

**WLAN TRAFFIC ANALYSIS AND HACKING THROUGH SNIFFING AND  
VULNERABILITY EXPOSED**

PEH WEI JIN

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

## BORANG PENGESAHAN STATUS TESIS

JUDUL: WLAN TRAFFIC ANALYSIS AND HACKING THROUGH SNIFFING AND VULNERABILITY EXPOSED

SESI PENGAJIAN: SESI 2010/2011

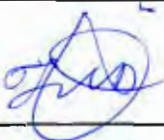
Saya PEH WEI JIN mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan penukaran antara institusi pengajian tinggi.
4. Sila tandakan(/)

\_\_\_\_\_ SULIT (Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

\_\_\_\_\_ TERHAD (Mengandungi maklumat TERHAD yang ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

  /   TIDAK TERHAD

  
\_\_\_\_\_

(TANDATANGAN PENULIS)

Alamat Tetap: 118-4-3 Jalan Batu Gajah

Desa Bukit Dumar, Jelutong

11600 Pulau Pinang,

Malaysia

Tarikh:

4/7/2011

  
\_\_\_\_\_

(TANDATANGAN PENYELIA)

En. Nor Azman Mat Ariff.

Tarikh:

4/7/2011

WLAN TRAFFIC ANALYSIS AND HACKING THROUGH SNIFFING AND  
VULNERABILITY EXPOSED

PEH WEI JIN

This report is submitted in partial fulfillment of the requirements for the  
Bachelor of Computer Science (Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA


2011




**DECLARATION**

I hereby declare that this project entitled  
**WLAN TRAFFIC ANALYSIS AND HACKING THROUGH SNIFFING AND  
VULNERABILITY EXPOSED**

is written by me and is my own effort and that no part has been plagiarized  
without citations.

STUDENT :  Date: 4/7/2011  
(PEH WEI JIN)

SUPERVISOR :  Date: 4/7/2011  
(EN. NOR AZMAN MAT ARIFF)

## DEDICATION

To my beloved parents...

## ACKNOWLEDGEMENTS

I would like to show my gratitude and appreciation to my supervisor, En. Nor Azman Mat Ariff, for all his ideas and advices in guiding me throughout the project.

I would also like to thank my family members especially my parents. They have been giving me moral supports and all sorts of material supports throughout my years studying in this University.

## ABSTRACT

This project is called WLAN Traffic Analysis and Hacking through Sniffing and Vulnerability Exposed. Sniffer is a computer hardware or software that can legitimately or illegitimately monitor, capture, and analyze the network traffic for some purpose. In this project, a control environment with an AP is setup with several workstations connected to it. The workstations are transmitted packets through the AP. A sniffer is setup near the AP to capture the data traffic. The sniffing process will be conducted over few days to collect certain amount of data. With the help of network protocol analyzer such as Wireshark, the collected data will be analyzed to produce some statistic information and also the traffic will be characterized. For example, transmission error rate of IEEE 802.11g network can be found out through this project. This project also covers about cracking WPA2-PSK in order to decrypt the traffic for further analysis. Finally, the current vulnerability of wireless network will be discussed. By completing this project, a better understanding of IEEE 802.11 network can be achieved, and also the techniques and approaches used to analyze the traffic can be mastered.

## ABSTRAK

Projek ini disebut *WLAN Traffic Analysis and Hacking through Sniffing and Vulnerability Exposed*. *Sniffer* adalah peralatan komputer atau perisian yang boleh memantau, menangkap, dan menganalisis lalu lintas rangkaian tanpa wayar secara sah atau tidak sah untuk beberapa tujuan. Dalam projek ini, satu persekitaran kawalan dengan sebuah *AP* akan dibangunkan dengan beberapa pelanggan yang akan terhubung dengannya. Pelanggan akan menyebarkan pakej tanpa wayar melalui *AP*. Satu *sniffer* akan diletakkan dekat *AP* untuk menangkap lalu lintas data. Proses *sniffing* akan dilakukan selama beberapa hari untuk mengumpul quantiti data yang tertentu. Dengan bantuan perisian protokol analisis seperti *Wireshark*, data yang terkumpul akan dianalisis untuk menghasilkan beberapa maklumat. Misalnya, tahap penghantaran kesalahan data rangkaian *IEEE 802.11g* boleh didapati melalui projek ini. Projek ini juga merangkumi *WPA2-PSK cracking* supaya untuk analisis yang selanjutnya. Akhir sekali, kelemahan rangkaian wayarles bagi masa kini akan dibincangkan. Dengan menyelesaikan projek ini, pemahaman yang lebih baik dari *IEEE 802.11* rangkaian dapat dicapai, dan juga teknik dan cara-cara yang digunakan untuk menganalisis lalu lintas dapat dikuasai.



