DECLARATION OF THESIS / POSTGRADUATE PROJECT PAPER AND COPYRIGHT

Author’s full name : Abdirahman Hussein Jibril

Date of birth : 1st January 1987

Title : DEVELOPMENT OF JAMMING METHOD FOR POLICY ENFORCEMENT IN WIRELESS Campus ENVIRONMENT

Academic Session : 2011/2012(1)

☐ CONFIDENTIAL (Contains confidential information under the Official Secret Act 1972)*

☐ RESTRICTED (Contains restricted information as specified by the organization where research was done)*

☐ OPEN ACCESS I agree that my thesis to be published as online open access (full text)

I acknowledged that Universiti Teknologi Malaysia reserves the right as follows:

1. The thesis is the property of Universiti Teknologi Malaysia.
2. The Library of Universiti Teknologi Malaysia has the right to make copies for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by: ________________________________

SIGNATURE

SIGNATURE OF SUPERVISOR

P00145263 PROF DR ABDUL HANAN

(NEW IC NO. /PASSPORT NO) NAME OF SUPERVISOR

NOTES : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.
“I hereby declare that I have read this project report and in my opinion this project report is sufficient in terms of scope and quality for the award of the degree of Master of Computer Science (Information Security)’’

Signature : ...................................................

Name of Supervisor : PROF DR. ABDUL HANAN

Date : JUNE 22, 2012
DEVELOPMENT OF JAMMING METHOD FOR POLICY ENFORCEMENT
IN WIRELESS CAMPUS ENVIRONMENT

ABDIRAHMAN HUSSEIN JIBRIL

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

JUNE 2012
I declare that this project report entitled “Development of Jamming Method for Policy Enforcement in Wireless Campus Environment” is the result of my own research except as cited in the references. The project report has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ....................................................
Name      : ABDIRAHMAN HUSSEIN JIRBIL
Date      : JUNE 22, 2012
To my beloved Mother and Father.
ACKNOWLEDGEMENT

In the name of Allah, Most Gracious, Most Merciful. First and foremost I thank Allah.

I am thankful to my main supervisors, Prof Dr. Abdul Hanan Abdullah for his professional guidance and support. I am also thankful to my co-supervisor, Assoc Prof Dr. Sulaiman Mohd Nor for his excellent guidance and support. I would never have been able to finish my thesis without the guidance of my supervisor and co-supervisor. I am thankful to University Technology Malaysia (UTM).

Thanks to my entire family members who gave me unforgettable support, especial thanks to my father and my Mother. They were always supporting me and encouraging me with their best wishes.

My gratitude also goes to my beloved sister, Rahma Hussein, thank you for the encouragements and endless supports.

Finally, I would like to thank everybody who was important to the completion of this thesis. I also like to express my apology that I could not mention personally one by one. Thank you all my friends, colleagues and lecturers.
ABSTRACT

Wireless network technology is one of the popular technologies and it is widely available in many areas. Some wirelesses networks are open (no encryption) while others are deployed with security features such as Wired Equivalent Privacy (WEP) or Wi-Fi protected access (WPA/WPA2). Because of unawareness of wireless threats, a wireless network owner may use WEP or WPA with weak password as security protection. Due to this, there are cases that unauthorized user get accessed into the wireless network. Wireless network is vulnerable to many attacks due to its nature. Hackers can capture user’s sensitive information such as password, bank account details, and credit card information etc. Using wireless network encryption technologies is not enough, knowing which technology provides the best security solution is important to avoid unauthorized access. This study analyzes some serious wireless network security flaws. In this study, Practical attack against WEP and WPA will be performed in order to analyze how easy or difficult to break weak wireless security encryption. The objectives of this study are: 1) to study vulnerabilities of Wired Equivalent Privacy (WEP) and WPA, 2) To analyze risks of Wired Equivalent Privacy (WEP) encryption and 3) To propose strategy to control the use of WEP in the campus. The scope of this study is to analyze wireless network security vulnerabilities by performing wireless security attack against WEP and WPA. University Technology Malaysia (UTM) wireless network has been chosen as case study. This study proposes two strategies to control the use of WEP in UTM campus. The first strategy is proposing enforcement policy for the departments and faculties that have or wishes to deploy wireless access points. The second strategy is proposing jamming program to suspend wireless access point if policy disobeyed.
ABSTRAK

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DECLARATION</td>
<td>ii</td>
</tr>
<tr>
<td></td>
<td>DEDICATION</td>
<td>iii</td>
</tr>
<tr>
<td></td>
<td>ACKNOWLEDGMENT</td>
<td>iv</td>
</tr>
<tr>
<td></td>
<td>ABSTRACT</td>
<td>v</td>
</tr>
<tr>
<td></td>
<td>ABSTRAK</td>
<td>vi</td>
</tr>
<tr>
<td></td>
<td>TABLE OF CONTENTS</td>
<td>vii</td>
</tr>
<tr>
<td></td>
<td>LIST OF TABLES</td>
<td>xi</td>
</tr>
<tr>
<td></td>
<td>LIST OF FIGURES</td>
<td>xii</td>
</tr>
</tbody>
</table>

1 INTRODUCTION
1.1 Overview 1
1.2 Internet and Wireless Communication 2
1.3 Problem Background 4
1.4 Problem Statement 6
1.5 Project Objective 6
1.6 Project Scope 6
1.7 Significance of the Study 7
1.8 Summary 7
2 LITERATURE REVIEW

2.1 Introduction 8
2.2 History of Wireless Network 9
2.3 Wireless Network Components 10
  2.3.1 Access Point 10
  2.3.2 Network Interface Card (NICS)/Client Adapters 10
  2.3.3 Antenna 11
2.4 The Importance of Security in Wireless Network 11
2.5 Methods of Attacking Wireless Network 12
2.6 Wired Equivalent Privacy (WEP) 13
  2.6.1 WEP Authentication 15
  2.6.2 Key Size and Configuration 18
  2.6.3 WEP Attacks 18
  2.6.4 WEP Secret Key 21
  2.6.5 RC4 Encryption Algorithm 21
  2.6.6 How Attacker Attacks WEP 22
  2.6.7 WEP Past Solution 23
2.7 Wi-Fi Protected Access (WPA) 23
  2.7.1 WPA VS WEP 25
  2.7.2 WPA the Four-Way Handshake 26
  2.7.3 WPA Weaknesses 27
2.8 WPA2 29
2.9 Summary 30

3 METHODOLOGY

3.1 Introduction 32
3.2 Methodology Stages 32
  3.2.1 Understand Wireless Security Vulnerabilities 34
  3.2.2 Analyze & Collect Proper Tools 34
    3.2.2.1 Airowizard 1.0 Beta 34
    3.2.2.2 Cain & Abel 35
    3.2.2.3 Commview 37
    3.2.2.4 Aircrack-ng 39
4 PRE-ANALYSIS RESULT AND FINDING

4.1 Introduction
4.2 Finding
4.3 Critical Analysis
4.4 WEP/WPA Key Cracking Steps
  4.4.1 Required Equipment
  4.4.2 Capture Data From Air
  4.4.3 Start Cracking From Captured Data
  4.4.4 The Whole Attack Steps
4.5 The Extensiveness of WEP in UTM Campus
4.6 WEP Attack Result
4.7 WPA Attack Result
4.8 Summary

5 IMPLEMENTATION AND RESULT
5.1 Introduction
5.2 Proposed Wireless Network Security Policy
  5.2.1 Overview
  5.2.2 Definition
  5.2.3 Purpose
  5.2.4 Scope
## LIST OF TABLES

<table>
<thead>
<tr>
<th>TABLE NO</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Summary of WEP Attacks</td>
<td>20</td>
</tr>
<tr>
<td>2.2</td>
<td>Comparison of WPA and WEP</td>
<td>25</td>
</tr>
<tr>
<td>2.3</td>
<td>Summary of WPA Attacks</td>
<td>29</td>
</tr>
<tr>
<td>2.4</td>
<td>Comparison of WPA, WPA2 and WEP</td>
<td>30</td>
</tr>
<tr>
<td>4.1</td>
<td>WEP Survey Result</td>
<td>53</td>
</tr>
<tr>
<td>5.1</td>
<td>Characteristics of Various Jammers</td>
<td>65</td>
</tr>
<tr>
<td>5.2</td>
<td>Advantage and Disadvantage of Proposed Jamming Program</td>
<td>66</td>
</tr>
<tr>
<td>5.3</td>
<td>Hardware/Software used for Program Testing</td>
<td>69</td>
</tr>
</tbody>
</table>
## LIST OF FIGURES

<table>
<thead>
<tr>
<th>FIGURE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>WEP Encryption Process</td>
<td>14</td>
</tr>
<tr>
<td>2.2</td>
<td>WEP Decryption Process</td>
<td>15</td>
</tr>
<tr>
<td>2.3</td>
<td>Open System Authentication Process</td>
<td>16</td>
</tr>
<tr>
<td>2.4</td>
<td>Shared Key Authentication Process</td>
<td>17</td>
</tr>
<tr>
<td>2.5</td>
<td>Successful Four-way Handshake</td>
<td>27</td>
</tr>
<tr>
<td>3.1</td>
<td>Project Methodology</td>
<td>33</td>
</tr>
<tr>
<td>3.2</td>
<td>Unencrypted password and Username Captured</td>
<td>36</td>
</tr>
<tr>
<td>3.3</td>
<td>ARP Spoofing to Intercept Data between machine A and B</td>
<td>36</td>
</tr>
<tr>
<td>3.4</td>
<td>Telnet Session Captured</td>
<td>37</td>
</tr>
<tr>
<td>4.1</td>
<td>WEP/WPA Attack Flowchart</td>
<td>50</td>
</tr>
<tr>
<td>4.2</td>
<td>CICT_AP Cracking Time</td>
<td>54</td>
</tr>
<tr>
<td>4.3</td>
<td>CICT_AP Key Found</td>
<td>54</td>
</tr>
<tr>
<td>4.4</td>
<td>Key Found in College</td>
<td>55</td>
</tr>
<tr>
<td>4.5</td>
<td>UKLP AP Handshake Captured</td>
<td>56</td>
</tr>
<tr>
<td>4.6</td>
<td>SMUHR AP Handshake Captured</td>
<td>56</td>
</tr>
<tr>
<td>4.7</td>
<td>Passphrase not Found in Dictionary</td>
<td>57</td>
</tr>
<tr>
<td>5.1</td>
<td>Jamming Program Flowchart</td>
<td>67</td>
</tr>
</tbody>
</table>
5.2 AP and Client Authentication and Deauthentication 68
5.3 Main Menu of the Program 70
5.4 Error Message 71
5.5 Option 1 has been selected 72
5.6 APs Scanning 72
5.7 Target AP’s BSSID has been selected 73
5.8 Target AP’s Channel has been selected 74
5.9 Target AP Jamming Started 79
CHAPTER 1

