

**BORANG PENGESAHAN STATUS TESIS**

JUDUL:

DEVELOPMENT OF WIRELESS LAN USER AUTHENTICATION APPLICATION

2006/2007

SESI PENGAJIAN: -----

Saya

MARHAINI BT MAT

(HURUF BESAR)

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 Kolej Universiti Teknikal Kebangsaan Malaysia.
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 pertukaran 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 telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD

(TANDATANGAN PENULIS)

Marhaini bt Mat

Alamat tetap : -----

Lot 2334, Kg Batu Tumboh, 22200 Besut

Tarikh : 21 November 2006



(TANDATANGAN PENYELIA)

En. Zulkiflee Bin Muslim

Fakulti Teknologi Maklumat dan Komunikasi  
Kolej Universiti Teknikal Kebangsaan Malaysia  
Karung Berkunci 1200

Ayer Keroh, 75450 Melaka

Tarikh : 23/11/06

CATATAN: \*\* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

^ Tesis dimaksudkan sebagai Laporan Projek Sarjana Muda (PSM).

**DEVELOPMENT OF WIRELESS LAN USER AUTHENTICATION  
APPLICATION**

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY  
KOLEJ UNIVERSITI TEKNIKAL KEBANGSAAN MALAYSIA  
2006

raf

TK5105.59 .M37 2006



0000038593


Development of wireless LAN user authentication application / Marhaini Mat.

i

I hereby declare that this project report entitled  
**DEVELOPMENT OF WIRELESS LAN USER AUTHENTICATION  
APPLICATION**

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

STUDENT

:  \_\_\_\_\_ Date : 23 NOVEMBER 2006  
(MARHAINI BT MAT)

SUPERVISOR

:  \_\_\_\_\_ Date : 23/11/06  
(ENCIK ZULKIFLEE B. MUSLIM)  
**ZULKIFLEE BIN MUSLIM**  
Pensyarah  
Fakulti Teknologi Maklumat dan Komunikasi  
Kolej Universiti Teknikal Kebangsaan Malaysia  
Karung Berkunci 1200  
Ayer Keroh, 75450 Melaka

## DEDICATION

I would like to dedicate my appreciation to my parents,  
Encik Mat Awang and Puan Maznah Ismail  
who have provided me with support emotionally  
and financially throughout this long journey called my college career

To my brother, Mazri  
And my sisters,  
Masitah, Mahirah and Madihah  
for their unconditional love and support.

This dedication also goes to  
Encik Zulkiflee Muslim  
For serving as my supervisor.  
Thanks for the priceless advice.

Not to forget my friends and my someone.  
Finally, this thesis is dedicated to all those  
who believe in the richness of learning.

## ACKNOWLEDGEMENTS

In the name of Allah s.w.t, the most gracious, the most merciful, I never would have taken on this final year project without the help of many people. I would like to express my gratitude to Encik Zulkiflee Muslim, my faculty supervisor of KUTKM for spending his precious time to make sure that the final year project running well. A deeply thanks for the unlimited guidance throughout the whole final semester. Not forgotten, special thanks to Encik Nurul Faisal, Encik Zulkifli Husin and Encik Ramli who contributed information to the wireless application project. To my family that always being with me for my ups and down, thanks for all the encouragement and supports. For my someone, thanks for your priceless advice and endless support that had encouraged me a lot. Thanks also to my colleagues for their support along the way. I am indebted to all my friends for their support and willingness. Last but not list, to all that had contributed during the period of final year project. I really appreciate the help and do my best to incorporate as much as I can.

