ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Wi-Fi Security and Test Bed Implementation for WEP and WPA Cracking

Dr.T.Pandikumar[1], Mohammed Ali Yesuf[2]
Associate Professor[1], M.Tech Student[2]
Department of Computer & IT
College of Engineering, Defense University, Debre Zeyit, Ethiopia

Abstract:
The purpose of this research work is the evaluation of the WEP/ WPA security algorithms for IEEE 802.11 and a penetration testing test bed. This study will include the analysis of the different encryption methods for standard WEP and WPA2. In addition, authentication methods of Open System and Shared Key and known vulnerabilities/ flaws of the algorithm will be presented in detail. Finally, it will present the evolution of the WEP and the 802.11i (WPA and WPA2) security protocol. As an outcome/ practical part of the research project, a presentation of the equipment, OS and the software used for the security penetration testing will be presented and a step by step guide of this procedure. The main focus of this research study is after reading and analyzing the practical parts to have a better understanding of, what security primitives or algorithms different WLAN security protocols use, how wireless communication channel is secured with different protocols, then how authentication is handled, how data is encrypted, and what are the benefits and vulnerabilities of each protocol.

Keywords: WPA2, IEEE 802.11i, IEEE 802.11X, WEP, WPA, TKIP, CCMP, WLAN, Security

1. INTRODUCTION

1.1 Background research

The modern way of living requires immediate and rapid access to information from the users, which are always on the move. This dynamic developed environment has created an increasing demand for simpler, better, effective and more economic solutions for local wireless access. With the term "local wireless access", we mean the access to a gateway which is already connected to a greater network Internet in order to take advantages of other services, like IP telephony, teleconference, data transfer, web serving etc. Many protocols have been developed over the years for the WLAN implementation, like Bluetooth IEEE 802.15, WiMAX 802.16 and IEEE 802.11. The last one is now the most widespread method for the WLAN access because combines, high data rates with the simplicity and the low cost equipment. According to the IEEE 802.11 standard on the basic characteristics are included:-

- The low cost
- The easiness to design and establish a WLAN
- The quality and high transmission data rates.

These characteristics are the main reasons, for the IEEE 802.11 protocol to be known as Wi-Fi, paraphrasing the Wireless Fidelity. IEEE 802.11 or Wi-Fi was firstly introduced back in the 1997 with two methods of transmission on the spread of the 2.4 GHz, which is an unlicensed band. The first method was the Frequency Hoping Spread Spectrum (FHSS) and offers data rate transmission up to one Mbps and the second method was the Direct Sequence Spread Spectrum (DSSS) with a data rate up to two Mbps on ideal conditions.

1I. LITEARTURE SURVEY

2.1 FHSS vs. DSSS in Broadband Wireless Access (BWA) and (WLAN):

2.1.1 Introduction:

Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in Broadband Wireless Access (BWA) and Wireless LAN (WLAN), a White Paper In 1997 IEEE defined the 802.11 Wireless LAN (WLAN) standard, intended to allow wireless connection of workstations to their "base" LAN. The original standard targeted the case in which both the workstation and the LAN were owned by the same entity, providing in fact a wireless extension to an existing, wired LAN. While this WLAN application represents a growing niche in the market, the technology on which it is based started to be used also for a new application, that of providing Broadband Wireless Access (BWA) to public networks. We are still connecting workstations to "base" LAN, but this time the "base" LAN is owned by a service provider (ISP, ITSP ,etc.) while the workstation is owned by a subscriber. [SCHWARTZ, 1997]

2.1.2 Spread Spectrum

The immediate effect of this elegant behavior is that Spread Spectrum systems may be operated without the need for license, and that made the Spread Spectrum modulation to be the chosen technology for license-free WLAN and BWA operation. However, as mentioned above, spread spectrum technologies have many other advantages, making them an excellent option for the operation of systems in licensed bands, too. There are two types of Spread Spectrum modulation techniques: Frequency Hopping (FHSS) and Direct Sequence (DSSS).

