focus on the latter because it is more interesting to know whether a network is open to a specific vulnerability that may lead to a Denial of Service.

When looking at the different kinds of Denial of Service attacks, we can see that there is a category that tries to exhaust the access point resources (section 3.6.1, 3.6.2, and 3.6.4). Experiments from researchers

[19] `https://github.com/vanhoefm/dragondrain-and-time`

have shown that spoofing 250 deauthentication frames per second is sufficient to make the access point stop servicing active TCP connections. However, with current hardware, the actual number may be a little higher. Different research has shown that spoofing as few as 16 commit frames per second may overload a WPA3 access point.

A different category of this attack type tries to reach a Denial of Service by triggering something more efficient than overloading the router with traffic and exhausting its resources. For example, TKIP employs countermeasures when it detects spoofed packets, dropping all connections for 60 seconds. An adversary can abuse this countermeasure by triggering it on purpose, causing a Denial of Service (section 3.6.3). This exploit is far more efficient than overloading the access point, as the adversary only needs to broadcast a single packet every minute.

4 Wi-Fi Pentester Framework

In the previous chapter, we constructed a comprehensive overview of Wi-Fi attacks, along with their countermeasures and recommendations for tools (section 3). In this chapter, we look at the gathered information from the viewpoint of a security professional. It's interesting to note that we can differentiate between different roles:

- **Security Auditor**: A security auditor is someone working for or hired by the company to provide an audit of systems used by the company. After completing the audit, the auditor delivers a detailed report outlining recommendations for improving the level of security. For this purpose, the auditor does not need to act as a malicious adversary, as it is sufficient to know that a certain vulnerability or risk exists.
- **Pentester**: A pentester is someone working for or hired by the company to perform a simulated cyberattack on their computer systems to evaluate the system's security. The pentester goes a step further than the auditor and actually exploits the vulnerabilities to understand the potential impact better. The pentester can use the same techniques and tools a malicious adversary would use within the exercise's scope.

The difference between both roles is that the pentester can act as a malicious adversary using the same techniques and tools. This chapter will focus on the last role, as it has the most expansive capabilities. In section 4.1, we go over the different security protocols and provide an overview of Wi-Fi attacks that target a specific protocol. In section 4.2, we compare and provide information on some of the popular Wi-Fi auditing tools. Also, we discuss the current state of support for auditing WPA3 networks by the tools.

Related work on Pentester Framework

In this section, we have a look at relating theoretical work regarding frameworks for pentesters.

- In 2015, Coll [53] published his Master's thesis on performing a penetration test on devices connected to a Wi-Fi 802.11 ac network. The thesis describes the generic phases during a penetration test: reconnaissance, scanning, exploitation, and post-exploitation. After this, the author looked into activities that fit in the defined stage and tools to help with the execution.
- In 2017, Esser [36] published his Master's thesis on exploiting client-side vulnerabilities using his Evil-Twin framework. Most Wi-Fi-capable devices actively scan for available networks and automatically connect when they are known to the device. This feature poses the risk of unknowingly connecting to a malicious access point. His thesis's goal was to raise awareness about client-side vulnerabilities and provide tools for the pentester to identify and showcase them. In contrast to our paper, Esser focuses on client-side vulnerabilities, for example, by capturing handshakes and attacking client devices. Our paper covers broader set of attack types by targeting both client and access point, and the communication between them. Esser's result is a framework that builds on top of well-known auditing tools, while we focus on steps for the pentester and make references to the tools.

- In 2018, Kohlios and Hayajneh [14] proposed an attacker framework against Wi-Fi networks by creating an overview of attacks against WPA2. The framework consists of four phases, in which an attacker can gain more access or capabilities over time using different methods. In the first phase, the attacker has no advantages and has not gained any access so far. In the second phase, the attacker has already acquired the network's pre-shared key or has access to the wireless network. The third phase begins when the attacker can either capture packets or be in a Man-in-the-Middle position. The fourth phase starts after the attacker has hijacked the session or the client. The paper describes techniques the attacker may use to achieve a certain state in their framework, for example, an Evil-Twin attack. However, the paper does not detail different kinds of Evil-Twin attacks, or what tools an attacker could use. Furthermore, the authors discussed to what extent WPA3 networks are vulnerable to the framework they described.

4.1 Steps for Pentester

The starting point is to figure out what security configuration a network is using. Networks broadcast Beacon frames that contain information about the network's capabilities and configuration, such as encryption details (section 2.2). Wireless auditing tools can scan for available Wi-Fi networks and display network related details, such as the security protocol, the security mode, and the cipher used by the network. These details aid a pentester to narrow down potential Wi-Fi attacks.

Table 11 provides an overview of attacks targeting WEP and WPA, and Table 12 covers attacks targeting WPA2 and WPA3. In both tables, the attacks are grouped by the targeted security protocol and attack type. The tables contain the same features and information as collected in the taxonomy. For more context on the features, see Appendix C. In this chapter, the columns on tools represent whether tools are available to target the specific security protocol.

In this section, we go over the different security protocols and guide the pentester. As we can see from comparing both tables, there is a large overlap between WPA and WPA2. The main difference is the existence of several Key-recovery attacks targeting WPA. As we concluded before, Traffic Decryption attacks are complex and lack the availability of tools. We only cover WPA2 and WPA3, as there is an overlap with WPA, and WEP has been deprecated for many years. We assume that the pentester aims to collect credentials or associate with the target network to expand the overall attack surface. In contrast with the attacker framework of Kohlios and Hayajneh [14], we focus on different methods to achieve this goal. Further steps after gaining the aimed capabilities are out of the scope of our pentester framework.

Protocol	Type	Interaction	Name	Tools
WEP	Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	++
		Active (MitM)	Hole196 Vulnerability 3.3.5	None
	Key-recovery	Passive	FMS Attack 3.4.1	++
		Passive	KoreK Attack 3.4.2	++
		Active (access point)	PTW Attack 3.4.3	++
	Traffic Decryption	Active (access point)	ChopChop Attack 3.5.1	++
	Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
		Active (access point)	Deauthentication Flooding Attack 3.6.2	++
WPA-Personal	Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	++
		Active (MitM)	Hole196 Vulnerability 3.3.5	None
	Key-recovery	Passive / Active	Dictionary Attack 3.4.5	++
		Active (access point)	WPS Brute-force Attack 3.4.4	++
		Active (access point)	WPS Pixie Dust Attack 3.4.8	++
		Active (access point)	PMKID Hash Dictionary Attack 3.4.7	++
	Traffic Decryption	Active (client)	Beck-Tews Attack 3.5.2	-
		Active (MitM)	Ohigashi-Morii Attack 3.5.3	None
		Active (client)	Michael Reset Attack 3.5.4	None
		Active (client)	Vanhoef–Piessens Attack 3.5.5	None
		Active (client)	NOMORE Attack 3.5.6	None
		Active (MitM)	KRACK Attack 3.5.7	-
	Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
		Active (access point)	Resource Exhaustion Attack 3.6.1	++
		Active (access point)	TKIP Michael MIC failure 3.6.3	++
WPA-Enterprise	Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	++
		Active (MitM)	EAP-PEAP Relay Attack 3.3.2	++
		Active (MitM)	Hole196 Vulnerability 3.3.5	None
	Key-recovery	Active (client)	EAP-GTC Downgrade Attack 3.4.6	++
	Traffic Decryption	Active (client)	Beck-Tews Attack 3.5.2	-
		Active (MitM)	Ohigashi-Morii Attack 3.5.3	None
		Active (client)	Michael Reset Attack 3.5.4	None
		Active (client)	Vanhoef–Piessens Attack 3.5.5	None
		Active (client)	NOMORE Attack 3.5.6	None
		Active (MitM)	KRACK Attack 3.5.7	-
	Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
		Active (access point)	Deauthentication Flooding Attack 3.6.2	++
		Active (access point)	TKIP Michael MIC failure 3.6.3	++

