

B.Sc. in Computer Science and Engineering Thesis

A Study of Security Protocols for Wireless Local Area Network

Submitted by

Ishrat Jahan Nawshin

201114023

Sharmin Jahan Jyoti

201114024

Shamme Akter Zeba

201114054

Supervised by

Md. Shohrab Hossain

Assistant Professor

Department of Computer Science and Engineering

Bangladesh University of Engineering and Technology

Dhaka-1000, Bangladesh



**Department of Computer Science and Engineering
Military Institute of Science and Technology**

December 2014

CERTIFICATION

This thesis paper titled “**A Study of Security Protocols for Wireless Local Area Network**”, submitted by the group as mentioned below has been accepted as satisfactory in partial fulfillment of the requirements for the degree B.Sc. in Computer Science and Engineering in December 2014.

Group Members:

Ishrat Jahan Nawshin

Sharmin Jahan Jyoti

Shamme Akter Zeba

Supervisor:

Md. Shohrab Hossain
Assistant Professor
Department of Computer Science and Engineering
Bangladesh University of Engineering and Technology
Dhaka-1000, Bangladesh

ACKNOWLEDGEMENT

We are thankful to Almighty Allah for his blessings for the successful completion of our thesis. Our heartiest gratitude, profound indebtedness and deep respect go to our supervisor, Md. Shohrab Hossain, Assistant Professor, Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology, Dhaka-1000, Bangladesh, for his constant supervision, affectionate guidance and great encouragement and motivation. His keen interest on the topic and valuable advices throughout the study was of great help in completing thesis. We also grateful to our reviewer Jahidul Arafat, Lecturer, CSE Dept, MIST.

We are especially grateful to the Department of Computer Science and Engineering (CSE) of Military Institute of Science and Technology (MIST) for providing their all out support during the thesis work.

Finally, we would like to thank our families and our course mates for their appreciable assistance, patience and suggestions during the course of our thesis.

Dhaka
December 2014

Ishrat Jahan Nawshin

Sharmin Jahan Jyoti

Shamme Akter Zeba

ABSTRACT

Wireless Local Area Networks (WLANs) have become more prevalent and are widely deployed and used in many popular places like university campuses, airports, residences, cafes etc. With this growing popularity, the security of wireless network is also very important. In this study we present the security mechanisms available for WLANs. These security mechanisms are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and 802.11i (WPA2). Our aim is to show how an attack can be made on systems using the above mentioned mechanisms. We have given a brief overview of their working, structure, algorithms used and have tried to explore the real time vulnerabilities by issuing successful attacks against WEP and WPA2 network. The attacks were done in an ad-hoc network, using three laptops with wi-fi facility. We begin with WEP protocol which employs a flawed RC4 algorithm is very much prone to attack and is easily crackable, then listing some of its weakness. Then we have a look on WPA as the enhanced standard of WEP, along with some flaws in it. Finally an attack on WPA is explained. CommView version 6.3 and Aircrack-ng 1.2 RC 1 are the tools (software) those we have used to launch the attacks. The process required for attacking are explained, along with the screen-shots to help understand the working.

TABLE OF CONTENT

<i>CERTIFICATION</i>	ii
<i>ACKNOWLEDGEMENT</i>	iii
<i>ABSTRACT</i>	1
List of Figures	3
List of Abbreviation	4
1 Introduction	6
1.1 Background of the Research	6
1.2 Problem Statement	7
1.3 Research Aim	7
1.4 Research Objective	7
1.5 Organization of Thesis	7
2 Literature Review	9
2.1 Security principles	9
2.1.1 General principles	9
2.2 Wireless Lan Overview	11
2.2.1 Stations and Access Points	11
2.2.2 Channels	11
2.2.3 Infrastructure and Ad Hoc Modes	12
2.2.4 Frames	12
2.2.5 Authentication	13
2.3 Wireless Security	13
2.3.1 IEEE 802.11 Security Protocols	14
2.4 WEP(Wired Equivalent Privacy)	14
2.4.1 History	15
2.4.2 Protocol Construction	15
2.4.3 Authentication	16
2.4.4 Pseudorandom Number Generator - RC4	18
2.4.5 Weakness of WEP	19
2.4.6 Attacks on WEP	20
2.5 WPA	21
2.5.1 History	21

2.5.2	Protocol Overview	22
2.5.3	WPA Improvement	22
2.5.4	Similarities between WPA and WEP	23
2.5.5	Encryption of WPA	24
2.5.6	WPA Weakness	24
2.5.7	WPA2-PSK	25
2.6	Wi-fi Protected Access-Temporal Key Integrity Protocol (WPA-TKIP)	26
2.6.1	History	26
2.6.2	Protocol overview	26
2.6.3	TKIP Encapsulation	27
2.6.4	TKIP Decapsulation	27
2.7	Previous work	29
3	Research Methodology	30
3.1	Experimental Procedures	30
3.1.1	Software Requirement for this experiment	30
3.1.2	Procedure for Cracking WPA-TKIP	31
4	Result, Analysis and Discussion	35
4.1	Test Results	35
4.1.1	Systems those are successfully cracked	35
4.1.2	Systems those are unsuccessful	35
4.1.3	System Review Statistics of cracking WPA, WPA2	36
4.1.4	Success Ratio of cracking WPA, WPA2	37
4.2	Analysis	37
4.3	Discussion	38
5	Conclusion and Recommendation	39
5.1	Conclusion	39
5.2	Recommendation	39
	References	39
A	Glossary	44

LIST OF FIGURES

2.1	IEEE 802.11 Frame	12
2.2	States and Services	13
2.3	Construction of expanded WEP MPDU	15
2.4	WEP encapsulation block diagram	16
2.5	WEP decapsulation block diagram	17
2.6	Sequence diagram of Shared Key Authentication	17
2.7	WPA Encryption Algorithm(TKIP)	24
2.8	TKIP encapsulation block diagram	27
2.9	TKIP decapsulation block diagram	28
3.1	Option for Capturing	32
3.2	Scanning	32
3.3	Discovering nearby network	33
3.4	Capturing packet	33
3.5	Bottom Toolbar	33
3.6	Choosing .CAP file and wordlist	34
4.1	Test Result 2	35
4.2	Test Result 2	36
4.3	Test Result 3	37
4.4	Success Ratioof cracking wlan protocols	38

LIST OF ABBREVIATION

AES	: Advanced Encryption Standard
AP	: Access point
ARC4	: Alleged RC4
BSSID	: Basic Service Set Identifier
BSS	: Basic Service Set
CCMP	: Counter Mode with Cipher Block Chaining Message
CRC	: Cyclic Redundancy Check
DA	: Destination Address
DHCP	: Dynamic Host Configuration Protocol
DNS	: Domain Name System
DoS	: Denial-of-Service
DS	: Distribution System
EAPOL	: Extensible Authentication Protocol Over LAN
EAP	: Extensible Authentication Protocol
ESSID	: Extended Service Set Identifier
FCS	: Frame Check Sequence
GUI	: Graphical User Interface
IEEE	: Institute of Electrical and Electronics Engineers
ICV	: Integrity Check Value
IP	: Internet Protocol
IV	: Initialization Vector
KSA	: Key Scheduling Algorithm
LAN	: Local Area Network
LLC	: Logical Link Control
LSB	: Least Significant Bit
MAC	: Media Access Control
MIC	: Message Integrity Code
MPDU	: MAC Protocol Data Unit
OP	: Operation
PRNG	: Pseudo Random Number Generator
SA	: Source Address
SSID	: Service Set Identifier
STA	: Station

TA : Transmitter Address or Transmitting Station Address
TCP : Transmission Control Protocol
TKIP : Temporal Key Integrity Protocol
TK : Temporal Key (Session Key)
WEP : Wired Equivalent Privacy
Wi-fi : Wireless Fidelity
WLAN : Wireless Local Area Network
WPA : WiFi Protected Access

CHAPTER 1

INTRODUCTION

Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. The most common types of wireless security are Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA). WEP is a notoriously weak security standard. The password it uses can often be cracked in a few minutes with a basic laptop computer and with widely available software tools [1]. WPA was a quick alternative to improve security over the WEP. But the vulnerabilities in security standards those these tools offer remains and its imposing challenges for the information security ventures to design a sophisticated modulation of these and to ensure robust security in information transaction and transmission [2]. Thereby this chapter in the form a generalized study has briefly assessed the background of the research in section 1.1. It has identified the specific research areas and problems those the study deals with in section 1.2, when section 1.3 defines the research contexts and aim of the study. Section 1.4 contains objective of our research and section 1.5 contains organization of thesis.

1.1 Background of the Research

Wireless local area network (WLAN) has been widely used in many sectors. The popularity gained is due to many reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. Wireless local area networks (WLANs) are of great importance in network technologies. WLANs, Bluetooth and cellular networks gained popularity in computer and business industry with many consequent security issues. Especially WLAN systems like IEEE 802.11 networks became common access networks in private and public environments [3]. They have lots of benefits like mobility and flexibility. Unlike a traditional wired LAN, users have much more freedom for accessing the network. Such benefits also come with several security considerations. Security risks in wireless environments include risks of wired networks plus the new risks as a result of mobility. To reduce these risks and protect the users from eavesdropping, organizations have been adopted several security mechanisms [4], [5]. The traditional WLAN security mechanism is WEP. WEP is an encryption algorithm designed in 1999 along with 802.11 standard to provide wireless security. It employs RC4 (Rivest Cipher 4) algorithm from RSA Data Security. However,

several serious weaknesses were identified by cryptanalysts and WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, and then by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite the serious security flaws WEP still provides a minimal level security [6].

1.2 Problem Statement

In this research , we will identify the vulnerabilities of WLAN security protocol by cracking them. We want to show that attacker can easily crack password of the networks using these kind of security type. It is usually performed during assessments to identify accounts with weak passwords.

1.3 Research Aim

The aim of this research is to investigate different security mechanisms available for WLANs and their real time vulnerabilities and ways of cracking them.

1.4 Research Objective

The specific objectives of this study are:

- To study the different WLAN security protocols.
- To identify the vulnerabilities of WEP, WPA and WPA2 WLAN protocols .
- To conduct an experiment to exploit the identified vulnerabilities of the WLAN security protocols.

1.5 Organization of Thesis

Chapter 1

This chapter contains introductory discussion of WLAN protocols and background of the research.