i) DSSS has the advantage of providing higher capacities than FHSS, but it is a very sensitive technology, influenced by

many environment factors (mainly reflections). The best way to minimize such influences is to use the technology in either (i) point to multipoint, short distances applications or (ii) long distance applications, but point-to-point topologies. In both cases, the systems can take advantage of the high capacity offered by DSSS technology, without paying the price of being disturbed by the effect of reflections. As so, typical DSSS applications include indoor wireless LAN in offices (i), building to building links (ii), Point of Presence (Pop) to Base Station links (in cellular deployment systems) (ii), etc.

ii) FHSS is a very robust technology, with little influence from noises, reflections, other radio stations or other environment factors. In addition, the number of simultaneously active systems in the same geographic area (collocated systems) is significantly higher than the equivalent number for DSSS systems. All these features make the FHSS technology the one to be selected for installations designed to cover big areas where a big number of collocated systems is required and where the use of directional antennas in order to minimize environment factors influence is impossible. Typical applications for FHSS include cellular deployments for fixed Broadband Wireless Access (BWA), where the use of DSSS is virtually impossible because of its limitations.

2.2 IEEE 802.11 Wireless LAN Security Overview

2.2.1 Introduction

Wireless Local Area Networks (WLANs) are cost effective and desirable gateways to mobile computing. They allow computers to be mobile, cable less and communicate with speeds close to the speeds of wired LANs. These features came with expensive price to pay in areas of security of the network. *[Al Naamany 2006]* This paper has identified and summarized these security concerns and their solutions. Broadly, security concerns in the WLAN world are classified into physical and logical. The paper overviewed both physical and logical WLANs security problems followed by a review of the main technologies used to overcome them. It addresses logical security attacks like man- in-the-middle attack and Denial of Service attacks as well as physical security attacks like rouge APs.

2.3 WPA password cracking Parallel Processing on the Cell BE

This project deals with the challenges of implementing WPA password cracker on an Cell Broadband Engine processor .The WPA security standards were investigated, to establish their potential weak points, As result of investigation was detected that WPA PSK authentication offers only one known possible weak point how to attack the WPA security during authentication. Further exploration of WPA-PSK authentication led to establish block diagram of designed application. The open source WPA supplicant code was used to extract the parts of code related to the WPA-PSK authentication. [Daniel 2009]

2.4 802.11 security protocols

2.4.1 Introduction

Wireless communication medium is, by its nature, vulnerable to variety of different threats, including unauthorized access, eavesdropping of communication, modification and repetition of data, denial of service, and fabrication of data. Therefore, it's essential that the security protocol can counter to these issues. In this seminar report, we introduce three commonly used WLAN security protocols that try to provide protection against these threats: WEP, WPA and WPA2. [Ihonen 2009]

2.4.2 Functionality Of 802.11 protocols

The paper starts by introducing the Wired Equivalent Protocol (WEP) and continue to the general authentication framework used by IEEE 802.11i security amendment: IEEE 802.1X and Extensible Authentication Protocol. Moreover, different key management schemes are discussed under this topic. Finally, we go through the data encryption protocols used in WPA and WPA2 that are TKIP and CCMP respectively. Since, WLANs are so widely used, we feel that it's important to understand the functionality of different wireless security protocols.

2.5 Practical Work: Wi-Fi Security

This practical work relies on the use of dedicated embedded platform based on a Raspberry Pi. A Raspberry Pi is a single board computer capable of running a GNU/Linux operating system and equipped with a Ethernet interface as long as two USB ports, on which can be connected various peripheral including a WiFi USB dongle. The operating system running on a Raspberry Pi is stored on a SD-card. The Raspberry Pi will be used as an experimental platform on which are installed all the required software and hardware required for this practical work. The system running on the Raspberry Pi will be accessed using a remote shell connection through a direct Ethernet link between the Raspberry Pi and a computer. [Mathieu Cunche2014]

I1I. WI-FI SECURITY

3.1 Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) first introduced in 1999 as a part of the IEEE 802.11 standard, related to security and it was intended to provide the same strong security in Wi-Fi like in traditional wired networks. Exactly what WEP acronym means, Wired equivalent Privacy. WEP's main goal was to provide data privacy by encapsulating data frames, however proved that it was not enough to cover all the security requirements and much vulnerability found while it was widely used. In chapter 5, it will be described a detailed cracking of WEP wireless networks in real conditions with the use of special equipment and open source software.