## ABSTRACT

The WLAN User Authentication Application focused on the development of wireless authentication to meet the networking security requirement and it dynamically controls all aspects of a wireless network. The basic requirement of the application was to authenticate against end user and the device that attached to it. Authentication is the act of verifying a claimed identity. The application has three parts: the authentication and authorization module, graphical user interface and data storage. Authorization was acted to determine whether a particular right can be granted to the presenter of a particular credential. A plan for the construction of the application used the Rapid Application Development. The add on modules that integrated with FreeRadius software was developed using JAVA and TCP/IP programming. PAP and CHAP are type of authentication protocol that had been used to encrypt and decrypt the password and shared secret. The characteristics of this application are it equips with graphical user interface and data storage. The web-based application used by the users and administrators to manage who is allowed access to the Wireless Local Area Network (WLAN) and for registration process. By using client/server approach, it ensures effective security management from a central point of control. As a result, WLAN User Authentication Application is an ideal solution that provide robust authentication of wireless clients.

## ABSTRAK

WLAN User Authentication Permohonan tertumpu pada pembangunan rangkaian tanpa wayar untuk memenuhi keperluan keselamatan rangkaian dan ia dikawal secara dinamik dari semua aspek dalam satu rangkaian. Keperluan aplikasi adalah untuk mengesahkan identity pengguna dan alat yang digunakan. Pengesahan adalah tindakan mengesahkan identity pengguna. Aplikasi ini mempunyai tiga bahagian: modul pengesahan dan kebenaran, grafik antara muka dan penyimpanan data. Kebenaran adalah untuk menentukan sama ada ia sesuai dan boleh dibenarkan untuk menggunakan perkhidmatan. Untuk proses pembinaan, ia menggunakan Pembangunan Aplikasi Pesat. Modul-modul tambahan yang disepadukan dengan perisian FreeRadius dimajukan menggunakan Java dan pengaturcaraan TCP/IP. PAP dan CHAP adalah jenis pengesahan protokol yang telah digunakan untuk encrypt dan decrypt kata laluan dan perkongsian identity rahsia. Aplikasi ini turut dilengkapi dengan grafik antara muka pengguna dan penyimpanan data. Aplikasi yang berpangkalan pada satu pusat digunakan oleh pengguna-pengguna dan pentadbir-pentadbir untuk mengurus yang dibiarkan akses kepada Rangkaian Tanpa Wayar (WLAN) dan untuk proses pendaftaran. Dengan menggunakan pendekatan pelanggan/pelayan, ia memastikan keselamatan yang berkesan hanya dari satu pusat kawalan. Hasilnya, aplikasi WLAN User Authentication adalah satu kaedah atau cara yang menyediakan pengesahan Dengan menggunakan pendekatan pelanggan dan pelayan, ia memastikan keselamatan berkesan pengurusan dari satu pusat titik kawalan. Hasilnya, aplikasi WLAN User Authentication adalah satu kaedah yang menyediakan pengesahan untuk keselamatan di dalam rangkaian tanpa wayar.

## TABLE OF CONTENTS

<b>CHAPTER</b>	<b>CONTENTS</b>	<b>PAGE</b>
	<b>DECLARATIONS</b>	<b>i</b>
	<b>DEDICATION</b>	<b>ii</b>
	<b>ACKNOWLEDGEMENTS</b>	<b>iii</b>
	<b>ABSTRACT</b>	<b>iv</b>
	<b>ABSTRAK</b>	<b>v</b>
	<b>TABLE OF CONTENTS</b>	<b>vi</b>
	<b>LIST OF TABLES</b>	<b>xi</b>
	<b>LIST OF FIGURES</b>	<b>xii</b>
	<b>LIST OF ABBREVIATION</b>	<b>xiv</b>
 <b>CHAPTER I</b>	 <b>INTRODUCTION</b>	
	1.1 Project Background	1
	1.2 Problem Statement	2
	1.3 Objectives	3
	1.4 Scopes	4
	1.5 Project Significance	5
	1.6 Conclusion	6
 <b>CHAPTER II</b>	 <b>LITERATURE REVIEW AND PROJECT METHODOLOGY</b>	
	2.1 Introduction	7
	2.2 Fact and Finding	8
	2.2.1 Terms of WLAN User Authentication Application	8
	2.2.2 WLAN Security	9