Chapter 2

This chapter presents background theory related to this thesis. This chapter starts with some basic security principles. It then continues by presenting wireless networks and wireless network security in detail, as well as attacks on the various security protocols. The chapter finishes by detailing some network protocols relevant to the work presented later in the thesis.

Chapter 3

This chapter contains an experiment of cracking security key of a wireless network with windows machine.

Chapter 4

This chapter contains results of our experiment which we will have done in previous chapter, analysis and discussion. Discussion evaluates the experimentation and results, and discusses some lessons learned during the research.

Chapter 5

summarizes the main findings of our research, and concludes the thesis. Further Work presents some ideas for further work on the topic.

CHAPTER 2

LITERATURE REVIEW

This chapter will cover the basic theory that will establish a fundament for the rest of the work in this thesis. First we will define some general security principles. Next, we will give introduction to wireless networking and wireless security. We will also give some description encryption technique WEP, WPA, TKIP and known attacks on these. These techniques are used for security purpose. But these techniques have some problem. For these problem, we can crack password and can see the data. We crack password by using Aircrack-ng and Commview in our research.

2.1 Security principles

Computers and computer networks, especially the Internet, have become a vital part of modern society. Hence the security of these systems is very important. Aspects ranging from the privacy of users to preserving important infrastructure and public services, are all relying on the security of computer systems and networks.

2.1.1 General principles

Posthumus et al. split information security into three main principles: Confidentiality, Integrity and Availability [7]. These principles go beyond the technical security implementations and include social and organizational aspects as well. This section will focus on the general technical principles of security.

Confidentiality

RFC4949 defines confidentiality as: The property that data is not disclosed to system entities unless they have been authorized to know the data [8].

As an example, if a user logs into a computer system the password must be kept secret to maintain confidentiality. This means that the password should never be sent over a network in cleartext. The user should never store it unprotected or disclose it to other persons [9].

Another aspect of confidentiality when talking about networks is traffic flow confidentiality [10]. It is the protection of information. It could be derived from observing network traffic flow. Confidentiality is a key aspect in maintaining the privacy of users.

Integrity

Integrity is defined by Stallings as: The assurance that data received is exactly as sent by an authorized entity [10]. (i.e. contain no modification, insertion, deletion or replay.) Information integrity can be compromised both intentionally and unintentionally. To detect modification of data, a Message Integrity Code (MIC) is often computed of the data. Any modification of the data will result in a different MIC. It will indicate that the data has been modified. There are many different means of providing integrity, ranging from simple Cyclic Redundancy Checks (CRC) to MICs based on advanced cryptographic hash functions like MD5 or SHA [11]. To be able to fully protect the integrity of the data, the MIC and/or data need to be encrypted. Otherwise, an attacker could simply modify the data and re-compute the MIC correspondingly. If encryption is used, some form of shared secret is needed, i.e. a key [9].

Simple MICs can only detect minor modifications like for example transmission errors and does not give protection against intentional tampering of the data. Cryptographic hash functions are designed to detect any change in the data. It should be computationally infeasible to modify the data without changing the hash value. It should also be impossible for an attacker to replay, or retransmit, previously sent data without triggering some form of replay protection scheme, this is most often achieved through the use of sequence numbers and/or time stamps [12].

Availability

Availability is defined in RFC4949 as: The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system [8].

An information system needs to be accessible to its users when needed. Otherwise it fails to meet its requirements. This property is especially important in computer networks and servers, which serve a large amount of users and are a vital part of modern society, e.g. banking systems. The largest intentional threat against availability is Denial-of-Service (DoS) attacks. DoS attacks are typically executed by generating an excessive amount of requests or traffic. This will make legitimate use of the service impossible [13]. Exploitation of protocol weaknesses could also compromise the availability of a system. Availability is achieved through the use of physical redundancy and safety, and proper management and control of

system resources [10].

2.2 Wireless Lan Overview

IEEE 802.11 refers to a family of specifications developed by the IEEE for over-the-air interface between a wireless client and an AP or between two wireless clients. To be called 802.11 devices, they must conform to the Medium Access Control (MAC) and Physical Layer specifications. The IEEE 802.11 standard covers the Physical (Layer 1) and Data Link (Layer 2) layers of the OSI Model. In this article, we are mainly concerned with the MAC layer and not the variations of the physical layer known as 802.11a/b/g [14].

2.2.1 Stations and Access Points

A wireless network interface card (adapter) is a device, called a station, providing the network physical layer over a radio link to another station. An access point (AP) is a station that provides frame distribution service to stations associated with it. The AP itself is typically connected by wire to a LAN.

The station and AP each contain a network interface that has a Media Access Control (MAC) address, just as wired network cards do. This address is a world-wide-unique 48-bit number, assigned to it at the time of manufacture. The 48-bit address is often represented as a string of six octets separated by colons (e.g., 00:02:2D:17:B9:E8) or hyphens (e.g., 00-02-2D-17-B9-E8) [15]. While the MAC address as assigned by the manufacturer is printed on the device, the address can be changed in software [16].

Each AP has a 0 to 32 byte long Service Set Identifier (SSID) that is also commonly called a network name. The SSID is used to segment the airwaves for usage. If two wireless networks are physically close, the SSIDs label the respective networks, and allow the components of one network to ignore those of the other. SSIDs can also be mapped to virtual LANs; thus, some APs support multiple SSIDs. Unlike fully qualified host names (e.g., gamma.cs.wright.edu), SSIDs are not registered, and it is possible that two unrelated networks use the same SSID [15].

2.2.2 Channels

The stations communicate with each other using radio frequencies between 2.4 GHz and 2.5 GHz [15]. Neighboring channels are only 5 MHz apart. Two wireless networks using neighboring channels may interfere with each other.

2.2.3 Infrastructure and Ad Hoc Modes

A wireless network operates in one of two modes. In the ad hoc mode, each station is a peer to the other stations and communicates directly with other stations within the network. No AP is involved [15]. All stations can send Beacon and Probe frames. The ad hoc mode stations form an Independent Basic Service Set (IBSS).

A station in the infrastructure mode communicates only with an AP. Basic Service Set (BSS) is a set of stations that are logically associated with each other and controlled by a single AP. Together they operate as a fully connected wireless network. The BSSID is a 48-bit number of the same format as a MAC address. This field uniquely identifies each BSS. The value of this field is the MAC address of the AP [15].

2.2.4 Frames

The station and AP radiate and gather 802.11 frames as needed. The format of frames is illustrated below. Most of the frames contain IP packets. The other frames are for the management and control of the wireless connection.

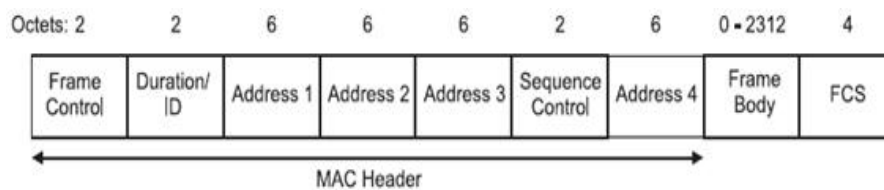


Figure 2.1: IEEE 802.11 Frame

There are three classes of frames. The management frames establish and maintain communications. These are of Association request, Association response, Reassociation request, Reassociation response, Probe request, Probe response, Beacon, Announcement traffic indication message, Disassociation, Authentication, Deauthentication types. The SSID is part of several of the management frames [15]. Management messages are always sent in the clear, even when link encryption (WEP or WPA) is used, so the SSID is visible to anyone who can intercept these frames. The control frames help in the delivery of data [15].

The data frames encapsulate the OSI Network Layer packets. These contain the source and destination MAC address, the BSSID, and the TCP/IP datagram. The payload part of the datagram is WEP-encrypted.

2.2.5 Authentication

Authentication is the process of proving identity of a station to another station or AP. In the open system authentication, all stations are authenticated without any checking. A station A sends an Authentication management frame that contains the identity of A, to station B. Station B replies with a frame that indicates recognition, addressed to A. In the closed network architecture, the stations must know the SSID of the AP in order to connect to the AP. The shared key authentication uses a standard challenge and response along with a shared secret key [15].

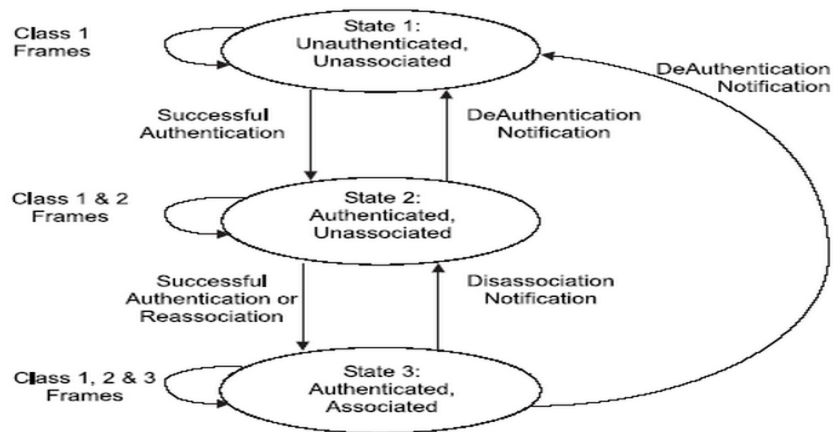


Figure 2.2: States and Services

2.3 Wireless Security

The deployment of wireless networks is increasing in both home and business environments due to the steady increase in both reliability and performance. The convenience of avoiding the physical infrastructure of a wired network often make wireless network favorable over wired networks. Wireless networks are more prone to security threats than wired networks due to their nature. In a wired network, computers are connected through wires. It is easy for the administrator to control this trusted zone [9].

In a wireless network traffic propagate in any direction over the air. It can be easily captured by a wireless interface within range on the correct channel. For that reason, if a wireless network is not protected, one should assume that everything that is being sent could be read by anyone. To protect the information one needs to apply encryption. If anyone can see the transmitted data, one have to make sure it is useless to them unless they are in possession of some shared secret; namely a key.

2.3.1 IEEE 802.11 Security Protocols

There exist much confusion and misinterpretation of the abbreviations of the security protocols available in wireless networks. In this section a historical overview of the security protocols of IEEE 802.11 will be given in order to clear up some of the confusion. Over the years, the development of wireless security protocols has been a race between the IEEE (the standardization committee) and the WiFi Alliance (the industry). In 1997, Wired Equivalent Privacy (WEP) (further explained in Section 2.4) became a part of the IEEE 802.11 standard. It aimed to provide security equivalent to the one we should get in a wired network. In 2001, WEP could no longer be considered secure after being proved to be completely broken [17].