3.1.1 Architecture

Wired Equivalent Privacy (WEP) is using two different algorithms during a transmission in order to provide data integrity between the transmitting nodes. First, RC4 algorithm is used for data encryption. Although, it was intended to be a strong algorithm, which can easily be implemented in software and hardware projects, nowadays tend to be decommissioned as many flaws found. Secondly, the 32 bit Cyclic Redundancy Code (CRC-32) as an integrity algorithm for the confidentiality aspect of security. CRC-32 is the prime algorithm for WEP to provide data integrity, and during a data transmission, it is calculated by polynomial equations. With more details, algorithm takes as an input the frame intended to be transmitted, the equations produce a checksum and it is added on the data frame. Frames moves to lower layers and it is transmitted over the air. Receiver receives the frame, calculates again the checksum with the CRC-32 algorithm and if it is the same, frame is considered as original without any alteration.

3.1.2 Encryption

WEP security protocols has many versions, depending on the bit key is used in each implementation, standard WEP is 64-

bit, because a 40-bit Pre Shared Key (PSK) is used with a 24-bit Initialization Vector (IV). Apart from standard WEP, vendors bypassing the protocols in order to provide more secured solutions introduced WEP versions with longer key lengths instead of 40 bits. For example, the 128-bit RCA key is a WEP with 104 bits key and 24-bit length IV. Initialization Vector (IV) factor, is an initial variable with predefined length which is used as an input to a cryptographic algorithm. WEP IVs are 24 bit long and are used as an input to the RC4 algorithm with a shared key, the WEP key that is necessary to every user wants to access the specific WLAN, though the idea of the IV was very promising, in real conditions proved to have very short length (only 24 bit) which is very easy to be repeated and in relation that there is no algorithm on the WEP to avoid recurrent it was the Achilles heel of WEP and worked as a Major security backdoor. The IEEE 802.11 standard defined a specific procedure as WEP is used for encryption and decrypting in both sides of a transmission in some predefined steps (Transmitter encrypts, Receiver decrypts). This procedure relies on a shared key between the transmitting parties.

3.1.3 WEP Encrypting process

First, the shared key (PSK) hashed with the IV and as output is generating a Sequential Key with the use of a Pseudo-Random Number Generator (PRNG).In parallel CRC-32 algorithm calculating Integrity Check Value (ICV) of the plaintext. Then, ICV and pure plaintext are hashed. At the last stage of the encryption procedure, Sequential Key and the hash of the previous step (plaintext and ICV) is the input on the RC4 algorithm. RC4 uses XOR operation and the encryption is completed. Figure 1 below depicts in brief, the previous stages.

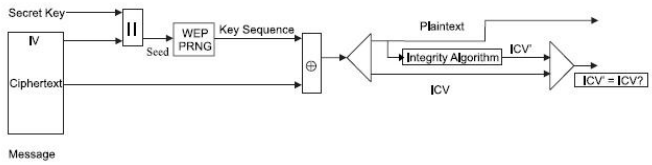

Figure.1. WEP Encapsulation Block Diagram

Now, the plaintext is encrypted and ready to wireless be transmitted.