Table 11: Overview Wi-Fi attacks targeting WEP and WPA

Protocol	Type	Interaction	Name	Tools
WPA2-Personal	Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	++
		Active (MitM)	Hole196 Vulnerability 3.3.5	None
	Key-recovery	Passive / Active	Dictionary Attack 3.4.5	++
		Active (access point)	WPS Brute-force Attack 3.4.4	++
		Active (access point)	WPS Pixie Dust Attack 3.4.8	++
		Active (access point)	PMKID Hash Dictionary Attack 3.4.7	++
	Traffic Decryption	Active (MitM)	KRACK Attack 3.5.7	-
	Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
		Active (access point)	Deauthentication Flooding Attack 3.6.2	++
WPA2-Enterprise	Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	++
		Active (MitM)	EAP-PEAP Relay Attack 3.3.2	++
		Active (MitM)	Hole196 Vulnerability 3.3.5	None
	Key-recovery	Active (client)	EAP-GTC Downgrade Attack 3.4.6	++
	Traffic Decryption	Active (MitM)	KRACK Attack 3.5.7	-
	Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
		Active (access point)	Deauthentication Flooding Attack 3.6.2	++
WPA3-Personal	Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	None
	Key-recovery	Active (client)	Downgrade Attack against WPA3-Transition 3.4.9.1	None
		Active (MitM)	Downgrade Attack against Security Group 3.4.9.2	None
		Active (access point)	Timing-Based Side-Channel Attack 3.4.9.3	-
		Active (client)	Cache-Based Side-Channel Attack 3.4.9.4	-
	Traffic Decryption	None	None	None
	Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
		Active (access point)	Dragonfly Resource Exhaustion Attack 3.6.4	+
WPA3-Enterprise	Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	None
	Key-recovery	Active (client)	EAP-GTC Downgrade Attack 3.4.6	None
	Traffic Decryption	None	None	None
	Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
		Active (access point)	Dragonfly Resource Exhaustion Attack 3.6.4	+

Table 12: Overview Wi-Fi attacks targeting WPA2 and WPA3

4.1.1 WPA2-Personal

This section provides guidance on attacks and tools covered in the taxonomy that can be used against WPA2-Personal networks. Table 13 provides an overview of attacks targeting WPA2-Personal, grouped by their attack type.

Type	Interaction	Name	Tools
Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	++
	Active (MitM)	Hole196 Vulnerability 3.3.5	None
Key-recovery	Passive / Active	Dictionary Attack 3.4.5	++
	Active (access point)	WPS Brute-force Attack 3.4.4	++
	Active (access point)	WPS Pixie Dust Attack 3.4.8	++
	Active (access point)	PMKID Hash Dictionary Attack 3.4.7	++
Traffic Decryption	Active (MitM)	KRACK Attack 3.5.7	-
Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
	Active (access point)	Deauthentication Flooding Attack 3.6.2	++

Table 13: Overview Wi-Fi attacks targeting WPA2-Personal

In Figure 15, we provide a flowchart of steps to target a WPA2-Personal network. As stated before, we assume that the pentester aims to collect the pre-shared key or associate with the target network to expand his capabilities. This flowchart refers to applicable Wi-Fi attacks from the taxonomy and discusses why a certain attack should be used.

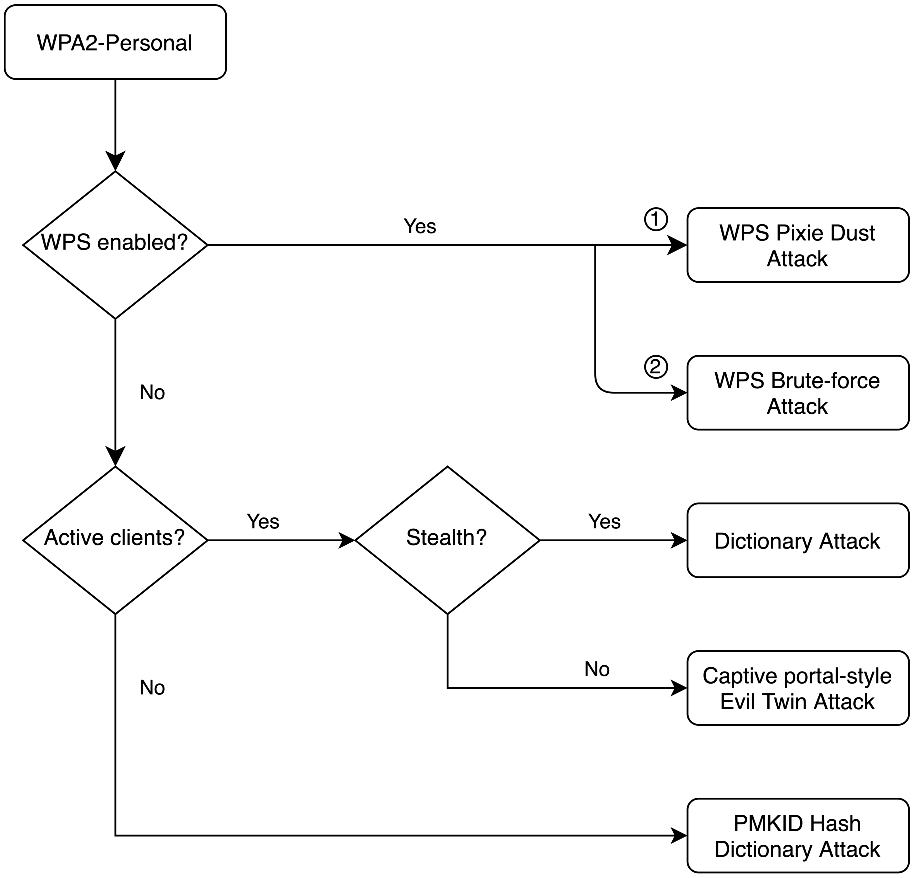

Figure 15: Attack flow diagram for WPA2-Personal

1. The Wi-Fi Protected Setup (WPS) feature of WPA2-Personal makes it easier to connect new devices to a wireless network. If the network uses WPS, it might allow the pentester to recover the PIN relatively quickly. Once the WPS PIN is recovered, it can be used to obtain the WPA2 pre-shared key.

   (a) **WPS Pixie Dust Attack**: Depending on the access point's chipset, it may be using a weak method to generate nonces. If the nonces are guessable, the PIN can be computed easily. This attack is potent, as it allows for the recovery of the PIN in a couple of seconds (section 3.4.8).

   (b) **WPS Brute-force Attack**: If the chipset is not vulnerable, the pentester can still attempt to brute-force all PIN combinations in less than 4 hours (section 3.4.4).

   The most popular tools to perform WPS attacks are Bully and Reaver, both of which are incorporated in the auditing tool Airgeddon (section 4.2.2).

2. The next consideration is whether the network has active clients connected to it. If this is the case, we can try to attack the clients or the transmitted traffic to recover the WPA2 pre-shared key.

   (a) **Evil Twin Attack**: In a captive portal-style Evil Twin attack, we set up an open network with the same SSID as the target network. To convince users to connect with our malicious network, we can deauthenticate them from the legitimate network (section 3.6.2). Upon connecting with the malicious Evil Twin network, the user is shown a portal requesting him to provide the network's pre-shared key (section 3.3.1). Note that this kind of Wi-Fi attack may draw attention, as users may distrust the portal asking for their credentials. As shown in Table 17, almost all Wi-Fi auditing tools have support for launching an Evil-Twin attack. We can recommend using Airgeddon (section 4.2.2) as it automates the whole process of launching the attack.

(b) **Dictionary Attack**: On a WPA2 network, the pre-shared key is used as the PMK for the 4-way handshake between the client and the access point. After capturing one handshake, we can attempt to brute-force the WPA2 pre-shared key offline without any other interaction (section 3.4.5).

3. **PMKID Hash Dictionary Attack**: Most modern routers with roaming functions enabled append an optional field at the end of the first EAPoL frame containing the PMKID. The PMKID is an identifier used by the access point to keep track of the PMK used for one client. If the network does not have active clients, we can still recover the WPA2 pre-shared key if the access point exposes this optional field. After capturing the EAPoL frame, we can attempt to brute-force the WPA2 pre-shared key offline without any other interaction (section 3.4.7).

4.1.2 WPA2-Enterprise

This section provides guidance on attacks and tools covered in the taxonomy that can be used against WPA2-Enterprise networks. Table 14 provides an overview of attacks targeting WPA2-Enterprise, grouped by their attack type.