To cope with the weaknesses in WEP, the IEEE established the 802.11i task group. The WiFi Alliance became restless in the time consuming process of IEEE to establish an 802.11i standard. As a result there is a development of WiFi Protected Access (WPA). It was released by the WiFi Alliance in 2003 [18]. The WPA standard has two modes. One is the Temporal Key Integrity Protocol (TKIP). Another optional mode is the Advanced Encryption Standard (AES). Both of these were developed on basis of the current work done by the 802.11i task group.

In 2004, the IEEE 802.11i task group finished their work on the 802.11i security standard. The standard was coined Robust Security Network (RSN) by the IEEE. RSN included two modes: the TKIP (an improved extension of WEP) and the Counter Mode CBC-MAC Protocol (CCMP3) with AES encryption. By then, the WPA brand (by the WiFi Alliance) was well established in access points and routers. The WiFi Alliance gave a name WPA2 to the RSN standard. A timeline of the development of security protocols [14].

2.4 WEP(Wired Equivalent Privacy)

WEP is a shared-key encryption system used to encrypt packets transmitted between a station and an AP (Access Point). The basic function of WEP protocol is to provide data security in wireless networks in the same way as it is in the wired networks. The algorithm used in WEP is intended to protect wireless communication from overhearing. WEP encrypts the payload of data packets. WEP uses RC4 algorithm. The shared secret key is either 40 or 104 bits long. The key is chosen by the system administrator. This section will give an overview of the history, background and technical detail of WEP as well as its weaknesses. The next section will explain the various attacks against WEP, of which some can be adopted to attack TKIP [15].

2.4.1 History

WEP was only intended to give Wired Equivalent Privacy. A normal wired network provides no confidentiality at the data link layer and all traffic is sent unencrypted as long as no higher layer encryption is used. The only protection at this layer is the physical protection from someone to plug a network cable into the network equipment. Wireless networks are implicitly more vulnerable than its wired counterparts. Anyone with a radio antenna and a wireless network card can eavesdrop on the data and also potentially gain network access [9].

It is obvious that wireless networks need additional protection. It should be from loss of confidentiality and unauthorized network access. The IEEE introduced WEP in the 802.11 1997 standard. As the popularity of wireless networks increased, it attracted the attention of the cryptographic community. Already in 2001, several weaknesses were discovered, and tools to crack WEP in short time with a personal computer became freely available on the Internet [4], [19], [20].

2.4.2 Protocol Construction

The construction of the WEP MPDU (MAC Protocol Data Unit) can be seen in Figure 2.3. The MPDU consists of three main parts:

The actual message or Data, an Integrity Check Value (ICV) and the Initialization Vector (IV). This MPDU is further encapsulated in an 802.11 header. In WEP, only the actual message data and the ICV are encrypted. The IV and the 802.11 headers are sent in the clear. The ICV consists of a 32-bit CRC-32 value. It is added to verify the integrity of the packet. The IV field is also 32 bits in length. It consists of the 24-bit IV, a 2-bit Key ID subfield and 6 bits of padding [3]. The 24-bit IV is used in combination with the shared secret key as input to the RC4 encryption algorithm. The Key ID subfield indicates which secret key, out of four possible, that was used to encrypt the packet.

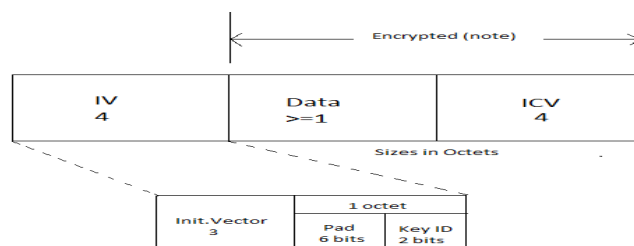


Figure 2.3: Construction of expanded WEP MPDU

The WEP was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication [21].

Scenario A, In the sender side : WEP try to use from four operations to encrypt the data(plaintext).At first, the secret key used in WEP algorithm is 40-bit long with a 24-bit Initialization Vector (IV) that is concatenated to it for acting as the encryption/decryption key. Secondly, the resulting key acts as the seed for a Pseudo-Random Number Generator (PRNG).Thirdly, the plaintext throw in a integrity algorithm and concatenate by the plaintext again. Fourthly, the result of key sequence and ICV will go to RC4 algorithm. A final encrypted message is made by attaching the IV in front of the Cipher text. Now in Figure 2.4 define the objects and explain the detail of operations [18].

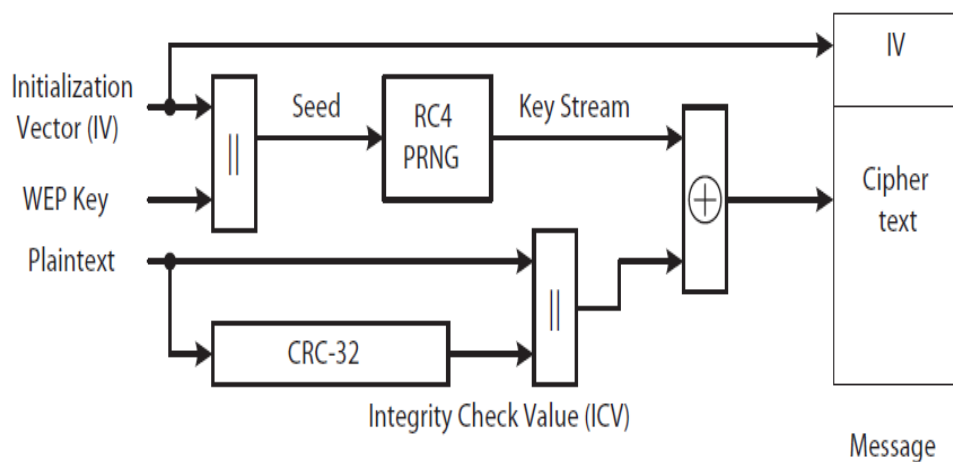


Figure 2.4: WEP encapsulation block diagram

Scenario B, In the Recipient side : WEP try to use from five operations to decrypt the received side (IV + Cipher text).At first, the Pre-Shared Key and IV concatenated to make a secret key. Secondly, the Cipher text and Secret Key go to in CR4 algorithm and a plaintext come as a result. Thirdly, the ICV and plaintext will separate. Fourthly, the plaintext goes to Integrity Algorithm to make a new ICV (ICV) and finally the new ICV (ICV)compare with original ICV. In Figure 2.5 you can see the objects and the detail of operations schematically [18] [21].

2.4.3 Authentication

Before any communication can take place between a station and the network,the station needs to authenticate to become associated with the network.WEP supports two types of authentication: Open System authentication and Shared Key authentication [4]. The Open System authentication is actually a null authentication algorithm [3].It means that any STA can authenticate if the AP is set to Open System Authentication [22]. This protocol simply

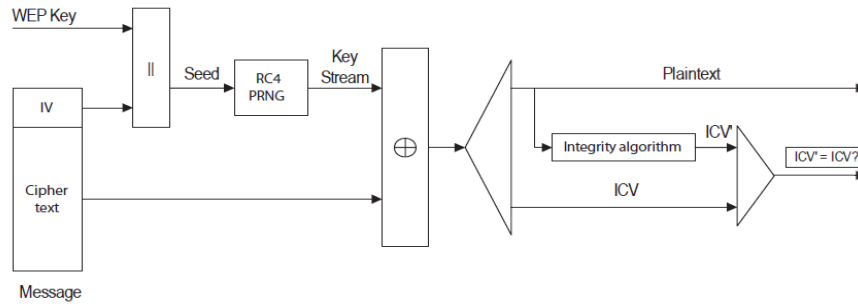


Figure 2.5: WEP decapsulation block diagram

consists of a Request and a Success message, and there is no actual authentication taking place.

The Shared Key authentication offers a one-way authentication, as opposed to mutual authentication. The STA authenticates with the AP, but the AP never authenticates with the STA. Only STAs that know the secret key are able to successfully authenticate with the AP. This protocol consists of a four-way handshake, and is initiated by the STA sending an Authentication request. A sequence diagram of the authentication can be seen in Figure 2.6. The AP will then respond with a challenge, which contains a 128-octet message generated by the WEP PRNG. When the STA receives this challenge, the 128-octet is encrypted using WEP with the secret shared key and sends this back to the AP. When the AP receives this message it is decapsulated and the ICV is checked. If this check is successful, the decrypted contents are compared with the challenge previously sent. If these match, the AP knows that the STA knows the shared key and sends an authentication success message [9].

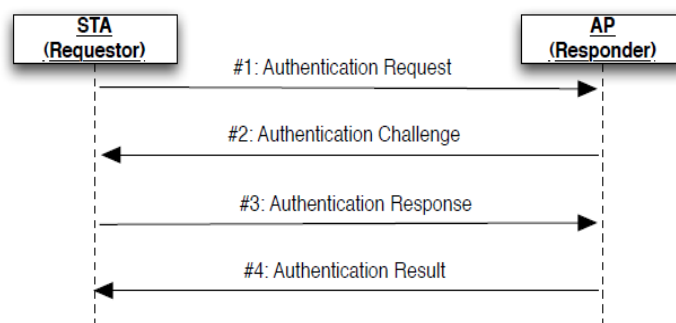


Figure 2.6: Sequence diagram of Shared Key Authentication

Even though this method of authentication may seem to be more secure than the Open System Authentication, it has some severe weaknesses. The Shared Key authentication is deprecated and if WEP (which is also deprecated) is used, only Open System authentication should be enabled.

2.4.4 Pseudorandom Number Generator - RC4

WEP makes use of the RC4 pseudorandom number generator for encryption. The algorithm is actually referred to as ARC4 (Alleged RC4) in the IEEE 802.11 standard, because the owner of the algorithm, RSA Security, has never actually published the details of it [3]. The source code of RC4 was anonymously posted on an Internet mailing list in 1994 [23]. RC4 is a stream cipher, which means it operates on the byte level, as opposed to a block cipher, which operates on blocks of several bytes. RC4 takes a variable size (1 to 256 bytes) key, or seed, as input and produces a pseudorandom stream of bytes. In WEP this key is 64 or 128 bits, the 24-bit IV concatenated with the 40 or 104-bit shared key. To encrypt data, the generated stream of pseudorandom bytes is XORed with the plaintext to construct the ciphertext. Decryption works the same way, this because XOR is a symmetric operation. The ciphertext is XORed with the stream of pseudorandom bytes to produce the plaintext [9]. The RC4 algorithm is surprisingly simple, and can be easily explained. RC4 operates on a 256-byte state vector S , which contains all 256 permutations of 8 bits. This state vector is first initialized to contain all the values in ascending order. A 256-byte temporary vector is also created which contain the key K . If the key is smaller than 256 bytes the key is simply repeated until the vector is filled. This initialization is described in Algorithm 1.

