

**SECURE WIRELESS IMPLEMENTATION
BASED ON IEEE 802.1X NETWORK STANDARD**

MAHMOUD H R ALSLAKHI

UNIVERSITI TEKNOLOGI MALAYSIA

UNIVERSITI TEKNOLOGI MALAYSIA

DECLARATION OF THESIS / UNDERGRADUATE PROJECT PAPER AND COPYRIGHT

Author's full name : MAHMOUD H R ALSLAKHI

Date of birth : 19 OCTOBER 1982

Title : SECURE WIRELESS IMPLEMENTATION BASED ON IEEE 802.1x NETWORK STANDARD

Academic Session : 2006/2007

I declare that this thesis is classified as:

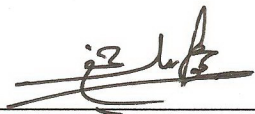
CONFIDENTIAL (Contains confidential information under the Official Secret Act 1972)*

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 declare that this thesis is classified as:

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.



SIGNATURE

2006536

(NEW IC NO. / PASSPORT NO.)

Certified by:



SIGNATURE OF SUPERVISOR

Associate Prof. Dr. Zailani Mohamed Sidek

NAME OF SUPERVISOR


Date : **14 NOVEMBER 2007**

Date: **14 NOVEMBER 2007**

NOTES : * If the thesis is CONFIDENTIAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.

SUPERVISOR DECLARATION

“I hereby declare that I have read this dissertation and in my opinion this thesis 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 : **Associate Prof. Dr.
Zailani Mohamed Sidek**

Date : **14 NOVEMBER 2007.**

SECURE WIRELESS IMPLEMENTATION BASED ON
IEEE 802.1X NETWORK STANDARD

MAHMOUD H R ALSLAKHI

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

Center for Advanced Software Engineering (CASE)
Faculty of Computer Science and Information System
Universiti Teknologi Malaysia

NOVEMBER 2007

DECLARATION

I declare that this thesis entitled: "*Secure Wireless Implementation based on IEEE 802.1x Network Standard*" is the result of my own research except as cited in references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : 

Name of Candidate : MAHMOUD H R ALSLAKHI

Date : 14 November 2007

To my beloved parents, brothers and sisters

ACKNOWLEDGMENT

All praise be to Allah, the Most Merciful, for His Love and Guidance. Salutations on the Prophet Muhammad (*PBUH*), his family, and fellow companions.

May I express my appreciation to ALLAH, the beneficent, the merciful, for making me a Muslim and blessing me with the privilege of acquiring a higher degree. My heart felt gratitude goes to my parents for bearing with me weakness upon weakness from cradle to date.

AP Dr. Zailani Mohamed Sidek, my supervisor gave me all the necessary support needed for success, as such, I owe it a duty to be appreciative. I wish thank my colleagues Usama, Ibrahim, Mustafa, Amir, Rizal, Marwan, Ali, Habeb, Naser, Yusuf, Salima and others for their support and encouragement. May ALLAH reward you all the relentless efforts to see through this academic pursuit.

ABSTRACT

Research in Information Technology has a tremendous growth in recent years mainly due to the affordability of the technology and consequently, a high increase in interest from users. In addition, the mobility systems which imply the use of wireless networks have increased rapidly. Currently, many organizations have provided extensive wireless services to their staffs. This poses a problem of securing the easy access to the wireless networks. Therefore, authentication has become an inevitable reality in the design of such systems. This research sought for the best authentication mechanism suitable for organizations in general, and to university campuses in particular. The result of this research is then the design and implementation of an authentication scheme based on IEEE 802.1x standard. The scheme provides secure access to users engaged in the wireless connection. It implements a two-factor authentication. The first factor is the username/password combination which the user provides prior logging onto the system. The second factor is the digital certificates that are stored locally in a client's desktop/laptop. The mechanism involved in the authentication is based on EAP-TLS, which is a type of authentication method provided by IEEE 802.1x standard. The result of the implemented system is a highly secure scheme that provides both users and computers (machines) authentication. Only legitimate users with legitimate machines can access the wireless network system in an authorized way. In addition, the idea of a Users Tracking System Application (UTSA) has been introduced. This application basically tracks the users' status and behavior (whether they are online or offline) as long as they are utilizing the network resources. It can later be utilized to track who, when and where the users are in the network systems.