INTRODUCTION

1.1 Overview

Wireless networks are more vulnerable to many attacks than wired networks, because wireless network transmits date over the air, and can be easily intercepted by an attacker who is within range of the signals. It is difficult to control accessing to wireless network resource, an attacker can get access outside of the organization and the wireless network administrator/owner might not aware of. The attacker can sniff sensitive data by impersonating as a legitimate user. The wireless security protocols especially WEP encryption is easy to crack. Wired equivalent privacy (WEP) is a security protocol specified in the IEEE. Wireless Fidelity (Wi-Fi) standard 802.11b. The software to hack WEP keys is widely available on the internet. The attacker can compromise a protected wireless access point by hacking wireless password key and share bandwidth; this is very challenging problem in wireless network.
Wireless network should provide confidentiality by protecting unauthorized access and eavesdropping (Lashkar and Danesh, 2009). In addition wireless network should provide integrity to the network data by protecting spoofing and man in the middle attack. Apart from the above requirements there are other security aspects that the wireless network should provide. The main security issues in wireless network include:

i. **Access:** wireless administrator or user must make sure that only authorized users can use the wireless network. Without proper access control someone in the surrounding area of the building can use the wireless network. Access control involves by using wireless security protocols (WPA/WPA2) to control access.

ii. **Privacy:** wireless administrator must make sure that no one can sniff the communication. Without proper security, anyone can sniff all communication on a wireless network.

1.2 **Internet and Wireless Communication**

The Internet is one of the most powerful tools throughout the world. Schools, hospitals, universities, business, government sectors and many more are highly depend on the internet. People use internet with variety of purposes. Using internet, users can communicate to each other via email or similar technologies. Email is now an essential communication tools in business. Email is free and fast when compared to telephone, fax and postal services.

People use internet for different purposes as mentioned above, people can buy or sell products by using internet. Users connect to the internet by using different methods such as DSL, cable or Wireless devices. Wireless network doesn’t require cable installation and it’s easy to configure compare to wired services like DSL and cable. Internet provides many services such as online banking, job seeking and application, and many more. Today Internet is one of the fundamental needs in our daily activities, however; internet can be source of risks. Using internet, someone
could steal sensitive information such as credit card details or username and password. Some internet users are not aware of internet risks and expose sensitive information through internet technologies. As mentioned earlier users connect to the internet using different methods such as wireless devices.

Wireless network is a flexible data communications system that provides communication over short distances using radio or infrared signals (Leonard and Mischa, 2010). Wireless network has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing, and warehousing. Wireless network is easier to install in comparison to wired network which consumes time during cabling. Wireless network plays important roles in many areas such business and many more. Wireless network provides mobility, convenience, and cost advantages over traditional wired network (Ramiro and Abdallah, 2002). Wireless networks provide users with access to real-time information. This nature mobility makes wireless network to attract many users especially business areas to support productivity and service opportunities that is not possible with wired networks. Organizations chose wireless network to improve their competitiveness. Many organizations prefer wireless network to avoid expensive cabling and wiring costs, installing wireless network is pretty easy at the same time fast and eliminates the needs to pull cable through walls and ceilings. Wireless network can be available in several areas such cafeterias, airport etc which is not possible in wired network.

Previously wireless network were single-vendor proprietary solutions, this means communication between two entities is not possible unless the wireless network products from same vendor. Therefore this was big problem that was required to eliminate. In 1997, the computer industry developed the IEE 802.11 wireless Ethernet standard that makes possible communication among different wireless network products from different vendors (Ranjana et al., 2010). The most commonly known of these standards is the 802.11a, b, g and n (Mingjun et al., 2011). 802.11a is an extension to 802.11 that applies to wireless LANs and provides up to 54-Mbps in the 5GHz band. 802.11a uses OFDM (Orthogonal Frequency Division Multiplexing). It is a very effective when performing more than one task at a time and or crowded time. 802.11b (also referred to as 802.11 High Rate or Wi-Fi)
is an extension to 802.11 that applies to wireless LANs and provides 11 Mbps transmission in the 2.4 GHz band. 802.11b has the straight addition of modulation technology same as in 802.11. Mostly 802.11b suffered from the intrusion of other products. 802.11g applies to wireless LANs and is used for transmission over short distances at up to 54-Mbps in the 2.4 GHz bands. 802.11g was authorized in 2003 as a third modulation device with 2.4 GHz band. It provide maximum data rate with 54Mbit/s at physical layer. The hardware of 802.11g is totally compatible with 802.11b. 802.11n recognized in 2009 as a final endorsement in 802.11 Standards family. All type of enterprises was previously transferred to 802.11n networks. These all enterprises based on Wi-Fi Alliance's. Wi-Fi is a certified product for 802.11n application to make 802.11 standard families more useful and compatible to new era because WiFi fulfill the requirements of new era where no need to spend time for the arrangement of wires or cables and so on.

1.2 Problem Background

Current wireless network is vulnerable to many attacks, hackers can break wireless network security protocols such as WEP and access protected wireless without owner’s knowledge. The weakness of WEP includes; lack of prevention forgery of packets, lack of replay attack prevention, WEP allows an attacker to undetectably modify a message without knowing the encryption key and easy forging of authentication messages (Lashkar and Danesh, 2009).

WPA was developed to overcome WEP security weakness; WPA provides better security and strong encryption. WPA is not easy to hack unless the user or the owner uses weak and dictionary word as password. WPA’s encryption method is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the weaknesses of WEP by including a per-packet mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism (Martin, 2008)
Access control and privacy are the main wireless security issues. Without proper access control someone in the surrounding area of the building can use the wireless network without the legitimate user’s knowledge. Some access points in UTM are open (no encryption) while others was deployed WEP encryption that is easy to break and access. Privacy is required in wireless networks; without privacy anyone can sniff all communication on a wireless network.

To provide more secure wireless (UTM wireless); it’s recommended to replace WEP and use WPA with strong password. It’s also recommended to use end to end encryption such as secure socket layer (SSL). Beside the above mentioned problems, the following are also vulnerabilities of wireless network:

i. Sensitive information that is not encrypted and that is transmitted between two wireless devices could be compromised and disclosed.

ii. Malicious entities may gain unauthorized access to an agency’s network through wireless connections.

iii. Denial of service (DOS) attacks

iv. Malicious entities may be able to violate the privacy of legitimate users

v. Malicious entities may deploy unauthorized access points to steal sensitive information

1.3 Problem statement

Wireless networks are difficult to control access areas. Unauthorized user might access to wireless network and sniff user’s communication. Attacker can break wireless security protocols such as wired Equivalent Privacy (WEP) easily. In this study, University Technology Malaysia (UTM) wireless network has been selected as case study. Several UTM wireless access points are being deployed with WEP which can be cracked in minute.
1.4 Project Objectives

i. To study vulnerabilities of Wired Equivalent Privacy (WEP) and WPA

ii. To analyze risks of Wired Equivalent Privacy (WEP) encryption

iii. To propose strategies to control the use of WEP in the campus.

1.5 Project Scope

The scope of this study is to analyze wireless network security vulnerabilities by performing wireless security attack against WEP and WPA. UTM wireless network has been chosen as case study. In the line with this scope, the study also covers the literature reviews about wireless network security issues.

1.5 Significance of the study

Several wireless networks are deployed with wireless security protocol such as WEP and WPA. However, several wireless access points are open (no encryption). Open wireless is very danger; an attacker can sniff sensitive data such as passwords and credit card details. WEP is easy to crack; anyone who have hacking tools can compromise wireless network and can access without owner’ knowledge. Numerous wireless network users are unaware of wireless security threats, this increases wireless security risks. The transmitted data/information over wireless network should be protected. Securing wireless network is very crucial due to the large data transmission over wireless network.
1.6 Summary

This chapter discussed about the project introduction, project problem background, problem statement, objectives, scope and significance of the research. Solution will be proposed at the end of this study.
CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter covers several literature reviews about wireless network security issues. The literature search is a very significant step in the research process (E. Reed, 1998). The literature review helps to understand and present the research area. In this study, the purpose of literal review is to point out the security issues in wireless network and to know what researchers have discovered in the past to get better understanding in the study.
2.2 History of Wireless Network

In 1888 Heinrich Rudolf Hertz has demonstrated the theory of electromagnetic waves. This theory was predicted by James Clerk Maxwell and Michael Faraday. Hertz demonstrated that electromagnetic waves could be transmitted and could travel via space and the transmitted waves were received by an experimental device. David E. Hughes induced electromagnetic waves in a signaling system. Hughes transmitted Morse code by an induction device. The work done by James Clerk Maxwell could be considered as the true history of the wireless technology because his contribution to science was effective. At the age of 42, he demonstrated the science of electromagnetism and he explained his initially controversial four equations which are known as Maxwell’s equations (Leonard and Mischa, 2010). The theory of electromagnetic radiation has led the use of radio waves for radio, television and personal mobile communications and so forth. By using his equations, he proved that electrical and electromagnetic phenomena can be used as waves.

In 1895 Italian electrical engineer Guglielmo Marconi has improved the transmission theory and he adopted the technology to send and receive wireless telegraph signals. This engineer has built the first transoceanic telegraphy transmitter in 1901. Gradually the quality of the voice transmission was improved since the technology was getting attention to many engineers and authors. In 1930s (Leonard and Mischa, 2010) small two-way transmitters were developed and used by law enforcement and civil emergency authorities.

In 1992 WLAN products that used the 2.4 gigahertz band was available at market. Even though these products were able transferring higher data compare to previous products which provided 900 MHz frequency band, but these products were based on proprietary designs. Lack of interoperability among different brands of WLAN products has made possible the development of wireless network standards.
2.3 Wireless Network Components

Wireless network is easy to install unlike wired network. Wireless network eliminates the needs to pull cable through walls and ceilings. Basic components of a wireless network are Access points (APs) and Network Interface Cards (NICs)/client adapters.

