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.

Certified by:

[Signature]

SIGNATURE

[New IC No. / Passport No.]

2006536

ASSOCIATE PROF. DR. ZAILANI MOHAMMED SIDEK

NAME OF SUPERVISOR

[Signature of Supervisor]

SIGNATURE OF SUPERVISOR

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

# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECLARATION</td>
<td>ii</td>
<td></td>
</tr>
<tr>
<td>DEDICATION</td>
<td>iii</td>
<td></td>
</tr>
<tr>
<td>ACKNOWLEDGMENT</td>
<td>iv</td>
<td></td>
</tr>
<tr>
<td>ABSTRACT</td>
<td>v</td>
<td></td>
</tr>
<tr>
<td>ABSTRAK</td>
<td>vi</td>
<td></td>
</tr>
<tr>
<td>TABLE OF CONTENTS</td>
<td>vii</td>
<td></td>
</tr>
<tr>
<td>LIST OF TABLES</td>
<td>xiii</td>
<td></td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xiv</td>
<td></td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>xvii</td>
<td></td>
</tr>
<tr>
<td>LIST OF APPENDICES</td>
<td>xix</td>
<td></td>
</tr>
</tbody>
</table>

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 scope  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
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
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
3 RESEARCH METHODOLOGY

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

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
5 SYSTEM IMPLEMENTATION AND TESTING