Algorithm 1 RC4 state vector initialization [10]

```
for i = 0 to 255 do
  S[i] = i;
  T[i] = K[i mod keylen];
end for
```

The next step is to use the temporary vector, T , to produce an initial permutation of the state vector, S . This is done by swapping two bytes in S according to a procedure given by T . Since the only operation done on S is swapping of bytes, S will still contain all permutations of eight bits. The algorithm for the initial permutation of S is given in Algorithm 2.

Algorithm 2 RC4 state vector initial permutation [10]

```
j = 0;
for i = 0 to 255 do
  j = (j + S[i] + T[i]) mod 256;
  Swap (S[i], S[j]);
end for
```

When the initial permutation is complete, the key and the temporary vector are never used again. The keystream is generated one byte at a time by swapping every byte of S , based

on its own state. Next, a byte k is selected for the keystream. This procedure is given in Algorithm 3.

Algorithm 3 RC4 S-Box stream generation [10]

```
i, j = 0;
while true do
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
Swap (S[i], S[j]);
t = (S[i] + S[j]) mod 256;
k = S[t];
end while
```

RC4, and especially the way WEP uses it, has some weaknesses. These weaknesses will be discussed in later section.

2.4.5 Weakness of WEP

WEP was originally created to provide security equivalent to the one we could expect of wired networks. Even though the name of the protocol does not imply the highest level of security, it implies to be reasonably secure [17].

The risk of Keystream reuse

In WEP protocol a key is extended by IV stream because of getting different keystreams for encryption of each of the transferred frames. But there are some deficiencies in using the keystreams. At the time of calculating XOR with the arguments that represents two messages encrypted by the same keystream. If messages are encrypted using same keystream, then we can decrypt not only one message but other messages using the identical keystream. The problem is caused by repeating IV sequence, since, the key is changed rarely, so, when the same IV is generated together with the same key that has not been changed, we get a repeated keystream. Attackers can very easily access the IV since it is not encrypted during the packet transmission [9].

Message Modification

Message Modification means modification of messages in the process of transmission. The receiver will not notice that the message was modified. Because of linear characteristics of

checksum there is a possibility to control modifications in the encrypted message without changing the checksum. So, it is possible to do any modification in the encrypted without changing the checksum with no fear that the receiver will notice these modifications [9].

Message injection

Two WEP protocol characteristics:

- WEP checksum is an unlocked function,
- It is possible to apply the old IV functions with no detection by receiver.

Due to first characteristics, anyone knowing the message can calculate the checksum field. This allows escaping access control measures. The second characteristic helps attackers to inject their message in case they know IV sequence and keystream. An attacker encrypts his own message by knowing the keystream and sends it to the receiver [9].

2.4.6 Attacks on WEP

WEP was created with the aim to provide equivalent security of wired networks. WEP contained so many obvious weaknesses that a complete key recovery attack almost was inevitable. A key recovery attack is the ultimate attack, from which the attacker obtains the master key that can be used to gain full access to the network. This section will explain the history and detail of the most serious and well-known attacks on the WEP protocol. Most of these attacks are attacks directed against the RC4 algorithm and the way it is used in WEP. However, there also exist that enables an attacker to decrypt single packets without ever knowing the encryption key. These non-cryptographic attacks exploits weaknesses in the WEP protocol itself rather than a statistical attack against RC4. All these attacks are available through tools such as the aircrack-ng suite [20]. It is a compilation of several tools and algorithms attacking wireless security.

The KoreK Attack

In 2004, a person under the pseudonym KoreK released two attacks on an Internet forum. These were later referred to as the KoreK attack and the Chopchop attack [24], [25]. The KoreK attack describes seventeen different attacks on WEP, which can be categorized as follows [26]:

- Key recovery based on the first byte of the keystream of the PRNG.
- Key recovery based on the first and second bytes of the keystream of the PRNG.

- Inverted attacks - reverse methods to reduce the search space.

Chopchop Attack

Around the same time as the KoreK attacks on RC4 were posted on an Internet forum the same anonymous hacker published a new attack called the Chopchop attack [24], [25]. The Chopchop attack belongs to a new group of attacks, which compared to all previously attacks may be considered a non-cryptographic attack. Rather than exploiting vulnerabilities in the RC4 algorithm, Chopchop attacks the WEP protocol itself and two of its design flaws, namely the lack of replay protection and the weakness of the ICV. The Chopchop attack is a remarkable and different attack on WEP than the previously explained. Even though it is not very efficient, it is of practical interest with packets that have a large amount of known data, e.g. an ARP packet. The Chopchop attack enables an attacker to decrypt a packet without ever knowing the key. In a real setting, the Chopchop attack can be used to decrypt a packet, modify it and inject it back into the network to generate traffic. The CRC-32 function was designed to detect errors and not to function the linearity of CRC-32 and the XOR operation used for WEP encryption, it is possible to flip a bit in the ciphertext and then calculate which bit in the encrypted CRC-32 value that in turn must be flipped in order for the checksum to validate. This fact combined with WEP's lack of replay protection, are the most important components of the Chopchop attack [9].

2.5 WPA

WPA is a security technology for Wi-Fi wireless computer networks. WPA improves on the authentication and encryption features of WEP (Wired Equivalent Privacy). In fact, WPA was developed by the networking industry in response to the weaknesses of WEP.

WPA provides stronger encryption than WEP through use of either of two standard technologies: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES). WPA also includes built-in authentication support that WEP does not offer. Overall, WPA provides comparable security to VPN tunneling with WEP, with the benefit of easier administration and use [27].

2.5.1 History

Wi-Fi Protected Access (WPA) is a security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined it in response to serious weaknesses researchers had found in the previous system,

WEP (Wired Equivalent Privacy).

WPA (sometimes referred to as the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the availability of the more secure and complex WPA2. WPA2 became available in 2004 and is a common shorthand for the full IEEE 802.11i (or IEEE 802.11i-2004) standard [18].

The Wi-Fi Alliance intended WPA as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard. WPA could be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999 [18]. However, since the changes required in the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs could not be upgraded to support WPA [18].

2.5.2 Protocol Overview

The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 40-bit or 104-bit encryption key that must be manually entered on wireless access points and devices and does not change. TKIP employs a per-packet key, meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP [28].

WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the cyclic redundancy check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled [29]. Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the keystream from short packets to use for re-injection and spoofing [30].

2.5.3 WPA Improvement

It wasn't long before a new technology called WPA, or Wi-Fi Protected Access debuted to address many of WEP's shortcomings. WPA aims to provide stronger wireless data encryption than WEP, but not everyone has or was able to jump onboard with the new wireless encryption technology. In order to use WPA all devices on the network must be configured

for WPA [31].

If a device is not configured for WPA, it will usually fall back to the lesser WEP encryption scheme, enabling the wireless devices to communicate on the network. The technology was designed to work with existing Wi-Fi products that have been enabled with WEP (i.e., as a software upgrade to existing hardware), but the technology includes two improvements over WEP:

- Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
- User authentication, which is generally missing in WEP, through the extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen [32]. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network [33].

WPA has been a mainstream technology for years now, but WEP remains a standard feature on virtually every wireless router on store shelves today. Although it's mainly there for backward compatibility with the oldest hardware, if reports and studies are accurate, a significant percentage of WLANs operating today (especially those used in homes) are still using outdated and insecure WEP for their encryption.

2.5.4 Similarities between WPA and WEP

The WPA came with the purpose of solving the problems in the WEP cryptography method, without the users needs to change the hardware. The standard WPA similar to WEP specifies two operation manners [21]:

1. Personal WPA or WPA-PSK (Key Pre-Shared) that use for small office and home for domestic use authentication which does not use an authentication server and the data cryptography key can go up to 256 bits. Unlike WEP, this can be any alphanumeric string and is used only to negotiate the initial session with the AP. Because both the client and the AP already possess this key, WPA provides mutual authentication, and the key is never transmitted over the air.
2. Enterprise WPA or Commercial that the authentication is made by an authentication server 802.1x, generating an excellent control and security in the users' traffic of the wireless network. This WPA uses 802.1X+EAP for authentication, but again replaces

WEP with the more advanced TKIP encryption. No preshared key is used here, but we will need a RADIUS server. And we get all the other benefits 802.1X+EAP provides, including integration with the Windows login process and support for EAP-TLS and PEAP authentication methods.

2.5.5 Encryption of WPA

The main reason why WPA generated after WEP is that the WPA allows a more complex data encryption on the TKIP protocol (Temporal Key Integrity Protocol) and assisted by MIC (Message Integrity Check) also, which function is to avoid attacks of bit-flipping type easily applied to WEP by using a hashing technique [21].

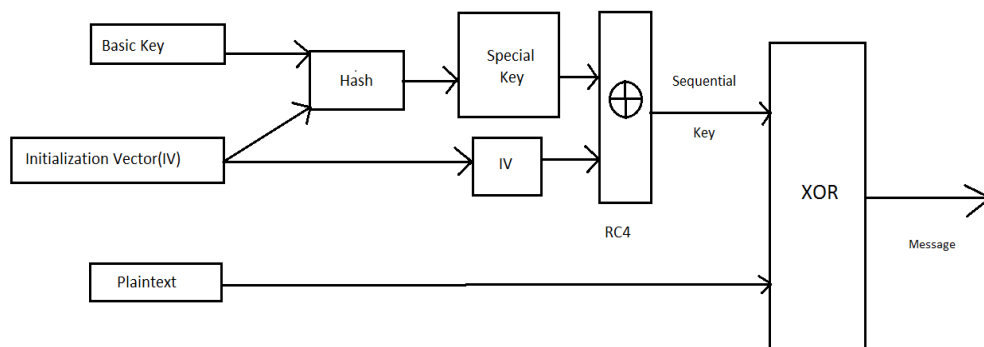


Figure 2.7: WPA Encryption Algorithm(TKIP)

In Figure 2.7 TKIP uses the same WEP's RC4 Technique, but making a hash before the increasing of the algorithm RC4. A duplication of the initialization vector is made. One copy is sent to the next step, and the other is hashed (mixed) with the base key. After performing the hashing, the result generates the key to the package that is going to join the first copy of the initialization vector, occurring the increment of the algorithm RC4. After that, there's the generation of a sequential key with an XOR from the text that we wish to cryptograph, generating then the cryptography text. Finally, the message is ready for send. It is encryption and decryption will performed by inverting the process.

