Computer Systems Department
Faculty of Computer and Information Sciences
Ain Shams University

A Methodology for WLAN Vulnerability Study

Thesis submitted as a partial fulfillment of the requirements for the degree of Master of Science in Computer and Information Sciences

By

Ahmed Ismail Mohamed Abdelrahman

Graduated from

Computer Systems Department, Faculty of Computer & Information Sciences, Ain Shams University 2012

Senior Embedded Software Engineer At Valeo.

Under Supervision of

Prof. Dr. Eman Shaaban

Computer Systems Department,

Faculty of Computer & Information Sciences,

Ain Shams University

Dr. Heba Khaled

Computer Systems Department,

Faculty of Computer & Information Sciences,

Ain Shams University

Acknowledgment

I would like to like to express my gratitude to my thesis supervisors , role models, technical experts and personal mentors: **Prof. Dr. Wail S. Elkilani**, **Prof. Dr. Eman Shaaban** and **Dr. Heba Khaled**. Honestly, without them I couldn't start my research path. I am more than lucky to work with their advice and support. Finally, I would thank my family for giving me the strength and power to finish this thesis.

Abstract

Nowadays, WPA/WPA2 is used for the authentication and encryptsion process of the most used WLANs. PSK mode is the dominant authentication mode for most of WLANs represented in small or non-professional networks. Cracking PSK password is discussed and implemented in many online tools and scientific papers with no clarification of links between the cracking process and WLAN standards. This thesis shows proficiency of all required aspects to cover that link's gap, and paves the way of proposing security and protection tools.

The thesis masters the related IEEE 802.11 MAC layer standards and the used protocols structures that relate to PSK authentication process. WLAN attacks are categorized to locate PSK cracking and define its related attacks and tools. Moreover the different used research platforms in PSK cracking are discussed like GPU, Multi Core CPU, FPGA and Cell BE.

To show WLAN Vulnerability, we used the acquired mastered knowledge to design and implement our PSK cracking tool "Vulnerability Research Study Tool" (VRST). VRST represents a unique edge through illustrating the relations between the cracking steps input and 802.11 standards. To the best of our knowledge, the previously research contributions didn't reveal the knowhow of extracting the cracking inputs from the raw exchanged data between the Access Point and the client.

To accelerate WPA/WPA2 PSK cracking, the single threaded VRST design and implementation is adapted to shared memory parallel platforms: GPU and Multi-Core. Performance results show that the cracking efficiency is upgraded to 16X by utilizing Multi-Core processor and to 41x by using GPU.s

List of Contents:

List of Figures:

List of Tables:

List of Abbreviations:

AES	Advanced Encryption Standard.
AKM	Authentication Key Management.
AP	Acces Point.
ARP	Address Resolution Protocol.
Bssid	Basic Service Set ID
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol.
DK	Derived Key
DoS	Denial of Service.
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
EAP-PSK	EAP Pre-Shared Key.
EAP-TLS	EAP Transport Layer Security
FPGA	Field Programmable Gate Array
HMAC	Hash Based Message Authentication Code
ISO	International Organization for Standardization
KCK	Key Confirmation Key
LEAP	Lightweight Extensible Authentication Protocol
LLC	Logical Link Control
MAC	Media Access Control
MD5	Message Digest Algorithm 5
MIC	Message Integrity Code
OSI	Open Systems Interconnection
PBKDF2	Password-Based Key Derivation Function 2
PFR	Pseudo Random Function.
PMK	Pairwise Master Key.
PSKs	Pre-Shared Key.
PTK	Pairwise Transient Key.
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service.
SHA1	Secure Hash Algorithm 1
SSID	Service Set Identification
VRST	Vulnerability Research Study Tool.
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access.

List of Publications:

1- A. Abdelrahman, H. Khaled, E.Shaaban, W.Elkilani, "WPA-WPA2 PSK Cracking Implementation on Parallel Platforms", IEEE International Conference on Computer Engineering and Systems, 2018.