2.3.1 Access Points

Access Point (AP) is essentially the wireless equivalent of a LAN hub. It is typically connected with the wired backbone through a standard Ethernet cable, and communicates with wireless devices by means of an antenna. AP authenticates and associates wireless clients to the wireless network.

2.3.2 Network Interface Cards (NICs)/Client Adapters

Wireless client should have network interface cards/client adapters in their workstation in order to communicate with wireless network. The NIC can scan the available access points and associate with. The NIC allows users to connect wireless network instantly.
2.3.3 Antenna

Antenna is required in order to send or receive data over wireless network. Antennae can degrade the performance of wireless network. Proper installation of the antenna is crucial for a wireless network.

2.4 The importance of Security in Wireless Network

Wireless networks are more vulnerable to hackers compare to wired networks (Srivatsa, 2008). Wireless network use radio waves and your network’s signal can be visible in distance areas such as your neighbor. Without using the latest security protocols, an attacker can view wireless network communication activities. In addition an attacker can access network hiding his/her IP and damage or steal sensitive information by using unauthorized wireless network. This is risk because if the attacker did illegal activity by using the victim’s network, it could be traced back to the victim’s wireless network and the victim has to take the responsibilities. Wireless signal is short range, but hacker can make your signal to reach many miles away by using antenna (Srivatsa, 2008).

Hacker hack wireless network either for personal use such as getting free internet or illegal reasons. Hacker can share your bandwidth, this makes wireless network slow and the victim should pay extra cost for the bandwidth usage. Unauthorized user can do malicious activities such as hacking, launching a DOS attack or distributing illegal material such as viruses by using your network (Liu et al., 2010).
A hacker may set up a fake AP and then capture all users’ traffic, and then the professional hacker can get victim’s email account password, face book account details and credit card information. Furthermore hacker may install spyware into the victim’s computer via wireless connection. As long as the victim uses that computer, the hacker will get an email that allows watching user’s activities even if the user is far away.

2.5 Methods of Attacking Wireless Network

Exploration is the first thing that the hackers do before attacking wireless network. Hackers use laptop or PDA, wireless card and sniffing tool that allows discovering any nearby wireless access point to obtain information about the AP. For example, the hacker will observe the type of wireless security protocol deployed. Since the wireless transmits data in the air, hackers can get data they want. These data includes access point name (SSID), security type, network type, channel number and MAC address. Hacker can break into wireless network by using the following methods (Peisong and Guangxue, 2010).

SSID spoofing: SSID is shared between clients and AP, therefore hackers can see it. The AP broadcasts data to all clients and the hacker can get AP name, channel, and MAC address. Hacker can perform attack against wireless using SSID association.

MAC spoofing: to prevent this attack, wireless LAN uses MAC filtering security mechanism, however it is insecure. In other word, MAC filtering is a security mechanism that only allows Valid MAC address to access into the wireless. If the hacker’ MAC address is rejected by this security mechanism, he can change his MAC address to a valid MAC address to get access into the wireless. Hacker can use some software that can get MAC addresses easily.
Authentication Spoofing of WEP: to access AP, client should know the shared WEP key to authenticate. Hacker can capture the data exchanged between client and AP, then Hacker can create a fake authentication message and the AP will authenticate as a legitimate user. In addition hackers can get the WEP key from windows register, this makes the attack easier. WEP uses RC4 algorithm that was found weakness, therefore attacker can crack WEP by breaking the RC4 algorithm.

2.6 Wired Equivalent Privacy (WEP)

Wired equivalent privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b (Jiang et al., 2008). Hackers can hack WEP by using an open source tools such as aircrack-ng that runs on Linux system and windows. These tools can compromise WEP keys in seconds after listening to 100MB-1GB of traffic.WEP is recognized as insecure since it uses static keys, however some wireless APs are being deployed without security (no encryption) and this increases the security risks of wireless networks.

WEP has three settings; off (no security), 64-bit and 128-bit. WEP was designed to provide three main security goals such as data integrity, access control and data confidentiality. However WEP fails to achieve these goals due to security weakness in the implementation (Peisong and Guangxue, 2010). WEP doesn’t fully protect the data integrity, because CRC checksum only protects against random errors. Therefore an attacker can modify the message and forward the packets to the legitimate clients and APs (Wang et al., 2010). WEP is still employed in many APs due to the fact that old network interface card may not match the requirements of newer security protocols.
i. **Seed generation**: The secret key is concatenated with an initialization vector (IV) (i.e. IV || Secret Key)

ii. **Compute ICV**: CRC-32 of the plaintext (payload data)

iii. **Compute Key stream**: Key stream = RC4 (seed)

iv. **Encryption**: Cipher text = Key stream XOR (Plaintext || ICV)

v. **Message** = IV || Cipher text

Once the message is encrypted and transmitted; the receiver side should able to read the message, therefore decryption process is required. The decryption is verified by the integrity check algorithm on the recovered plaintext and the output of the ICV’ will be compared to the ICV submitted with the message. However; the problem is that the CRC-32 ICV an attacker can modify the encrypted message and the message will appear authentic. Figure 2.2 Shows how WEP is decrypted.
2.6.1 WEP Authentication

Wireless network has no physical connection between nodes, this make the wireless links susceptible to eavesdropping and information theft. To prevent those problems and to provide security, the IEEE 802.11 standard has defined two types of authentication methods, open system authentication (OSA) and shared key authentication (SKA) (Arbaugh et al., 2001).

The Open system authentications does not have authentication. The station or user can access any available access points and he/she can listen to data that sent in plaintext. This type of authentication is not secure as you already realized. This authentication normally used when the network administrator does not care about the security issues. This type of authentication deploys access points at airports, cafeterias and similar public areas to give users free wireless access points.
The following steps occur when two devices use Open System Authentication:

i. The station sends an authentication request to the access point.

ii. The access point authenticates the station.

iii. The station associates with the access point and joins the network.

The shared key authentication uses a shared key to authenticate the station to the access point. The user should have a shared key to access the wireless, failing so won’t be able to connect and access the network. This authentication uses wireless security protocols such WEP. The shared key authentication is much better and secure compare to the open system authentication. Figure 2.4 shows the authentication process.
The following steps occur when two devices use Shared Key Authentication:

i. The station sends an authentication request to the access point.

ii. The access point sends challenge text to the station.

iii. The station uses it’s configured 64-bit or 128-bit default key to encrypt the challenge text, and it sends the encrypted text to the access point.

iv. The access point decrypts the encrypted text using its configured WEP key that corresponds to the station’s default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP key, and the access point authenticates the station.

v. The station connects to the network.

The challenge text from AP to client is sent in clear which means an attacker can read it (Arbaugh et al., 2001). The client responds with encrypted text. Therefore an attacker can eavesdrop on both challenges and he may obtain key stream by exclusive-oring the challenges. Access point and client use the same WEP key and the key is not dynamic. The attacker can also modify and redirect the packets from network to himself (IP redirection) (Maocai et al., 2008). The attacker may also release the modified packets to obtain information about ACK (TCP Reaction Attack).
2.6.2 Key Size and Configuration

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit (G. Zeynep et al., 2006). These bits were added 24-bit (factory-set), 40-bit+24-bit gives 64-bit encryption key. Similarly 128-bit WEP key consists of 104-bit (user-configurable bit) and 24-bit IV (104-bit+24-bit) which provides 128-bit WEP data encryption (Dongsheng Yin et al., 2011). For the encryption/decryption data those keys will be used. Some vendors consider 64-bit WEP data encryption as 40-bit WEP data encryption because the functionality is same. When 40-bit encryption used, each 40-bit WEP defined five sets of hexadecimal digits. 128-bit WEP key gives 13 sets of two hexadecimal digits. For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP key. The same key should be entered in both access point and client PC. For example, WEP key 1 on client pc should match WEP key 1 on the AP.

2.6.3 WEP Attacks

In 2001 Fluhrer, Mantin and Shamir published a paper titled “Weaknesses in the Key Scheduling Algorithm of RC4” that introduced FMS attack. This was the first recovery key attack. This attack involves sniffing packet traffic of WEP protected network and captures several packets such as initial vectors (IV) used for the packets. The first bytes of the plaintext could be predictable by an attacker. After capturing enough cipher text, the attacker can determine the secret key. The attacker should know the first few bytes of the plain text otherwise the attack won’t be success. The number of packets needs to success is 4 to 6 million with probability greater or equal to 50% (Caneill and Gilis, 2010). There are tools that facilitates FMS attack, these tools includes AirSnort and aircrack which used to crack WEP.
In 2004, a person under the name KoreK posted [kor04b] an implementation of a WEPcracker; a person posted in netstumbler forum. This attack was based on the FMS attack but extended with 16 more correlations between the first bytes of an RC4 key and the next key bytes (Caneill and Gilis, 2010). This attack reduced the number of needed packets to 700,000 for 50% success probability.

In 2007, PTW attack has released by Tews, Weinmann, and Pyshkin. The researchers used a tool named Aircrack-PTW to proof their work. To perform successful attack, attacker should capture number of IVS from 35,000 to 40,000 packets (Caneill and Gilis, 2010) for 50% success probability; this amount can be captured in less than 60 seconds if the network is fast. Later some modifications were made to the PTW attack and the number packets needed was reduced.

Another attack named Chopchop attack was discovered by Korek, this attack allows the attacker to decrypt a packet without knowing the key. In other word this attack Allows an attacker to decrypt the last $m$ bytes by sending $m * 128$ packets to the network (Caneill and Gilis, 2010). Due to lack of replay protection in WEP network; the attacker can brute force the value to get the correct key. Once the correct value is found, the attacker can calculate the byte of plaintext and key stream and finally the attacker will be able to decrypt a packet without knowing the master key. Here are the main WEP security problems:

i. WEP does not prevent replay attacks: an attacker can replay packets and can impersonate as authorized party.

ii. WEP uses RC4: the WEP keys are easily to brute-force in hours or minutes by using widely available software.

iii. WEP allows an attacker to modify communication messages between legitimate users without knowing the encryption keys.

iv. Key management is lack and updating is poor.

v. Most users usually do not change their keys. This gives hackers more time to crack the WEP keys.
Utilizing these problems, attacker can get access into wireless network in many ways. There are many tools that can decrypt and crack WEP security. By using these widely available tools WEP key can crack in short period of time. One of the fastest tools that the hackers use to break WEP security is BackTrack Linux Distribution. Hackers just need normal computer with wireless card that supports monitoring mode and the software (BackTrack). BackTrack combines several tools such as aircrack-ng, airdump-ng, aireplay-ng and much more. Hackers can either install BackTack in their computer or they can run from Live CD. As long the wireless is deployed with WEP, BackTrack can compromise the key. The time required to break WEP depends on the speed of the AP and the distance of the AP.