Type	**Interaction**	**Name**	**Tools**
Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	++
	Active (MitM)	EAP-PEAP Relay Attack 3.3.2	++
	Active (MitM)	Hole196 Vulnerability 3.3.5	None
Key-recovery	Active (client)	EAP-GTC Downgrade Attack 3.4.6	++
Traffic Decryption	Active (MitM)	KRACK Attack 3.5.7	-
Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
	Active (access point)	Deauthentication Flooding Attack 3.6.2	++

Table 14: Overview Wi-Fi attacks targeting WPA2-Enterprise

In Figure 16, we provide a flowchart of steps to target a WPA2-Enterprise network. As stated before, we assume that the pentester aims to collect Enterprise credentials or associate with the target network to expand the overall attack surface. This flowchart refers to applicable Wi-Fi attacks from the taxonomy and discusses why a certain attack should be used. All of the attacks targeting WPA2-Enterprise require active clients, as the attacks rely on tricking devices or users into giving their credentials.

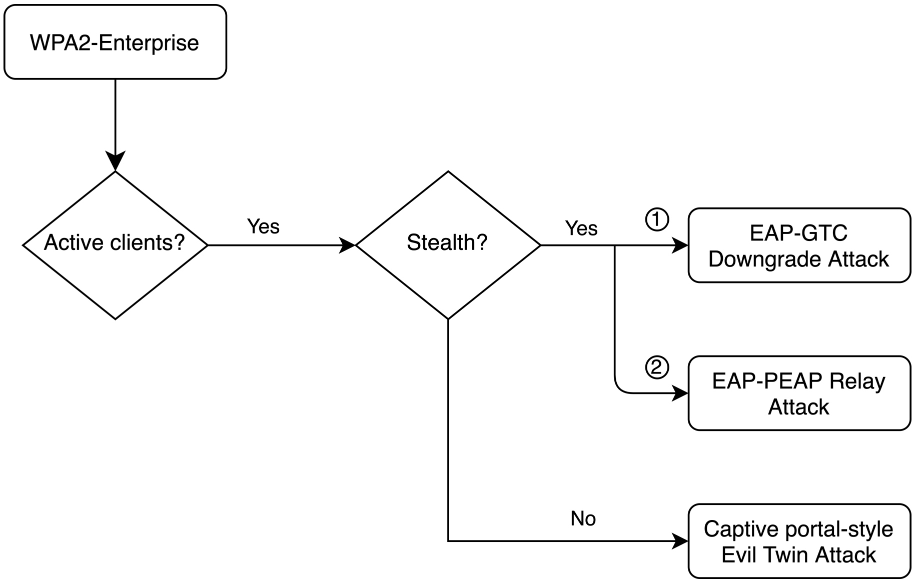

Figure 16: Attack flow diagram for WPA2-Enterprise

1. **EAP-GTC Downgrade Attack**: The EAP-GTC Downgrade attack can recover enterprise credentials by downgrading the authentication method during the EAP negotiation. The attack starts by setting up an Evil Twin network for the target network using Generic Token Card (EAP-GTC) as the prefered authentication method. Upon connecting with the network, the device will prompt the user to provide their (one-time) password to authenticate with the network. Some improperly configured devices may even share the Enterprise credentials automatically. Since the method is intended for one-time passwords, the credentials are sent in plaintext (section 3.4.6). We would recommend trying this attack first, as it is a relatively easy method to obtain the plaintext credentials. The toolkit Eaphammer (section 4.2.3) is the only tool on our list that can execute this attack.

2. **Evil Twin Attack**: In a captive portal-style Evil Twin attack, we set up an open network with the same SSID as the target network. To convince users to connect with our malicious network, we can deauthenticate them from the legitimate network (section 3.6.2). Upon connecting with the malicious Evil Twin network, the user is shown a portal asking him to provide his Enterprise credentials (section 3.3.1). This kind of Wi-Fi attack may draw attention, as users may distrust the portal requiesting for their credentials and notify the network administrators. As shown in Table 17, almost all Wi-Fi auditing tools have support for launching an Evil-Twin attack. We can recommend using Airgeddon (section 4.2.2), as it automates the whole process of launching the attack.

3. **EAP-PEAP Relay Attack**: With the EAP-PEAP Relay attack, an adversary can act as a middleman and relay an authentication attempt (usually challenge-response) between a connecting client and the legitimate authentication server. The first step would be to launch an Evil Twin network and trick a user into connecting with it. If successful, the legitimate RADIUS server will allow us to connect to the targeted network instead of the client (section 3.3.2). This attack will not recover plaintext Enterprise credentials, but access to the Wi-Fi network allows other opportunities. The patch Hostapd-mana (section 4.2.5) is the only tool on our list with support for the EAP-PEAP Relay attack.

4.1.3 WPA3-Personal

This section provides guidance on attacks and tools covered in the taxonomy that can be used against WPA3-Personal networks. Table 15 provides an overview of attacks targeting WPA3-Personal, grouped by their attack type. As we can see from the table, there is a lack of tools capable of auditing WPA3 networks. The lack of support does not mean that it is currently impossible to launch an Evil Twin attack, for example. The pentester has to manually set up a malicious network or wait until auditing tools are made available or updated.

Type	**Interaction**	**Name**	**Tools**
Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	None
Key-recovery	Active (client)	Downgrade Attack against WPA3-Transition 3.4.9.1	None
	Active (MitM)	Downgrade Attack against Security Group 3.4.9.2	None
	Active (access point)	Timing-Based Side-Channel Attack 3.4.9.3	-
	Active (client)	Cache-Based Side-Channel Attack 3.4.9.4	-
Traffic Decryption	None	None	None
Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
	Active (access point)	Dragonfly Resource Exhaustion Attack 3.6.4	+

Table 15: Overview Wi-Fi attacks targeting WPA3-Personal

In Figure 17, we provide a flowchart of steps to target a WPA3-Personal network. As stated before, we assume that the pentester aims to collect the pre-shared key or associate with the target network to expand the overall attack surface. This flowchart aims to refer to applicable Wi-Fi attacks from the taxonomy and discuss why a certain attack should be used. For the flowchart, we assume that tools are present to execute a certain attack.

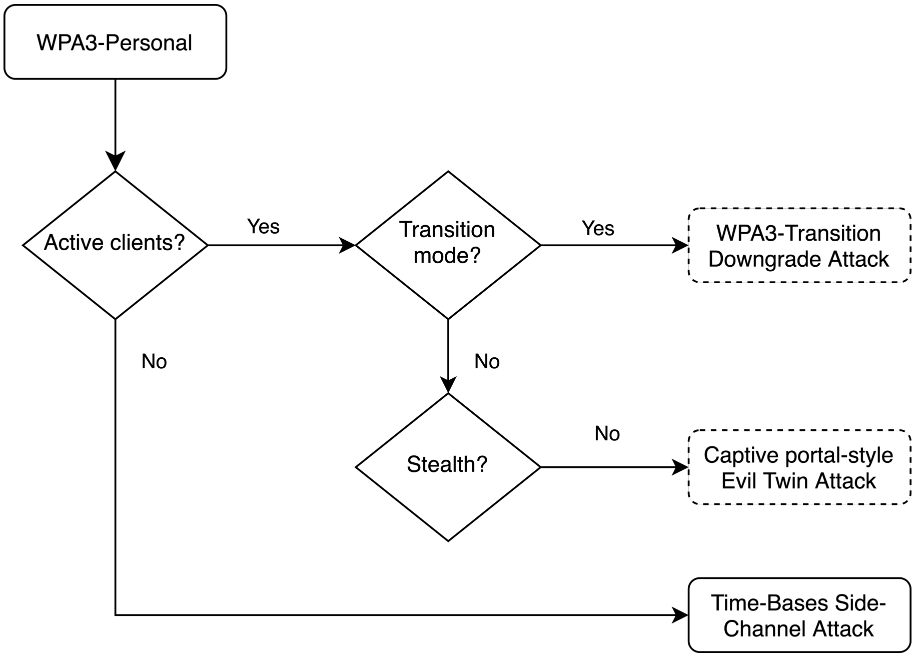
WPA3-Personal
Active clients?
Yes
Transition mode?
Yes
WPA3-Transition Downgrade Attack
No
No
Stealth?
No
Captive portal-style Evil Twin Attack
Time-Bases Side-Channel Attack

Figure 17: Attack flow diagram for WPA3-Personal

1. The first consideration is whether the network has active clients connected to it. If this is the case, we can try to attack the clients to recover the WPA3 pre-shared key.