**TABLE OF CONTENTS**

<b>CHAPTER</b>	<b>SUBJECT</b>	<b>PAGE</b>
	<b>PROJECT TITLE</b>	i
	<b>ADMISSION</b>	ii
	<b>DEDICATION</b>	iii
	<b>ACKNOWLEDGEMENTS</b>	iv
	<b>ABSTRACT</b>	v
	<b>ABSTRAK</b>	vi
	<b>TABLE OF CONTENTS</b>	vii
	<b>LIST OF TABLES</b>	x
	<b>LIST OF FIGURES</b>	xi
	<b>LIST OF ATTACHMENTS</b>	xiv
<b>CHAPTER I</b>	<b>INTRODUCTION</b>	
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Objective	4
	1.4 Scope	5
	1.5 Project Significance	5
	1.6 Expected Output	5
	1.7 Conclusion	6

<b>CHAPTER II</b>	<b>LITERATURE REVIEW AND PROJECT METHODOLOGY</b>	
2.1	Introduction	7
2.2	Literature Review	7
2.2.1	Domain	8
2.2.2	Keyword	9
2.2.3	Previous Research	12
2.3	Proposed Solution	20
2.3.1	Project Methodology	20
2.4	Project Schedule and Milestones	24
2.5	Conclusion	24
<b>CHAPTER III</b>	<b>ANALYSIS</b>	
3.1	Introduction	25
3.2	Problem Analysis	26
3.2.1	Network Architecture	26
3.2.2	Logical and Physical Design	29
3.3	Requirement analysis	35
3.3.1	Quality of Data	35
3.4	Conclusion	36
<b>CHAPTER IV</b>	<b>DESIGN</b>	
4.1	Introduction	37
4.2	Possible Scenarios	38
4.3	Security Requirement	45
4.4	Conclusion	46
<b>CHAPTER V</b>	<b>IMPLEMENTATION</b>	
5.1	Introduction	47

5.2	Network Configuration Management	48
5.2.1	Configuration Environment Setup	48
5.2.2	Version Control Procedure	49
5.3	Hardware Configuration Management	50
5.3.1	Hardware Setup	50
5.4	Security	52
5.4.1	Security Policies and Plan	52
5.5	Development Status	53
5.6	Conclusion	53
<b>CHAPTER VI</b>	<b>TESTING</b>	
6.1	Introduction	54
6.2	Test Plan	55
6.2.1	Test Organization	55
6.2.2	Test Environment	55
6.2.3	Test Schedule	55
6.3	Test Results and Analysis	56
6.4	Conclusion	96
<b>CHAPTER VII</b>	<b>PROJECT CONCLUSION</b>	
7.1	Observation on Weaknesses and Strengths	97
7.2	Propositions for Improvement	98
7.3	Contribution	98
7.4	Conclusion	98
	<b>REFERENCES</b>	99
	<b>BIBLIOGRAPHY</b>	101
	<b>APPENDICES</b>	102

**LIST OF TABLES**

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
<b>2.1</b>	<b>Summary of Previous Researches</b>	<b>18</b>
<b>3.1</b>	<b>Basic Setting for Network Topology</b>	<b>30</b>
<b>3.2</b>	<b>IPv4 Classes</b>	<b>30</b>
<b>3.3</b>	<b>Private IP Address</b>	<b>31</b>
<b>3.4</b>	<b>Allocation of IP Address</b>	<b>31</b>
<b>4.1</b>	<b>Radio Frequency Channel</b>	<b>44</b>
<b>5.1</b>	<b>Version of Software Tools</b>	<b>49</b>
<b>5.2</b>	<b>Summary of AP Configuration Management</b>	<b>51</b>
<b>5.3</b>	<b>Summary of Sniffer Configuration Management</b>	<b>51</b>
<b>6.1</b>	<b>Percentage of Different MAC Frame Type</b>	<b>76</b>

