AUTHENTICATION STUDY AND IMPLEMENTATION USING IPSEC AND IEEE 802.1X TECHNOLOGY

AHMED OMAR AL-AMODI

UNIVERSITI TEKNOLOGI MALAYSIA
AUTHENTICATION STUDY AND IMPLEMENTATION USING
IPSEC AND IEEE 802.1X TECHNOLOGY

AHMED OMAR AL-AMODI

This dissertation is submitted in partial fulfillment
of the requirements for the award of degree of
Masters of Computer Science (Information Security)

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

APRIL 2009
To my beloved parents, brothers and sisters
ACKNOWLEDGEMENT

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.

Assoc. Prof. 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 Elfadil, Haniza, Chan, Abdal Alem, Mysam, Hamed, Nema, Ala Aldeen and others for their support and encouragement. May ALLAH reward you all the relentless efforts to see through this academic pursuit.
ABSTRACT

Researches in Information Technology have been subjected to a tremendous speed-up in recent years mainly due to the affordability of the technology and consequently, to a strongly increased interest of users. In addition, the security systems which imply networks have increased rapidly. Currently, many organizations provide extensive network services to their staff. This poses a problem of securing access to the organization networks. Therefore, authentication has become an inevitable reality in the design of such systems. The research sought for the best authentication mechanism suitable for organizations generally, and to university campuses, particularly. The result is an authentication scheme based on IPSec and IEEE 802.1x technology. The scheme provides secure access to users engaged in the network connection. It implements a two-factor authentication. The first factor is the network policy combination which the user provides prior logging onto the system. The second factor is the 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 technology. The result of the implemented system is a highly secured scheme that provides both user and computer (machine) authentication. Only legitimate users with legitimate machines (computers) can access the organization network system in an authorized way.
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>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 APPENDICES</td>
<td>xvi</td>
<td></td>
</tr>
</tbody>
</table>

1 OVERVIEW  
1.1 Introduction  
1.2 Background problem  
1.3 Problem statement  
1.4 Project objective  
1.5 Project scope  
1.6 Importance of the Study  
1.7 Summary  

2 LITERATURE REVIEW  
2.1 Introduction  
2.2 Computer network  
2.3 Network topology  
2.3.1 Bus topology  
2.3.2 Ring topology  
2.3.3 Star topology
2.3.4 Mesh topology
2.3.5 Consideration when choosing topology

2.4 Network security
2.4.1 Overview of network security
2.4.2 Overview of OSI Technology

2.5 The Five layers of security model
2.5.1 Authentication
2.5.2 Authorization
2.5.3 Encryption
2.5.4 Integrity
2.5.5 Audit

2.6 General security threats and attacks on LANs
2.6.1 Passive attacks
2.6.2 Active attacks
2.6.3 Man-in-the-middle attack
2.6.4 Jamming attack

2.7 Authentication in network
2.7.1 Authentication elements

2.8 Network access control
2.8.1 Types of network access control
2.8.1.1 Discretionary access control (DAC)
2.8.1.2 Mandatory access control (MAC)
2.8.1.3 Role-based access control (RObAC)
2.8.1.4 Rule-based access control (RUbAC)
2.8.1.5 Quandary of network access control
2.8.1.6 Security issue in network access control

2.9 Planning network access controls

2.10 IEEE 802.1x technology
2.10.1 Elements of 802.1X
2.10.2 Supplicant
2.10.3 Pass-through authenticator
2.10.4 Authentication server
2.10.5 Controlled and uncontrolled ports 39
2.10.6 Security Provided by IEEE 802.1x 39
2.10.7 Advantages of using IEEE 802.1x 40
2.10.8 Limitations and vulnerabilities on using iee 802.1x 42
2.10.9 The absence of mutual authentication 42
2.10.10 Session hijacking 44
2.11 Extensible authentication protocol (EAP) 45
  2.11.1 General concepts of extensible authentication 45
    protocol (EAP)
  2.11.2 EAP-MD5 47
  2.11.3 EAP-TLS 49
  2.11.4 EAP-TTLS 51
  2.11.5 EAP-PEAP 53
  2.11.6 Comparison between previous four EAP methods 54
2.12 IPsec technology 57
  2.12.1 IPsec security properties 57
  2.12.2 How IPsec protects IP traffic 59
  2.12.3 Authentication header (AH) 60
  2.12.4 Encapsulating security payload (ESP) 60
  2.12.5 Security provided by IPsec 62
  2.12.6 Some limitation of the IPsec with network quarantine 63
2.13 Comparing 802.1x for wired network with IPsec 63
  2.13.1 Compression summary 66
2.14 Network access quarantine 67
  2.14.1 Benefit of network quarantine 68
  2.14.2 How network access quarantine works 68
  2.14.3 Quarantine Mode 69
  2.14.4 Components of Network access quarantine control 70
  2.14.5 Important of network access quarantine control 71
  2.14.6 Network Quarantined Resources 72
2.14.6.1 DNS