   (a) **Evil Twin Attack**: In a captive portal-style Evil Twin attack, we set up an open network with the same SSID as the target network. Unfortunately, with WPA3, it is not possible to deauthenticate clients from the legitimate network, as the Protected Management Frames (PMF) feature is required by default. Upon connecting with the malicious Evil Twin network, the user is shown a portal requesting him to provide the network's pre-shared key (section 3.3.1). Note that this kind of Wi-Fi attack may draw attention, as users may distrust the portal asking for their credentials. At this moment, there is no tool available capable of executing an Evil Twin attack for a WPA3 network.

   (b) **Downgrade Attack against WPA3-Transition**: WPA3 comes with a transition mode in which both WPA3 and WPA2-supported clients to connect with the network using an identical pre-shared key. We can exploit this feature by setting up a malicious Evil Twin network and announcing that the network only supports WPA2-PSK. When a client connects with the network, we collect the partial 4-way handshake, which allows an offline brute-force attack against the pre-shared key (section 3.4.9.1). The authors of the Dragonblood paper did not release tools to execute this attack.

2. **Timing-Based Side-Channel Attack**: Depending on the multiplicative group used by the SAE handshake, the time the access point takes to respond to commit frames may leak information about the pre-shared key. We can attempt to guess the number of iterations it takes to encode the pre-shared. We can use this number to eliminate candidates until a Dictionary attack (section 3.4.5) becomes feasible (section 3.4.9.3). The authors of the Dragonblood paper released a proof-of-concept tool for this attack.

4.1.4 WPA3-Enterprise

This section provides guidance on attacks and tools covered in the taxonomy that can be used against WPA3-Enterprise networks. Table 16 provides an overview of attacks targeting WPA3-Enterprise, grouped by their attack type. As we can see from the table, there is a lack of tools capable of auditing WPA3 networks. The lack of support does not mean that it is impossible to launch an Evil Twin attack, for example. The pentester has to manually set up a malicious network or wait until auditing tools are made available or updated.

Type	Interaction	Name	Tools
Man-in-the-Middle	Active (client)	Evil Twin Attack 3.3.1	None
Key-recovery	Active (client)	EAP-GTC Downgrade Attack 3.4.6	None
Traffic Decryption	None	None	None
Denial of Service	Active (access point)	Resource Exhaustion Attack 3.6.1	++
	Active (access point)	Dragonfly Resource Exhaustion Attack 3.6.4	+

Table 16: Overview Wi-Fi attacks targeting WPA3-Enterprise

In Figure 18, we provide a flowchart of steps to target a WPA3-Enterprise network. As stated earlier, we assume that the pentester aims to collect Enterprise credentials or associate with the target network to expand the overall attack surface. This flowchart aims to refer to applicable Wi-Fi attacks from the taxonomy and discuss why a certain attack should be used. For the flowchart, we assume that tools are present to execute a certain attack.

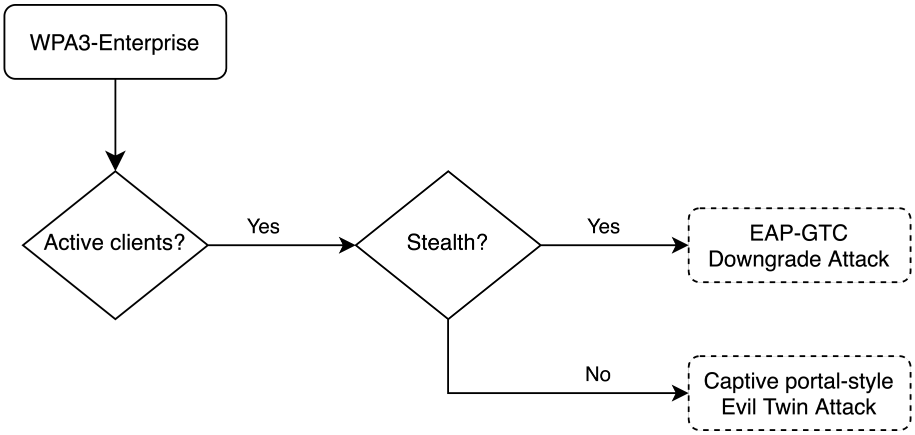

Figure 18: Attack flow diagram for WPA3-Enterprise

1. **EAP-GTC Downgrade Attack**: The EAP-GTC Downgrade attack can recover enterprise credentials by downgrading the authentication method during the EAP negotiation. The attack starts by setting up an Evil Twin network for the target network and suggests Generic Token Card (EAP-GTC) as the authentication method. Upon connecting with the network, the device will prompt the user to provide their (one-time) password to authenticate with the network. Some improperly configured devices may even share the Enterprise credentials automatically. Since the method is intended for one-time passwords, the credentials are sent in plaintext (section 3.4.6). At the moment, there are no

tools that implement this attack for WPA3 networks.

2. **Evil Twin Attack**: In a captive portal-style Evil Twin attack, we set up an open network with the same SSID as the target network. To convince users to connect with our malicious network, we can deauthenticate them from the legitimate network (section 3.6.2). Upon connecting with the malicious Evil Twin network, the user is shown a portal requesting him to provide his Enterprise credentials (section 3.3.1). This kind of Wi-Fi attack may draw attention, as users may distrust the portal asking for their credentials and notify the network administrators. At the moment, there are no tools that implement this attack for WPA3 networks.

4.2 Tools

In this section, we discuss the differences and functionality of several Wi-Fi auditing tools. On websites like Github, there exist a large number of repositories containing scripts, often not actively maintained. It can be hard to get a clear overview of the available tools; therefore, we only focused on more popular tools, capable of launching several attacks.

In Table 17, we give an overview of popular auditing tools that implement a certain attack part of our taxonomy. We understand that there is an overlap in functionality between the tools, as some tools have the same purpose and have implemented similar attacks. However, it is still interesting to include similar tools, as the pentester may be more familiar with one of them. Later, we describe the purpose and capabilities of each tool in more detail.

WPA3 Support When looking at the most popular auditing tools, there are none with proper support for auditing WPA3 networks.

- **Aircrack-ng**: Starting from version 1.6, Airodump-ng, can detect WPA3 networks. Airodump-ng can be used to capture packets, for example, with the goal of capturing an WPA2/WPA3 handshake. However, since SAE is resistant to offline brute-force attacks, capturing the handshake is not useful. Other tools in the suite do not seem to have support for WPA3 at the moment.

- **Airgeddon**: Airgeddon can detect WPA3 networks and capture packets, as it is using Aircrack-ng under the hood. However, since SAE is resistant to offline brute-force attacks, capturing the handshake is not useful. Airgeddon is currently not supporting WPA3, due to the lack of hardware support for testing purposes[20].

- **Eaphammer**: Eaphammer uses Hostapd with support for WPA3. However, the team reports that support has not been integrated with the rest of the project[21].

- **Wifiphisher**: Eaphammer uses Hostapd, however, it is unknown if it has support for WPA3. None of the wiki-pages or issues mention anything about WPA3.

- **Hostapd**: Starting from version 2.7, Hostapd has added support for the new SAE handshake. Therefore, we would be able to set up a malicious WPA3 network manually. However, both of the patches are not updated yet, and therefore do not work with WPA3 networks at the moment.