Table 2.1 Summary of WEP attacks

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Year</th>
<th>Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>FSM</td>
<td>Statistical</td>
<td>2001</td>
<td>4 to 6 million</td>
</tr>
<tr>
<td>KoreK</td>
<td>Statistical</td>
<td>2004</td>
<td>700,000</td>
</tr>
<tr>
<td>PTW</td>
<td>Statistical</td>
<td>2007</td>
<td>35,000 to 40,000</td>
</tr>
<tr>
<td>Chopchop</td>
<td>fake ARP</td>
<td>2004</td>
<td>1 at begin (later: injection-capture)</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>Fragmentation</td>
<td>2005</td>
<td>1 at begin (later: injection-capture)</td>
</tr>
<tr>
<td>Google replay</td>
<td>Replay</td>
<td>2010</td>
<td>1 at begin (later: injection-capture)</td>
</tr>
<tr>
<td>Coolface</td>
<td>man-in-the-middle</td>
<td>2010</td>
<td>0 at begin (later: injection-capture)</td>
</tr>
</tbody>
</table>
2.6.4 WEP Secret Key

WEP incorporates two main types of protection: a secret key and encryption. The secret key is a simple 5- or 13-character password that is shared between the access point and all wireless network users. WEP creates a unique secret key for each packet using the 5- or 13-characters of the pre-shared key and three more pseudo-randomly selected characters picked by the wireless hardware. For example, if our pre-shared key was “games”. This key would be combined with “abc” the secret key would be “abcgames”, which would be used to encrypt the packet. As mentioned above each packet has unique secret key, therefore next packet’s secret key would be “xyzgames”. The process of changing secret keys is called the initialization vector it initializes the encryption process for each packet of data sent.

2.6.5 RC4 Encryption Algorithm

RC4 is the encryption algorithm used to cipher the data sent over the airwaves. Encryption is important to protect privacy. RC4 is a method of encryption that encrypts each and every byte of data sent in a packet. RC4 consists of two parts: the key scheduling algorithm (KSA) whose key size is 40-256 bits, and the pseudo random Generation algorithm (PRGA). This algorithm deals with encryption and decryption processes. RC4 used by standards such as IEEE 802.11 within WEP with different key size 40 and 128-bit keys (Yao et al., 2010).

RC4 was found two main weaknesses, large class of weak keys and key vulnerability. The weak key is the key that is used in several times and makes the cipher vulnerable to attack (Pamnani and Chawan, 2009). Attacker can discover the key by collecting enough packets.

Key vulnerability means that the attacker can observe the cipher operation specially if the attacker knows the mathematical connection between different keys (IV, WEP key) of a cipher. The key can be compromised since the WEP key is static
and the IV is reusing as mentioned earlier. These weaknesses in RC4 (Yao et al., 2010) allow the attacker to perform passive attacks to recover RC4 key. This attack can be implemented by either forcing the traffic on the network (IP redirection) or eavesdropping on the network traffic. The time needed to obtain the key depends on the speed of the network and the number of packets captured.

Automated tools were used to attack WEP. WEPCrack was the first automated tool that was publically available and was released on Aug 12, 2001. One week later, another tool named AirSnort that can collect packets and compute the key was released. These automated tools allow the attacker to crack RC4 key in 2 minutes or less and attacker could use normal computer (Pamnani and Chawan, 2009).

2.6.6 How Attacker Attacks WEP

WEP was found security flaws due to the way it implemented the RC4 streaming cipher (I. P. Mavridis et al., 2011). Key is shared between the access point and the client and is used to perform an XOR function on the plaintext; to decrypt the original plaintext the receipt should XORed the ciphertext.

As mentioned above WEP uses RC4 to generate a stream of random bytes. RC4 initiates a secret key, the secret key generates before the random bytes generated. If two users in the range both use the same secret key, they will generate the same random bytes. Once the user receives the message, the user can XOR the random bytes out of the encrypted message and then re-create the original.

WEP’s IV size is only 24-bit which provides $2^{24} (16,777,216)$ random keys and 9,000 of these keys are weak (I. P. Mavridis et al., 2011). This number $(16,777,216)$ seems large but busy network can use these keys within few hours. Therefore the problem of 24-bit IV is reusing the key. Furthermore IV is sent in the
clear (can be read) with each packet. The attacker can capture the IV or can forge packets.

### 2.6.7 WEP Past Solutions

After number of flaws has been found, WEP protocol was extended to overcome the security flaws. The first extension was releasing WEP2 (Arbaugh et al., 2001). WEP2 extended the IV and key values to 128 bit in order to avoid brute force attack. WEP2 did not eliminate the reuse of IV; therefore WEP2 could provide a solid security solution.

The second extension was WEPPlus. WEP+ is a proprietary protocol that is intended to enhance WEP security. WEP avoids weak IVs, however; it doesn’t prevent replay attacks. The disadvantage of WEP+ security was that it had to be employed at both ends of wireless connections, which was difficult to enforce. Since WEP2 and WEP+ failed to overcome security weakness, the need for better security solution continued to grow.

### 2.7 Wi-Fi Protected Access (WPA)

WPA is a security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. WPA is intended to solve problems in WEP by implementing cryptography method. WPA provides mutual authentication, and the key is never transmitted over the air (Kołodziejczyk, and R. Ogiela, 2010). WPA provides more complex data encryption on the protocol Temporal Key Integrity Protocol (TKIP) than WEP. In addition WPA assisted by MIC (Message Integrity Check), MIC uses a hashing technique to avoid attacks of bit-flipping. WPA has two operational manners; Personal WPA or WPA-PSK (Pre-
shared key) and Enterprise WPA or Commercial (Kołodziejczyk, and R. Ogiela, 2010).

WPA-PSK is a special mode of WPA for home and small office users which can’t afford the authentication server. WPA-PSK provides strong encryption where encryption keys automatically changed (rekeying) and authenticated between devices after a specified number of packets has been transmitted. WPA-PSK uses a method called shared secret, the shared secret must be entered in WPA clients and access point/ router (Vallikumar et al., 2011). The users are authenticated to the AP with a passphrase which is between 8 to 63 ASCII characters or 64 hexadecimal digits long.

Enterprise WPA or Commercial uses 802.1 x authentications by means of a Radius server to authenticate users with their username and password or a certificate (Tavallae, 2007). This implemented in large enterprises that have many clients. WPA was developed to overcome the weakness of WEP headers, which are called initialization vectors (IV), and insures the integrity of the messages by using MI (Michael or message integrity check) and TKIP (the Temporal Key Integrity Protocol) to improve data encryption (Tavallae, 2007). WPA is more secure than WEP; hackers cannot extract the PSK from intercepted packets. However; it is possible to capture handshake packets. When the handshake from successful authentication is captured, a hacker can use data from this handshake to perform offline efforts to unmask the passphrase against a dictionary of possibilities. To use WPA, all access points, computers and wireless adapters must be installed with WPA software.

2.7.1 WPA VS WEP

WPA and WEP both use RC4 stream cipher for encryption. WPA has improved the short IV and employs 48-bit IV with the 128-bit key. WEP’s security was inadequate due to the IV collisions and modified packets. WPA has solved these
problems by implementing the combination of temporal key integrity protocol (TKIP), message integrity check (MIC) and the extended IV (Maocai et al., 208). TKIP changes the encryption key on every packet. MIC prevents the message modification and also prevents packet forgery.

As mentioned earlier WPA uses 802.11x/EAP and PSK-mode which provides concrete user authentication mechanism. In WEP user can get access the network by using the shared-key authentication mechanism that involves the use of challenges between AP and client. This process uses the same pre-shared WEP key that was used in encryption, this increases the security risks. Unlike WPA the encryption and the authentication are separated. A summary of the differences between WEP and WPA is shown in Table 2.2.

Table 2.2 Comparison of WPA and WEP

<table>
<thead>
<tr>
<th>Feature</th>
<th>WEP</th>
<th>WPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master keys</td>
<td>Used directly</td>
<td>never used directly</td>
</tr>
<tr>
<td>Encryption Key Management</td>
<td>None</td>
<td>802.1x</td>
</tr>
<tr>
<td>Encryption Key Size</td>
<td>40 bits</td>
<td>128 bits</td>
</tr>
<tr>
<td>Message integrity checking</td>
<td>CRC-32</td>
<td>MIC (Michael)</td>
</tr>
<tr>
<td>Encryption Key Change</td>
<td>None</td>
<td>For Each Packet</td>
</tr>
<tr>
<td>IV Size</td>
<td>24 bits</td>
<td>48 bits</td>
</tr>
<tr>
<td>Authentication</td>
<td>Weak</td>
<td>802.1x – EAP</td>
</tr>
<tr>
<td>Header Integrity</td>
<td>None</td>
<td>MIC (Michael)</td>
</tr>
<tr>
<td>Replay Attack Prevention</td>
<td>None</td>
<td>IV Sequence</td>
</tr>
</tbody>
</table>
2.7.2 WPA Four-way Handshake

In WPA both client and access point have a shared key known as the Pairwise Master Key (PMK). PMK is derived from the WPA passphrase/ pre-shared key (PSK) or provided by the end user using this function. The difference between PSK and PMK is that PMK has a 256 bit secure key that is generated from the PSK and the wireless network (SSID) uses as a seed while PSK is a random word entered by the user. WPA ensures that no attacker can pre-compute all possible PMK’s by using diction word as PSK’s.

When a wireless client tries to gain access to an access point (AP) there will be a little conversation between the client and access point (AP); this is the so called “4-way handshake”. An attacker can capture a handshake and can start dictionary attack. To capture a handshake it can take some time, therefore the attacker can launch de-authentication attack to force a client to de-authenticate (Kadlec et al., 2009).

To perform de-authentication attack the attacker can use aireplay-ng. As soon as the hacker capture 4-way handshake, he can start aircrack-ng or similar tools to perform dictionary attack. Due to unawareness of wireless threats, a network owner may use simple and short passphrase that can be predictable and can be found in a wordlist. Dictionary attack can be success or can be fail depends on the weakness of the passphrase used. Figure 2.4 shows WPA-PSK authentication process.
In November 2003, Robert Moskowitz released “Weakness in Passphrase Choice in WPA Interface”. In his paper he explains a formula that would expose the passphrase by performing a dictionary attack against WPA-PSK networks. The weakness he found was based on the SSID, length of SSID, the pairwise master key (PMK) and nonces (a number or bit string used only once in each session) (Ohigashi and Morii, 2009).