ABSTRAK

Kebelakangan ini, penyelidikan teknologi maklumat telah berkembang pesat kerana pertambahan keupayaan kuasa memiliki teknologi dan hasil pertambahan minat pengguna. Tambahan pula, sistem mudah alih ini bererti penggunaan teknologi tanpa wayar yang semakin meningkat. Sekarang ini banyak organisasi menyediakan perkhidmatan tanpa wayar secara meluas untuk kegunaan kakitangan. Ini menyebabkan terdedahnya keselamatan ke atas mudahnya mencapai rangkaian tanpa wayar. Oleh itu, pengesah-betulan (authentication) menjadi suatu kemestian bagi mereka-bentuk sistem sebegini. Penyelidikan ini dijalankan untuk mencari kaedah pengesah-betulan yang terbaik dan sesuai bagi organisasi secara umum dan bagi kampus universiti khususnya. Maka, penyelidikan ini menghasilkan reka-bentuk dan pelaksanaan satu skema pengesah-betulan berdasarkan piawaian IEEE 802.1x. Skema ini menyediakan capaian selamat bagi pengguna yang terlibat dalam hubungan tanpa wayar. Skema ini melaksanakan pengesah-betulan menggunakan dua factor. Faktor pertama menggunakan nama pengguna dan kata laluan sebelum dibenarkan masuk ke dalam sistem. Faktor kedua menggunakan sijil digital yang disimpan dalam komputer pengguna. Mekanisme pengesah-betulan tersebut adalah berdasarkan EAP-TLS iaitu satu kaedah pengesah-betulan yang diberi oleh piawaian IEEE 802.1x. Hasil daripada pelaksanaan sistem adalah satu skema berkeselamatan tinggi bagi pengesah-betulan pihak pengguna dan komputer (mesin). Hanya pengguna sah yang menggunakan mesin sah dibenarkan mencapai sistem rangkaian tanpa wayar ini secara sah. Cadangan satu sistem aplikasi bernama Aplikasi Sistem Menjejak Pengguna (UTSA) telah diperkenalkan. Pada asasnya, aplikasi ini akan menjejak status dan tingkah laku pengguna (sama ada mereka berada dalam talian atau pun tidak) selagi mereka menggunakan sumber-sumber rangkaian. Pada masa hadapan, aplikasi ini boleh dikembangkan untuk mengetahui siapa, bila, dan di mana pengguna sedang berada dalam suatu rangkaian sistem.

TABLE OF CONTENTS

CHAPTER	TITLE	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGMENT	iv
	ABSTRACT	v
	ABSTRAK	vi
	TABLE OF CONTENTS	vii
	LIST OF TABLES	xiii
	LIST OF FIGURES	xiv
	LIST OF ABBREVIATIONS	xvii
	LIST OF APPENDICES	xix
1	INTRODUCTION	1
	1.1 Introduction	1
	1.2 Background of the Problem	2
	1.3 Problem Statement	5
	1.4 Project objective	5
	1.5 Project scop e	6
2	LITERATURE REVIEW	9
	2.1 Introduction	9
	2.2 Network Security	10
	2.2.1 Overview	10
	2.2.2 Five layers security model	11
	2.2.2.1 Authentication	11

2.2.2.2	Authorization	12
2.2.2.3	Encryption	12
2.2.2.4	Integrity	13
2.2.2.5	Audit	13
2.3	Wireless security	15
2.3.1	Overview of Wireless Technology	15
2.3.2	Modes of Wireless Network	17
2.3.2.1	Infrastructure (access point preferred) mode	17
2.3.2.2	Ad-hoc (peer-to-peer) mode	18
2.3.3	General security threats and attacks on WLANs	20
2.3.3.1	Passive attacks	21
2.3.3.2	Active attacks	22
2.3.3.3	Man-in-the middle attack	22
2.3.3.4	Jamming attack	23
2.4	Authentication in Wireless Network	23
2.4.1	Types of authentication used in wireless network	23
2.4.1.1	Open System Authentication	24
2.4.1.2	Shared key authentication	25
2.4.1.3	Network-EAP	26
2.4.2	Comparison between different authentication mechanisms used	27
2.4.2.1	Open Network	27
2.4.2.2	Media Access control (MAC) based authentication	28
2.4.2.3	Wired Equivalent Privacy (WEP)	29
2.4.2.4	Virtual Private Network (VPN) gateway	30
2.4.2.5	Web-based authentication gateway	32
2.4.2.6	IEEE 802.1x	33

2.4.3	Best authentication choice based on organizations types	34
2.4.3.1	Level 1: Home and SOHO WLAN security	35
2.4.3.2	Level 2: Small business WLAN security	36
2.4.3.3	Level 3: Medium to large WLAN security	37
2.4.3.4	Level 4: Military grade maximum level WLAN security	38
2.5	IEEE 802.1x authentication scheme	39
2.5.1	General concepts and architectural framework	39
2.5.2	Packet format and protocol exchange	45
2.5.3	Advantages of using IEEE 802.1x	47
2.5.4	Limitations and vulnerabilities on using IEEE 802.1x	49
2.5.4.1	The absence of mutual authentication	50
2.5.4.2	Session Hijacking	51
2.6	Extensible Authentication Protocol (EAP)	53
2.6.1	General concepts of Extensible Authentication Protocol (EAP)	53
2.6.2	EAP-MD5	55
2.6.3	EAP-TLS	57
2.6.4	EAP-TTLS	60
2.6.5	EAP-PEAP	61
2.6.6	Comparison between previous four EAP methods	64
2.7	Remote Authentication Dial-in Service (RADIUS)	66
2.7.1	General concepts and features of RADIUS	66
2.7.2	RAIUDS Packet format and basic operation	67