[20] https://github.com/v1s1t0r1sh3r3/airgeddon/issues/274

[21] https://github.com/s0lst1c3/eaphammer/pull/91

Type	**Attack**	**Aircrack-ng**	**Airgeddon**	**Eaphammer**	**Wifiphisher**	**Hostapd**
Man-in-the-Middle	Evil Twin Attack 3.3.1	Yes	Yes	Yes	Yes	Yes
	KARMA Attack 3.3.3	-	-	Yes	Yes	-
	EAP-PEAP Relay Attack 3.3.2	-	-	-	-	Yes
	MANA Attack 3.3.4	-	-	-	-	Yes
	Hole196 Vulnerability 3.3.5	-	-	-	-	-
	Lure10 Attack 3.3.6	-	-	-	-	-
	Known Beacon Attack 3.3.7	-	-	Yes	Yes	-
Key-recovery	FMS Attack 3.4.1	Yes	Yes	-	-	-
	Dictionary Attack 3.4.5	Yes	Yes	Yes	Yes	Yes
	KoreK Attack 3.4.2	Yes	-	-	-	-
	PTW Attack 3.4.3	Yes	-	-	-	-
	WPS Brute-force Attack 3.4.4	-	Yes	-	-	-
	EAP-GTC Downgrade Attack 3.4.6	-	-	Yes	-	-
	WPS Pixie Dust Attack 3.4.8	-	Yes	-	-	-
	PMKID Hash Dictionary Attack 3.4.7	Yes	Yes	Yes	-	-
	Dragonblood Vulnerabilities 3.4.9	-	-	-	-	-
Traffic Decryption	ChopChop Attack 3.5.1	Yes	Yes	-	-	-
	Beck-Tews Attack 3.5.2	Yes	-	-	-	-
	Ohigashi-Morii Attack 3.5.3	-	-	-	-	-
	Michael Reset Attack 3.5.4	-	-	-	-	-
	Vanhoef–Piessens Attack 3.5.5	-	-	-	-	-
	NOMORE Attack 3.5.6	-	-	-	-	-
	KRACK Attack 3.5.7	-	-	-	-	-
DoS	Resource Exhaustion Attack 3.6.1	-	Yes	-	-	-
	Deauthentication Flooding Attack 3.6.2	Yes	Yes	-	-	-
	TKIP Michael MIC failure 3.6.3	-	Yes	-	-	-
	Dragonfly Resource Exhaustion Attack 3.6.4	-	-	-	-	-

Table 17: Overview of the support of Wi-Fi attacks by the most popular auditing tools

4.2.1 Aircrack-ng

Aircrack-ng[22] is one of the best-known suites for assessing the security of Wi-Fi networks. The suite is available for Linux, FreeBSD, OpenBSD, macOS, and Windows. It requires a network card whose drivers support monitor mode and packet injection. Monitor mode allows the suite to monitor all traffic on the wireless channel, including packets intended for other devices. Packet injection refers to the capability to send constructed packets with a different MAC address so that they appear to be originating from a different

[22] `https://www.aircrack-ng.org/`

Wi-Fi device.

The suite consists of around 15 different tools, focusing on different areas of Wi-Fi security;

- Monitoring: Capture packets for further processing.
- Attacking: Allow the security auditor to audit the security of wireless clients or access points.
- Testing: Verify whether Wi-Fi cards and drivers possess packet capture and injection capabilities.
- Cracking: Allow the security auditor to crack WEP and WPA/WPA2 pre-shared keys.

Monitor Airodump-ng is a tool in the suite that can be used as a packet sniffer; it can capture raw 802.11 frames. Recently, support for WPA3 was added so that Airodump-ng can collect packets from networks that are using any of the currently available security protocols. The main purpose is to collect and filter packets, which then can be exported in different formats for processing with other tools. For example, the collected WEP packets with their IV's can be processed by Aircrack-ng to crack the WEP key. By connecting a GPS receiver to the computer, Airodump-ng can also be used during wardriving to log observed networks and coordinates.

Attack Airodump-ng is a tool in the suite aimed at attacking Wi-Fi clients by setting up a malicious access point and encouraging clients to associate with it. The tool Aireplay-ng can be used to deauthenticate clients from the legitimate network by sending disassociation packets. Furthermore, Airbase-ng contains the Caffe Latte attack and Hirte attack for attacking clients on a WEP network.

Testing The tool Aireplay-ng can test attack capabilities. When you attach two different wireless network cards that support monitor mode, it uses one of the wireless interfaces mimicking an access point and the other as the adversary. After that, Aireplay-ng tests different attack scenarios and will tell you if the network card is suitable for performing a security audit.

Cracking Aircrack-ng is a tool in the suite that can recover the encryption key for WEP, WPA-Personal, and WPA2-Personal networks. For WEP networks, it can recover the key once enough encrypted packets have been collected using the FMS attack (section 3.4.1) or the PTW attack (section 3.4.3). For both WEP and WPA networks, the tool can capture the authentication handshake between a client and the access point and perform a Dictionary attack.

4.2.2 Airgeddon

The toolkit Airgeddon[23] is designed to perform a wide range of attacks against wireless access points and clients. One of its strengths is that it tries to automate the process by integrating different tools. Airgeddon is compatible with any Linux distribution and comes as a bash script or as a Docker container.

DoS Attack Airgeddon integrates with MDK4 and Aireplay-ng to offer Denial of Service attack capabilities. It can execute a deauthentication attack against clients, and it can flood a target with traffic in order to exhaust system resources.

[23] `https://github.com/v1s1t0r1sh3r3/airgeddon`

Evil Twin Attack The toolkit can launch a complete Evil Twin attack to gain a Man-in-the-Middle position on wireless clients. It can automate the whole process of selecting the target network, de-authenticating the clients, capturing handshakes, setting up the access point, providing a captive portal, and eavesdropping on traffic. Furthermore, it integrates with various other tools like sslstrip2, and BeEF, to gain more advanced attack capabilities, such as forcing clients to use an unencrypted HTTP connection and exploit client-side attack vectors.

Key Recovery Attack The toolkit offers an all-in-one attack to recover the key for WEP networks by combining different techniques: ChopChop (section 3.5.1), Caffe Latte, ARP Replay, Hirte, Fragmentation. Airgeddon integrates with Bully and Reaver to offer WPS attack capabilities. It can execute a brute-force attack, Pixie Dust attack (section 3.4.8), null PIN attack, and Known WPS PIN attack to recover the WPS key. For WPA and WPA2 networks, it can attempt to brute-force the pre-shared key after capturing the 4-way handshake first.

4.2.3 Eaphammer

The toolkit Eaphammer[24] is designed to perform Evil Twin attacks targeting WPA/WPA2-Enterprise networks, and it supports a wide range of EAP methods; EAP-PEAP, EAP-TTLS, EAP-MD5. The first step with Eaphammer would be to create a self-signed x.509 certificate and launch an Evil Twin network. Now we have to rely on clients that do not verify the presented certificate or users that blindly accept it by themselves. When clients connect with the network, EAP challenge and responses are logged and can be used to brute-force the RADIUS credentials. Another method supported by Eaphammer is to downgrade the authentication mechanism to a weaker type making it easier for the attacker to obtain credentials. Furthermore, Eaphammer can launch an Evil Twin attack showing a captive portal to convince users to disclose their credentials.

4.2.4 Wifiphisher

Wifiphisher[25] is a rogue Access Point framework for auditing wireless networks. It allows the security auditor to launch various Evil Twin attacks and gain a Man-in-the-Middle position. It has support for KARMA, Known Beacons, and Lure10 attacks. As the name of the tool might suggest, it can also be used to perform phishing attacks on connected clients to collect credentials. At the same time, Wifiphisher can forge deauthenticate packets to disconnect clients with the target network.

4.2.5 Hostapd

Hostapd is a software program that enables users to use their wireless network interface card to act as an 802.11 access point, including 802.1X/WPA/WPA2/EAP Authenticators. It is not designed for security professionals, as it has no attack capabilities. However, over time, developers have created patches for Hostapd that weaponize the access point capabilities.

[24] `https://github.com/s0lst1c3/eaphammer/`

[25] `https://wifiphisher.org/`

- FreeRADIUS-WPE[26] is technically not a patch of Hostapd; however, it is well known in the Wi-Fi auditing community, and it was deprecated in favor of the more modern Hostapd-patches. It is a patch for the open-source FreeRADIUS implementations, capable of logging credentials of various EAP authentication methods.
- Hostapd-wpe[27] was the first patch, and it replaces FreeRADIUS-WPE. It can facilitate access point impersonation attacks, where the adversary lures clients to connect with its malicious access point. Once connected, Hostapd-wpe will return an EAP-Success message, so the client believes it is connected to the target network. After having connected clients, the adversary can launch various attacks, such as redirecting DNS and eavesdrop on traffic or credentials.
- Hostapd-mana[28] is a more recent patch that supports newer KARMA attacks. It can track and deanonymize devices, collect credentials from Enterprise networks, and perform Man-in-the-Middle style attacks.

[26] https://github.com/brad-anton/freeradius-wpe/blob/master/README

[27] https://github.com/aircrack-ng/aircrack-ng/tree/master/patches/wpe/hostapd-wpe

[28] https://github.com/sensepost/hostapd-mana

5 Future work

In this chapter, we discuss future work that relates to our taxonomy or pentester framework.