2.14.6.1.1 Benefits of adding a third-party DNS server

2.14.6.2 DHCP

2.15 Types & Comparison between different authentication mechanisms used

2.15.1 Null authentication

2.15.2 Virtual Private Network

2.15.3 Media Access control (MAC) based authentication

2.15.4 Wired equivalent privacy (WEP)

2.16 Network access quarantine implementation method

2.16.1 Network quarantine with VPN

2.16.2 Network quarantine with IPsec

2.16.4 Network quarantine with DHCB

2.16.5 Network quarantine with IEEE802.1x

2.16.5.1 Benefit of Network quarantine with IEEE802.1x

2.17 Best authentication choice based on organizations types

2.17.1 Home network security

2.17.2 Small business security

2.17.3 Medium to large enterprise security

2.17.3 Military grade maximum level security

2.18 Summary

3 RESEARCH METHODOLOGY

3.1 Introduction

3.2 Project framework

3.3 Observations and problem formulation

3.4 Literature review

3.5 Requirement specification

3.5.1 Hardware requirement specification

3.5.2 Software requirement specification

3.6 Scheme design

3.7 System implementation

3.8 Testing the system
3.9 Report writing 96
3.10 Summary 97

4 System Design 98
4.1 Introduction 98
4.2 Selected operating system 98
4.3 Overall system design 99
4.4 DC server 100
4.4.1 Infrastructure services 101
4.4.1.1 Active directory (AD) 102
4.4.1.2 Domain name system (DNS) 103
4.4.1.3 Dynamic host configuration protocol (DHCP) 103
4.5 NPS server 103
4.6 The entire network 105
5.7 The overall authentication process of the designed system 105
4.8 Summary 106

5 System Implementation and Testing 108
5.1 Introduction 108
5.2 Infrastructure server 108
5.2.1 Infrastructure and service installation and configuration 109
5.2.1.1 Active directory & DNS (DC server) 109
5.2.1.2 Certification authority (DC server) 110
5.2.1.3 IPSec 111
5.2.1.4 Dynamic host configuration protocol (DHCP) 112
5.2.1.5 Network policy server 113
5.2.2 IEEE802.1X technology 114
5.3 Testing the system 115
5.3.1 Testing the authentication 116
5.4 Summary 117