2.2.3	Security Mechanism	10
2.2.4	Access Point Compatibility	12
2.2.5	Existing Software of RADIUS Server	12
2.3	Project Methodology	13
2.4	Project Requirements	17
2.4.1	Software Requirements	17
2.4.2	Hardware Requirement	19
2.5	Project Milestones and Schedule	21
2.5.1	Project Milestones	21
2.5.1	Project Schedule	22
2.6	Conclusion	23

### **CHAPTER III ANALYSIS**

3.1	Introduction	24
3.2	Problem Analysis	25
3.2.1	Background of Current System	25
3.2.2	Problem Statement	26
3.3	Requirement Analysis	28
3.3.1	Functional Requirement	28
3.3.2	Business Flow	30
3.3.3	Use Case View	31
3.3.4	Actors	32
3.3.5	Use Case Description	33
3.3.6	Interaction Diagram	36
3.4	Software Requirement	38
3.5	Hardware Requirement	40
3.6	Network Requirement	42
3.7	Conclusion	42

**CHAPTER IV DESIGN**

4.1	Introduction	43
4.2	High Level Design	44
4.2.1	Raw Data	44
4.2.2	System Architecture	47
4.2.2.1	High Level Logical View/Architecture	
4.2.2.2	Static Organization	49
4.2.2.3	High-Level Class Diagram	50
4.2.2.4	Deployment Diagram	53
4.2.3	User Interface Design	55
4.2.3.1	Navigation Design	55
4.2.3.2	Input Design	56
4.2.3.3	Output Design	58
4.2.4	Database Design	59
4.2.4.1	Conceptual Database Design	59
4.2.4.2	Data Dictionary	60
4.3	Network Architecture	69
4.3.1	Client/Server Architecture Model	69
4.3.2	Conceptual Design	71
4.4	Logical Design	73
4.4.1	Secure WLAN Logical Design	74
4.5	Physical Design	75
4.5.1	Prototype Design	75
4.6	Security Requirement	76
4.7	Conclusion	78

**CHAPTER V IMPLEMENTATION**

5.1	Introduction	79
5.2	Software Configuration Management	79
5.2.1	Configuration Environment Setup	79

5.2.1.1	Installation of Fedora Core 4	80
5.2.1.2	Configuration of Apache	81
5.2.1.3	Configuration of PHP	83
5.2.1.2	Configuration of MySQL	84
5.2.2	Version Control Procedure	86
5.2.2.1	Patches and Contribution	86
5.2.2.2	Module Setup	87
5.2.2.3	Database Implementation	89
5.2.2.4	FreeRadius with WLAN User Authentication Support	89
5.3	Hardware Configuration Management	91
5.3.1	Configuration of Access Point	92
5.3.2	Configuration of Wireless Client	96
5.4	Implementation Status	99
5.5	Conclusion	102

## **CHAPTER VI TESTING**

6.1	Introduction	103
6.2	Test Plan	103
6.2.1	Test Organization	103
6.2.2	Test Environment	103
6.2.3	Test Schedule	104
6.3	Test Strategy	105
6.4	Test Design	105
6.4.1	Test Description	105
6.4.2	Test Data	107
6.5	Test Result and Analysis	107
6.6	Conclusion	111

**CHAPTER VII PROJECT CONCLUSION**

7.1	Observation on Weaknesses and Strengths	112
7.1	Strengths	112
7.2	Weaknesses	113
7.2	Proposition for Improvements	113
7.3	Contribution	115
7.4	Conclusion	116