3.1.4 WEP Decrypting process

The decryption procedure is the encryption reversed, once data reach its destination and one can divide this procedure in four different stages. Decryption's main purpose is to detach the cipher text from the plaintext. First, the Pre Shared Key (PSK) that, it was used in encryption and is a common secret in both ends in this first step is combined with the IV and the hash provided is used as an input to the PRNG to create a Sequential Key. Then, the encrypted text and the Sequential Key produced in the previous stage are used as an input to the RC4 algorithm for "XOR ing" and produce the unencrypted plain text. Figure 2 below depicts in brief, the previous stages.

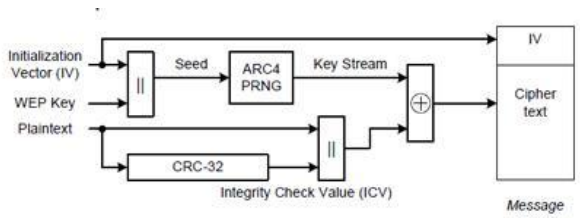

Figure 2: WEP Decipherment Block Diagram

Until now, cipher text is decrypted but it is not yet checked for integrity, so the receiver is not sure that the message received is not altered during the transmission. As the plaintext is already detached from the Integrity Value Check (ICV), CRC-32 integrity algorithm is applied on the plaintext in order to produce a new ICV. If the new ICV matches with the first one, data transmitted securely.

3.1.5 Security Issues or Vulnerabilities of WEP

- Security features in Vendor products are frequently not enabled
- Ivs are short (static)
- Cryptographic Keys are short
- Cryptographic Keys are share
- Cryptographic Keys cannot be updated automatically and frequently
- RC4 has a weak key Schedule and is in appropriately used in WEP
- Packet integrity is poor
- No user Authentication Occurs
- Authentication is not enabled only simple SSID identification occurs
- Device Authentication is simple shared Key challenge Response
- The Client Does not authenticate the AP

3.2 Wi-Fi Protected Access (WPA)

In this Section, it will be presented the Wi-Fi Protected Access (WPA) security protocol, as it was introduced by the Wi-Fi Alliance in late 2002. Wi-Fi Alliance working together with the Electrical and Electronics Engineers (IEEE) specified the weak aspects of the previously presented WEP protocol and introduced the WPA as a quick solution of this weakness. WEP introduced on 1999 and until 2001, its cryptographic fragility was a common assumption to the community.

3.2.1 Architecture

WPA, as a subset of 802.11i protocol, main purpose was to be applied in all 802.11 devices (a/ b/ g) and to be compatible with all vendors and their already existing equipment. That was the principal goal, to overcome the WEP flaws without the users to change their equipment WPA was The Solution.
By adding Temporal Key Integrity Protocol (TKIP) for encryption and 802.1X EAP for authentication purposes, WPA offers a high-level security. As a last security enhancement for data forgery (bit flipping) avoidance, WPA adopted the Message Integrity Check (MIC) algorithm, also known as "Michael". Similarly, to the previous security protocol, WPA designed to operate in two separate solutions.

- **WPA Pre- shared Key (WPA- PSK)**

It named as Personal WPA, ideal for Small office/ Home office (SOHO) users, which can offer all the security enhancements of the WPA with 256-bit cryptography but without the need for additional equipment such as servers, dedicated for the authentication. One of the weakest parts of WEP was the repeat of the Key to all users, something that WPA overcame. In WPA- PSK, the key is only used once to establish the session between user and AP, and then is never used again.

- **Enterprise WPA**

The second solution regards the adaptation of WPA in enterprise WLANs. Unlike to the previous, PSK- WPA, this solution needs additional equipment, a server complied with

802.1X and Extensible Authentication Protocol (EAP) for user authentication. 802.1X will be analyzed in detail, in next chapter of this study.