6 Discussion Future Work and Conclusion 118
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 Introduction</td>
<td>118</td>
</tr>
<tr>
<td>6.2 Discussion</td>
<td>118</td>
</tr>
<tr>
<td>6.2.1 Justification of choosing windows as an operating system in this project</td>
<td>119</td>
</tr>
<tr>
<td>6.2.2 Justification of the authentication level in this project</td>
<td>120</td>
</tr>
<tr>
<td>6.2.3 Features of the implemented authentication in this project</td>
<td>121</td>
</tr>
<tr>
<td>6.2.4 Comparing UTM authentication with proposed project solution</td>
<td>122</td>
</tr>
<tr>
<td>6.3 Future works</td>
<td>123</td>
</tr>
<tr>
<td>6.4 Conclusion</td>
<td>124</td>
</tr>
<tr>
<td>Reference</td>
<td>125</td>
</tr>
<tr>
<td>Appendix</td>
<td>Xvi</td>
</tr>
</tbody>
</table>
# 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 EAP methods</td>
<td>55</td>
</tr>
<tr>
<td>2.2</td>
<td>Summary between 802.1X and IPsec</td>
<td>63</td>
</tr>
<tr>
<td>2.3</td>
<td>Compare between different Network quarantine implementation method</td>
<td>64</td>
</tr>
<tr>
<td>2.4</td>
<td>Comparison between different authentication mechanisms</td>
<td>83</td>
</tr>
<tr>
<td>3.1</td>
<td>The servers’ requirements</td>
<td>92</td>
</tr>
<tr>
<td>3.2</td>
<td>The client desktop/laptop minimum requirement</td>
<td>92</td>
</tr>
<tr>
<td>6.1</td>
<td>Comparisons between UTM authentication &amp; network quarantine using IEEE802.1x and IPsec</td>
<td>123</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>Figure 1.1</td>
<td>Machine is not accessing the network because it’s not authenticate &amp; validate from the server</td>
<td>2</td>
</tr>
<tr>
<td>Figure 1.2</td>
<td>PC0 only can access the network if the machine fulfills the security Requirement</td>
<td>5</td>
</tr>
<tr>
<td>Figure 1.3</td>
<td>(a) Unauthorized state port  (b) Authorized state port</td>
<td>6</td>
</tr>
<tr>
<td>Figure 2.1</td>
<td>Bus topology</td>
<td>10</td>
</tr>
<tr>
<td>Figure 2.2</td>
<td>Ring topology</td>
<td>11</td>
</tr>
<tr>
<td>Figure 2.3</td>
<td>Star topology</td>
<td>12</td>
</tr>
<tr>
<td>Figure 2.4</td>
<td>Mesh topology</td>
<td>13</td>
</tr>
<tr>
<td>Figure 2.5</td>
<td>802.11 Network and The OSI model</td>
<td>16</td>
</tr>
<tr>
<td>Figure 2.6</td>
<td>Security Pyramid</td>
<td>20</td>
</tr>
<tr>
<td>Figure 2.7</td>
<td>Security incidents or attacks on network in 2002</td>
<td>22</td>
</tr>
<tr>
<td>Figure 2.8</td>
<td>Discretionary access control</td>
<td>29</td>
</tr>
<tr>
<td>Figure 2.9</td>
<td>Mandatory access control</td>
<td>30</td>
</tr>
<tr>
<td>Figure 2.10</td>
<td>Role-based access control</td>
<td>31</td>
</tr>
<tr>
<td>Figure 2.11</td>
<td>Rule-based access control</td>
<td>32</td>
</tr>
<tr>
<td>Figure 2.12</td>
<td>Shows these components for a wired network</td>
<td>36</td>
</tr>
<tr>
<td>Figure 2.12.1</td>
<td>Shows the interaction between supplicant and server</td>
<td>37</td>
</tr>
<tr>
<td>Figure 2.13</td>
<td>Shows the different types of ports</td>
<td>39</td>
</tr>
<tr>
<td>Figure 2.14</td>
<td>Man-in-the-middle attack</td>
<td>43</td>
</tr>
<tr>
<td>Figure 2.15</td>
<td>Session Hijacking Attack</td>
<td>44</td>
</tr>
<tr>
<td>Figure 2.16</td>
<td>EAP packet format</td>
<td>46</td>
</tr>
<tr>
<td>Figure 2.17</td>
<td>EAP-MD5 process details</td>
<td>49</td>
</tr>
<tr>
<td>Figure 2.18</td>
<td>EAP-TLS process details</td>
<td>51</td>
</tr>
<tr>
<td>Figure 2.19</td>
<td>EAP-TTLS process detail</td>
<td>52</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Figure 2.20</td>
<td>PEAP process detail</td>
<td>54</td>
</tr>
<tr>
<td>Figure 2.21</td>
<td>An IP packet without any IPsec protection</td>
<td>59</td>
</tr>
<tr>
<td>Figure 2.22</td>
<td>An IP packet without any IPsec protection</td>
<td>60</td>
</tr>
<tr>
<td>Figure 2.23</td>
<td>An IP packet with ESP and encryption protection</td>
<td>61</td>
</tr>
<tr>
<td>Figure 2.24</td>
<td>An IP packet with ESP and no encryption protection</td>
<td>61</td>
</tr>
<tr>
<td>Figure 2.25</td>
<td>Components of windows access for network access</td>
<td>70</td>
</tr>
<tr>
<td>Figure 2.26</td>
<td>VPN authentication</td>
<td>76</td>
</tr>
<tr>
<td>Figure 2.27</td>
<td>Shows virtual private network</td>
<td>80</td>
</tr>
<tr>
<td>Figure 2.28</td>
<td>Network quarantine with IEEE802.1x</td>
<td>82</td>
</tr>
<tr>
<td>Figure 3.1</td>
<td>Project framework</td>
<td>89</td>
</tr>
<tr>
<td>Figure 3.2</td>
<td>System architecture</td>
<td>94</td>
</tr>
<tr>
<td>Figure 4.1</td>
<td>Overall system implementation plan</td>
<td>99</td>
</tr>
<tr>
<td>Figure 4.2</td>
<td>Overall system design</td>
<td>100</td>
</tr>
<tr>
<td>Figure 4.3</td>
<td>DC server</td>
<td>101</td>
</tr>
<tr>
<td>Figure 4.4</td>
<td>The project domain namespace</td>
<td>103</td>
</tr>
<tr>
<td>Figure 4.5</td>
<td>NPS server</td>
<td>104</td>
</tr>
<tr>
<td>Figure 4.6</td>
<td>The sequence of the authentication process</td>
<td>105</td>
</tr>
<tr>
<td>Figure 5.1</td>
<td>Active directory users and computers</td>
<td>110</td>
</tr>
<tr>
<td>Figure 5.2</td>
<td>Shows the Certificate Authority</td>
<td>111</td>
</tr>
<tr>
<td>Figure 5.3</td>
<td>Shows the DHCP</td>
<td>112</td>
</tr>
<tr>
<td>Figure 5.4</td>
<td>Network policy server set up</td>
<td>113</td>
</tr>
<tr>
<td>Figure 5.6</td>
<td>Switch software</td>
<td>114</td>
</tr>
<tr>
<td>Figure 5.7</td>
<td>Show the policy you can set to your network</td>
<td>115</td>
</tr>
<tr>
<td>Figure 5.8</td>
<td>Show’s the client is not comply with network policy</td>
<td>116</td>
</tr>
<tr>
<td>Figure 5.9</td>
<td>Client comply with policy &amp; connects to the network</td>
<td>117</td>
</tr>
<tr>
<td>Figure 6.1</td>
<td>OSI layer</td>
<td>121</td>
</tr>
<tr>
<td>Figure 6.2</td>
<td>Snapshot of the SMAC V2.0 tool</td>
<td>122</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 implementation</td>
<td>132</td>
</tr>
</tbody>
</table>
CHAPTER 1