- **Extend Taxonomy**: We started by defining the attack types and the features that we cover in the taxonomy. After that, we searched for papers describing Wi-Fi attacks and grouped the attacks in our taxonomy. There are several ways to extend the taxonomy.
  - **Include vulnerabilities in specific models**: We decided to only include attacks in our taxonomy that are applicable, regardless of the router model or firmware that is being used. It could be interesting to include vulnerabilities that only apply to specific models or firmware versions. Likely, the vulnerabilities will still fit in the defined attack types, as it may lead to the recovery of credentials or a Denial of Service, for example.
  - **Include more attacks**: Especially with WEP, we noticed that researchers are constantly finding new ways to make existing attacks more efficient. We did not include all of the evolution of attacks in our taxonomy, as our goal was to group different attacks, and WEP is not relevant enough anymore to cover extensively. It could still be interesting to extend the taxonomy with other existing attacks and newly discovered attacks.
- **Extend Pentester Framework**: We described steps for the pentester for WPA2 and WPA3, and provided information on the most popular auditing tools.
  - **Cover more capabilities**: We assume that the pentester aims to collect credentials or associate with the target network to expand the overall attack surface. Additional steps can extend the framework after the pentester has succeeded in recovering credentials. For example, the pentester can scan for vulnerable machines on the network, or attack other connected clients.
  - **Cover legacy security protocols**: We decided to limit our framework to WPA2 and WPA3, as the older security protocols are deprecated and outdated. However, it would still be interesting to cover these protocols in the attacker framework, as a pentester may be equipped with the task of auditing a legacy network.
  - **Cover more tools**: We decided to limit our information on auditing tools to the most popular ones. Of course, there are many other tools available. On websites like Github, there exists a large number of repositories containing scripts, often not actively maintained. It could be interesting to make a more comprehensive comparison between auditing tools. One starting point could be the Wifi-arsenal repository[29].
- **Implement Tools**: As mentioned in section 4.2, there is a lack of support for WPA3 among the popular Wi-Fi auditing tools. Only Hostapd supports WPA3, while the patches of the library are not updated yet. Some of the tools use Hostapd internally, however, they have not been officially tested against WPA3 networks. It would be interesting to verify whether tools support WPA3 already, or have it supported. It would be especially interesting for Evil Twin attacks, as cracking the exchanged handshakes is no longer feasible on WPA3 Personal networks.

[29] `https://github.com/0x90/wifi-arsenal`

6 Conclusion

In this chapter, we discuss the process of writing this thesis and list the conclusions we came to during our research.

Process

Gathering information on different Wi-Fi attacks from theoretical papers and creating an overview can be challenging. This is especially true when papers use varying terminology, different attack types have additional features, and there are various ways to define the types and structure the taxonomy.

At first, we combined Key-recovery and Traffic Decryption as Encryption Cracking with a feature that specified the adversaries' goal, for example, to recover the pre-shared key. However, while working on the taxonomy, we found out that the attacks only attempt to crack the network's pre-shared key or attempt to recover plaintext material (along with key material). To be complete, we should mention that some of the key recovery attacks against WEP are considered 'injection attacks', as the recovered key material can be used to spoof packets.

Another thing we struggled with was how to label the different Man-in-the-Middle attacks. At first, we differentiated between internal and external rogue access points. However, we left vulnerable access points out of scope, and some attacks were technically not involving rogue access points. It took us a few iterations to get the attack types defined and the taxonomy's structure set-up.

Initially, we planned an initial part of creating an overview of Wi-Fi attacks, while also reserving time to look into areas for further exploration. However, while working on the paper, we found out that it took more time than we first anticipated, as we wanted to be extensive.

Taxonomy

In chapter 3. Taxonomy of Wi-Fi Attacks, we constructed a comprehensive overview of Wi-Fi attacks along with their countermeasures and recommendations for tools.

From looking at the taxonomy table, we can see it is an interesting cat-and-mouse game, in which researchers try to develop new attacks and countermeasures using each other's work. For example, the first statistical Key-recovery attacks against WEP were passive in nature. Later, researchers found that injection attacks increase the amount of encrypted traffic transmitted by the access point, allowing a faster recovery (section 3.4). We can see the same happening with Evil Twin attacks and their variations, such as KARMA, MANA, Lure10, and Known Beacons. Some variations target all clients regardless of the network, and others try to get around countermeasures such as limited active probing.

- Man-in-the-Middle (section 3.3) is a type of attack where the adversary secretly relays communication between the client and the access point. We can conclude that Evil Twin attacks and their variations are versatile, as an adversary can launch them against almost any network and security configuration. The adversary can also use this type of attack with a different goal in mind, such as eavesdropping on traffic or tricking the user or its device to handover credentials. Another factor is that we often deal with varying devices with different implementations and security settings. An adversary only has to trick one of them to connect with its Evil Twin network and expose key material. WPA3 offers higher level protection for open networks by implementing a new feature called Opportunistic Wireless Encryption (OWE); this feature ensures that clients cannot eavesdrop on traffic for other devices.

- Key-recovery (section 3.4) is a type of attack where the adversary attempts to recover the pre-shared key used to associate with a network. We can conclude that the WEP protocol is the most vulnerable, as the RC4 cipher is broken. Starting from WPA, the pre-shared key is no longer used to encrypt traffic directly, therefore making statistical analysis infeasible. All attacks that target Personal networks secured with WPA or WPA2 uses some sort of brute-forcing the pre-shared key or the WPS PIN. To counter brute-force attacks, we can only recommend administrators to disable the WPS feature and choose a strong passphrase. WPA3-Personal replaces the authentication with Simultaneous Authentication of Equals (SAE), which is resistant to offline dictionary attacks.

- Traffic Decryption (section 3.5) is a type of attack where the adversary attempts to recover the plaintext of a packet. We can conclude that it is hard to perform such an attack for the adversary or pentester. Almost all papers propose a complicated scheme to recover the plaintext of an encrypted packet, and there is a lack of available tools.

- Denial of Service (section 3.6) is a type of attack that aims to affect the availability of system resources to legitimate clients. There exist two different types of DoS attacks; one that tries to exhaust the access point resources, and another tries to trigger some countermeasures preventing the access point from serving clients. The attack against TKIP is especially effective, as the adversary only needs to transmit one packet per two minutes.

Pentester Framework

In chapter 4. Wi-Fi Pentester Framework, we looked at the gathered information on Wi-Fi attacks from a pentester's viewpoint. The starting point for the pentester would be to figure out what security settings a network is using. We divided the chapter by the different security protocols and provided an overview of the applicable attacks.

On websites like Github, we can find repositories containing a large number of tools and scripts. Often, these repositories are not actively maintained and are outdated. So, within the Pentester Framework, we focused on the most popular Wi-Fi auditing tools.

When comparing Table 11 and Table 12, we can conclude that there is a large overlap between the attacks applicable to WPA and WPA2 networks. WPA is more vulnerable to attacks that attempt to recover the plaintext of a packet, due the use of the TKIP protocol. However, as it is complicated to execute Traffic Decryption attacks, there are no different steps for the pentester.

There are a lack of support for auditing WPA3 networks among popular tools. Some of the tools use Hostapd internally, which supports WPA3; however, the tools themselves have not been tested with WPA3 networks officially. It would be especially interesting for tools that can launch Evil Twin attacks to adopt support, as cracking the exchanged handshakes is no longer feasible. The lack of support does not mean that it is currently impossible to launch an Evil Twin attack against WPA3 networks, as the pentester can manually set up a malicious network.