2.8	Summary	68
3	RESEARCH METHODOLOGY	70
3.1	Introduction	70
3.2	The research development phases	71
3.2.1	Determine the research requirements	72
3.2.2	System Design	74
3.2.3	System Implementation	76
3.2.4	System Testing	77
3.2.5	Report Writing	77
3.3	Operational framework	78
3.3.1	Hardware requirement specification	78
3.3.2	Software requirement specification	80
3.4	Summary	81
4	SYSTEM DESIGN	82
4.1	Introduction	82
4.2	The overall system design	82
4.3	CA Server	84
4.3.1	Certificate Service	85
4.3.2	Infrastructure Services	89
4.2.2.1	Active Directory (AD)	89
4.2.2.2	Domain Name System (DNS)	90
4.2.2.3	Dynamic Host Configuration Protocol (DHCP)	91
4.4	Remote Authentication Dial-in User Authentication (RADIUS)	91
4.5	The entire network / Internet Information Service (IIS)	92
4.6	The overall authentication process of the designed system	92

4.7	Users Tracking System Application	94
4.8	Summary	97
5	SYSTEM IMPLEMENTATION AND TESTING	98
5.1	Introduction	98
5.2	CA Server Configuration	98
5.2.1	Infrastructure and Certificate Service Installation and configuration	99
5.2.1.1	Active Directory and DNS	99
5.2.1.2	Dynamic Host Configuration Protocol (DHCP)	100
5.2.1.3	Certificate Service Installation and configuration	101
5.2.2	Preparing the CA server for authentication	102
5.2.2.1	Create Wireless Group object	103
5.2.2.2	Create and configure certificate template	104
5.2.2.3	Configure the auto-enrollment and auto certificate request feature	104
5.3	RADIUS server configuration	105
5.4	The 3Com wireless Access Point configuration	106
5.5	Web Server (IIS) configuration	107
5.6	Users Tracking System Application (UTSA)	108
5.6.1	Client's side Code	109
5.6.2	CA server's code (UTSA)	111
5.7	Testing the system	114
5.7.1	Testing the authentication	115
5.7.2	Testing the UTSA	117
5.8	Summary	120
6	DISCUSSION, FUTURE WORKS AND CONCLUSION	121

6.1	Introduction	121
6.2	Discussion	121
6.2.1	Justification of choosing windows as an operating system in this project	122
6.2.2	Justification of the authentication level in this project	123
6.2.3	Features of the implemented authentication in this project	123
6.2.4	Comparing UTM wireless authentication with proposed IEEE 802.1x	124
6.3	Contribution	126
6.4	Future works	127
6.5	Conclusion	128
	LIST OF REFERENCES	129
	APPENDICES A – C	134 - 190

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	comparison between different authentication mechanisms used in WLAN	34
2.2	comparison between EAP methods	64
3.1	The three desktop servers' requirements	79
3.2	The client laptop/desktop machine requirements	79
3.3	Minimum Access Point Specifications	80
6.1	Comparison between UTM wireless authentication & IEEE 802.1x	126

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
1.1	(a) unauthorized state port (b) authorized state port	7
2.1	Security Pyramid [Graham Doug, 2003]	14
2.2	802.11 wireless systems and The OSI model [Ouellet et al., 2002]	15
2.3	US College campuses with strategic plans for wireless deployment[Schmidt,(2006)]	17
2.4	Infrastructure Mode [Hernández Heidi, 2005]	18
2.5	Ad-hoc mode [Hernández Heidi, 2005]	19
2.6	Security incidents or attacks on Wireless LANs in 2002	20
2.7	Open System (Null) authentication [Barken et al., 2004]	25
2.8	Shared Key Authentication [Barken Lee et al., 2004]	26
2.9	VPN authentication over Wireless	31
2.10	Web-based authentication	32
2.11	wireless authentication representation in OSI model	40
2.12	The three entities in general architecture of an IEEE 802.1x system [Kelati, 2001]	41
2.13	unauthorized state	43
2.14	authorized state.	44
2.15	EAPOL Diagram	46
2.16	IEEE 802.1x basic protocol exchange	47
2.17	Man-in-the middle attack	50
2.18	Session Hijacking Attack	52
2.19	EAP packet format [<i>Earl Aaron, 2006</i>]	54
2.20	EAP-MD5 process details [<i>Earl Aaron, 2006</i>]	57