OVERVIEW

1.1 Introduction

Nowadays communication is very important. It leads to exchange information between people, organization and worlds. In fact most organization they use computer in order to communicate. However most of this computer is connected to each other and to the internet, as a result it can communicate with rest of the world. That communication attracts a lot of group to develop malicious program or unwanted software to harm computer network. And that will lead to communication & network failure in the organization, which it will cost the organization time, money and lack of availability, integrity & confidentiality of the network system.

Basically authentication & Network Access Control (NAC) come as security solution for network administrator fundamental proposal behind NAC is that when a user dials into a network, the server will validate & authenticate the user's machine to make sure that it’s authenticate as the other computers on the same network. If the machine successfully authenticated and validated, then the user is granted access to the rest of the network. If the machine's not authenticated or validate then, then the machine is not accessing until the user it authenticate & validate. Figure 1.1 below it show example of the authentication & validation.
Figure 1.1: Machine is not accessing the network because it’s not authenticate & validate from the server

1.2 Background Problem

Most users are authenticated and allowed access to network only on the basis of their identity. They can prove that they are who they say they are, and that's good enough for a lot of deployments. But problematically, no effort is made to verify that their hardware and software on their machines meets a certain baseline requirement to access the network. For example a normal user access a network by authenticate himself but inside his machine unwanted software application installed or Trojan infection, that will produce a lot of problem to the network and other machines.