3.2.2 Encryption

Encryption in WPA is synonym to the Temporal Key Integrity Protocol (TKIP) that also is the main difference with the previous security standard WEP.
TKIP is a security protocol which is used in WPA. Although TKIP still uses RC4 cipher to generate key streams, it improves WEP's flaw by using new algorithms:

i) The sender calculates a cryptographic MIC and appends it to the messages. The receiver checks the MIC when receiving the massages. If the MIC is invalid, the receiver will discard the message.

ii) TKIP uses a TKIP sequence counter (TSC), or extended IV, to assign numbers to the sending messages. The receiver will drop the messages, which are out of order.

iii) TKIP uses the mixing function to combine the temporal key and the TSC into the WEP seed, which includes the IV. The receiver can use the mixing function to compute the same WEP seed to decrypt messages.

3.3 IEEE 802.11i/ Wi-Fi Protected Access II (WPA2)

Previously described the Wi-Fi Protected Access (WPA) security protocol as a subset of IEEE 802.11i standard defined on July 23 of 2004. WPA was the transition from the weak WEP to something more secured, free of the all the previous flaws, the 802.11i standard also known as WPA2 security protocol. According to Lashkari and to a relevant research, "WPA2 is not just the future of wireless access authentication, is the future of wireless access designed as future- proof technology"WPA2 designed to offer MAC layer security enhancements in order to provide better encryption with more efficient and secure key management by adopting a new algorithm. In WEP such as in WPA, RC4 was the main encryption algorithm. To overcome the RC4 weakness and the entrusting doubt of the community especially for enterprise networks, WPA2 designed to use the Advanced Encryption Standard (AES).AES standardized and announced from National Institute of Standards and Technology (NIST) in November 26th of 2001 many years later from the old RC4 which introduced in 1987. WPA2' s main objectives are to improve Authentication, Key Management and Secured Data transmission by better encrypting data packets with different strong keys which is difficult for someone to decrypt if he is able to eavesdrop them.

3.3.1 Architecture

As it was noted, in the general description of WPA2, this newest protocol uses the AES algorithm for encryption. More detailed, WPA2 implements the Counter Mode- Cipher Block Chaining MAC Protocol (CCMP), which is based on the AES for encryption. WPA2's encryption main objective was to overcome the drawbacks of the previous standards by offering data integrity and of course better security using the AES algorithm.

3.3.2 Encryption

CCMP Protocol can be separated in two different functionalities, the Counter Mode responsible for the encryption and the Cipher Block Chain MAC, also known as CBC MAC, which main objective is data integrity.

3.3.3 Authentication

From the Authentication point of view, WPA2 also divides users in two different categories depending on the network purposes, in enterprise-purposed networks, User Authentication is revised since WPA and WPA2 adapts a new Authentication- Authorization- Accounting (AAA) protocol, the Diameter. According to Internet Engineering Task Force (IETF), Diameter offers more functionalities as an AAA protocol instead of Radius used on WPA. Details and comparison will be provided on a next paragraph, dedicated to IEEE 802.1X protocol and User Authentication. User Authentication is SOHO users, is the part that remained attached between WPA and WPA2. A 64 character long ASCII code or a 256-bit auto generated code works as Pre-shared Key and all involved parts are configured manually one by one.

3.3.4 Known Issues

Although, at the time of writing, WPA2 has not proved any major security breaches, any limitations is related to the existing hardware where 802.11i and WPA2 is not backward compatible. A kind of proved security issue is that WPA2 has vulnerability to any insider potential attackers, especially for SOHO networks where a Pre- Shared Key is common for all users on each AP.

IV. EXPERIMENTS AND EVALUATION

4.1 Hardware requirements

In previous it was noted that for an active attack there is need for a NIC able to promiscuous mode. This mode is not available to all NICs that are available to the market. For this project, it is chosen a NIC of Networks, which is equipped with the Realtek RTL8187 chipset, a very popular chipset for Wi-Fi security evaluations. This NIC used to the host computer, which a laptop without any special characteristic. A USB port was the only requirement of the host computer. At the other side, for the AP role it was used a retail AP manufactured by TP- Link brand, the TL-WR741ND model available in every retail market. Instead of this, every Wi-Fi modem router can be used if it is able to support WEP and WPA/ WPA2 security protocols.