<b>REFERENCES</b>	<b>117</b>
-------------------	------------

<b>BIBLIOGRAPHY</b>	<b>118</b>
---------------------	------------

<b>APPENDIX 1 : GANTT CHART</b>	
---------------------------------	--

<b>APPENDIX 2 : USER MANUAL</b>	
---------------------------------	--

## LIST OF TABLES

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
Table 2.1	Activity of Project Milestones	21
Table 4.1	Table of Entity and Attributes of WLAN User Authentication Application	50
Table 4.2	Table of User Information	65
Table 4.3	Table of Network Access Server Information	65
Table 4.4	Table of Authentication	66
Table 4.5	Table of Accounting Information	66
Table 4.6	Table of Class Login	67
Table 4.7	Table of Class User Registration	68
Table 4.8	Table of Class NAS Administration	69
Table 4.9	Table of Class Authentication Report	69
Table 4.10	Table of Class Accounting Report	70
Table 5.1	Description of Programming implementation status	99
Table 5.2	Description of Database Implementation status	99
Table 5.3	Description of User Interface implementation status	100
Table 5.4	Description of Hardware Setup implementation status	100
Table 5.5	Description of Module Integration implementation status	101
Table 6.1	Test Duration	104
Table 6.2	Test Case and Expected Results for Every Module	106
Table 6.3	Test Data for Every Module	107

## LIST OF FIGURES

FIGURES	TITLE	PAGE
Figure 2.1	Authentication Mechanism	11
Figure 2.2	RUP Diagram	14
Figure 3.1	Activity Diagram for Open System Authentication	27
Figure 3.2	Sequence Diagram for Open System Authentication	28
Figure 3.3	Activity Diagram for Shared Key Authentication	30
Figure 3.4	Overview of Wireless LAN User Authentication Application (To-Be System)	33
Figure 3.5	To-be System of Wireless LAN User Authentication Application	35
Figure 3.6	Global view of use-case model	36
Figure 3.7	Interaction diagram for Logon	41
Figure 3.8	Interaction diagram for Authentication and Authorization	42
Figure 3.9	Interaction diagram for Accounting	42
Figure 4.1	WLAN User Authentication Application overview based on 3-tier architecture	51
Figure 4.2	WLAN User Authentication Application Package	53
Figure 4.3	Class Diagram of WLAN User Authentication Application	55
Figure 4.4	Deployment Diagram of WLAN User Authentication Application	57
Figure 4.5	Main page for general user status overview	59
Figure 4.6	Client Registration	60
Figure 4.7	Network Access Server Registration	61
Figure 4.8	View Online User	62
Figure 4.9	User accounting overview	63
Figure 4.10	The Entity Relationship Diagram (ERD) for WLAN User Authentication Application	64
Figure 4.11	Client/Server Architecture Model	72
Figure 4.12	Conceptual View of network access	73
Figure 4.13	Logical Design of WLAN Environment	75
Figure 4.14	Secure WLAN Logical Design	76
Figure 4.15	Physical Layout of a network prototype	77
Figure 5.1	The environment architecture of WLAN User Authentication Application	79
Figure 5.2	Screenshot of /etc/httpd/conf/httpd.conf file	82
Figure 5.3	Apache Test Page	83
Figure 5.4	Screenshot of PHP Installation	83
Figure 5.5	PHP Test Page	84
Figure 5.6	PHP with MySQL Test Page	85

Figure 5.7	phpMyAdmin provides a graphical front	86
Figure 5.8	FreeRadius Patch	87
Figure 5.9	phpMyAdmin Database	89
Figure 5.10	Screenshot of modules	90
Figure 5.11	Screenshot of radius service	91
Figure 5.12	TCP/IP Properties	92
Figure 5.13	LAN Properties	93
Figure 5.14	Command Prompt Windows	93
Figure 5.15	Home Screen of Access Point	94
Figure 5.16	LAN Screen of Access Point Configuration	95
Figure 5.17	Wireless Screen of Access Point Configuration	95
Figure 5.18	Network Property	97
Figure 5.19	PEAP Property	98
Figure 6.1	The NTRadPing Application Window	108