2.5.6 WPA Weakness

In November 2003, Robert Moskowitz released Weakness in Passphrase Choice in WPA Interface. In this paper he explains a formula that would reveal the passphrase by performing a dictionary attack against WPA-PSK (pre-shared key) networks. This weakness was based on the pairwise master key (PMK) that is derived from the concatenation of the

passphrase, SSID, length of the SSID and nonces (a number or bit string used only once in each session). The result string is hashed 4,096 times to generate a 256-bit value and then combine with nonce values. The required information for generate and verify this key (per session) is broadcast with normal traffic and is really obtainable; the challenge then becomes the reconstruction of the original values. He explains that the pairwise transient key (PTK) is a keyed-HMAC function based on the PMK; by capturing the fourway authentication handshake, the attacker has the data required to subject the passphrase to a dictionary attack. Finally he found that a key generated from a passphrase of less than about 20 characters is unlikely to deter attacks [34].

For confirmation, in late 2004, Takehiro Takahashi, then a student at Georgia Tech, released WPA Cracker and Josh Wright, a network engineer and well-known security lecturer, released cowpatty around the same time [17]. Both tools are written for Linux systems and perform a brute-force dictionary attack against WPA-PSK networks in an attempt to determine the shared passphrase. Both require the user to supply a dictionary file and a dump file that contains the WPA-PSK four-way handshake. Both function similarly; however, cowpatty contains an automatic parser while WPA Cracker requires the user to perform a manual string extraction. Additionally, cowpatty has optimized the HMAC-SHA1 function and is somewhat faster. Each tool uses the PBKDF2 algorithm that governs PSK hashing to attack and determine the passphrase. Neither is extremely fast or effective against larger passphrases, though, as each must perform 4,096 HMAC-SHA1 related to the values as described in the Moskowitz paper [35].

2.5.7 WPA2-PSK

Short for Wi-Fi Protected Access 2-Pre-Shared Key, and also called WPA or WPA2 Personal, it is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server.

To encrypt a network with WPA2-PSK we provide our router not with an encryption key, but rather with a plain-English passphrase between 8 and 63 characters long. Using a technology called TKIP (for Temporal Key Integrity Protocol), that passphrase, along with the network SSID, is used to generate unique encryption keys for each wireless client. And those encryption keys are constantly changed. Although WEP also supports passphrases, it does so only as a way to more easily create static keys, which are usually comprised of the hex characters 0-9 and A-F [36].

2.6 Wi-fi Protected Access-Temporal Key Integrity Protocol (WPA-TKIP)

When WEP was proved completely broken [37], a new security scheme for wireless networks was desperately needed. The Temporal Key Integrity Protocol (TKIP) was designed on top of WEP to fix all its known weaknesses. In this section a brief historical overview of TKIP will be given, followed by a thorough technical walkthrough of the protocol [19].

2.6.1 History

TKIP's predecessor, WEP, has several severe weaknesses and is considered completely broken. An attacker can obtain the secret key used in WEP within a minute, or even decrypt packets without the knowledge of the key [9].

In 2001, the IEEE 802.11i task group was established to design the new security protocols for the 802.11 family of WLANs.

The standardization process took quite some time, and the WiFi Alliance wanted to be able to provide secure equipment to their customers. Consequently, the WiFi Alliance made their own security standard based on a draft version of 802.11i, which they named WPA (WiFi Protected Access). Even though TKIP provides vastly improved security over the old WEP standard, it is still built using some of the same building blocks as WEP. TKIP has some weaknesses, most significantly the Message Integrity Code (MIC). This is used in the new attack on TKIP. TKIP will be deprecated in the next version of the 802.11 standard [3].

2.6.2 Protocol overview

TKIP had one important design goal; it should be implementable on old WEP hardware [4]. For that reason, there were some serious limitations on how TKIP could be designed. Because of this limitation the protocol still uses WEP encapsulation, but was designed to provide additional protection against all known attacks on WEP. The 802.11 2007 standard defines four modifications of WEP that is made by TKIP [3].

- The use of a new Message Integrity Check (MIC), which is generated by the keyed cryptographic algorithm Michael.
- The MIC is, because of the design constraints, not very secure. Therefore TKIP implements countermeasures to handle this.
- Replay protection, with the use of a per-MPDU TKIP sequence counter (TSC).
- TKIP uses a cryptographic per-packet key mixing function to defeat weak-key attacks against the WEP key.

2.6.3 TKIP Encapsulation

In Figure . 2.8 The 128-bit session key, TK, is obtained through an EAPOL handshake and is explained later in this section. As can be seen from the figure, the first step of TKIP is to generate the per-packet key. This is done in two phases, labeled Phase 1- and Phase 2 key mixing in the figure. The Phase 1 key mixing takes three inputs: TA, TK and the 32 Most Significant Bits (MSBs) of the TSC. The output of this function is the 80-bit TTAK. Next, the second key mixing function uses the TTAK together with the TK and the 16 Least Significant Bits (LSBs) of the TSC. This results in the WEP seed, which is represented as the 24-bit WEP IV and a 104-bit RC4 key. The reason for mixing the key in two phases is to make the computation of the key less intensive, and thus ease the burden for older WEP hardware. The first phase only has to be computed for every $2^{16} = 65536$ packet, since it uses the 32 MSBs of the TSC. The second phase calculation changes for every packet. The TSC increases monotonically, and therefore the calculation could be performed in advance [9].

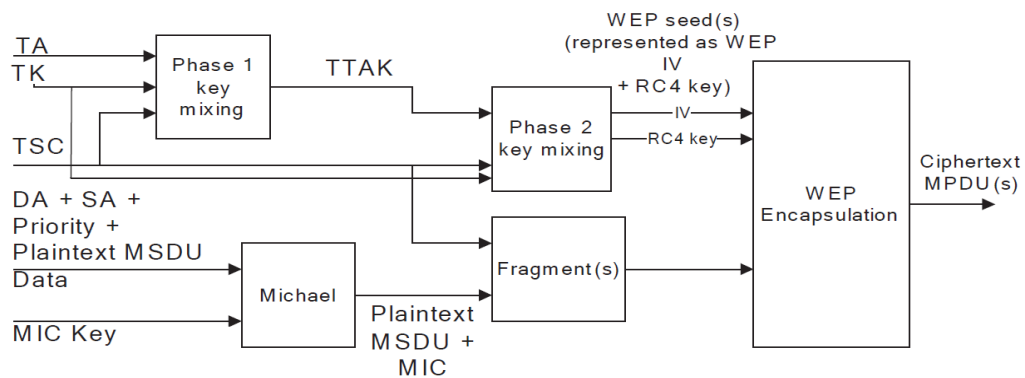


Figure 2.8: TKIP encapsulation block diagram

In addition to the ICV, TKIP introduced a new integrity check called a MIC. The MIC is generated by the Michael algorithm, which computes an 8-byte message integrity code (MIC) on the Plaintext MSDU. In addition to the MSDU, the Michael algorithm takes three inputs: DA, SA and a one-byte Priority field. The MSDU, the TSC and the computed MIC is fragmented to two or more MPDUs if needed. The MPDU is then inputted to the WEP encapsulation as the WEP Plaintext.

2.6.4 TKIP Decapsulation

When receiving a TKIP encapsulated packet, a decapsulation process is performed as depicted. First, the extraction of the TSC sequence number and key identifier from the WEP IV and TKIP Extended IV is performed. In Figure 2.9, Packets that violate the sequencing

will be discarded, i.e., packets that do not have a higher TSC than the previous packet are dropped [9].

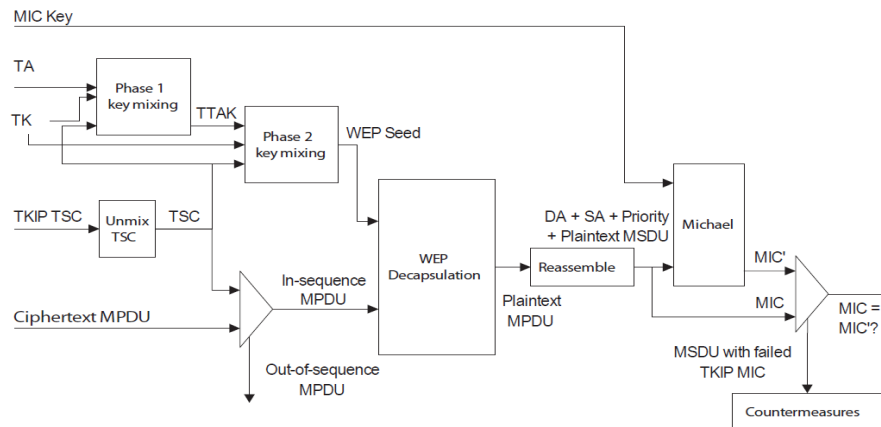


Figure 2.9: TKIP decapsulation block diagram

The construction of the WEP Seed is performed with the same two-phase key-mixing as in the encapsulation. The In-Sequence MPDU and the WEP Seed are then fed into the WEP Decapsulation. The MPDU, outputted from the WEP decapsulation, is then reassembled if it was a part of a fragmented MSDU. Next, the reassembled Plaintext MSDU, DA, SA and Priority field is sent to the Michael algorithm to produce MIC. If MIC matches the decrypted MIC, the packet is accepted. If not, TKIP Countermeasures will be activated.