2.21	EAP-TLS process details [<i>Earl Aaron, 2006</i>]	59
2.22	EAP-TTLS process detail [<i>Earl Aaron, 2006</i>]	61
2.23	PEAP process detail [<i>Earl Aaron, 2006</i>]	63
2.24	RADIUS packet format [<i>Earl, 2006</i>]	67
3.1	Research Development phases	71
3.2	the overall system architecture	75
4.1	The overall system design components	83
4.3	Certificate Service components and operations' sequence	85
4.4	X.509 V3 certificate structure	86
4.5	the project Domain Namespace	91
4.6	The overall authentication process of the system	93
4.7	The machine start-up mode and user login mode	95
4.8	Users Tracking System Application demonstration diagram	96
5.1	Active Directory Users and Computers tool	100
5.2	DHCP snap-in tool	101
5.3	Certificate Authority snap-in tool	102
5.4	WirelessUsers group and the users created in AD	103
5.5	the project Domain Namespace	104
5.6	IAS snap-in tool	106
5.7	3Com Wireless Access Point configuration page	107
5.8	The testing connectivity web page in the IIS server	108
5.9	(A) logon flow chart (B) Logoff flow chart	110
5.10	Snapshot of WirelessUsers table created in the UTM database	111
5.11	The Users Tracking System Application GUI	112
5.12	The "Add to DB" button flow chart	113
5.13	The "Refresh" button flow chart.	114
5.14	Validating the user identity	115
5.15	Warning balloon shows the user's access denied	116
5.16	The user granted the access through the "UTM Wireless" Access Point	116

5.17	snapshot of the logon script running on the client's machine	117
5.18	snapshot of the logoff script running on the client's machine	118
5.19	snapshot of the User Tracking System Application (UTSA)	119
6.1	snapshot of the SMAC V2.0 tool	125

LIST OF ABBREVIATIONS

AAA	-	Authentication Authorization Accounting
ACL	-	Access Control List
AD	-	Active Directory
AES	-	Advanced Encryption Standard
ANSI	-	American National Standards Institute
AP	-	Access Point
CA	-	Certificate Authority
CHAP	-	Challenge Handshake Authentication Protocol
CRC-32	-	Cyclic Redundancy Check-32
CSP	-	Cryptographic Service Provider
DC	-	Domain Controller
DHCP	-	Dynamic Host Configuration Protocol
DNS	-	Domain Name System
EAP	-	Extensible Authentication Protocol
EAPOL	-	Extensible Authentication Protocol over LAN
EAPOW	-	Extensible Authentication Protocol over Wireless
IAS	-	Internet Authentication Service
IEEE	-	Institute of Electrical and Electronic Engineering
IETF	-	Internet Engineering Task Force
IIS	-	Internet Information Services
IP	-	Internet Protocol
LAN	-	Local Area Network
LDAP	-	Lightweight Directory Access Protocol
LLC	-	Logical Link Control
MAC	-	Media Access Control
MD5	-	Message Digest 5

MitM	-	Man-in-the-Middle
MSCHAP	-	Microsoft Challenge Handshake Authentication Protocol
NAS	-	Network Access Server
NDS	-	Novell's NetWare Directory Service
OU	-	Organizational Unit
PAE	-	Port Access Entity
PAP	-	Password Authentication Protocol
PCT	-	Private Communication Technology
PEAP	-	Protected Extensible Authentication Protocol
PHY	-	Physical
PKI	-	Public Key Infrastructure
PPP	-	Point-to-Point Protocol
RADIUS	-	Remote Authentication Dial-in User Service
RC4	-	Rivest Cipher 4
RFC	-	Request for Comments
RF	-	Radio Frequency
SAM	-	Security Account Manager
SNMP	-	Simple Network Management Protocol
SSL	-	Secure Socket Layer
STD	-	Standard
TKIP	-	Temporal Key Integrity Protocol
TLS	-	Transport Layer Security
TTLS	-	Tunnel Transport Layer Security
UTM	-	Univresiti Teknologi Malaysia
UTSA	-	Users Tracking System Application
WEP	-	Wired Equivalent Privacy
WLAN	-	Wireless Local Area Network
WPA	-	Wi-Fi Protected Access
WPA PSK	-	Wi-Fi Protected Access Pre-Shared Key
VPN	-	Virtual Private Network

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Step-by-Step System Configuration	134
B	Users Tracking System Application (UTSA)	178
C	Testing the authentication system	190

CHAPTER 1

INTRODUCTION

1.1 Introduction

A Wireless local area network (WLAN) is a flexible data communication system implemented as an extension to or as an alternative for a wired LAN. By using radio frequency (RF) technology, wireless LANs transmit and receive data over air, minimizing the need for wired connection. Thus, wireless LANs combine data connectivity with user mobility.

Wireless LANs have gained strong popularity in a number of vertical markets including health-care, retail, manufacturing, warehousing, and academia. These industries have profited from the productivity gains of using hand-held terminals and notebook computers to transmit real-time information to centralized hosts for processing. Today's wireless LANs is becoming more widely recognized as a general-purpose connectivity alternative for a broad range of business customers.

A WLAN connects users within a local area, which might be a building or campus, using radio signals to exchange data. The basic issues, which differentiate WLANs from telephone cellular networks or satellite networks, are frequencies, data rates, coverage area and legal issues. The emphasis of the wireless LANs environments is driven by the strong efforts spent by companies in order to improve data rates, reliability, and quality of service of such networks.