## LIST OF FIGURES

DIAGRAM	TITLE	PAGE
2.1	Wireless Local Area Network	9
2.2	IEEE 802.11 Protocol Stack	11
2.3	Wireless Network being Discovered using Network Stumbler	13
3.1	Wireless Network in Infrastructure Mode	26
3.2	Basic Network Topology	29
3.3	Transparent Bridges Table that Determines a Host's Accessibility	32
3.4	Logical Network Design	33
3.5	Physical Network Design	34
4.1	Infrastructure Network Design	39
4.2	IBSS Network Architecture	40
4.3	Ad Hoc (IBSS) Network Design	42
4.4	ESS Network Diagram	43
4.5	Extended Service Set Network Design	45
6.1	Filters for Management Frame	56
6.2	Summary of Management Frame	57
6.3	Filters for Data Frame	58
6.4	Summary of Data Frame	59
6.5	Daily Number of MAC Frame Transferred	59
6.6	Filters for Management Frame	61

6.7	<b>Summary of Management Frame</b>	<b>61</b>
6.8	<b>Filters Data Frame</b>	<b>62</b>
6.9	<b>Summary of Data Frame</b>	<b>63</b>
6.10	<b>Daily Traffic Volume Transferred</b>	<b>64</b>
6.11	<b>Filters for Data Frame and Frames towards AP</b>	<b>65</b>
6.12	<b>Numbers of User on Friday</b>	<b>66</b>
6.13	<b>Numbers of Daily User</b>	<b>67</b>
6.14	<b>Filters for Frames from AP to Stations</b>	<b>68</b>
6.15	<b>Filters for Retransmission Frames</b>	<b>69</b>
6.16	<b>Filters for Frames from Stations to AP</b>	<b>69</b>
6.17	<b>Filters for Retransmission Frames</b>	<b>70</b>
6.18	<b>Daily Transmission Error Rate</b>	<b>71</b>
6.19	<b>Filters for Data Frame from Specified Network</b>	<b>72</b>
6.20	<b>Filters for Association Request Frame</b>	<b>73</b>
6.21	<b>Filters for Association Response Frame</b>	<b>73</b>
6.22	<b>Filters for Authentication Frame</b>	<b>74</b>
6.23	<b>Filters for Probe Response Frame</b>	<b>74</b>
6.24	<b>Filters for Beacon Frame</b>	<b>75</b>
6.25	<b>Percentage of Different MAC Frame Type</b>	<b>76</b>
6.26	<b>Summaries of Data Frames</b>	<b>77</b>
6.27	<b>Average Frame Sizes of Different MAC Frames Type</b>	<b>78</b>
6.28	<b>Filters for Null Data Frames</b>	<b>79</b>
6.29	<b>Daily Percentage of Null Data Frames</b>	<b>80</b>
6.30	<b>Filters for Data Frames from Specified Station which Retry bit set to 1</b>	<b>81</b>
6.31	<b>Filters for Data Frames from Specified Station which Retry bit set to 1 and RSSI Value <math>\leq</math> -25</b>	<b>82</b>
6.32	<b>Percentage of Frames from Specified Stations where RSSI Frame Value <math>\leq</math> -25</b>	<b>83</b>

6.33	Command for Determine Network Card Driver	84
6.34	Commands for Monitor Mode	85
6.35	Commands for Scanning Wireless Network	85
6.36	Wireless Network being scanned	86
6.37	Commands for Packets Capturing	86
6.38	Interface of Specified Wireless Network that being captured	86
6.39	Commands for De-authenticating Clients	87
6.40	WPA handshake is being captured	87
6.41	Commands for Cracking by Using Dictionary Provided	88
6.42	Cracking Failed	88
6.43	Passphrase is entered manually into Dictionary	89
6.44	Cracking Succeed	89
6.45	Cracking by Using John The Ripper	90
6.46	Enabling of Decryption on Wireshark	90
6.47	Encrypted Packets are decrypted	91
6.48	Commands for Displaying Packets of Specified Host	91
6.49	Step for showing Protocol Hierarchy	92
6.50	Protocol Hierarchy Statistics	92
6.51	Percentage of Protocol Hierarchy for Specified Station	93
6.52	Filters for HTTP Packet	94
6.53	Filters for HTTP POST Request Method	94
6.54	Steps for Retrieving Sensitive Information	95
6.55	Login Name and Login Password Shown	96

**LIST OF ATTACHMENTS**

<b>ATTACHMENT</b>	<b>TITLE</b>	<b>PAGE</b>
<b>A</b>	<b>Gantt Chart</b>	<b>102</b>
<b>B</b>	<b>Project Proposal</b>	<b>103</b>
<b>C</b>	<b>Log Book</b>	<b>108</b>



## CHAPTER I

### INTRODUCTION

#### 1.1 Project Background

Today, wireless computing is in the steep upside rise toward its peak in the marketplace. Wireless networks broadcast their packets either using radio frequency or optical wavelengths. A modern laptop computer can listen on any packets from selected channel. Besides, an attacker can generate new packets on the fly and persuade wireless stations to accept his packets as genuine. Wireless networks and access points (APs) are some of the easiest and cheapest types of targets to be attacked or exploited.