Message Integrity Code (MIC)

One of the biggest flaws in WEP was that it did not protect against message forgery. This was because the ICV, based on CRC-32, was not sufficiently secure. To defend against message modification and other active attacks, TKIP includes a MIC. The MIC is calculated on the MSDU, which can be fragmented into several MPDUs. The MIC is based on the Michael algorithm, which is a simple algorithm, but with considerably improved security over CRC-32. Michael is a keyed MIC, which means it takes a secret key as input in addition to the plaintext. The key and the output of the algorithm are both 64 bits in length. The Michael key is derived from the master key. Although more secure than CRC-32, the Michael algorithm is a weak Message Integrity Check compared to keyed cryptographic hash functions like e.g. SHA-1. However, the designers of TKIP had to consider the compatibility of legacy hardware when choosing an algorithm. Michael had a design goal of only 20 bits of security [4]. This means that a randomly chosen MIC has 1 in $2^{20} = 1,048,576$ chance of being accepted as valid. The WEP ICV is still calculated on the plaintext. This results in two Message Integrity Checks being calculated on the data. When a packet is received, the WEP ICV is calculated the same way as in WEP. As in WEP the packet is discarded if the calculated ICV does not

match the received ICV. If the ICV check is successful, the MIC is calculated and checked against the received MIC as described earlier. It is very unlikely that the ICV computes correctly (Remember that CRC-32 is very good at detecting transmission errors), while the MIC fails, unless an attack is taking place.

2.7 Previous work

In paper ,the authors have showed the Procedure for Cracking WEP, Cracking WPA and Cracking WPA2 [38]. There has been a lot of research previously regarding attacks on security protocol.Most of the work had been done in different operating system like Mac, Linux, Ubuntu and windos XP.

Previous work on WPA-TKIP is primarily related to the work done by Beck and Tews [39], [40]. Their paper from November 2008 describes how a modified version of the Chopchop attack [24], can be executed on a Quality of Service (QoS) or WiFi MultiMedia (WMM) enabled network to obtain keystream for communication from the access point to a station. Their attack is, in contrast to the previous attacks on WEP, not a key recovery attack [39]. It enables an attacker to inject packets into the network and may thus lead to attacks on the different control protocols of the network. The new attack on TKIP is based on previous attacks on WEP such as the Chopchop attack by KoreK [24]. KoreK discovered a way of obtaining keystream without ever knowing the encryption key. A modified version of this attack is used to attack TKIP. We also feel that it is relevant to relate to all previous attacks on WEP and view these in a evolutionary perspective which have led to more and more sophisticated attacks on the wireless security protocols [19], [41].

Above we have discussed the literature review of our dissertation in the next chapter we are going to conduct an experiment of cracking security key of TKIP.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter will conduct an experiment of cracking security key of security type WPA-TKIP. Here we are going to use two software CommView version 6.3 and Aircrack-ng 1.2 RC 1 .

3.1 Experimental Procedures

In WEP, statistical methods can be used to speed up the cracking process, usually only plain brute force dictionary techniques may be used against WPA/WPA2 in an attempt to determine the shared passphrase. That is, because the key is not static, so collecting IVs like when cracking WEP encryption does not speed up the attack. This means that the passphrase must be contained in the dictionary we are using to break WPA/WPA2. Here we are applying the Dictionary Attack on captured encrypted IVs. The aim of this experiment is to show how easy it is to crack a wireless network with WPA-TKIP encryption with windows machine.

3.1.1 Software Requirement for this experiment

CommView(For capturing)

CommView version 6.3 for WiFi is a powerful wireless network monitor and analyzer for 802.11 a/b/g/n/ac networks. Loaded with many user-friendly features, CommView for WiFi combines performance and flexibility with an ease of use unmatched in the industry [42].

CommView version 6.3 for WiFi captures every packet on the air to display important information such as the list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. By providing this information, CommView for WiFi can help you view and examine packets, pinpoint network problems, and troubleshoot software and hardware [42].

Click for more screen shotsCommView for WiFi includes a VoIP module for in-depth analysis, recording, and playback of SIP and H.323 voice communications.

Packets can be decrypted utilizing user-defined WEP or WPA-PSK keys and are decoded

down to the lowest layer. With over 100 supported protocols, this network analyzer allows you to see every detail of a captured packet using a convenient tree-like structure to display protocol layers and packet headers. Additionally, the product provides an open interface for plugging in custom decoding modules.

A number of case studies describe real-world applications of CommView for WiFi in business, government, and education sectors.

CommView for WiFi is a comprehensive and affordable tool for wireless LAN administrators, security professionals, network programmers, or anyone who wants to have a full picture of the WLAN traffic. This application runs on Windows XP / Vista/ 7 / 8 or Windows Server 2003 / 2008 / 2012 (both 32- and 64-bit versions) and requires a compatible wireless network adapter.

Aircrack-ng (cracking tool)

Aircrack-ng 1.2 RC 1 is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless network interface controller whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux and Windows; the Linux version is packaged for OpenWrt and has also been ported to the Zaurus and Maemo platforms; and a proof of concept port has been made to the iPhone [20].

In April 2007 a team at the Darmstadt University of Technology in Germany developed a new attack method based on a paper released on the RC4 cipher by Adi Shamir. This new attack, named 'PTW', decreases the number of initialization vectors or IVs needed to decrypt a WEP key and has been included in the aircrack-ng suite since the 0.9 release.

Aircrack-ng 1.2 RC 1 is a fork of the original Aircrack project.

3.1.2 Procedure for Cracking WPA-TKIP

Download required softwares

We download Aircrack-ng for windows. <http://download.aircrack-ng.org/aircrack-ng-1.2-rc1-win.zip> [20]

Then we download CommView For Wifi <http://www.tamos.com/files/ca6.zip> [42]

Install CommView for WiFi

It doesn't matter whether we install it in VoIP mode or Standard mode. It automatically installs the necessary drivers. Allow it to install. We will not be able to connect to any Network using WiFi when using CommView version 6.3.

Choosing the Network

Now open your CommView for Wifi and go to file option and click on file capture like shown in the figure below:

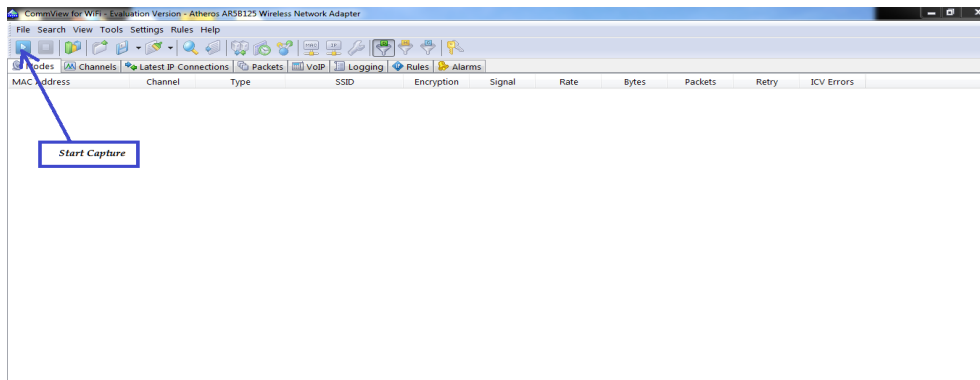


Figure 3.1: Option for Capturing

A new window should pop up now. Click on the START SCANNING button.

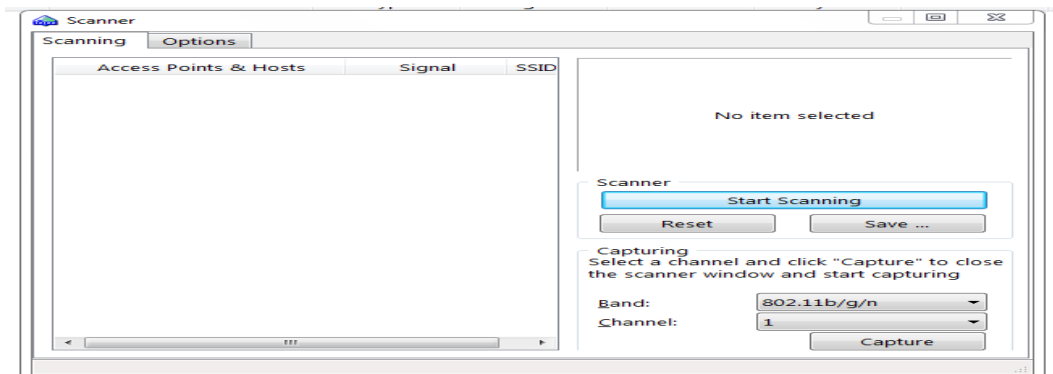


Figure 3.2: Scanning

After scanning it shows the list of all channels and the wireless networks which are running on specified channels. Click on the WiFi network you want to hack in the Right Column and Click on CAPTURE.

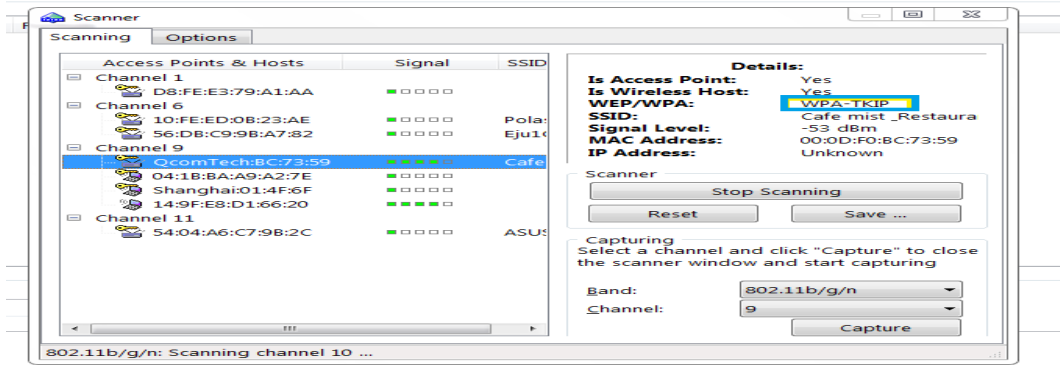


Figure 3.3: Discovering nearby network

Capturing the Packets

The windows should close now and you should see that CommView has started Capturing Packets .

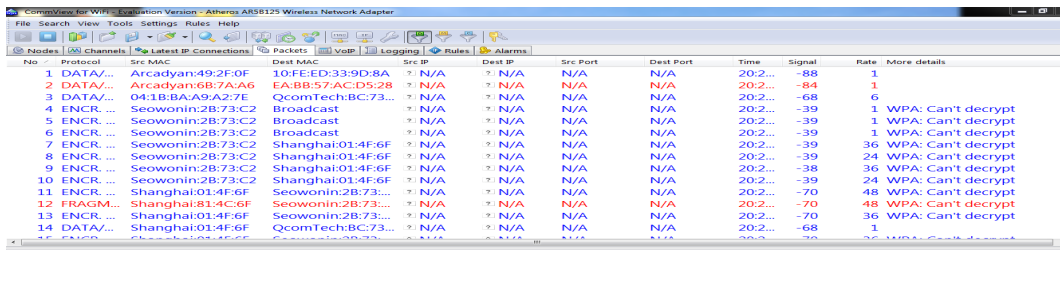


Figure 3.4: Capturing packet

Saving the Packets

Now that the Packets are getting captured you need to Save them. Click on Settings ⇒ Options ⇒ Memory Usage Change Maximum Packets in buffer to 20000.