The researcher also explains that the pairwise transient key (PTK) is a keyed-HMAC function based on the PMK; by capturing the four-way authentication handshake, the attacker can perform dictionary attack to find the passphrase. Finally he found that a key generated from a passphrase of less than 20 characters is unlikely to prevent attacks.

In 2004, Takehiro Takahashi and a student at Georgia Tech released WPA Cracker. Josh Wright, a network engineer and well-known security lecturer, released cowpatty around the same time (Ohigashi and Morii, 2009). These tools were
developed for Linux systems to perform a brute-force dictionary attack against WPA-PSK networks to crack and find the shared passphrase. To use these tools users are required to use dictionary file to crack the shared passphrase. Each tool uses the PBKDF2 algorithm that governs PSK hashing to attack and determine the passphrase, however; cowpatty is faster than WPA cracker.

In 2008 it was reported flaws had been found in WPA and it was partially cracked. WPA that use TKIP was found by researchers to be crackable in 15 minutes (a window later shortened to 60 seconds) (Padilla and Guillen, 2010).

In 2009, The Ohigashi-Morii Attack was published by by T. Ohigashi and K. Mori in a paper titled “A Practical Message Falsification Attack on WPA”. This attack is an improvement of the Beck-Tews attack and it reduced the time to inject a fake packet approximately to 1 minute, therefore its faster, simpler compare to the implementation of the Beck-Tews attack (Martin Beck, 2010). This attack introduces man in the middle (MIM) between the victim client and the access point to intercept the packets transmitted. The attacker creates holes in client’s sequence number counter to replay packets.

In 2010, Airtight Networks published details about a vulnerability that is called Hole 196, in which a malicious client spoofs packets from access point. This malicious impersonates as access point and sniff traffic on the network or cause service disruption. This vulnerability caused by the use of the group temporal key (GTM) that is shared among all authorized clients in a WPA2 network. Authorized user can sniff and decrypt data from other authorized users and install malware or compromise the authorized user’s devices. To perform this attack, malicious user must know the group temporal key (GTM) that is shared by the authorized users in that network. Therefore only an insider user of a WPA can do this attack. As can be understood WPA is not without its vulnerabilities. Table 2.3 show summary of WPA attacks.
Table 2.3 Summary of WPA Attacks

<table>
<thead>
<tr>
<th>Name</th>
<th>Year</th>
<th>Utility</th>
<th>Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beck and Tews</td>
<td>2008</td>
<td>inject traffic (QoS features)</td>
<td>24</td>
</tr>
<tr>
<td>Ohigashi-Morii</td>
<td>2009</td>
<td>inject traffic (in all modes)</td>
<td>2</td>
</tr>
<tr>
<td>Michael</td>
<td>2010</td>
<td>inject traffic (in all modes)</td>
<td>1</td>
</tr>
<tr>
<td>Hole196</td>
<td>2010</td>
<td>man-in-the-middle, inject traffic, DoS attack</td>
<td>-</td>
</tr>
<tr>
<td>Dictionary attack</td>
<td></td>
<td>key-recovery</td>
<td>-</td>
</tr>
</tbody>
</table>

2.8 WPA2

WPA2 is a new version of WPA and is based on IEEE 802.11i (Shaneel et al., 2009) standard. WPA2 uses new an algorithm called advance encryption standard (AES) algorithm CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) to eliminate the use of RC4 stream cipher.

AES encryption uses 256-bit (Abidalrahman and yaser, 2011) block ciphers to provide stronger protection for the wireless. Here is how the AES processes data before being sent.

i. **Intial** Data is converted into 256-bit blocks.

ii. **SubByte** Each byte goes through 8-bit lookup tables.

iii. **ShiftRows** Shift each row in the block by an offset.

iv. **MixColumns** Each column 4-bytes are mixed.

v. **AddRoundKey** Each block is XOR with subkey.

WPA2 uses a 48-bit IV as a sequence number to prevent replay attack (Prof. Dr. Gamal et al., 2006). WPA2 supports IEEE 802.1X/EAP authentication or PSK technology. WPA2 has two versions; WPA2 Personal and WPA2 Enterprise (Shaneel et al., 2009). WPA2 personal requires setting up password to protect
unauthorized network access. WPA2 enterprise authenticates network user via a server. The relationship between WPA2, WPA and WEP shown in table

<table>
<thead>
<tr>
<th></th>
<th>WEP</th>
<th>WPA</th>
<th>WPA2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Cipher</td>
<td>RC4</td>
<td>RC4</td>
<td>AES</td>
</tr>
<tr>
<td>IV size</td>
<td>24 bit</td>
<td>48 bit</td>
<td>48 bit</td>
</tr>
<tr>
<td>Data integrity</td>
<td>CRC-32</td>
<td>Michael</td>
<td>CCM</td>
</tr>
<tr>
<td>Replay detection</td>
<td>None</td>
<td>IV sequences</td>
<td>IV sequences</td>
</tr>
<tr>
<td>Key management</td>
<td>None</td>
<td>802.1X</td>
<td>802.1X</td>
</tr>
</tbody>
</table>

**2.9 Summary**

This chapter analyzed some existing literature reviews related to this research. The literature views have addressed that WEP is weak; it can be cracked in minutes. The literature also addressed the WPA vulnerabilities. Types of attacks on wireless security protocols has discussed in this chapter. In addition this also chapter has discussed the importance of securing wireless networks, history of wireless network, advantage and disadvantages of wireless networks. As mentioned several times WEP is weak; however WEP is better than no security.
CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter covers the methodology that will be used to make this project complete. The methodology is intended to prepare research steps.

3.2 Methodology Stages

The methodology of this project will be as follows. Each stage will be discussed in the following sections.
Figure 3.1 Project Methodology

Phase 1

Understand wireless security vulnerabilities

Analyze & Collect proper Tools

Do attack against WEP/WPA in Lab environment (A)

Survey: Extensiveness of WEP In the campus

Repeat (A) in College

Attack Result

Phase 2

Prepare enforcement Policy

Verify policy

Develop Jamming Program

Implement Program

Result
3.2.1 Understand Wireless Security Vulnerabilities

In this stage; several literature reviews about wireless security issues will be study. Several literature reviews will be read to understand the latest wireless security vulnerabilities. This stage ensures the achievement of the first objective of this research.

3.2.2 Analyze & Collect proper Tools

In this stage; different tools and approaches to carry out attack against will be explored WEP and WPA. The main task of this stage is to collect and explore the effectiveness of hacking tools to perform attack. Once several tools collected then next step will be started. The following sections will discuss some tools that have been explored during this stage.

3.2.2.1 Airowizard 1.0 Beta

Airowizard is GUI software for windows users to crack WEP key. To use this tool first you have to install the commview driver. You have to verify if your wireless device is compatible from comview site, if your wireless card does not include in the list, then this tool won’t work for you. Airowizard uses airodump-ng to find the target wireless access points to perform cracking. It’s also uses aireplay-ng to perform fake authentication and packet injection, and Aircrack-ng to crack WEP.

User who doesn’t like command lines, Airowizard is their choice. Airowizard is not an excellent chose for cracking activities because it doesn’t support many wireless cards and also take long time.
3.2.2.2 Cain & Abel

Cain & Abel is a password recovery tool for window; it allows recovering various kinds of passwords by performing network sniffing. Cain & Abel also have the ability of cracking encrypted passwords by using dictionary, brute-force, cryptanalysis attacks, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. Cain & Abel have interesting features such as ARP poison routing. ARP enables sniffing on switched LANs by hijacking IP traffic of multiple hosts at the same time. The sniffer also has the ability to analyze encrypted protocols (Thawatchai Chomsiri, 2008) such as SSH-1 and HTTPS if APR and man in the middle attack used. Cain & able can be used to crack WEP but it needs AirPcap adapter.

Cain also comes with routing protocol authentication monitors. Route extractors, crackers all common hashing algorithms and for other various specific authentications, password calculators (Cisco PIX Hashes, RSA SecurID Tokens), decoders (AccessDatabases, Base64, Cisco Type-7, Enterprise Manager, Dialup, Remote Desktop) Cisco Config Downloader/Uploader, SiD-Scanner, LSA Secrets Dumper, Protected Storage Passwords Viewer, NT Hash-Dumper, Abel Remote Console, MAC Scanner, Promiscuous-Mode Scanner, Wireless Scanner, and TCP/UDP/ICMP Traceroute + DNS Resolver + Netmask Discovery + WHOIS resolver. Cain can hack non encrypted passwords and usernames via network as shown Figure 3.2 below.
Cain was configured to use ARP spoofing referred to as APR (ARP poisoned routing) within the application to intercept network traffic between machines A and B as shown Figure 3.3 below.

Figure 3.3 ARP Spoofing to intercept Data between Machines A and B

Cain can capture telnet sessions by recording a telnet secession activity between two machines as shown in Figure 3.4.


3.2.2.3 Commview

CommView for WiFi is a powerful wireless network monitor and analyzer for 802.11 a/b/g/n networks. Commview has user-friendly features that make the usage easy and understandable. Commview for wifi has the ability to capture every packet transmitted over the air and it can display important information such as the available access point and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. these information will help you to identify and examine packets, network problems can be identified. User can decrypt packets by using this tool. This tool supported by over 70 protocols, this feature allows you to view details of captured packets using a convenient feature. CommView for Wi-Fi 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 under Windows XP/2003/Vista/2008/7 and requires a compatible wireless network adapter. Commview for Wi-Fi can be used to crack WEP but you need to use together with aircrack-ng, however; it takes too long to crack WEP by using this tool.
Commview has several features that user can select. The following are the features of commview:

i. Scan the air for WiFi stations and access points.
ii. Capture 802.11a, 802.11b, 802.11g, and 802.11n WLAN traffic.
iii. Specify WEP or WPA keys to decrypt encrypted packets.
iv. View detailed per-node and per-channel statistics.
v. View detailed IP connections statistics: IP addresses, ports, sessions, etc.
vi. Reconstruct TCP sessions.
vii. Configure alarms that can notify you about important events, such as suspicious packets, high bandwidth utilization, unknown addresses, rogue access points, etc.
viii. View protocol "pie" charts.
ix. Monitor bandwidth utilization.
x. Browse captured and decoded packets in real time.
xi. Search for strings or hex data in captured packet contents.
xii. Log individual or all packets to files.
xiii. Load and view capture files offline.
xiv. Import and export packets in Sniffer, EtherPeek, AiroPeek, Observer, NetMon, Tcqdump, hex, and text formats.
xv. Export any IP address to SmartWhois for quick, easy IP lookup.
xvi. Capture data from multiple channels simultaneously using several USB adapters.
3.2.2.4 Aircrack-ng

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. Aircrackng is much faster compared to other WEP cracking tools. Aircrack-ng is suitable for linux users, however; windows user can also use aircrack-ng but the cracking result can’t be guarantee.