This project is concerned with the security of the WLANs. Issues involved in wireless security include confidentiality, integrity, authenticity, accountability...etc. However, this project mainly focuses on the authentication perspective.

1.2 Background of the Problem

The security in wireless LANs environment is harder than the wired LANs especially with respect to the issue of accessibility. The accessibility in wired LANs can be achieved by applying physical security to the room, building or the place where the network is located.

In Contrast, The wireless LANs are not restricted or tied to physical limitations. Anyone, who has a wireless device and exists in the wireless LANs range, can access it. The range of the wireless coverage could lead to leakage outside the premises, thereby exposing the system to outside threats. In this case, People on the street, car riders, hackers and others, all can access the system.

Therefore, there is an increasing demand to secure the access to the WLANs and prevent unauthorized users from accessing the network. Building a solid authentication scheme can solve this problem. Hence, companies endeavor to secure their respective wireless networks.

Authentication encompasses the first piece of wireless security. Many technologies are available to provide secure authentication schemes. Typically, universities have implemented robust authentication services to support their information technology infrastructures. Authentication is comprised of one or more of the following categories (Allen and Wilson, 2002):

- a) Something you know (i.e. username and password combinations)

- b) Something you have (i.e. smart card and token technology)
- c) Something you are (i.e. biometric solutions such as fingerprint technology)

To achieve the high level of security, there is a need to implement these three factors. This kind of implementation called three-factor authentication. However, the implementation of such scheme is so expensive, and in addition clients or users are obliged to purchase new biometric devices and attach them to their laptops or PCs (to satisfy option c). Such additional expenditure is affordable by companies, unlike normal users, who find it hard to absorb such extra costs.

Therefore, many organizations implement only one or two-factor authentication. Most of these implementations used the first two options, because they are stronger than one factor. According to Cheswick *et al.* (2003), “Most Simple applications use single-factor authentication. More important ones require at least two. We recommended two-factor authentication using the first two (something you know and something you have) when authenticating to a host from untrusted environment like the internet.”

The early approach was just to implement an authentication by using the username/password, which is so weak and people impersonated each other or stole the others' username/password. According to Zahur and Yang (2004), “A new proposed security solution was Wired Equivalent Privacy (WEP). According to the 802.11 standard, WEP was intended to provide confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy". WEP was ratified in September 1999. It uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity (Wikipedia, 2007b). In addition to that, WEP can also provide authentication by using the shared secret key as password, which is the case of some public café shops. Even in the field of encryption, which WEP is specialized in, news is talking about cracking WEP in minutes. Microsoft (2002) mentioned that “During the summer of 2000, a hacker tool released on the Internet

enabled a nearby malicious intruder with a high-gain, directional antenna to pick up a WLAN RF signal and easily break the encryption of WEP-key, 802.11b-based WLANs, thereby rendering them inherently unsecured. A 40-bit WEP-key can be broken in approximately 30-40 minutes; a 128-bit WEP-key can be compromised within two hours. An intruder with a valid WEP-key can gain access to internal network resources easily". An example of such tool is Kismac, which can crack 64-bit WEP in 4min 27sec (video source - Google (2007)).

Some organizations used MAC address (MAC filtering) and username/password authentication as a two-factor authentication. In the beginnings of this implementation, it was completely secure and only authorized person can access the system. It was believed that each network card has its unique MAC address and can't be changed. Nowadays there are many tools that can spoof the MAC address e.g SMAC 2.0 and MAC Makeup. Once the hacker spoofs the MAC address to authorized one, he can log on and try to impersonate the username/password combination of the victim. An example of such organization using this technique is UTM *CityCampus* in KL-Malaysia. The authentication scheme introduced in this project can be easily integrated to the local wireless environment in UTM *CityCampus-KL*, which will enhance the security of the wireless system on campus.

Based on the recommendation of Cheswick *et al.*, the proposed solution is the implementation of IEEE 802.1x standard, which was lately revised in 2004. The system uses two-factor authentication. The IEEE 802.1x network access control standard supports the mutual authentication of the client and corporate network using certificates. This method of authentication requires the physical possession of the digital certificates and cannot be imitated by simply knowing a username/password; and certificate-based authentication never transmits authentication credentials in the clear over the network whether it is comprised of cables (IEEE 802.1x can also be implemented over wire LAN with the same structure) or radio waves.

1.3 Problem Statement:

Wireless environment is not restricted to any physical limitations. People can access the wireless network from outside of the premises. Therefore, demands on implementing a secure authentication scheme for wireless network arise these days. This kind of scheme should prevent any unauthorized access whether it is done within the building or from outside.

Many researches carried out to implement such schemes. However, not all of them are effective and some suffer from breaches. Examples of these are WEP, MAC, and web-based authentication. An illustration of one of them is the using of MAC address (MAC filtering) and username/password as a two factor authentication. This scheme suffers from the masquerade, in which the attacker can spoof legitimate MAC address to access the network as a legitimate user. Adding to that, this is hardware solution (MAC address), so in case the administrator requests changing the MAC addresses of all PCs for security reason; this will cost the company huge amount of money.