5.1 Introduction

5.2 CA Server Configuration

5.2.1 Infrastructure and Certificate Service Installation and configuration

5.2.1.1 Active Directory and DNS

5.2.1.2 Dynamic Host Configuration Protocol (DHCP)

5.2.1.3 Certificate Service Installation and configuration

5.2.2 Preparing the CA server for authentication

5.2.2.1 Create Wireless Group object

5.2.2.2 Create and configure certificate template

5.2.2.3 Configure the auto-enrollment and auto certificate request feature

5.3 RADIUS server configuration

5.4 The 3Com wireless Access Point configuration

5.5 Web Server (IIS) configuration

5.6 Users Tracking System Application (UTSA)

5.6.1 Client’s side Code

5.6.2 CA server’s code (UTSA)

5.7 Testing the system

5.7.1 Testing the authentication

5.7.2 Testing the UTSA

5.8 Summary

6 DISCUSSION, FUTURE WORKS AND CONCLUSION
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>
<thead>
<tr>
<th>TABLE NO.</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>comparison between different authentication mechanisms</td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>used in WLAN</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>comparison between EAP methods</td>
<td>64</td>
</tr>
<tr>
<td>3.1</td>
<td>The three desktop servers’ requirements</td>
<td>79</td>
</tr>
<tr>
<td>3.2</td>
<td>The client laptop/desktop machine requirements</td>
<td>79</td>
</tr>
<tr>
<td>3.3</td>
<td>Minimum Access Point Specifications</td>
<td>80</td>
</tr>
<tr>
<td>6.1</td>
<td>Comparison between UTM wireless authentication &amp; IEEE 802.1x</td>
<td>126</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>1.1</td>
<td>(a) unauthorized state port (b) authorized state port</td>
<td>7</td>
</tr>
<tr>
<td>2.2</td>
<td>802.11 wireless systems and The OSI model [Ouellet et al., 2002]</td>
<td>15</td>
</tr>
<tr>
<td>2.3</td>
<td>US College campuses with strategic plans for wireless deployment [Schmidt, (2006)]</td>
<td>17</td>
</tr>
<tr>
<td>2.4</td>
<td>Infrastructure Mode [Hernández Heidi, 2005]</td>
<td>18</td>
</tr>
<tr>
<td>2.5</td>
<td>Ad-hoc mode [Hernández Heidi, 2005]</td>
<td>19</td>
</tr>
<tr>
<td>2.6</td>
<td>Security incidents or attacks on Wireless LANs in 2002</td>
<td>20</td>
</tr>
<tr>
<td>2.7</td>
<td>Open System (Null) authentication [Barken et al., 2004]</td>
<td>25</td>
</tr>
<tr>
<td>2.8</td>
<td>Shared Key Authentication [Barken Lee et al., 2004]</td>
<td>26</td>
</tr>
<tr>
<td>2.9</td>
<td>VPN authentication over Wireless</td>
<td>31</td>
</tr>
<tr>
<td>2.10</td>
<td>Web-based authentication</td>
<td>32</td>
</tr>
<tr>
<td>2.11</td>
<td>wireless authentication representation in OSI model</td>
<td>40</td>
</tr>
<tr>
<td>2.12</td>
<td>The three entities in general architecture of an IEEE 802.1x system [Kelati, 2001]</td>
<td>41</td>
</tr>
<tr>
<td>2.13</td>
<td>unauthorized state</td>
<td>43</td>
</tr>
<tr>
<td>2.14</td>
<td>authorized state.</td>
<td>44</td>
</tr>
<tr>
<td>2.15</td>
<td>EAPOL Diagram</td>
<td>46</td>
</tr>
<tr>
<td>2.16</td>
<td>IEEE 802.1x basic protocol exchange</td>
<td>47</td>
</tr>
<tr>
<td>2.17</td>
<td>Man-in-the-middle attack</td>
<td>50</td>
</tr>
<tr>
<td>2.18</td>
<td>Session Hijacking Attack</td>
<td>52</td>
</tr>
<tr>
<td>2.19</td>
<td>EAP packet format [Earl Aaron, 2006]</td>
<td>54</td>
</tr>
<tr>
<td>2.20</td>
<td>EAP-MD5 process details [Earl Aaron, 2006]</td>
<td>57</td>
</tr>
<tr>
<td>Number</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>5.17</td>
<td>snapshot of the logon script running on the client’s machine</td>
<td>117</td>
</tr>
<tr>
<td>5.18</td>
<td>snapshot of the logoff script running on the client’s machine</td>
<td>118</td>
</tr>
<tr>
<td>5.19</td>
<td>snapshot of the User Tracking System Application (UTSA)</td>
<td>119</td>
</tr>
<tr>
<td>6.1</td>
<td>snapshot of the SMAC V2.0 tool</td>
<td>125</td>
</tr>
</tbody>
</table>
### LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAA</td>
<td>Authentication Authorization Accounting</td>
</tr>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>ANSI</td>
<td>American National Standards Institute</td>
</tr>
<tr>
<td>AP</td>
<td>Access Point</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CHAP</td>
<td>Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>CRC-32</td>
<td>Cyclic Redundancy Check-32</td>
</tr>
<tr>
<td>CSP</td>
<td>Cryptographic Service Provider</td>
</tr>
<tr>
<td>DC</td>
<td>Domain Controller</td>
</tr>
<tr>
<td>DHCP</td>
<td>Dynamic Host Configuration Protocol</td>
</tr>
<tr>
<td>DNS</td>
<td>Domain Name System</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPOL</td>
<td>Extensible Authentication Protocol over LAN</td>
</tr>
<tr>
<td>EAPOW</td>
<td>Extensible Authentication Protocol over Wireless</td>
</tr>
<tr>
<td>IAS</td>
<td>Internet Authentication Service</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronic Engineering</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IIS</td>
<td>Internet Information Services</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>LLC</td>
<td>Logical Link Control</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>MitM</td>
<td>Man-in-the-Middle</td>
</tr>
<tr>
<td>MSCHAP</td>
<td>Microsoft Challenge Handshake Authentication Protocol</td>
</tr>
<tr>
<td>NAS</td>
<td>Network Access Server</td>
</tr>
<tr>
<td>NDS</td>
<td>Novell’s NetWare Directory Service</td>
</tr>
<tr>
<td>OU</td>
<td>Organizational Unit</td>
</tr>
<tr>
<td>PAE</td>
<td>Port Access Entity</td>
</tr>
<tr>
<td>PAP</td>
<td>Password Authentication Protocol</td>
</tr>
<tr>
<td>PCT</td>
<td>Private Communication Technology</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>PHY</td>
<td>Physical</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PPP</td>
<td>Point-to-Point Protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-in User Service</td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher 4</td>
</tr>
<tr>
<td>RFC</td>
<td>Request for Comments</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>SAM</td>
<td>Security Account Manager</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Socket Layer</td>
</tr>
<tr>
<td>STD</td>
<td>Standard</td>
</tr>
<tr>
<td>TKIP</td>
<td>Temporal Key Integrity Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TTLS</td>
<td>Tunnel Transport Layer Security</td>
</tr>
<tr>
<td>UTM</td>
<td>Univresiti Teknologi Malaysia</td>
</tr>
<tr>
<td>UTSA</td>
<td>Users Tracking System Application</td>
</tr>
<tr>
<td>WEP</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WLAN</td>
<td>Wireless Local Area Network</td>
</tr>
<tr>
<td>WPA</td>
<td>Wi-Fi Protected Access</td>
</tr>
<tr>
<td>WPA PSK</td>
<td>Wi-Fi Protected Access Pre-Shared Key</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
# LIST OF APPENDICES

<table>
<thead>
<tr>
<th>APPENDIX</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Step-by-Step System Configuration</td>
<td>134</td>
</tr>
<tr>
<td>B</td>
<td>Users Tracking System Application (UTSA)</td>
<td>178</td>
</tr>
<tr>
<td>C</td>
<td>Testing the authentication system</td>
<td>190</td>
</tr>
</tbody>
</table>
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.
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


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


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