3.2.2.5 Backtrack 4

BackTrack is an operating system based on the Ubuntu GNU/Linux distribution aimed at digital forensics and penetration testing use. BackTrack is one of the most popular distributions in the white hat circles. It is specially suited for penetration testing, with more than 300 tools available for the task. Backtrack works primarily as a live CD, with good hardware detection and low memory footprint, intended to make it usable even on older machines. It is also possible to install BackTrack on computer. To install backtrack on a computer; you need to create empty hard disc partition. After you create hard dick partition you need to do several steps to successfully install backtrack without losing your windows operation system. To start backtrack you need username “root” and password “toor” and then type startx. The network is not enabled by default and you'll have to enable it manually. Backtrack is familiar with lots of hacking tools. Backtrack provides users with large security-related tools that is easy to access. These security related tools ranging from port scanners to password crackers.

BackTrack supports for live CD and also Live USB. To use live CD, you just need to burn iso image into DVD and then insert your DVD to your computer and restart your computer to read your CD. Live USB can be used to run backtrack, however you need another tool to install the iso image, the recommended USB size is 8 GB. Backtrack includes many well know security related tools, these includes:
i. Metaspoil integration
ii. RFMON Injection capable wireless drivers
iii. Kismet
iv. NMAP
v. OphCrack
vi. EtterCap
vii. Wireshark (formerly known as Ethereal)
viii. BeEF
ix. Hydra

Backtrack 4 will be used for attack against WEP and WPA. As mentioned above backtrack can be run from live CD or through USB.

3.2.3 Redo Attack Against WEP/WPA in Lab Environment (A)

In this stage, attack activities begins by testing the entire above mentioned tools to choose the most effective tool to perform attack against WEP and WPA. The above tools will be tested to check if it’s possible to crack WEP in short period of time. This step will be repeated several times until the required result is achieved.

A specific access point that was deployed with WEP will be targeted to attempt whether the access point’s security defense can be compromised. The most important aspect is time; the time it takes to compromise the key will be recorded. This attack will be done in Lab environment.

3.2.4 Survey: Extensiveness of WEP in the Campus

In this stage, a survey about the extensiveness of WEP in UTM campus will be done. The researcher will walk around some faculties and colleges to explore their
wireless access point’s security. This survey will help to know about how UTM wireless access points were deployed by focusing on security implementation. Insider 2.0 will be used to analyze wireless access points. This tool has the ability to capture all available APs and also displays whether the access point is deployed with security or none encrypted APs. APs at Faculty of Architecture, Library, CICT building, Faculty of Management and Human Resource, Faculty of Science, Block N24, N28 building and Kolej Rahman Putra (KRP) Wi-Fi zone areas will be analyzed.

3.2.5 Repeat (A) in College

In this stage, the attack against WEP/WPA will be done in college. Attack against researcher’s access point in college to test security capabilities of the AP will be performed. The result of the attacks in term of speed (time) will be compared.

3.2.6 Attack Result

In this stage, result of the attack will be tested to check whether the comprised key is valid. If the key is valid, wireless network will be accessed successfully. The process involving in this stage will be documented and screen shoots will be taken.

3.2.7 Prepare Enforcement Policy

The researcher will prepare wireless security policy for the departments/faculties that currently posses access points. This policy is intended to alert wireless departments and faculties about wireless security risks by encouraging
them to change WEP. This policy will help departments and faculties to understand
the wireless security risks and make them prepare precautions to avoid wireless
security interceptions. By following the imposed policy will ensure that all wireless
access points are secure.

3.2.7.1 Policy Verification

The policy will be reviewed and verified by CICT department personnel. The
comments from the CICT personnel will be followed and adjust to the policy.

3.2.8 Develop Jamming Program

This stage will be the last stage; in this stage the researcher will develop a
jamming program that makes enabled WEP access points busy in order to force users
to change WEP. The program will enable wireless admin to implement the policy of
the wireless security usage by forcing any user who disobeys the policy of the
wireless security. The program gives three options that the admin can select and
work on it. The details of this program will be discussed in chapter 5.

3.2.8.1 Implement Program

In this stage program will be tested to check whether the program can run and
perform the intended purpose. This stage will be continues until the desired result has
achieved.
3.2.8.2 Result

In this stage the result of the program will be shown and discussed in details. The details of the result discussed in chapter 5.

3.3 Summary

The methodology of this study was discussed in this chapter. The stages involved in the methodology were discussed in details. This chapter is intended to provide an overview of the project implementation to make clear the project final destination/outcomes.
CHAPTER 4

PRE-ANALYSIS RESULT AND FINDING

4.1 Introduction

This chapter analyses the research finding and the result of the research will be shown at the end of this chapter. The penetration steps are also discussed in this chapter.

4.2 Finding

Several wireless administrators still do not aware of wireless vulnerabilities, and they use WEP as their security defenses. UTM wireleses are secure since they are encrypted and it’s not easy to intercept, however some Access points in UTM are using WEP which can be easily cracked. Once WEP is cracked, the attacker can share the bandwidth which can affect network performance in term of speed.
CICT_AP access point which is located in block D07 UTM has been tested, this access point was deployed with WEP. We have done several tests and we have finally cracked and decrypted the WEP key in 50 minutes. This shows that how WEP is vulnerable, WEP even can be cracked in 3 minutes or less that depends on the number of IVS packets captured.

In addition some internet providers are using WEP which is vulnerable as mentioned above. One of these is called “P1” which is a company that provides wireless internet. We also have tested whether P1 key can be cracked. Only 3 minutes and 44 seconds took to crack our own P1 password key. As can be understood from the above any wireless network that has been deployed with WEP is insecure. The attacker can just scan all available wireless and can crack WEP and share bandwidth without paying.

Since WEP insecure; WPA/WPA2 was developed to replace and solve the vulnerabilities of WEP. Some access points in UTM employed WPA and WPA2; However WPA has also security vulnerabilities even though it’s not serious problem. WPA can be intercepted by using dictionary attack but the result is not guarantee. A dictionary attack is a process of trying every word in the dictionary as a possible password. Computer programs are developed which can automatically generate and try all the dictionary words.

Dictionary attacks are rarely successful if the passphrase is in dictionary, to test all combinations in the dictionary may be take hours, weeks or even years depends on the size of the dictionary file.

Two access points that were deployed with WPA has been tested. These APs are smuhr and UKPL. The tool that we have used is called Backtrack 4. Backtrack 4 has came with its own wordlist to implement dictionary attacks; therefore we have used the wordlist that backtrack provided.
To crack WPA by using dictionary attacks it’s necessary to get 4-way handshake. To capture 4-way handshake, you can either wait until a client connect to the AP or you can force clients to reconnect the AP. To force clients to reconnect AP, you can use a tool called “aireplay-ng” which can be found in backtrack. We have captured 4-way handshake of both smuhr and Ukpl and we have implemented with dictionary attack to crack the WPA key, however we were not able to crack the WPA as the passphrase was not in the dictionary.

Hackers can hack wireless network by using free available tools that can be run on linux and windows systems. Hackers can also collect information about wireless network and attempt to unlock WEP/WPA keys. WEP can be compromised by hackers in minutes; however WPA may not be successfully compromised. To perform successful attack against protected network, supported wireless card that can do packet injection is required. By getting the right tools, hackers can change their wireless card into monitoring mode to see all available wireless networks and select the target access point. Hackers can kick the client off the connection then de-authenticate to capture handshake packets. After compromising the network, the hackers can sniff sensitive information and can see communication activities such as email passwords, face book account details and credit card information.

4.3 Critical Analysis

WEP can be cracked in minute but can take several hours if there is no clients connect to the target access point. In addition if the target access point is far then the process will take more time. The attack that we have done in lab took 50 minutes to crack WEP. The time that the test occurred was 4:30pm and this time there is fewer clients connect to access point. As mentioned earlier WEP cracking time can be faster two conditions are meet. The first condition is the access point should be near. The second condition is that there must be client connect to the access point otherwise the key cannot be found.

The attack against WEP/WPA that we have done in college took 3 minutes and 44 seconds. This shows the cracking time of WEP is short. There were 2 clients
connected to the AP during our attack. Once more than one client connects to the AP, the cracking period will be shorter.

WPA has less security vulnerabilities compares to WEP. However, WPA can be compromised if dictionary word is used as password. Attacker use dictionary attack in order to check whether the password is taken from the dictionary. If the password is not taken from dictionary then the attacker cannot comprise the access point. In our test dictionary attack has been used but the result shows that the password is not taken from the dictionary.

4.4 WEP/WPA Key Cracking Steps

i. Setup Equipment: Required equipment can be hardware and software. Network interface card (NIC) and laptop are the main required equipments. Beside the hardware requirements, software and Linux based OS is also required.

ii. Find the target: Select specific APs to start testing the security weakness and strength of those APs.

iii. Capture Data from Air: Before testing it’s required to collect enough packets in order to make the process run. Therefore; to achieve enough packets it’s necessary to be near to the target APs otherwise the required packets could not be collected as the signal is far away.

iv. Start Cracking from Captured Data: The collected packets should be analyzed in order to crack the key. This process may need sometimes. If key is not found in the analyzed packet, then more packets are needed to collect to get the correct key.
4.4.1 Required Equipments

i. Computer: Compaq version Presario V3000 is used for this research

ii. Wireless LAN card supports: A wireless card that supports monitoring mode is needed. If the wireless card is not supporting monitoring then the process cannot be success. B43 wireless driver was used for this project. Change wireless card from managed mode into Monitoring mode

iii. Software: The best operation system (OS) for this task is linux. Therefore, Linux based software that is called BackTrack version 4 has been selected to perform attack against WEP and WPA. There are several steps that need to be followed. Below flowchart will help to understand how the attacks have been done.
The first thing is to check whether wireless card is support in monitoring mode. To check wireless card compatibility; type this command “\texttt{airmon-ng start wlan0/eth0/wlan1/eth1}” then wireless card will be changed from managed mode to monitoring mode.
4.4.2 Capture Data from Air

To do this step, you have to type this command “airodump-ng mon0/mon1”; then all available AP will be detected by showing their SSID, channel number and BSSID. The next step you have to select your tagged AP by running this command “airodump-ng -c [channel number] -w [write file name] -bssid [write target bssid] mon0/1”.