**LIST OF ABBREVIATION**

<b>AP</b>	Access Point
<b>DoS</b>	Denial-of-Service
<b>EAP</b>	Extensible Authentication Protocol
<b>EAPOL</b>	EAP over LAN
<b>HTML</b>	Hypertext Mark Up Language
<b>ISP</b>	Internet Service Provider
<b>NAS</b>	Network Access Server
<b>NOC</b>	Network Operations Center
<b>PEAP</b>	Protected Extensible Authentication Protocol
<b>PMK</b>	Pairwise Master Key
<b>RAD</b>	Rapid Application Development
<b>RADIUS</b>	Remote Authentication Dial-In User Service
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SSH</b>	Secure Shell
<b>WEP</b>	Wi-Fi Encryption Protocol
<b>WLAN</b>	Wireless Local Area Network
<b>WPA</b>	Wi-Fi Protected Access



## CHAPTER I

### INTRODUCTION

#### 1.1 Project Background

Wireless Local Area Network (WLAN) transmits and receives data through the air. It has an expensive and easy method of providing high-speed Internet access. WLAN provide users with the ability to access the information from almost anywhere.

Many wireless networks are skipped to run Open System Authentication by default. Anyone who connects to the wireless networks is granted access. This is used primarily in the universities where the end users are transient and managing encryption is not feasible. There is no form of data encryption used, given that this intended to be used in a public setting.

Authentication server software includes three parts: an authentication server, client protocols and accounting server. It works by having a user dial in to a remote access server and pass logon name and password information to it. The information is forwarded to an authentication server that validates the user and returns the information necessary for the access server to initiate a session with the user. Users who install this application on their laptops or other computing devices can connect wirelessly to the network.

## 1.2 Problem Statement(s)

A wireless network gives security architect's different problem to overcome.

- Physical access versus proximity

Tapping into traditional wires Local Area Networks requires some sort of physical access. Not an impossible feature, but there is a greater risk of detection. Tapping into a wireless LAN only requires an intruder be in the general proximity of the transmitter. That makes it much easier to avoid detection and much more difficult to trace.

- MAC masquerade

By creating the list of allowed MAC addresses on the access point's address filters page, the intruders can create counterfeit MAC Address. A hacker can obtain information such as client and access point MAC addresses, MAC addresses of internal hosts and time of association or disassociation. The hacker can use such information to do long-term traffic polling and analysis that may provide user or device details.

- Open authentication

Authenticating a user before granting access to a network is a basic security requirement that wireless networks typically lack. With open authentication, the entire authentication done in clear text and a client can connect to the network without supplying the correct key. An attacker tries to connect their wireless client to a network connection without authorization.

### 1.3 Objective

The goals of the project are to:

- Enables safe and secure access over a wireless LAN network

Consistently provides some level of protection against sniffing or any active attacker. An efficient and secure infrastructure facility that enabled access network because nothing is transmitted over the air in the clear text.

- Ensure authenticity of each user, not just devices that accessing the wireless LAN network

The authentication method must be set on each client, and the setting should match the access point which the client wants to associate. If the client has the wrong key, it will fail authentication and will not be allowed to connect to the access point.

- Establish user accountability to critical information by providing end-to-end user identification.

This application supports authentication based on username, password and the physical address or Media Access Control (MAC) address of a client.

- Manages wireless LAN user access security policies centrally through the authentication server

Network managers can authenticate all dial-in users against a single or central database. An organization with hundreds or thousands of

wireless LAN users needs a security solution that can be managed from one point of control.

- Keep track of user account information as part of accounting process.

By monitoring, the administrator can obtain information such as time of association or disassociation and detailed logging of user sessions. Any suspicious accounts can be blocked, thus preventing the suspicious user to log on to the network at all.

#### **1.4 Scopes**

This project has the following characteristics:

- Prototype model that contains one server where authentication application resides in it. Wireless station communication is passed through using one access point at one time.
- Limit every user to only 1 session by having each user allowed to connect only from 1 MAC address.
- Includes three parts: an authentication server, client and an accounting server for monitoring.