In contrast, the proposed project is a software solution based on certificates instead of MAC address. It uses two-factor authentications, which are username/password and certificates. This scheme is based on the IEEE 802.1x standard for port-based network access control. It is effective and does not suffer from previous mentioned problems.

1.4 Project objective:

This project covers the implementation of a two-factor authentication scheme over wireless network. The goal is to make the client and the machine authentications together, so only authorized client with authorized machine (desktop)

can access the internet. The client authentication involves assigning a username/password and the machine authentication requires the physical possession of the certificate, which is stored in each authorized machine. The project has the following objectives to be achieved:

1. Design of the two-factor authentication scheme based on IEEE 802.1x standard.
2. Implement the IEEE 802.1x authentication scheme.
3. Enhance the organization security and prevent attacks from outsiders.
4. Centralize the management through the use of Windows Active Directory.
5. Automate the wireless clients' laptop/desktop configuration with the least amount of user intervention.
6. Provide mutual authentication by authenticating both the server and the client

1.5 Project scope:

This project focuses on the authentication over wireless network. This is done by implementing the IEEE Std. 802.1x - 2004. IEEE 802.1x is also called a port-based network access control. The supplicant (client) logs indirectly through RADIUS (Authentication) server to the network. The network (internet) port is kept in unauthorized state until the RADIUS verifies the identity of the client (Figure 1.1(a)). Once it is verified the port changes to authorized state (Figure 1.1 (b)). The Figure below illustrates this.

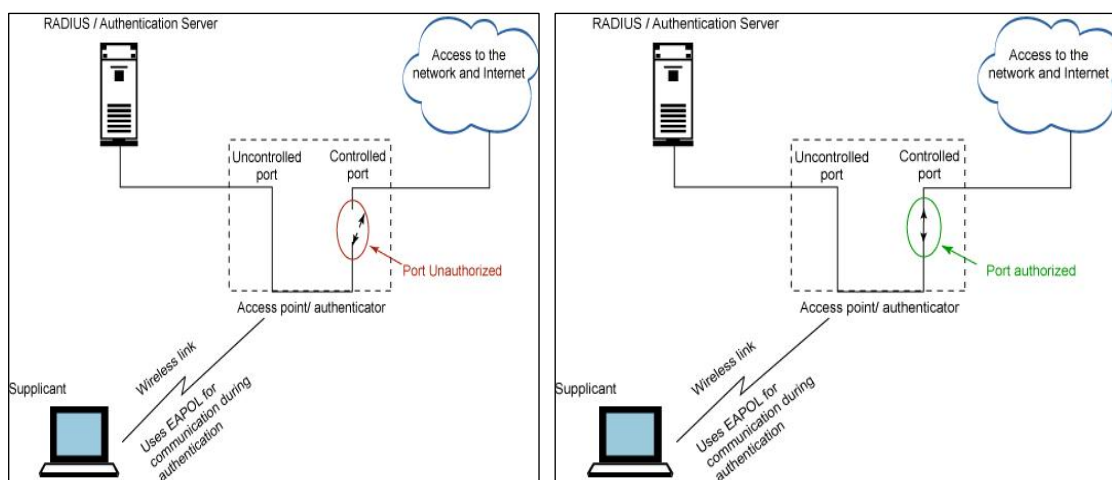


Figure 1.1: (a) unauthorized state port (b) authorized state port

In general, the project scope is an implementation of IEEE 802.1 x standard, as illustrated in the Figure 1.1. The project is lab-based; whose success could enhance the security inside a university campus. It is implemented by using one wireless Access Point (AP) and four computers. The four computers used are as follows:

- ❖ A Certificate Authority (CA) server that is used to generate and manage certificates for the users. To achieve the automated system objective, this server is equipped with the following:
 - Dynamic Host Configuration Protocol (DHCP) server.
 - Domain Name System (DNS) server.
 - Windows Active Directory
- ❖ Web and file server, Internet Information Services (IIS), which is used as a target network to test the authentication scheme.
- ❖ Authentication server, Internet Authentication Service (IAS), which is acting as a Remote Authentication Dial-In Service (RADIUS) server. This server is used to authenticate users before granting access to them.

- ❖ One Client Desktop/laptop is used for testing and evaluating the system.