4.4.3 Start Cracking from Captured Data

This is the last step, to do this step you have to run this command “aircrack-ng -b[write target bssid] your file name with -01.cap”.

4.4.4 The whole Attack Steps

i. Sudo apt-get install macchanger (linux user): This step installs macchanger. Macchanger allows changing your real MAC address into fake MAC address. To change the real MAC address is optional.

ii. Sudo apt-get install aircrack-ng (linux user): This step installs the aircrack-ng that performs the brute force attack. Aircrack-ng analyses the collected packets in order to decrypt the key.

iii. iwconfig (find your interface i.e. eth0/wlan0): This step is required in order to find out the interface of the device. Identification of the device interface is import since several tasks is depending on the interface.

iv. Sudo airmon-ng stop wlan0/eth0/wlan1/eth1: Airmon-ng starts the process by running the inface. Airmon-ng also disconnects the wireless during the attack process.
v. **Sudo ifconfig wlan0/eth0/wlan1/eth1 down (optional):** This step is required when the attacker wants to change his real MAC address. In order to change the real MAC address it is necessary to disconnect the wireless interface.

vi. **Sudo macchanger --mac [any desired MAC address] wlan0/eth0 (optional):** This step changes the real MAC address into desired MAC address just for temporary usage.

vii. **Sudo airmon-ng start wlan0/eth0:** This step makes the wireless interface up. The interface can be either wlan or eth.

viii. **Sudo airodump-ng mon0/mon1:** This step scans all the available access points and the target access point will be selected. When the interface is up it displays mon that allows AP scan.

ix. **Get BSSID, Client/station bssid and channel:** After scan these information (BSSID, Client/station bssid and channel) can be seen. Control-c is used to stop scan process.

x. **Open new terminal**

xi. **Sudo airodump-ng -c [channel number] -w [write file name] -bssid [write target bssid] mon0/1.** Channel number can be seen during scanning. In order save all the packets transaction, it’s necessary to create a file to store the packets. -w allows creating and saving a file on desktop.

xii. **Open new terminal**

xiii. **Ls (check saved files .i.e. file with .cap extension):** This step allows displaying all the files that have been saved including the newly created file.

xiv. **Sudo aircrack-ng -b[write target bssid] saved file name with -01.cap:** This steps attempts to analyze the captured packet in order to find the key. If key not found, step 15 will automatically repeated after collecting enough packets.
4.5 The Extensiveness of the WEP in UTM Campus

As mentioned earlier, short survey about security implementation in the wireless access points has done. We have visited some Wi-Fi zone areas in UTM to check the security implementation. It is found that number of access points are still using WEP, in addition some access points are open (no encryption). Table 4.1 shows the details of security implementation of some access points.

<table>
<thead>
<tr>
<th>No</th>
<th>Number of AP</th>
<th>location</th>
<th>No encryption</th>
<th>WEP</th>
<th>WPA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14</td>
<td>Faculty of science</td>
<td>3</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>14</td>
<td>Library foyer</td>
<td>8</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>14</td>
<td>Faculty of HRM</td>
<td>4</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>14</td>
<td>Faculty of Architecture</td>
<td>13</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

4.6 WEP Attack Result

Several wireless administrators still don not aware of wireless vulnerabilities, and they deploy with WEP as their security defenses. Some Access points in UTM are using WEP which can be easily cracked. Once WEP is cracked, the attacker can share the bandwidth which can affect network performance in term of speed. I have tested CICT_AP access point which located in block D07 UTM, this access point was deployed with WEP. I have done several tests and I finally cracked the WEP key in 50 minutes. This shows that how WEP security is weak, WEP even can be cracked in 1 minute or less that depends on the number of IVS packets.
**Figure 4.2** CICT_AP cracking time

**Figure 4.3** CICT_AP Key Found
4.7 WPA Attack Result

After we have successfully cracked CICT-AP that was deployed with WEP, we have tested some APs that were deployed with WPA by using dictionary attack to brute force the key. To crack WPA, it’s required to capture 4-way handshake without getting this the process won’t be success. We have tested two APs (SMUHR, UKLP) that were deployed with WPA. We have captured their 4-way handshake but we failed to get the passphrase.
Figure 4.5 UKLP AP handshake captured

Figure 4.6 SMUHR AP handshake captured
4.8 Summary

This chapter discussed about the WEP and WPA attack processes and the result of the attack. The techniques that the hackers use to break protect wireless network was also discussed in this chapter. Wireless network can be high risk especially free Wi-Fi or open wireless networks; anyone who has the right tool can watch your communications and capture sensitive information such as username and password, credit card details and so on.
CHAPTER 5

IMPLEMENTATION AND RESULT

5.1 Introduction

This chapter discusses about project implementation and final result. The implementation of the achieved result will be discussed in this chapter. The process of the implementation will also be discussed in this chapter in order to make clear how to the result has been achieved. The proposed solutions will also be discussed in this chapter. WEP is recognized as a weak encryption since it can be compromised within a short period of time, however; there are still some people who use WEP. Some people may not aware of the security weaknesses of WEP while others may not consider the security part of the wireless network. To minimize wireless network security strategies to reduce the use of WEP have been proposed.
5.2 Proposed Wireless network security Policy

This policy verified by Dr. Alias Bin Mohd, Deputy Director Infrastructure and CICT Security Centre of information and communication Technology University Technology Malaysia.

5.2.1 Overview

Wireless network offers great benefits to the university community to achieve their learning objectives. Wireless network has several advantages compare to wired network. The following situations justify the use of wireless technology:

i. To extent a distance beyond the capabilities of typical cabling,
ii. To provide a backup communications link in case of normal network failure,
iii. To overcome situations where normal cabling is difficult or financially impractical

Wireless network provides several benefits but wireless network can be risk if weak security encryption is used. Universiti Technologi Malaysia (UTM) plans to provide reliable and secure wireless network to the university community in order to protect intruders. Therefore, UTM imposes new policy towards security of the wireless network in the campus.
5.2.2 Definitions

i. **Wireless Network**: The network technology that uses radio frequency spectrum to connect devices to communicate.

ii. **Wireless Infrastructure**: The wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless network.

iii. **Base Station**: A network device that serves as a common connection point for devices in a wireless network.

iv. **Coverage**: The physical area where a level of wireless connectivity is available.

v. **Channel**: The chosen frequency for communication between the end point and the base station.

vi. **Security**: The condition that provides for the confidentiality of data transmitted over a wireless network.

vii. **SSID**: Service Set Identifier, essentially a name that identifies a wireless network. All devices on a specific wireless network must know the SSID of that network.

viii. **Access Point**: Any piece of equipment that allows wireless communication using transmitters and receivers to communicate

ix. **Privacy**: Privacy is the condition that is achieved when successfully maintaining the confidentiality of users

x. **Wired equivalent privacy (WEP)**: security algorithm for wireless local area networks (WLANs) defined in the 802.11b standard.
5.2.3 Purpose

The goal of this policy is to protect the confidentiality, integrity, and availability of the wireless network. To achieve the above mentioned goals; UTM CICT department imposes new wireless security policy in order to protect information interception. All departments/faculties in UTM campus are required to abide by this policy. This policy guides wireless network and its related security features.

5.2.4 Scope

The scope of this policy applies to all owners/admin of wireless access points at UTM campus. UTM is primarily responsible for providing a secure and reliable wireless network. This policy is for the departments/faculties that have deployed or plans to deploy access points inside UTM campus.

5.2.5 Roles and Responsibilities

Security is everybody’ responsibility, therefore all departments and faculties in University Technology Malaysia (UTM) should abide by this policy in order to achieve secure wireless communication network.
5.2.6 The Policy

All department/faculties are required to use strongest available wireless security encryption (WPA/WPA2) to avoid wireless security risks. Wired Equivalent Privacy (WEP) should not be used in UTM campus due to security flaws found in Wired Equivalent Privacy (WEP). Any wireless security incidents should be reported to the CICT department. Physical security should be considered when planning the deployment of wireless access point.

5.2.7 Policy Non-Compliance

Failure to comply with the Wireless Access Policy may result fine and suspension of wireless access point.

5.3 Existing Jammers

Wireless networks are more depicted to intentional or unintentional threats than their wired based equivalent networks (Ahsan et al., 2011). Jamming is a special category of DoS attacks which is used in wireless networks, where an attacker disrespects the medium access control (MAC) protocol and transmits on the shared channel; either continuously or periodically to target all or some communication, respectively (Ahsan et al., 2011). Earlier works on jamming focused on military applications (Huang et al., 2011) More recent works considered jamming in civilian wireless networks, especially wireless sensor networks because of their vulnerability from unattended field deployments (Huang et al., 2011).