Acronyms

AES Advanced Encryption Standard. 8, 11, 13, 14, 15

ARP Address Resolution Protocol. 19, 28, 29, 30, 31, 42, 65

BSS Basic Service Set. 5

BSSID Basic Service Set Identifier. 5, 19, 23

CCMP Counter Mode CBC-MAC Protocol. 8, 13, 14, 15, 45

EAP Extensible Authentication Protocol. 11, 16, 20, 22, 23, 25, 26, 32, 35, 36, 41, 58, 61, 65, 66, 72, 73

EAPoL Extensible Authentication Protocol over LAN. 36, 57

FS Forward Secrecy. 8

GCMP Galois/Counter Mode Protocol. 8, 15

GPS Global Positioning System. 64

GTK Group Transient Key. 11, 12, 28, 29, 45

HTTP Hypertext Transfer Protocol. 24, 65

ICMP Internet Control Message Protocol. 44

ICV Integrity Check Value. 42

IEEE Electrical and Electronics Engineers. 5, 7, 15, 45, 48

IP Internet Protocol. 42

IV Initialization Vector. 8, 9, 10, 11, 13, 32, 43, 64

MAC Media Access Control. 5, 10, 13, 19, 23, 27, 28, 36, 40, 48, 63

MIC Message Integrity Code. 8, 11, 12, 13, 14, 35, 36, 42, 43, 44, 45, 47, 48, 49

MSDU MAC Service Data Unit. 49

OSI Open Systems Interconnection. 20, 47, 49

OWE Opportunistic Wireless Encryption. 14, 31, 69

PEAP Protected Extensible Authentication Protocol. 16, 25, 26, 35, 58, 65, 72

PMF Protected Management Frames. 7, 8, 48, 60

PMK Pairwise Master Key. 11, 12, 16, 19, 34, 35, 36, 37, 41, 45, 57

PMKID Pairwise Master Key Identifier. 36, 37, 57

PSK Pre-shared key. 8, 11, 14, 15, 16, 20, 22, 32, 34, 38, 60, 73

PTK Pairwise Transient Key. 11, 28, 34, 45

QoS Quality of Service. 42, 43, 44, 49

RADIUS Remote Authentication Dial-In User Service. 15, 16, 25, 26, 58, 65

RC4 Rivest Cipher 4. 8, 9, 11, 13, 14, 18, 32, 33, 40, 44, 45, 69, 72

RSN Robust Security Network. 36

SAE Simultaneous Authentication of Equals. 14, 15, 35, 37, 38, 39, 40, 41, 60, 62, 69, 72

SSID Service Set Identifier. 5, 7, 12, 16, 19, 23, 24, 25, 26, 56, 58, 60, 62

TCP Transmission Control Protocol. 45, 47, 50

TKIP Temporal Key Integrity Protocol. 8, 11, 13, 14, 15, 18, 20, 42, 44, 45, 47, 48, 49, 50, 69

TLS Transport Layer Security. 16, 26, 44, 45

TSC Time Stamp Counter. 43

UDP User Datagram Protocol. 44

WEP Wired Equivalent Privacy. 1, 4, 6, 7, 8, 9, 10, 11, 13, 18, 19, 20, 22, 32, 33, 40, 41, 42, 47, 52, 53, 64, 65, 67, 68, 69, 72, 73

WIDS Wireless Intrusion Detection System. 25, 48

WLAN Wireless Local Area Network. 5

WPA Wi-Fi Protected Access. 1, 4, 6, 7, 8, 9, 11, 12, 13, 14, 15, 18, 19, 20, 22, 23, 28, 32, 34, 36, 37, 41, 42, 43, 44, 45, 47, 48, 49, 52, 53, 64, 65, 69, 72, 73

WPA2 Wi-Fi Protected Access II. 1, 4, 6, 8, 9, 11, 13, 14, 17, 20, 22, 23, 25, 28, 32, 34, 36, 37, 38, 39, 41, 45, 47, 52, 54, 55, 56, 57, 58, 60, 62, 64, 65, 67, 69, 72, 73

WPA3 Wi-Fi Protected Access III. 1, 4, 8, 9, 14, 15, 16, 17, 19, 20, 22, 23, 25, 31, 32, 35, 37, 38, 39, 41, 46, 47, 48, 49, 50, 51, 52, 54, 59, 60, 61, 62, 64, 67, 68, 69, 72, 73

WPS Wi-Fi Protected Setup. 17, 34, 37, 41, 56, 65, 69

Appendices

A List of Figures

B List of Tables

C List of Features of Wi-Fi Attacks

Protocol

Most attacks exploit a weakness that comes with the configuration of the network. In our taxonomy, we consider the following security protocols: WEP, WPA, WPA2, and WPA3. Some attacks may target Personal or Enterprise networks specifically. In our overview tables, we use a combination of the security protocol and the security mode. In the list below, we use WPA as an example, however, the same structure applies to the other security protocols.

- ***-***: The attack targets all considered security protocols WEP, WPA, WPA2, and WPA3 on both Personal and Enterprise networks.
- **WPA-***: The attack targets the WPA security protocol on both Personal and Enterprise networks.
- **WPA-Open**: The attack targets the WPA security protocol on open networks.
- **WPA-PSK**: The attack targets the WPA security protocol on Personal networks.
- **WPA-EAP**: The attack targets the WPA security protocol on Enterprise networks.

Interaction

Another feature that we consider is whether the adversary needs to interact with the network components to make its attack succeed. By interaction, we mean that the adversary has to transmit packets with one other party.

- **Passive**: The adversary does not need to interact with any clients or access points. However, the adversary might listen for broadcasted packets.
- **Active (client)**: The adversary interacts with the client device.
- **Active (access point)**: The adversary interacts with the access point.
- **Active (MitM)**: The adversary relays packets between the client and the access point.

Tools

Another feature we consider is whether tools are available for a security auditor to test if a network is vulnerable to an attack.

- **None**: To our knowledge, there are no tools available implementing the attack.
- **-**: There is a proof-of-concept available implementing the attack.
- +: There is a tool available for verifying whether a network is vulnerable for the attack.
- ++: There are multiple tools available for verifying whether a network is vulnerable for the attack or is included in a well-known suite.

References

[1] M. Gast, *802.11 Wireless Networks: The Definitive Guide*, ser. Definitive Guide Series. O'Reilly Media, 2005. [Online]. Available: https://books.google.com/books?id=9rHnRzzMHLIC

[2] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, Sep. 2016.

[3] A. Sari, M. Karay *et al.*, "Comparative analysis of wireless security protocols: WEP vs WPA," *International Journal of Communications, Network and System Sciences*, vol. 8, no. 12, p. 483, 2015.

[4] D. Hucaby, *CCNA Wireless 640-722 Official Cert Guide*, ser. Official Cert Guide Series. Cisco Press, 2014. [Online]. Available: https://books.google.com/books?id=TB7yAgAAQBAJ

[5] Institute of Electrical and Electronics Engineers, "802.11w-2009 - IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames," Institute of Electrical and Electronics Engineers, Tech. Rep., 2009. [Online]. Available: https://standards.ieee.org/standard/802_11w-2009.html

[6] P. Ebbecke, "Protected Management Frames enhance Wi-Fi® network security," 2020, https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security.

[7] Institute of Electrical and Electronics Engineers, "802.11i-2004 - IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) speci," Institute of Electrical and Electronics Engineers, Tech. Rep., 2004. [Online]. Available: https://standards.ieee.org/standard/802_11i-2004.html

[8] M. Caneill and J.-L. Gilis, "Attacks against the WiFi protocols," 2010, https://matthieu.io/dl/papers/wifi-attacks-wep-wpa.pdf.

[9] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11," in *Proceedings of the 7th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '01. New York, NY, USA: Association for Computing Machinery, 2001, p. 180–189. [Online]. Available: https://doi.org/10.1145/381677.381695

[10] Institute of Electrical and Electronics Engineers, "802.11-2012 - IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Spec," Institute of Electrical and Electronics Engineers, Tech. Rep., 2012. [Online]. Available: https://standards.ieee.org/standard/802_11-2012.html

[11] Arash Habibi Lashkari, Mir Mohammad Seyed Danesh, and B. Samadi, "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)," in *2009 2nd IEEE International Conference on Computer Science and Information Technology*, 2009, pp. 48–52.

[12] A. H. Adnan, M. Abdirazak, A. B. M. S. Sadi, T. Anam, S. Z. Khan, M. M. Rahman, and M. M. Omar, "A comparative study of WLAN security protocols: WPA, WPA2," in *2015 International Conference on Advances in Electrical Engineering (ICAEE)*, 2015, pp. 165–169.

[13] A. Bensky and a. O. M. C. Safari, *Short-range Wireless Communication, 3rd Edition.* Newnes, 2019. [Online]. Available: https://books.google.com/books?id=vK06zQEACAAJ

[14] C. Kohlios and T. Hayajneh, "A Comprehensive Attack Flow Model and Security Analysis for Wi-Fi and WPA3," *Electronics*, vol. 7, p. 284, 10 2018.