## 1.5 Project Significance

The intended use is for user within the open area with WLAN connections to complete a strong authentication before joining the network. While, the administrator can control access to the network at one central point.

Wireless LAN User Authentication Application offers the following advantages:

- Tight security

This application allows user information to be stored on one host. All authentication and access to network services is managed by one authentication server.

- Simplified management

Security information is stored in text files at a central location, the authentication server. Adding new users to the database or modifying existing user information can be easily accomplished by editing these text files.

- Extensive logging capabilities

RADIUS provides extensive audit trail capabilities, referred to as RADIUS accounting. Information collected in a log file can be analyzed for security purposes, or used for billing.

- Web based administration

This application turns the web browser into a remote control. A web browser can be configured as RADIUS settings from anywhere, view all currently online sessions, modify the subscriber record, and more.

- Support for the latest RFCs

This application supports the latest RADIUS RFC which is RFC2865 and guaranteed a solution that will continue evolving into the future.

## **1.6 Conclusion**

One of the major concerns with wireless is the issue of security. Weaknesses in wireless network create the possibility of an attack that lead to develop wireless authentication software. Authentication is one of the fundamental requirements to provide secure and feasible Wireless LAN. With an authorized and centralized security management system enabling secure wireless access to the wireless network.

The next chapter will present the understanding of standards and applications based on literature reviews. The development of this application will be constructed and implemented using the suitable project methodology.

## CHAPTER II

### LITERATURE REVIEW AND PROJECT METHODOLOGY

#### 2.1 Introduction

Literature reviews aims to give information through a process of searching, collecting, analyzing and drawing conclusion of the research, journal or past notes. From the reviews conducted, it gives enough information to help in order to adapt application to the particular needs. This chapter begins with the description of the overall meaning of Wireless LAN User Authentication Application. The chapter describes how 802.1x and Protected Extensible Authentication Protocol (PEAP) work to secure access to the network. The middle portion of literature reviews describes the solutions of WLAN security including Authentication server placement, selection of hardware and software and client configuration.

One of the major influences on the quality of the system developed is the software development approach adopted. The approach used in this project was the Object-Oriented Analysis and Design (OOAD), which is the standard method for implementing any new system. Based on proven software engineering expertise, the chosen object oriented model is RUP which stands for Rational Unified Process.

## 2.2 Fact and Finding

Fact and finding techniques used to investigate requirements of the application that will be developed by reading or doing research. The kind of documents that are suitable sources of information include documentation of the existing software, reports and journal.

### 2.2.1 Terms of WLAN User Authentication Application

According to Randall and Sosinky (2004), wireless means without wires where all wireless communication takes place over radio waves, electromagnetic waves that carry signals. The term of wireless LAN or WLAN (LAN means Local Area Network) is referring to network in which the user device that connects to the network via radio waves. The Institute of Electrical and Electronics Engineers (IEEE) group has outlined the primary standard for wireless LAN is IEEE 802.11 with 802.11g. 802.11g runs on the same radio frequency (RF) band as 802.11b (2.4 GHz) but uses the transmission techniques of 802.11a. The G standard also permits vendors to incorporate proprietary techniques that can potentially push the speeds of G to 108 Mbit/s. IEEE 802.11g compliant and offers some level of security like WEP and WPA.

In network communication terminology, authentication is a mechanism that determines whether the client can use the services provided by the authenticator. Authentication is one of the fundamental requirements to provide secure and feasible Wireless LAN. The RADIUS protocol is currently defined in RFC 2865 for Remote Authentication Dial In User Service. Based on Wikipedia encyclopedia, RADIUS is an AAA (Authentication, Authorization and Accounting) protocol for application protocol utilized by 802.1x wireless security standard. RFC 2865 describes a protocol for carrying authentication, authorization and configuration information between a