The packets tab include a small toolbar shown below:



Figure 3.5: Bottom Toolbar

The sixth button allows you to open the contents of the current packet buffer in a new window. For saving,click File ⇒ Export Logs ⇒ Wireshark/Tcpdump files , type the

filename and save as .CAP file. In our experiment, the filename is 'cafe-mist-3.CAP'.

Choosing File

Open up the aircrack folder on desktop. then go into bin folder, and open up aircrack-ng-gui when it comes up just click the open/browse and find the 'cafe-mist-3.CAP'. just have been saved.

Choosing Wordlist

Choose WPA option, and we have to browse for a wordlist. Here we use password.lst as a wordlist.

Giving ESSID and BSSID

Check the advanced option and give the ESSID and BSSID of the network that we want to crack password.

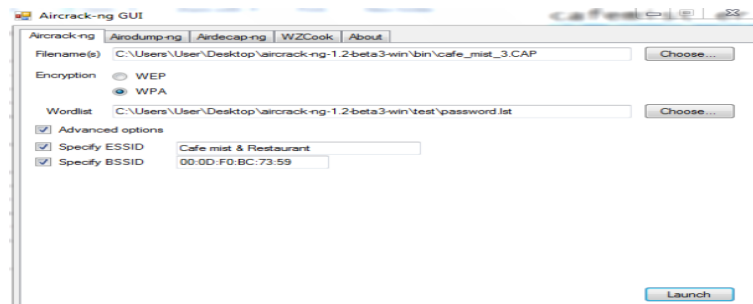


Figure 3.6: Choosing .CAP file and wordlist

Launch

Then click Launch.

Above we have discuss how to crack password of WPA-TKIP. In the next chapter we will show the results and analyze them along with a discussion.

CHAPTER 4

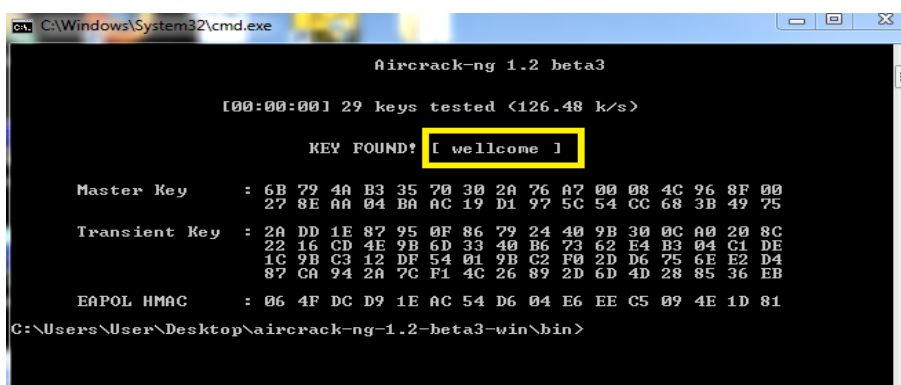
RESULT, ANALYSIS AND DISCUSSION

This chapter contains analysis of the results as well as a short discussion of our experiment and the experiences we have achieved during the thesis.

4.1 Test Results

4.1.1 Systems those are successfully cracked

- Security Mechanism : WPA-TKIP
- ESSID : Cafemist and Restaurant
- BSSID : 00:0D:50:BC:73:59
- TimeRequired : 2hours
- AttackType : Dictionary
- Result : Successful



```
C:\Windows\System32\cmd.exe
aircrack-ng 1.2 beta3
[00:00:00] 29 keys tested (126.48 k/s)
KEY FOUND! [ wellcome ]
Master Key   : 6B 79 4A B3 35 70 30 2A 76 A7 00 08 4C 96 8F 00
                27 8E AA 04 BA AC 19 D1 97 5C 54 CC 68 3B 49 75
Transient Key : 2A DD 1E 87 95 0F 86 79 24 40 9B 30 0C A0 20 8C
                22 16 CD 4E 9B 6D 33 40 B6 73 62 E4 B3 04 C1 DE
                1C 9B C3 12 DF 54 01 9B C2 F0 2D D6 75 6E E2 D4
                87 CA 94 2A 7C F1 4C 26 89 2D 6D 4D 28 85 36 EB
EAPOL HMAC   : 06 4F DC D9 1E AC 54 D6 04 E6 EE C5 09 4E 1D 81
C:\Users\User\Desktop\aircrack-ng-1.2-beta3-win\bin>
```

Figure 4.1: Test Result 2

4.1.2 Systems those are unsuccessful

- Security Mechanism : WPA-AES

- ESSID : Connectify-me
- BSSID : 5C:AC:4C:AA:4D:14
- TimeRequired : 2hours
- AttackType : Dictionary
- Result : Unsuccessful

```

C:\Windows\System32\cmd.exe
aircrack-ng 1.2 beta3
[00:00:01] 235 keys tested (194.93 k/s)

Current passphrase: property

Master Key   : 39 10 30 CB D5 8E FE DC ED 8D 70 35 F2 A2 13 C0
              7A 8D 8B CA E2 A2 18 24 A5 26 9E 47 E8 3D FC 3B

Transient Key : 3A 93 23 55 0C 11 9A AE 86 2B 5F D5 2B 00 4A FD
              13 60 95 90 A2 EC 7B 19 E8 6C A3 21 BC A0 F1 DE
              11 9F 89 1C 88 67 9E A4 71 62 6D 52 95 D5 5F 95
              03 E3 49 F8 1F 4D 2F A1 BB 61 32 27 9A 51 ED 7C

EAPOL HMAC   : E9 57 21 6E BF A7 33 D2 8E 9E 46 0E C4 17 95 6C

Passphrase not in dictionary

```

Figure 4.2: Test Result 2

- Security Mechanism : WPA-CCMP
- ESSID : jakia net Wifi
- BSSID : 5C:AC:4C:AA:4D:14
- TimeRequired : 2hours
- AttackType : Dictionary
- Result : Unsuccessful

4.1.3 System Review Statistics of cracking WPA, WPA2

System Ratio Statistics

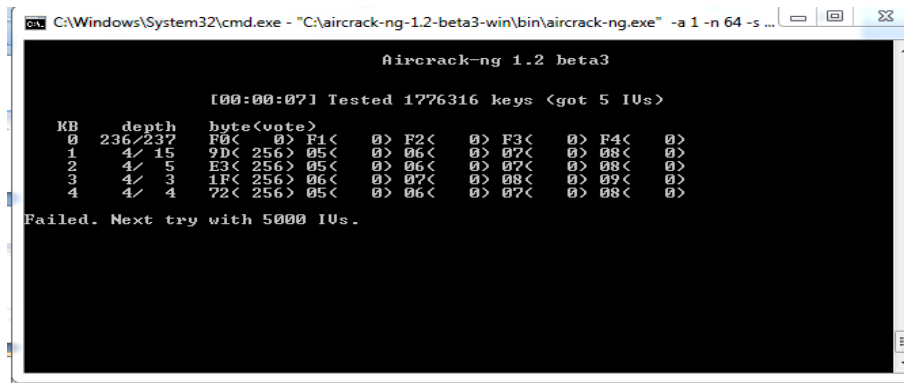


Figure 4.3: Test Result 3

Table 4.1: System Review Statistics of Cracking WPA,WP2

System Reviewed	Crack Down Status	
	Successful	Unsuccessful
Cafemist ESSID:Cafe mist & Restuarant BSSID:00:0D:F0:BC:73:53	Yes	-
Home network ESSID:jakia net Wifi BSSID:00:0D:F0:BC:73:53	-	Yes
Connectify me ESSID:Connectify-me BSSID:5C:AC:4C:AA:4D:14	-	Yes

4.1.4 Success Ratio of cracking WPA, WPA2

4.2 Analysis

We have cracked security key of the network "cafemist" and its security type is WPA-TKIP. We have done dictionary attack and have found the security key. This means that the passphrase must be contained in the dictionary we are using to break WPA/WPA2. If it is not in the dictionary then aircrack-ng will be unable to determine the key. The wordlists we have used here, contains the word which was the security key of the network. So, Aircrack-ng has found matching between the word from the wordlist and the security key from the captured file. So we were successful to crack the security key of the specified network. If the security key had not been matched with any word of the wordlist, then we would have to choose another wordlist or dictionary file.

We could not crack the two networks Connectify-me and jakia net Wifi that are of security type WPA-AES and WPA-CCMP respectively. AES is a very strong security type. In fact,

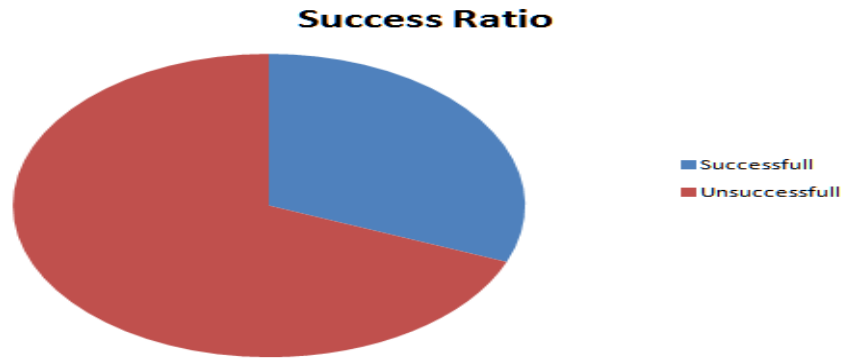


Figure 4.4: Success Ratio of cracking wlan protocols

AES has been well tested by cryptographers, and there is no known easy way of breaking it if the key is well chosen. CCMP is based on AES processing. To break an AES-based security is not so easy. So we were unsuccessful to crack the security keys of the two networks.

4.3 Discussion

This chapter will discuss the results and discoveries made throughout this thesis. We will discuss how well these attacks are applicable in a real world environment. We will also present both positive and negative lessons that we have learned during our research. Actually, TKIP (WPA1) is not vulnerable: for each packet, the 48-bit IV is mixed with the 128-bit pairwise temporal key to create a 104-bit RC4 key, so there's no statistical correlation at all. Furthermore, WPA provides counter-measures against active attacks (traffic reinjection), includes a stronger message integrity code (MIC), and has a very robust authentication protocol (the 4-way handshake). The only vulnerability so far is a dictionary attack, which fails if the passphrase is robust enough.