LIST OF REFERENCES

- Ali, K. (2007). Selection of EAP authentication method for WLAN. *Int. J. Information and computer security*. 1(2): 210-233
- Allen, J., and Wilson J. (2002). Securing a wireless network. *Proceedings of the 30th annual ACM SIGUCCS conference on User services*, New York, NY, USA:ACM Press, 213-215
- Arbaugh, W., Shankar, N., WAN, J. (2002). Your 802.11 wireless network has no clothes. *IEEE wireless communication*. IEEE press, 9(6): 44-51. Last accessed at 26 March 2007, Available at <http://ieeexplore.ieee.org/iel5/7742/26001/01160080.pdf>
- Badra, M., Urien, P., Hajjeh, I. (2007). Flexible and Fast security solution for wireless LAN. *Passive and mobile computing*. 3(1): 1-14
- Bai, C. (2004). Enhancing network security via error-correcting codes. University of Louisiana at Lafayette: Ph. D thesis
- Barken, L., Bermel, E., Eder, J., Fanady, M., Mee, M., Palumbo, M. Koebrick, A. (2004). *Wireless Hacking – Projects for Wi-Fi Enthusiasts*. Rockland, MA02370: Syngress Publishing Inc.
- Boland, H., and Mousavi, H. (2004). Security Issues of IEEE 802.11b Wireless LAN. *Electrical and Computer Engineering, 2004. Canadian Conference on*. 2-5 May 2004. Niagara Falls, Canada: IEEE: 333-336 Vol. 1
- Burnside, M., Clarke, D., Mrills, T., Maywah, A., Devadas, S., Rivest, R. (2002). Proxy-based security protocols in networked mobile devices. *Proceedings of the 2002 ACM symposium on Applied computing SAC '02*, New York, NY, USA: ACM Press, 265-272
- Brawn, S., Koan, R., Caye, K. (2004). Staying secure in an insecure world: 802.1x secure wireless computer connectivity for students, faculty, and staff to the campus network. *Proceedings of the 32nd annual ACM SIGUCCS conference on User services*. Baltimore, MD, USA: ACM Press, 273-277.
- Chen, J., and Wang, Y. (2005). Extensible authentication protocol (EAP) and IEEE 802.1x: tutorial and empirical experience. *Communications Magazine, IEEE*. 43(12): S26-S32
- Cheswick, W., Bellovin, S., and Roubin, A. (2003). *Firwalls and Internet Security, Repelling the wily Hacker*. 2nd ed. Boston, USA: Addison Wesley.

- Danto, R., Clothier, G., and Atri A. (2007). EAP methods for wireless networks. *Computer Standards & Interfaces*. 29(3): 289-301
- Earl, A. (2006). *Wireless Security Handbook*. Boca Raton, New York: Auerbach Publications – Taylor and Francis Group
- Ennis, D. (2005). The wireless tightrope: an economical, secure, and user friendly approach for the wireless campus. *Proceedings of the 33rd annual ACM SIGUCCS conference on User services table of contents*. Monterey, CA, USA: 62 - 67
- George, O. (2007). Wireless LAN security guide. Last modified on 3 January 2005. Last accessed on 14 March 2007, Available at:
<http://www.lanarchitect.net/Articles/Wireless/SecurityRating/>
- Google (2007). Cracking WEP in 4min 27sec by kismac. Last accessed at 7 February 2007, Available at
<http://video.google.com/videoplay?docid=-1021256519470427962>
- Graham, D. (2003). It's All about Authentication, white paper published by SANS Institute, March 15, 2003. Last accessed 13 March 2007, http://www.sans.org/reading_room/whitepapers/authentication/?portal=bee2d1edce59d3e4422272070b7937dd
- He, C. (2005). Analysis of Security Protocol for Wireless Networks. Stanford University: Ph. D thesis
- Hernández, H. (2005). Security Enhancement for IEEE 802.11 wireless LANs. University Of Puerto Rico: Msc. Thesis
- Higby, C. and Bailey, M. (2004). Wireless Security Patch Management System. *Conference On Information Technology Education- Proceedings of the 5th conference on Information technology education*. New York, NY, USA. ACM Press: 165-168
- IEC – International Engineering Consortium (2007). EAP methods for 802.11 Wireless LAN security. Last accessed at 5 April 2007, Available at:
http://www.iec.org/online/tutorials/eap_methods/topic03.html
- IEEE -Institute of Electrical and Electronic Engineering (1990). *IEEE standard for local and metropolitan networks: overview and architecture*. New York, USA, IEEE STD 802-1990
- IEEE-Institute of Electrical and Electronic Engineering (2004). *IEEE standard for local and metropolitan networks: Port-Based network access control*. New

York, USA, IEEE STD 802.1x-2004 (Revision of IEEE STD 802.1x-2001)

Intel website (2007). Wireless security – 802.1x and EAP types. Last accessed at 1 April 2007, available at: <http://www.intel.com/support/wireless/wlan/sb/CS-008413.htm>

Intelligraphics (2007). Introduction to IEEE 802.11. Last accessed at 19 March 2007, available at: http://www.intelligraphics.com/articles/80211_article.html

Jones, D. (2004). Confidentiality and security of information. *Anaesthesia & intensive care medicine*, 5(12): 404-406

Jun, L. Fu, X., Hogrefe, D., Tan, J. (2007). Comparative studies on authentication and key exchange methods for 802.11 wireless LAN. *Computers and Security*. In Press, Corrected proof. Available online on 9 January 2007. Pages: 1-9

Kelati, A. (2001). Application of IEEE 802.1x in HyperLAN type 2. Chalmers University of Technology & Ericsson Enterprise: Msc. thesis

Khan, J., and Khawaja, A. (2003). *Building secure wireless networks with 802.11*. Indianapolis, Indiana: Wiley Publishing Inc.