2- A. Abdelrahman, H. Khaled, E.Shaaban W.Elkilani, “Detatiled Study of WLAN PSK Cracking Implementation", International Journal of Network Security. (Submitted)

Chapter 1

Introduction To WLAN 802.11

1.1 Introduction

As a matter of fact, Wireless Local Area Network (WLAN) is one of the most used networks types today because of its easy mobility access and it's compatibility with almost all the electronic devices in our daily life. We can find working WLANs anywhere and anytime just by searching for the available WLANs from any mobile or laptop. Because of the previous illustrated facts, WLAN security becomes a point of interest for a lot of research studies and even illegal hacking communities. This thesis studies all the related aspects of a vulnerability in the dominant authentication protocol for most of WLANs. In this chapter we are going to explore the standards around our research point "WLAN Vulnerability Study". Section 1.1 clarifies the main stack of networks standards "OSI Model" and it's relation with our research layer in IEEE 802.11. Then we dig more deep in the standards of WLAN IEEE 802.11 to get aware what's the related network layer part to our research in section 1.2. Section 1.3 previews the main important points of IEEE 802.11 History. Finally we put the spot on the main authentication modes in 1.4 and 1.5.

1.2 IEEE 802.11:

The International Organization for Standardization (ISO) is a global organization identifies the Open Systems Interconnection (OSI) model, which standardizes the communication stack of computer systems in the following seven layers. Application, Presentation, Session, Transport, Network, Data-Link and Physical layers [1]. Data Link layer is the point of interest in this thesis, It's divided to Logical Link Control (LLC) and Media Access Control (MAC) sub layers. IEEE 802.11 is a set of MAC and PHY specifications

and standards to establish WLANs [2]. Wi-Fi Alliance is a nonprofit organization of 600 member companies dedicated to promote the wireless technologies, certify WLAN products and to enhance the costumer awareness of the new 802.11 standards [3]. Regarding the PHY layer IEEE standards, Table1.1 shows the main PHY amendments with their frequencies and data rates.

Table 1.1 PHY Layer Amendments [3]

Wi-Fi technology	Frequency band	Maximum data rate
802.11a	5 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps
802.11n	2.4 GHz, 5 GHz, 2.4 or 5 GHz (selectable), or 2.4 and 5 GHz (concurrent)	450 Mbps
802.11ac	5 GHz	1.3 Gbps

Regarding the Mac Layer, the rest of this chapter declares more about its standards and the related amendments and protocols.

1.3 Data-Link Layer:

The 802.11 Data-Link layer is the same for all 802 based networks and divided into two sub layers. LLC is the top sub layer and MAC is the down sub layer. Some types of information are exchanged between MAC sub layer and the upper layers like quality of service (QOS). LLC is an adaptor between MAC layer and Network layer. When the data is sent from Network layer to Data-Link layer, the data is handled to the LLC and becomes known as MSDU (MAC Service Data Unit). When the data is sent from LLC to MAC layer, it's encapsulated inside MPDU (MAC Protocol Data Unit) or what is called 802.11 MAC frame as shown in

Figure 1.1. Only 802.11 Data type frame can carry LLC upper layer information [1].

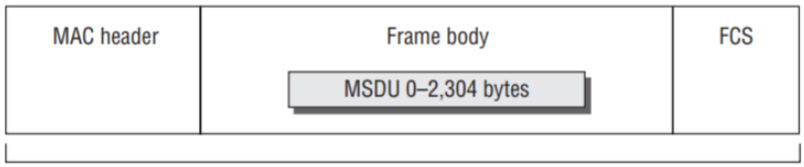

Figure 1.1 Mac Frame Structure

1.4 802.11 Security History:

The free mobility main advantage of WLAN became its main security risk because WLAN data is transmitted over open air frequencies unlike the wired networks. IEEE 802.11 standards guarantee two major components Encryption and Authentication. Encryption main goal is to secure the data privacy by making the transmitted data vague in the open access air by using cipher encryption technologies. Authentication is needed to identify the authorized user for accessing the WLAN and its resources. Authentication is based on verifying the credentials of the users like the user name and password. Table 1.2 illustrates the main Encryption and Authentication methodologies used in WLAN [4-6]. The following sections study and clarify the content of this table in details.