Commonly, wireless network operates in one of two modes. In the ad hoc mode, each station is a peer to the other hosts and communicates directly with other stations within the network. No AP is involved. All stations can send management frames such as Beacon and Probe frames. The ad hoc mode stations also known as Independent Basic Service Set (IBSS). A station in the infrastructure mode communicates only with an AP. Basic Service Set (BSS) is a set of hosts that are logically connected with each other and controlled by a single AP. Together they operate as a fully connected wireless network. The BSSID is a 48-bit number of the usually also is MAC address of AP. This field uniquely identifies each BSS.

## 1.2 Problem statement

With the rapid development of wireless technologies in the past few decades, uses of wireless local area network (WLAN) has been gradually replaced the old traditional wired network. Home and business networkers now are looking to buy wireless networking devices like wireless router. News from Internet World Stats show that in 2004 the number of internet subscribers was 2.9 million, in 2005 it increased to 3.5 million subscribers, and in 2006 the number of subscribers in Malaysia was close to five million. This is an encouraging growing tendency, and most of the Internet subscribers were eyeing for high speed broadband infrastructure.

Recently, there are many products conform to the 802.11a, 802.11b, 802.11g, or 802.11n wireless standards, collectively known as Wi-Fi technologies. Additionally, Bluetooth and various other non-Wi-Fi technologies also exist, and each also designed for specific networking applications.

The first WLAN technology introduced by Institute of Electrical and Electronics Engineers (IEEE) is called 802.11, after the name of the group formed to manage its development. Unfortunately, 802.11 only supported a maximum network bandwidth of 2 Mbps which is too slow for most applications. IEEE expanded on the original 802.11 standard in July 1999, creating the 802.11b specification, which supports bandwidth of up to 11 Mbps, comparable to traditional Ethernet. 802.11b uses the same unregulated radio signaling frequency (2.4 GHz) as the original 802.11 standard. Vendors often prefer using these frequencies to lower their production costs. Being unregulated, 802.11b gear can suffer interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b devices at a reasonable distance from other appliances, interference can easily be avoided.

While 802.11b was in development, IEEE created a second extension to the original 802.11 standard which is called 802.11a. 802.11a supports bandwidth up to 54

Mbps and signals in a regulated frequency spectrum around 5 GHz. In 2002 and 2003, WLAN products supporting a new IEEE standard called 802.11g emerged on the market. 802.11g tries to combine the best of both 802.11a and 802.11b. 802.11g supports bandwidth up to 54 Mbps, and it uses the 2.4 GHz frequency for greater transmission range. Finally, the latest IEEE standard in the Wi-Fi category is 802.11n. It was designed to improve on 802.11g in the amount of bandwidth supported by exploiting multiple wireless signals and antennas instead of one.

Although WLAN consumes less cost and is easy to setup than wired network, its network security is the main concern. WLAN is too simplified to access to the network compared to traditional wired networks such as Ethernet. With wired networking one must either gain access to a building or break through an external firewall. Most business networks protect sensitive data and systems by trying to disallow external access. Enabling wireless connectivity provides an attack direction, particularly if the network uses inadequate or no encryption. An attacker who has gained access to a Wi-Fi network router can start a DNS spoofing attack against any other user of the network by counterfeiting a response before the queried DNS server has a chance to reply.

In order to increase wireless network protection and defend data from unauthorized access, a data encryption protocol is introduced in 1997 with the intention to provide confidentiality, which is Wired Equivalent Privacy (WEP). WEP affords data confidentiality services by encrypting the data sent between wireless nodes. WEP encryption for an 802.11 frame is indicated by setting a WEP flag in the MAC header of the 802.11 frame. WEP supports data integrity for random errors by including an integrity check value (ICV) in the encrypted portion of the wireless frame.

However, WEP has been broadly criticized for a number of weaknesses. Thus, Wi-Fi Protected Access (WPA) was developed by the networking industry in response to the shortcomings of WEP. One of the crucial technologies behind WPA is the Temporal Key Integrity Protocol (TKIP). TKIP addresses the encryption weaknesses of WEP. Another key component of WPA is built-in authentication that WEP does not

offer. With this feature, WPA provides unevenly comparable security to VPN tunneling with WEP, with the benefit of easier administration and use.