KMJ communications (2007). Remote Authentication Dial-in Service- Remote Network Access Security in an open systems environment. Last accessed at 5 April 2007, Available at: <http://www.kmj.com/radius.html>

Liang, W. (2005). Design and analysis of authentication mechanisms in single- and multi-hop wireless networks. North Carolina State University: Ph. D Thesis

Microsoft IT showcase (2002). Empowering people through wireless networks. Last accessed at 7 February 2007, Available at <http://download.microsoft.com/download/0/6/7/06733aec-4941-4eac-b0be-7e716dd80d8d/SecureWirelessLAN.ppt>

Microsoft TechNet (2007a). Security administration. Last accessed at 5 March 2007, Available at <http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsecad.aspx>

Microsoft TechNet (2007b). PEAP with MS-CHAP V2 for secure password-based wireless access. Last accessed at 6 April 2007, Available at: <http://www.microsoft.com/technet/community/columns/cableguy/cg0702.mspx>

Miller, S. (2003). *WiFi Security*. New York, USA: McGraw-Hill companies

- Ouellet, E., Padjem, R., Pfund, A., Fuller, R., Blankenship, T. (2002). Building a CISCO wireless LAN. Rockland, MA02370: Syngress Publishing Inc.
- PC Magazine (2007). Definition of authorization. Last accessed at 22 March 2007, Available at http://www.pcmag.com/encyclopedia_term/0,2542,t=authorization&i=38202,00.asp
- Phifer, L. (2002). Understanding Wireless LAN vulnerabilities. *Business Communication Review*. September 2003. 26-32. Last accessed at 22 March 2007, Available at: <http://www.corecom.com/external/bcsmag/bcsmag-wlansec-sep02.pdf>
- Potter, B. (2003). Wireless authentication options for up and down the stack. *Network Security*. 2003(6): 4-5
- Ramakrishnan, K. (2006). Wireless Network Security using a low cost pseudo random number generator. State University of New York at Buffalo: Msc. thesis
- Regan Kevin (2003). Wireless LAN Security: Things you should know about WLAN security. *Network Security*. 2003(1): 7-9.
- SANS (2007). Definition of Network Security, Last accessed at 21 March 2007, Available at http://www.sans.org/network_security.php
- Schmidt, M. (2006). Deployment and analysis of a model for assessing perceived security threats and characteristics of innovating for wireless networks. Mississippi State University: Ph. D thesis
- Schneier B. (2007). A brief talk about security of linux with comparison to windows. Last accessed at 20 April 2007, Available at: http://www.schneier.com/blog/archives/2005/01/linux_security_1.html
- SURFnet website (2007). Authentication and authorization for WLAN using 802.1x. Last modified on 17 November 2003. Last accessed at 29 March 2007, Available at <https://www.surfnet.nl/innovatie/wlan/>
- Uskela, S. (2007). Security in Wireless Local Area Network. Last modified on Friday, 26 December 1997. Last accessed at 15 February 2007, Available at http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/wireless_lan.html
- UTM, (2007). A statistics about student and staff numbers in 2006. Last accessed at 28 March 2007, Available at <http://web.utm.my/today/index.php?option=content&task=view&id=318&Itemid=103>

- Wee, O. (2004). Wireless Network security: Design and considerations for an enterprise network. NAVAL Postgraduate School: Msc. Thesis
- Wohlmacher, P. (2000). Digital Certificates: A survey of Revocation Methods. *International Multimedia Conference-Proceedings of the 2000 ACM workshops on Multimedia*. New York, NY, USA. ACM Press: 111-114
- Wikipedia (2007a). Definition of authentication. Last accessed at 22 March 2007, Available at <http://en.wikipedia.org/wiki/Authentication>
- Wikipedia (2007b). Wired Equivalent Privacy (WEP). Last accessed at 27 March 2007, Available at: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
- Wikipedia (2007c). Definition of Dictionary attack. Last accessed at 5 April 2007, Available at: http://en.wikipedia.org/wiki/Dictionary_attack
- Wikipedia (2007d). Active Directory. Last accessed at 5 April 2007, Available at: http://en.wikipedia.org/wiki/Active_Directory
- Wirelessdefense.org (2007). Rouge Access Point: HOWTOs. Last accessed at 26 March 2007, Available at: <http://www.wirelessdefence.org/Contents/RougeAPHowtoMain.htm>
- Zahur, Y. (2004). Wireless Local Area Networks – Security & performance. The University of Houston Clear Lake: Msc. Thesis
- Zahur, Y., and Yang, A. (2004). Wireless LAN security and laboratory designs. *Journal of computing sciences in colleges*. 19(3): 44-60
- Zhiguo, W., Robert, H., Feng, B., Akkihebbal, L. (2007). Access control protocols with two-layer architecture for wireless networks. *Computer Networks*. 51(3): 655-670