4.2 Wi-Fi Software requirements

A Linux distribution (distro) named KALI was the one-way software choice for this cracking purpose. But why this Linux distribution and not another one, or another operating systems like Windows? The answer is that KALI Linux like almost every Linux distribution is free. In general is a Linux distro, offering more than 300 penetration testing tools from Wi-Fi penetration to database exploits but for the security test bed of this study it was used only four different tools.

Airmon-ng:-According to its author's description this is more script than tool and helps to set NIC is monitor (promiscuous) mode.

Airodump-ng: - This tool is used for the 802.11 packet capturing, suitable for collecting IVs (Initialization Vector) in WEP and the handshake packets of WPA/ WPA2 in order to be used with Aircrack-ng.

Aireplay-ng: - This tool is used to increase traffic by injecting frames to the attacked AP, very vital function for faster WEP, WPA/ WPA2 cracking. In WEP just increasing the transmitted

but for WPA/ WPA2 is used to cause de authentication in order to capture the re authentication handshake data.

Aircrack-ng: Is the main tool used in this demonstration. Based on its description is a WEP and WPA-PSK cracking tool that can recover keys once enough amount of data packets have been captured.

4.3 Cracking of Security Protocols

4.3.1 WEP penetration test

In previous chapter, where WEP was analyzed, it was noted that this security protocol is using 24 to 48 bit key called Initialization Vector (IV). IV proved as the weak part of the protocol and is what it will be exploited in this scenario. In brief by using Kali Linux and the tools described earlier, IVs will be captured and after a good amount of IVs, cracking process will follow. For this scenario, AP is set with:

- SSID: **DCOM_test1**
- Authentication: **WEP**
- WEP key: **fdcda**
- **Enable monitor mode**

Firstly there is need to set NIC in monitor- promiscuous mode with the airmon-ng tool by using Linux terminal window.
Command: root@kali:~# *airmon-ng*
Output*:* Returns the connected Wireless NICs, the interface number in this scenario the wlan0 and the chipset.
Command: root@kali:~# *airmon-ng start wlan0*
Output*:* Starts the monitor mode for interface wlan0 in mon0

4.3.2 WPA/ WPA2 penetration test

In this scenario, the main objective is to capture the handshake of WPA/ WPA2 authentication. In brief by using Kali Linux and the tools like WEP before, data will be captured. Then this data file will be compared with a preloaded wordlist with potential passwords in order to reveal the PSK password.

For this scenario, AP is set with:

- SSID: **DCOM_test2**
- Authentication: **WPA2**
- PSK Password: **dcom_pass**

In WPA / WPA2, demonstration has many common steps with the WEP procedure. Therefore, steps from 1 to 3 are the same. The difference relies on that in WPA/ WPA2 there is need for a wordlist on the last step. The WPA and WPA2 schemes do not suff er from the weaknesses of WEP. More particularly, there it is not possible to run a statistical attack based on the IVs to recover the key. However it is possible to crack a WPA scheme by performing a research that involve testing for the possible passwords. To perform the search, it is sufficient to obtain a WPA handshake. Indeed, based on this handshake, it will be possible to determine whether password x is the password used by the WPA scheme. The attack therefore requires capturing a handshake and then searching for the password. A good news is that the search can be performed offline (it is not required to stay in range of the AP during this phase of the attack). To crack WPA password, we will use aircrack-ng in combination with a software called john the ripper. John is a command line tool used to crack passwords. It is particularly efficient at generating a large number of passwords given a set of rules. For instance, the following commands will generate all the password of length 4 and composed only of digit (resp. all) characters.