[15] W.-F. Alliance, "Wi-Fi CERTIFIED Wi-Fi Protected Setup™: Easing the User Experience for Home and Small Office Wi-Fi® Networks," 2014, https://www.wi-fi.org/downloads-registered-guest/wp_Wi-Fi_CERTIFIED_Wi-Fi_Protected_Setup_20140409.pdf/7670.

[16] A. Sadeghian, "Analysis of WPS Security in Wireless Access Points," in *6th International Conference on Security for Information Technology and Communications*, 2013.

[17] E. Tews, "Attacks on the WEP protocol," Cryptology ePrint Archive, Report 2007/471, 2007, https://eprint.iacr.org/2007/471.

[18] E. Tews and M. Beck, "Practical Attacks against WEP and WPA," in *Proceedings of the Second ACM Conference on Wireless Network Security*, ser. WiSec '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 79–86. [Online]. Available: https://doi.org/10.1145/1514274.1514286

[19] M. Ghering, "Evil Twin vulnerabilities in Wi-Fi networks," Bachelor Thesis, Radboud University, 2016. [Online]. Available: https://www.cs.ru.nl/bachelors-theses/2016/Matthias_Ghering___4395727___Evil_Twin_Vulnerabilities_in_Wi-Fi_Networks.pdf

[20] Norton, "Report of Online Survey Results in 15 Global Markets," 2017. [Online]. Available: https://www.nortonlifelock.com/about/newsroom/press-releases/2017/symantec_0709_01

[21] S. Vinjosh Reddy, K. Sai Ramani, K. Rijutha, S. Mohammad Ali, and C. Pradeep Reddy, "Wireless hacking - a WiFi hack by cracking WEP," in *2010 2nd International Conference on Education Technology and Computer*, vol. 1, Jun. 2010, pp. V1–189–V1–193.

[22] M. Hangargi, "Denial Of Service Attacks In Wireless Networks," Packet Storm Security, Tech. Rep., 2015. [Online]. Available: https://dl.packetstormsecurity.net/papers/wireless/DoS_attacks_in_wireless_networks.pdf

[23] P. Sharma, P. K. Kaushal, and P. R. Sharma, "Survey on Evil Twin Attack," *International Journal of Scientific Engineering and Research (IJSER)*, vol. 4, no. 4, pp. 54–58, 2015.

[24] R. Beyah and A. Venkataraman, "Rogue-Access-Point Detection: Challenges, Solutions, and Future Directions," *IEEE Security Privacy*, vol. 9, no. 5, pp. 56–61, Sep. 2011.

[25] A. Bartoli, "Understanding Server Authentication in WPA3 Enterprise," https://www.researchgate.net/publication/338792851. The paper is currently unpublished due to copyright issues.

[26] N. Asokan, V. Niemi, and K. Nyberg, “Man-in-the-middle in tunnelled authentication protocols,” in *International Workshop on Security Protocols.* Springer, 2003, pp. 28–41.

[27] P. Robyns, B. Bonné, P. Quax, and W. Lamotte, “Short paper: exploiting WPA2-enterprise vendor implementation weaknesses through challenge response oracles,” in *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, 2014, pp. 189–194.

[28] D. A. Dai Zovi and S. A. Macaulay, “Attacking automatic wireless network selection,” in *Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop*, Jun. 2005, pp. 365–372.

[29] A. Networks, “WPA2 Hole196 Vulnerability: Exploits and Remediation Strategies,” 2010, http://securedsolutions.com.my/pdf/WhitePapers/WPA2-Hole196-Vulnerability.pdf.

[30] S. R. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4,” in *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography*, ser. SAC ’01. Berlin, Heidelberg: Springer-Verlag, 2001, p. 1–24.

[31] R. Chaabouni, “Break WEP Faster with Statistical Analysis,” 2006, Semester Project. Responsible: Prof. Serge Vaudenay; Supervisor: Martin Vuagnoux. [Online]. Available: http://infoscience.epfl.ch/record/113785

[32] E. Tews, R.-P. Weinmann, and A. Pyshkin, “Breaking 104 Bit WEP in Less Than 60 Seconds,” in *Information Security Applications*, S. Kim, M. Yung, and H.-W. Lee, Eds. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 188–202.

[33] S. Viehböck, “Brute forcing Wi-Fi Protected Setup,” 2011, https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf.

[34] R. Moskowitz, “Weakness in Passphrase Choice in WPA Interface.” [Online]. Available: https://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html

[35] C. Chen and T. Chang, “The Cryptanalysis of WPA & WPA2 in the Rule-Based Brute Force Attack, an Advanced and Efficient Method,” in *2015 10th Asia Joint Conference on Information Security*, May 2015, pp. 37–41.

[36] A. Esser, “Evil-twin framework: a Wi-Fi intrusion testing framework for pentesters,” Master Thesis, ISCTE - Lisbon University Institute, 2017. [Online]. Available: https://repositorio.iscte-iul.pt/bitstream/10071/15151/1/evil-twin-framework%283%29.pdf

[37] M. Vanhoef and E. Ronen, “Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd,” in *IEEE Symposium on Security & Privacy (SP).* IEEE, 2020.

[38] J. Snodgrass and J. Hoover, “BYO-Disaster and Why Corporate Wireless Security Still Sucks,” Presentation at DEF CON, 2013, https://www.defcon.org/images/defcon-21/dc-21-presentations/djwishbone-PuNk1nPo0p/DEFCON-21-djwishbone-PuNk1nPo0p-BYO-Disaster-Updated.pdf.

[39] J. Steube, “New attack on WPA/WPA2 using PMKID,” 2018, https://hashcat.net/forum/thread-7717.html.

[40] D. Bongard, “Offline bruteforce attack on WiFi Protected Setup,” Presentation at Hack.lu, 2014, http://archive.hack.lu/2014/Hacklu2014_offline_bruteforce_attack_on_wps.pdf.

[41] M. Guennoun, A. Lbekkouri, A. Benamrane, M. Ben-Tahir, and K. El-Khatib, “Wireless networks security: Proof of chopchop attack,” in *2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks*, 2008, pp. 1–4.

[42] M. Vanhoef and F. Piessens, “Practical verification of WPA-TKIP vulnerabilities,” in *ASIA CCS 2013 - Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, 05 2013, pp. 427–436.

[43] T. Ohigashi and M. Morii, “A Practical Message Falsification Attack on WPA,” 2009, https://pdfs.semanticscholar.org/6718/9cd24091ea9f2322bd23699383b923fe13b0.pdf.

[44] M. Beck, “Enhanced TKIP Michael Attacks,” 2010, https://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf.

[45] M. Vanhoef and F. Piessens, “All Your Biases Belong to Us: Breaking RC4 in WPA-TKIP and TLS,” in *Proceedings of the 24th USENIX Conference on Security Symposium*, ser. SEC’15. USA: USENIX Association, 2015, p. 97–112.

[46] ——, “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’17. New York, NY, USA: ACM, 2017, p. 1313–1328. [Online]. Available: https://doi.org/10.1145/3133956.3134027

[47] ——, “Release the Kraken: new KRACKs in the 802.11 Standard,” in *Proceedings of the 25th ACM Conference on Computer and Communications Security (CCS)*. ACM, 2018.

[48] M. Hangargi, “Denial of service attacks in wireless networks,” 2015, https://dl.packetstormsecurity.net/papers/wireless/DoS_attacks_in_wireless_networks.pdf.

[49] R. Singh and T. P. Sharma, “On the ieee 802.11i security: a denial-of-service perspective,” *Security and Communication Networks*, vol. 8, no. 7, pp. 1378–1407, 2015. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/sec.1079

[50] R. Bidou, “Denial of service attacks,” 2000, https://pdfs.semanticscholar.org/cbf5/e7c51fee22d2fff2302321c424df8a648b02.pdf.

[51] D. Harkins, “Attacks against Michael and Their Countermeasures,” 2003, https://mentor.ieee.org/802.11/dcn/03/11-03-0211-00-000i-michael-attacks-and-countermeasures.ppt.

[52] S. Glass and V. Muthukkumarasamy, “A Study of the TKIP Cryptographic DoS Attack,” in *2007 15th IEEE International Conference on Networks*, 2007, pp. 59–65.

[53] F. Coll, “An augmented penetration testing framework for Mobile Devices on 802.11 ac Wireless Networks,” Master Thesis, Letterkenny Institute of Technology, 2015. [Online]. Available: https://research.thea.ie/handle/20.500.12065/1193