There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications. It is impractical to cover all the possible attack models that might exist, in this study, the most known jammers will be discussed. The most efficient jamming attacks can be classified into four types (Le Wang et al., 2011):
i. **Constant Jamming:** It continuously emits a signal on the medium meaning that there are no silent time intervals in its transmission. In other word, it continually emits radio signals on the wireless medium. Constant jamming is normally used in mobile applications by the military or the police to prevent explosives being detonated remotely; usually a broadband jamming signal is emitted. The goal of this type of jammer is (Pelechrinis et al., 2011): (a) to pose interference on any transmitting node in order to corrupt its packets at the receiver and (b) to make a legitimate transmitter (employing carrier sensing) sense the channel busy, thereby preventing it from gaining access to the channel (Wenyuan et al., 2006) implemented this jammer using two types of devices. The first type of device used was a wave form generator which continuously sends a radio signal. The second type of device used was a normal wireless device. These researchers proved that constant jammer continuously sends out random bits to the channel without following any MAC-layer protocol. In addition these researchers also implemented the below jammer using Berkeley Motes that employ a ChipCon CC1000 RF transceiver and use TinyOS as the operating system. TinyOS is an open source software program used for WSN written in the nesC (similar to C language) programming language (Michael A. and Captain, 2012).This type of jammer aims at keeping the channel busy and disrupting nodes’ communication

ii. **Deceptive Jamming:** Deceptive jamming denotes attacks where false messages are sent to the channel with the objective of disturbing the organization of the network. Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions

iii. **Random Jamming:** In contrast to the constant jammer, a periodical jammer suspends its transmission during a specified time in regular intervals. In brief, the jammer performs constant jammer or deceptive jammer for a random period then shut down the jammer for another random period of time. The benefit of this jammer is saving energy.
During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. This jammer model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply.

iv. **Reactive Jamming:** Reactive jamming requires the sensing of the channel. As the transmission is detected, jammer starts its intrusion. A more advanced form of reactive jamming includes the analysis of the detected regular data stream. The jamming is then applied systematically to frames from or to specific nodes or to frames of a certain type. In brief, Reactive Jamming Stay quiet till there is activity on the channel then spoil the reception. While spoiling only selected packets, the adversary minimizes its risk of being detected. One might hope for reactive jamming to be too challenging or uneconomical for an attacker to conceive and implement due to its strict real-time requirements. Reactive jammer must be able to destroy transmissions at the receiver even if a sender has already started a transmission. As a result, a reactive jammer targets the reception of a message. The primary advantage for a reactive jammer, however, is that it may be harder to detect. Reactive jamming is normally used by the military, the police and justice enforcement authorities to suppress data transmissions and phone calls to and from certain fixed premises and compounds.
Table 5.1 Characteristics of various jammers

<table>
<thead>
<tr>
<th>Jammer name</th>
<th>Implementation Complexity</th>
<th>Energy Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Deceptive</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Random</td>
<td>Low</td>
<td>Adjustable</td>
</tr>
<tr>
<td>Reactive</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

These jammers are energy-inefficient (energy-constrained). Although random jammers save energy by sleeping, they are less effective.

5.4 Proposed Jamming program

This program is designed to implement the proposed policy by enforcing whoever disobeys the policy. The program is intended to make jam with any access points that are being deployed with WEP in order to enforce wireless network’s owner to change WEP. The program has three options: jam target access point (AP), help and Exit. Jam target option allows scanning all available wireless access points in order to see specific APs that are using WEP. During scanning it’s required to make note on the target AP’ basic service set identifier (BSSID) and the channel that the target AP is on. Once the target AP’ basic service set identifier (BSSID) and channel has been collected then the program will allow to enter the BSSID/MAC address of the AP and the channel. After the BSSID and channel is selected then the program will start jamming on the target AP to make it unavailable for the users to access. The target access point will remain jam until the program is terminated. Help option gives guidelines about the program usage. Exit option allows exiting the program. The user can only select the above mentioned options. If the user select option that is not in list, then the program displays error message that indicates invalid entry and the program displays the main menu in order to give user another try.
Table 5.2 Advantage and disadvantage of proposed jamming program

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Does not require additional hardware</td>
<td>• Can’t scan remote access points</td>
</tr>
<tr>
<td>• Does not require particular knowledge (any one can run)</td>
<td>• Requires Linux platforms</td>
</tr>
<tr>
<td>• Provides user friendly instruction usage</td>
<td>• No graphical user interface (GUI)</td>
</tr>
<tr>
<td>• Can jam a particular access point (AP) without interfering other APs.</td>
<td></td>
</tr>
</tbody>
</table>

To understand how the proposed jamming program designed, the below flowchart illustrates the program.
**Jamming Program Flowchart**

1. **Scan all available APs**
2. **Get target AP’s BSSID & channel**
3. **Enter target AP’s BSSID**
   - **Correct BSSID?**
     - **No**
     - **Correct Channel**
       - **No**
         - **Enter target AP’s Channel number**
           - **Correct Channel**
             - **Yes**
               - **AP Jamming begins**
     - **Yes**

Normally when client wants to connect access point, the client must first authenticate and then associate itself with an access point (AP) before communication occurs. Stopping the communication requires either the client or the AP to request deauthentication. The proposed program sends disassociate packets to a particular access point. The program forces the clients and AP to deauthenticate by sending continuous packets which makes the communication between AP and client jam as shown in figure 5.2.

![Diagram](image)

**Figure 5.2** AP and client authentication and Deauthentication
5.5 Program Implementation and Result

Three laptops were used to test program functionality. Two of the laptops were the clients connected to the access point and the other laptop was used for programmer implementer. The clients were asked to access Google and YouTube. Both Google and YouTube could not access at that time, this indicates the effectiveness of the proposed program. The test was repeated in different times to make sure the functionality of the program and the same result was found.

Table 5.3 Hardware/Software used for Program Implementation

<table>
<thead>
<tr>
<th>Laptop Model</th>
<th>CPU</th>
<th>RAM</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client 1</td>
<td>Acer Aspire 4730Z</td>
<td>2GB</td>
<td>Windows 7 professional 32-bit (6.1, Build 7600)</td>
</tr>
<tr>
<td></td>
<td>Intel® Pentium® Dual CPU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jam implementer</td>
<td>Compaq Presario v3000</td>
<td>2GB</td>
<td>Linux Version 11.04</td>
</tr>
<tr>
<td></td>
<td>Intel® core TM Duo CPU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Client 2</td>
<td>Dell inc. Inspiron 1420</td>
<td>3GB</td>
<td>Windows 7 professional 32-bit (6.1, Build 7600)</td>
</tr>
<tr>
<td></td>
<td>Intel® Pentium® Dual CPU</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The program scans all available access points and shows relay information, SSID, and other parameters regarding the access point. Once target access point’s basic service set identifier (BSSID) and channel specified, the program begins to jam the specified access point and the clients will be unable to maintain a connection to the wireless access point.
The following screenshots gives more details about the program and how the program works.

As can be seen in the above figure this program has three main options that can be selected.

**Figure 5.3 Main Menu of the Program**
As mentioned earlier the program only allows selecting the displayed options. If the user selects wrong option the program displays the above error message.

**Figure 5.4 Error Message**
Figure 5.5 Option 1 has been Selected

Once this option is selected, a new window pops up and starts access point (AP) scanning as shown in figure 5.6

Figure 5.6 Access Points Scanning
Basic server set identifier (BSSID) and the channel of the target AP can be seen during scanning as can be seen in the above figure. In addition the type of security that the target AP is using can be seen. Once the user closed the scanning AP windows, the program will display the below features.

![Image](image.png)

**Figure 5.7** Target AP’ BSSID has been Selected

After the user enters the target AP’ BSSID, the program inquires the user to fill the channel that the target AP is on as can be seen in the figure 5.8.
Once the channel is selected, the program will start jamming to the target AP. While the program performing jamming the users on that access point will not be able to communicate.
Figure 5.9 Target AP jamming Started

The program sends deauthentication in order to disturb the normal communication between the AP and the clients.

5.6 Summary

This chapter highlighted the proposed solutions and how it was designed. The advantages of disadvantages of the proposed solution were discussed in this chapter. The two proposed solutions are intended to reduce the use of Wired Equivalent Privacy (WEP). The developed jamming program has been discussed in details in this chapter.
CHAPTER 6

CONCLUSION

6.1 Achievements

This chapter concludes the study. The main issues in this study will be highlighted in this chapter. The main purpose of this chapter is to summarize the whole study in understandable and concise ways.

Referring to Chapter 1 Section 1.4, this research has successfully achieved the three objectives which are 1) To study wired Equivalent Privacy (WEP) and WPA vulnerabilities, 2) To analyze risks of Wired Equivalent Privacy (WEP) encryption and 3) To propose strategy to control the use of WEP in the campus.

Objective (1) was achieved through studying literate reviews. The author has reviewed several literature reviews related to the research topic. The knowledge gathered from literature reviews enlightened the success end of this study.
Objective (2) was achieved by performing attack against WEP and WPA. The attack was done in lab and in college and the results are shown in chapter 4. The main purpose of this objective is to analyze the security weakness of WEP and how easy or difficult to break down WEP encryption.

For objective 3, two solutions to control the use of WEP have proposed. The first solution is by preparing enforcement policy for departments and faculties that have or plans to deploy wireless network in UTM campus. The second solution that researcher came out is the development of a program that can make access point (target access point) jam. The program is intended to enforce wireless network’s owners to change wired equivalent privacy (WEP). The program will make the access point jam and nobody can access internet while the program is running. The program ensures the implementation of the proposed policy.

6.2 Future enhancement

Due to time constraints the researcher was focusing on the program functionality rather than the outlook or the interface of the program. Graphical interface can be developed for the proposed program. The researcher suggests that simultaneous wireless security awareness program should be organized in order to make everybody aware of wireless network security risks.

One of the most effective ways to minimize the wireless security risks is to educate and make people aware of wireless security risks. Technology alone cannot minimize the security risks of wireless network, therefore educating people is necessary. The researcher wishes that the proposed solution will minimize the security risks of wireless network.


Caneill and Gilis. (2010). Attacks against the WiFi protocols WEP and WPA


Hong Huang, Nihal, and Karthik. (2011). On a New Type of Denial of Service Attack in Wireless Networks: The Distributed Jammer Network


Kadlec, Kuchta, and Vrba. (2009). Comparison of the WLAN’s security functions time consumption


Lashkari and towhidi. (2009). Wired Equivalent Privacy (WEP)


Martin Beck.(2008). Practical attacks against WEP and WPA
Michael A. and Captain.(2012). The Effects of Cognitive Jamming on Wireless
Sensor Networks used for Geolocation
Padilla and Guillen. (2010). Weaknesses and Strengths Analysis over Wireless
Network Security Standards
Pamnani and Chawan. (2009). Building a secured wireless LAN. International
Journal of Recent Trends in Engineering, Vol 2, No. 4, November, pp120-122
Networks: The Case of Jammers. IEEE COMMUNICATIONS SURVEYS &
TUTORIALS, VOL. 13, NO. 2, SECOND QUARTER 2011, pp245-257
network security attacks
Ramiro and Abdallah. (2002). Wireless communication and networking: an overview
IEEE Antenna’s and Propagation Magazine vol.44, No.1, February, pp185-193
Raju, Vallikumari, and KVSVN. (2011). Modeling and Analysis of IEEE802.11i
WPA-PSK Authentication Protocol
Thawatchai Chomsiri. (2008). Sniffing Packets on LAN without ARP Spoofing
Wang, Zhigang, and Zhao. (2010). Practical Defence against WEP and WPA-PSK Attack for WLAN
Yao, Chong, and Xingwei. (2010). Enhancing RC4 algorithm for WLAN WEP Protocol