Most administrators work hard to make sure that software on workstations is kept up to date. Simply it’s very difficult to have a secure network unless workstations are secure. Keeping workstations secure means keeping the operating system and
applications up to date with the latest patches and loading the latest definitions for anti-virus and anti-spyware programs.

As hard as it is keeping workstations on network up to date, it's practically impossible to ensure that remote workstations or large number of machine such as laptops and home computers connecting via virtual private network (VPN) are up to date. For example typical home machine has no virus protection and is infected with about 800 different types of spyware and other Trojans. Can you imagine if this machine access to the network. In fact if a network have large number of computers, and one machine been infected it will be very difficult for the network administrator to check every machine physically; the successful of find the infected machine will be very low, because of the large computers number. And if the administrator find the machine, by the time been the network is already infected with the Trojan and viruses.

The basic idea in controlling large network is to access control the network. Network access control (NAC) is a computer networking design and set of protocols used to define how to secure the network from infected machine. NAC might integrate the automatic remediation process as in fixing the infected machine before allowing access the into the network systems, allowing the network infrastructure such as routers, switches and firewalls to work together with back office servers and end user computing equipment to ensure the information system is operating securely before interoperability is allowed.

Network access control aims to do exactly what the name implies. Control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.
1.3 Problem Statement

Most of the time networks administrators have difficulty of examine the machine in the network, especially in local area network (LAN). Indeed nowadays with all this groups and people who develop different malicious software and program that harm computers & networks is very difficult to validate and examine each machine. And those arguments produce question need to consider by the organization:

- How the administrator going to manage and secure the network?

1.4 Project Objective

This project covers the implementation of a network quarantine authentication scheme with IEEE802.1x over local area network. The goal is to make the client and the machine authentications together, so only authorized client with authorized machine (desktop) can access the network. The client authentication involves a set of policy 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. Study the authentication methods.
2. Recommend implementation authentication scheme
3. Implement the recommend authentication scheme.
4. To achieve centralized network management.
5. Provide mutual authentication by authenticate the client.
In easy way when a user dials into network, a server will authenticate & validate the user's PC to make sure that only validate user enter the network. If the machine passes the test, then the user is granted access to the rest of the network. If the machine's security isn't quite up to the network standard, then the machine is not accessing until the user repair the machine & installs the necessary matter. Figure 1.2 below show that a client been rejected from access local area network because he didn’t fulfill the security requirement.

**Figure 1.2:** PC0 only can access the network if the machine fulfills the security requirement

### 1.5 Project Scope

This project is lab based focuses on authentication & access control in local area network (LAN) in the same department based on examines the client or the user. That’s done by after study & implementing the security mechanism needed. Mostly network
This project will not cover the wide area network (WAN), metropolitan area network (MAN) and wireless network.

This project focuses on the authentication over LAN 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 3(a)). Once it is verified the port changes to authorized state (Figure 1.3 (b)). The Figure below illustrates this.

![Figure 1.3: (a) unauthorized state port (b) authorized state port](image)

### 1.6 Importance of This Study

This study will help the network administrator to secure the network by authenticate and authorized the user, if the user want access the network. In fact the study will help to discuss network quarantine.

This study concerned for Network and system administrators who want to enforce system health requirements for client computers connecting to the networks such as:
• Ensure the health of desktop computers on the local area network (LAN) or any user want access the network.
• Determine the health and restrict access of laptops brought to an organization by visitors and partner.

This study is very important for organization that want secure and ensure that the network based on examine the user are healthy with no trouble or unwanted application.

1.7 Summary

The purpose of this overview is a plan to secure local area network (LAN) by using network quarantine method. Discuss in the introduction the definition of network quarantine. In fact it shows in the problem statement how it’s difficult for the network administrator to secure and manage the network. This project set an objective to achieve and scope, one of the objectives is to implement network quarantine method in LAN.
Referencing


Microsoft Corporation Published: March 2003 Updated: October 2004, 2003


Available at: http://en.wikipedia.org/wiki/Dictionary_attack