Like many security standards, the problem with those wireless security solutions is not that they don't work, it's because of the network administrators who are resistant to change and don't wholly implement them. They don't like to reconfigure their wireless systems and don't want to implement new security mechanisms, feeling that the management becomes difficult. These look like ignorable things, but they set off many wireless networks defenseless and waiting to be compromised.

The problem really is not with these wireless networks, in and of themselves. It's with the malicious hackers waiting there for an opportunity over vulnerabilities to make our work harder. So as to better defend our systems, we have to think like a hacker. Even though it's impossible to reach the identical wicked mindset as hackers, we will be able to see where they're approaching from technically and what could be their upshot on us.

### **1.3 Objective**

The project's objectives are:

- i. To analyze the wireless traffics using sniffing tools.
- ii. To characterize the wireless traffics with the aid of suitable software.
- iii. To expose the vulnerability that current wireless architecture possesses

## 1.4 Scope

The scopes of this project are:

- i. Only 1 Access Point (AP) will be used
- ii. 2 to 5 clients will be connected to the AP
- iii. Only 1 laptop will be used to perform packets sniffing
- iv. The AP will be configured to use WPA for password encryptions during testing
- v. The traffic analysis is focused on IEEE 802.11 header

## 1.5 Project Significance

This project will greatly benefits those who are going to involve in wireless network analysis. Whether they are lecturers who will do further research on wireless networking, or students who will be network administer for a company in the future, this project can be as a guideline for them on analyzing wireless traffic. They can learn the techniques or methods for identifying the network anomalies, and troubleshoot it with appropriate solutions.

## 1.6 Expected Output

The outputs of this project are:

- The analysis of wireless traffic using wireless sniffers
- Understanding on characteristic of IEEE 802.11 network
- Mastering of hacking and analysis's techniques and approaches
- Awareness of security vulnerability that come upon

## 1.7 Conclusion

This project is called WLAN Traffic Analysis and Hacking through Sniffing and Vulnerability Exposed. First, the basic concept of wireless network will be introduced. The tools and devices involved in wireless communication will be stated out, like stations and access points, and the infrastructure of wireless network will be explained. Before moving on to packet sniffing, we must understand the process involved while stations communicate with each other and have a big picture about the encryption and authentication techniques used. Next, we will apply several analyzing methods and techniques to carry out the project findings. Wireless traffic analysis can provide many purposes for forensics. One of the purposes of forensics on wireless traffic is to allow us to identify a wireless security occurrence. We can detect and categorize the intrusion or attack by looking at the traffic that is passed on the network. After identifying the anomalies, we can troubleshoot wireless networks and track down the issues that are causing poor performance, discontinuous connectivity, and other common problems.

## CHAPTER II

### LITERATURE REVIEW AND PROJECT METHODOLOGY

#### 2.1 Introduction

There are two parts in this chapter which are literature review and project methodology. First of all, the domain which related with this project will be stated out with some explanation. Next, several keywords and terms that are being used in project will be explained, such as IEEE 802.11 and WPA. The most important part is previous research. By reading and understanding the way and method used by other research which is relate to this project, it can provide guideline on how to carry out this project research, like which techniques should be used and what tools should be chose. The next part is proposed solution, where the reason why implementing this methodology instead of others will be justified, and write out detail descriptions about what works will be done on each stage. At last, an action plan will be come out, which will be the milestone for all the activities carried out during project. A Gantt chart will be attached too. And a conclusion which will summarize the chapter and explain the next activities to be developed will end this chapter.

## **2.2 Literature Review**

### **2.2.1 Domain**

The domains which related to this project are ICT in Defense and ICT in Training and Education. A journal titled “Wireless Hacking - A WiFi Hack By Cracking WEP” by K Sai Ramani and K Rijutha (2010) mentioned that wireless networks like Wi-Fi being the most spread technology over the world is vulnerable to the threats of Hacking. Wireless sniffing is one kind of wireless hacking techniques that intercepts and decodes network traffic broadcast through a medium. Since wireless LAN technology has been introduced, wireless security on how to defense the network from various attacks has been the main issue. Thus, it is undeniable that wireless sniffing is closely related to ICT in Defense. Besides, as stated in Chapter I of this project, this research will greatly benefits those who are going to involve in wireless networking and as a guideline for carrying other related researches. Therefore, ICT in Education and Training also is the domain for this project.