V. CONCLUSION AND FUTURE WORK

5.1. WLAN Security Evaluation

In this chapter work is dedicated to the cracking of Wi-Fi Security Protocols and how a potential hacker is able to break the security of WEP and WPA/ WPA2 security protocols. According to the first scenario, a WLAN is secured with WEP, which proved incapable to keep the potential attacker outside. WEP key revealed easily with the use of Kali Linux and Aircrack-ng tools. An attack to a WLAN secured by WEP is usually successful, but time is something that cannot be estimated. If WEP cannot be avoided on a network the implementation of longer IVs and longer keys, (128 bit) will add an extra difficulty to the attacker. The second penetration test, implemented with WPA2 encryption proved more solid than WEP and an attack cannot have a successful result. Even though for cracking WPA/WPA2 there is need for a wordlist, if the PSK password is a common word or phrase including is this wordlist, the results are the same like WEP. In this second scenario, deliberately the password was added to the wordlist to defend the previous sentence. Based on this we assume that the more long and complex is the PSK password the stronger WPA and WPA2 are.

5.2 Future work

As the attacks to WLANs increased rapidly because of the low cost equipment that is needed and the wide variety of free tools that is available to anyone on the internet, like Kali Linux and Aircrack-ng, researchers tried to find new security barriers to avoid spoofing attacks in the PHY layer. Studies about the Secure and Efficient Key Management (SEKM) with Public Key Infrastructure (PKI), MAC sequence number and traffic patterns radiometric signatures etc proved capable to offer a more secured WLAN with only one disadvantage, the additional overhead. Received Signal Strength (RSS) seems to be very promising for detection and localization against the spoofing attackers in WLANs. Experimental results show that RSS in combination with a Generalized Attack Detection Model (GADM) technique can achieve over 90 percent Hit Rate and Precision when determining the number of attackers. Even though this technique had great results in laboratory environment tested in IEEE 802.11 and in 802.15 (ZigBee) networks is still under development.

VI. REFERENCES

[1]. [802.11-2007] IEEE Std. 802.11 -2007, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", *IEEE Computer Society*, June 2007

[2]. [802.11i-2004] IEEE Std. 802.11i -2004, "Medium Access Control (MAC) Security Enhancements", *IEEE Computer Society*, June 2004

[3]. *Al Naamany 2006] Ahmed M. Al Naamany, Ali Al Shidhani, Hadj Bourdoucen "*IEEE 802.11 Wireless LAN Security Overview "IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.5B, May 2006.

[4]. [Daniel 2009] Martin Daniel "WPA password cracking Parallel Processing on the Cell BE" Master thesis, AAU, Applied Signal Processing and Implementation Spring 2009

[5]. [Halv2009] F. Halvorsen and O. Haugen, "Cryptanalysis of IEEE 802.11i TKIP", *Master's thesis*, Norwegian University of Science and Technology, 2009

[6]. [Mathieu Cunche2014] “Practical Work: Wi-Fi Security “Master RTS, INSA-Lyon - Lab. CITI, Inria – Privatics, January 2014

[7]. [Nazar 2009] Arbab Nazar “Evaluation of VoIP Codecs over 802.11 Wireless Networks “, Master Thesis, Halmstad University, November 2009

[8]. [SCHWARTZ] Sorin M. SCHWARTZ Frequency Hopping Spread Spectrum (FHSS) vs. Direct Sequence Spread Spectrum (DSSS) in Broadband Wireless Access (BWA) and Wireless LAN (WLAN), White Paper

[9]. [Ihonen 2009] Marko Ihonen Anssi Salo Tuomo Timonen” 802.11 security protocols” Seminar work Lappeenranta University of Technology Faculty of Technology Management Laboratory of Communications Software CT30A8800 Secured Communications, 2009

[10]. [Wee2004]Oh Khoum Wee ”WIRELESS NETWORK SECURITY: DESIGN CONSIDERATIONS FOR AN ENTERPRISE NETWORK”, Master’s Thesis, NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA, December 2004

[11]. [Yi-Ken Ho2007]Yi-Ken Ho, and Jyh-Cheng Chen 2007 Implementation of WIRE1x WPA Module “Wireless Internet Research and Engineering Laboratory National Tsing Hua University Hsinchu, Taiwan ,November 15, 2007