TKIP uses the RC4 stream encryption algorithm as its basis. On the other hand, AES stands for Advanced Encryption Standard and is a totally separate cipher system. It is a 128-bit, 192-bit, or 256-bit block cipher and is considered the gold standard of encryption systems today. It offers a higher level of security. CCMP is based on AES processing. So CCMP is also highly secured. Our experiments show that the success rate of the attack varies with different systems.

It had taken a lot of time to find appropriate dictionary file. We have done so many Internet search for word lists and dictionaries. We had to change the dictionary file frequently until any word of it matches with the security key. Finally we got an appropriate dictionary file.

CHAPTER 5

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

Wireless networks are becoming the most rapidly spread technology over the world, but have still some weakness in their security architectures. So, they should be well protected, in order to prevent exploitation of confidential data. In this paper we presented a brief overview of them, focusing on three main security protocols WEP, WPA and WPA2. The problem of WEP is solved by WPA. WPA is upgraded to WPA2 which is basically known as 802.11i standard. WPA uses the RC4 stream cipher algorithm while AES algorithm is used in 802.11i. TKIP uses RC4 algorithm but CCMP uses AES algorithm. We discussed and presented the overall detail procedure for cracking WPA-TKIP.

Wireless network is vulnerable to attacks. These attacks can be overcome by understanding the wireless security technologies, strong security policies, enforcement of security policies, strong system configuration. Our motivation was the need for increased wireless security and the common feel that nowadays WPA/WPA2 security protocols are difficult for a stranger to hack; however, our study depicted that any wireless network may be suffering from successful hacking attempts, if it is not carefully setup and protected.

5.2 Recommendation

In our dissertation, it had taken a lot of time to choose appropriate dictionary file. We recommend that more effective process using more effective tool should be conducted in future. The information of our dissertation can be used to configure password-cracking tools for more efficient performance.

Password cracking generally requires increased processing power and memory, so we may wish to have a dedicated password-cracking server. A dedicated system will allow us to execute other test objectives during the password-cracking process.

It is hoped that with a continuing paper in the next conference, we will explain the process of breaking AES and CCMP using an effective process and effective tools within a short time and completely discuss its weaknesses and improvements.

REFERENCES

- [1] <http://www.cisco.com/c/en/us/products/wireless/wireless-lan-controller/index.html>. last accessed December 17 2014.
- [2] <http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access>. last accessed December 17 2014.
- [3] T. I. of Electrical and E. Engineers, “Ieee standard for information technology telecommunications and information exchange between systems local and metropolitan area networks specific requirements,” *Amendment to IEEE Std 802.11TM, 1999 Edition (Reaff 2003)*, 2003.
- [4] J. Edney and W. A. Arbaugh, “Real 802.11 security: Wi-fi protected access and 802.11i,” 2003.
- [5] “Crack.” <http://www.ross.net/crc/crcpaper.html>. last accessed December 20 2014.
- [6] <http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>. last accessed December 17 2014.
- [7] S. Posthumus and R. von Solms, “A framework for the governance of information security,” *Computers & Security*, vol. 23, no. 8, pp. 638–646, 2004.
- [8] “Rc4.” <http://www.ietf.org/rfc/rfc4949.txt>. last accessed December 20 2014.
- [9] F. M. Halvorsen, O. Haugen, M. Eian, and S. F. Mjølsnes, “An improved attack on TKIP,” in *Identity and Privacy in the Internet Age, 14th Nordic Conference on Secure IT Systems, NordSec 2009, Oslo, Norway, 14-16 October 2009. Proceedings*, pp. 120–132, 2009.
- [10] W. Stallings, *Cryptography and network security - principles and practice (3. ed.)*. Prentice Hall, 2003.
- [11] “Hash function.” <https://code.google.com/p/crypto-js/>. last accessed December 20 2014.
- [12] “cryptographic.” <http://www.sans.edu/research/security-laboratory/article/hash-functions>. last accessed December 17 2014.

- [13] “Dos.” <http://searchsoftwarequality.techtarget.com/definition/denial-of-service>. last accessed December 17 2014.
- [14] “ieee802.11.” <http://www.ieee802.org/11>. last accessed December 20 2014.
- [15] “Hacking.” <http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm>. last accessed December 17 2014.
- [16] “Mac.” <http://compnetworking.about.com/od/networkprotocolsip/l/aa062202a.htm>. last accessed December 20 2014.
- [17] “Wep.” http://www.webopedia.com/DidYouKnow/Computer_Science/WEP_WPA_wireless_security.asp. last accessed December 17 2014.
- [18] “Wpa.” http://compnetworking.about.com/cs/wirelesssecurity/g/bldef_wpa.htm. last accessed December 17 2014.
- [19] S. Vaudenay and A. M. Youssef, eds., *Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001, Revised Papers*, vol. 2259 of *Lecture Notes in Computer Science*, Springer, 2001.
- [20] “Aircrack.” <http://aircrack-ng.org/>. last accessed December 17 2014.
- [21] A. H. Lashkari, S. Farmand, O. B. Zakaria, and R. Saleh, “Shoulder surfing attack in graphical password authentication,” *CoRR*, vol. abs/0912.0951, 2009.
- [22] “wep authentication.” <http://documentation.netgear.com/reference/sve/wireless/WirelessNetworkingBasics-3-09.html>. last accessed December 20 2014.
- [23] “Cypher.” <http://web.archive.org/web/20080120083537/http://cypherpunks.venona.com/date/1994/09/msg00304.html>. last accessed December 20 2014.
- [24] “Webattack.” <http://www.netstumbler.org/f50/chopchop-experimental-wepattacks-12489/>. last accessed December 20 2014.
- [25] <http://www.netstumbler.org/showpost.php?p=93942&postcount=35>. last accessed December 20 2014.

- [26] R. Chaabouni, “Break WEP faster with statistical analysis,” *IACR Cryptology ePrint Archive*, vol. 2013, p. 425, 2013.
- [27] “Wpa.” <http://www.webopedia.com/TERM/W/WPA.html>. last accessed December 17 2014.
- [28] N. Sklavos, “Book review: Samuelle, T.J. *Mike Meyers’ CompTIA Security + Certification Passport (Exam SY0-301)* - 3rd ed. new york: Mcgraw-hill osborne media, 2011, 480p., \$30.00. ISBN: 13: 978-0071770385,” *Information Security Journal: A Global Perspective*, vol. 23, no. 1-2, pp. 47–48, 2014.
- [29] M. Ciampa, “A comparison of password feedback mechanisms and their impact on password entropy,” *Inf. Manag. Comput. Security*, vol. 21, no. 5, pp. 344–359, 2013.
- [30] “Wpa crack.” <http://arstechnica.com/security/2008/11/wpa-cracked/>. last accessed December 20 2014.
- [31] “improvement.” <http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption/> last accessed December 20 2014.
- [32] “Sniffing.” <http://www.tamos.com/products/commwifi/>. last accessed December 17 2014.
- [33] <http://www.crn.com/news/security/18839317/wpa-brings-significant-improvements-to-wlan-security.htm>. last accessed December 20 2014.
- [34] “Auditing wi-fi protected access (wpa) pre-shared key mode.” <http://www.linuxjournal.com/article/8312>. last accessed December 20 2014.
- [35] S. Kurkovsky, Bhagyavati, A. Ray, and M. Yang, “Wireless security techniques: An overview,” in *International Conference on Information Technology: Coding and Computing (ITCC’04), Volume 2, April 5-7, 2004, Las Vegas, Nevada, USA*, p. 135, 2004.
- [36] “Wpa2-psk.” <http://www.webopedia.com/TERM/W/WPA2.html>. last accessed December 17 2014.
- [37] S. R. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” in *Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001 Toronto, Ontario, Canada, August 16-17, 2001, Revised Papers*, pp. 1–24, 2001.
- [38] 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.

- [39] M. Beck and E. Tews, “Practical attacks against wep and wpa. cryptology eprint archive,” 2008.
- [40] M. Beck and E. Tews, “Practical attacks against wep and wpa,” *WiSec*, p. 7986, 2009.
- [41] A. Stubblefield, J. Ioannidis, and A. D. Rubin, “A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP),” *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 2, pp. 319–332, 2004.
- [42] “Comview.” <http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm>. last accessed December 17 2014.

APPENDIX A

GLOSSARY

Integrity Check Value - CRC-32

The ICV field of the WEP MPDU consists of a 32-bit Cyclic Redundancy Check (CRC-32) value. A CRC value is computed on the message to verify the integrity of the received data, i.e. to confirm that no intentional or unintentional modification of the data has taken place. If this value was to be sent unencrypted an attacker could simply modify the message and re-compute the CRC, but WEP encrypts both the message and the ICV to avoid this. CRC has some properties that make it vulnerable to attacks. This vulnerability resulted in the Chopchop attack (See Section 2.4.8). It is an essential part of the attack on TKIP.

Initialization Vector - IV

WEP uses one static pre-shared key for encryption. This key is used for encryption in both directions. An important rule in cryptography is to never use the same key more than once. If the same key were used more than once in a stream cipher, the keystream would be identical for these messages. Now, if an attacker figured out the plaintext for one single message, because the keystream can be obtained by XORing the plaintext with the ciphertext. WEP tries to avoid key reuse by concatenating the key with a 24-bit IV and feeding this to the RC4 PRNG.

Cracking Password

When a user enters a password, a hash of the entered password is generated and compared with a stored hash of the user's actual password. If the hashes match, the user is authenticated. Password cracking is the process of recovering passwords from password hashes stored in a computer system or transmitted over networks. It is usually performed during assessments to identify accounts with weak passwords.

Dictionary Attack

In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.

CCMP

Counter Mode Cipher Block Chaining Message Authentication Code Protocol, Counter Mode CBC-MAC Protocol or simply CCMP (CCM mode Protocol) is an encryption protocol designed for Wireless LAN products that implement the standards of the IEEE 802.11i amendment to the original IEEE 802.11 standard. CCMP is an enhanced data cryptographic encapsulation mechanism designed for data confidentiality and based upon the Counter Mode with CBC-MAC (CCM) of the AES standard. It was created to address the vulnerabilities presented by WEP, a dated, insecure protocol.

AES

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes.