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

Penyelidikan dalam bidang teknologi maklumat semakin pesat yang mana berpunca dari harga kos yang semakin rendah terhadap barangan elektronik yang sekaligus merancakkan lagi bilangan penguna. Di samping itu, bidang system dan rangkaian maklumat yang menerajui tahap keselamatan yang lebih efisen juga semakin mendapat sambutan dari pengguna. Pada masakini, kebanyakkan organisasi memberikan kemudahan system rangkaian maklumat yang efisen kepada staf mereka. Ini, kemungkinan akan menyebabkan masalah keselamatan di dalam rangkaian maklumat berkenaan. Oleh yang demikian, mekanisme untuk memastikan keselamatan rangkaian maklumat ini perlu di praktikkan. Projek ini memberi pandangan terhadap mekanisma alternatif yang terbaik bagi menjaga keselamatan rangkaian maklumat di organisasi dan kampus university dengan lebih terperincinya. Keputusan analisasi projek ini adalah berdasarkan skema IPSec dan IEEE 802.1x teknologi. Skema ini memberi kadar keselamatan yang tinggi kepada pengunanya. Ia menggunakan factor-dua authentikasi. Faktor pertama merujuk kepada polisi system rangkaian maklumat yang merujuk kepada login kali pertama pada sistem. Faktor yang kedua merujuk kepada rekod yang disimpan secara local di dalam komputer pengguna. Mekanisma ini adalah berdasarkan EAP-TLS, di mana cara autentikasinya adalah berdasarkan teknologi IEEE 802.1x. Keputusan sistem yang digunakan mempunyai kadar keselamatan yang tinggi pada penggunanya dan komputer yang digunakan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

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.

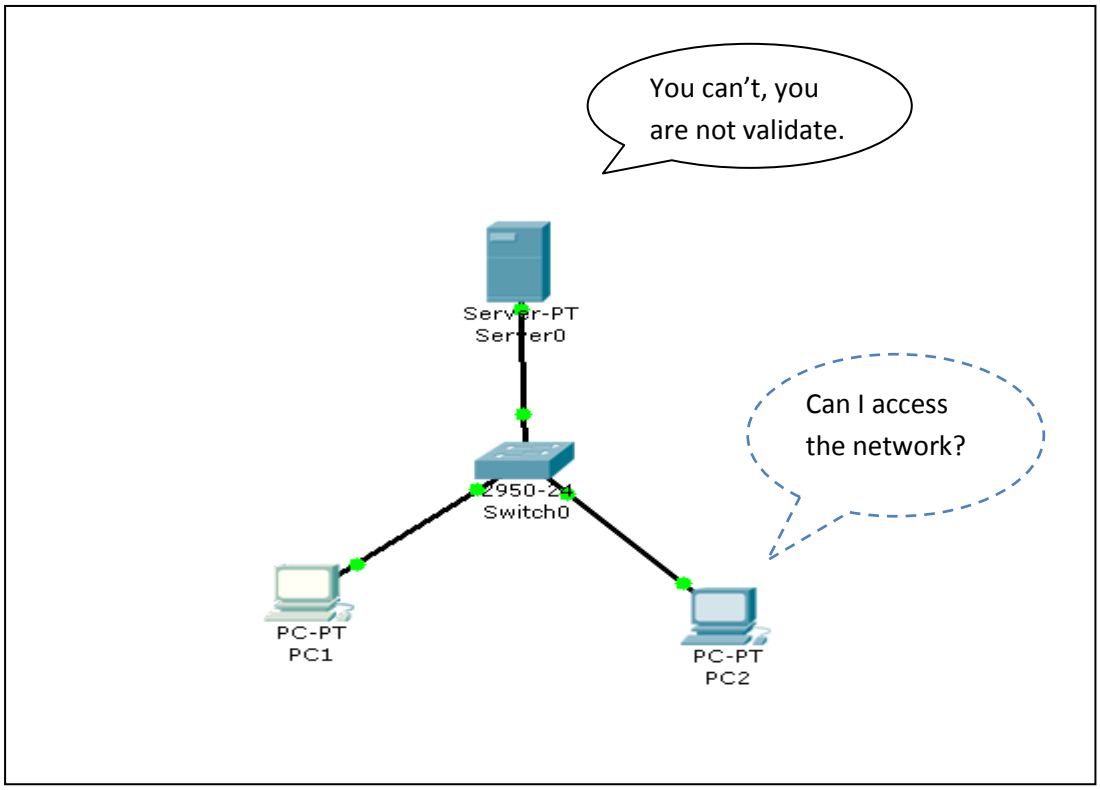

Figure 1.1: Machine is not accessing the network because it's not authenticate & validate from the server

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.

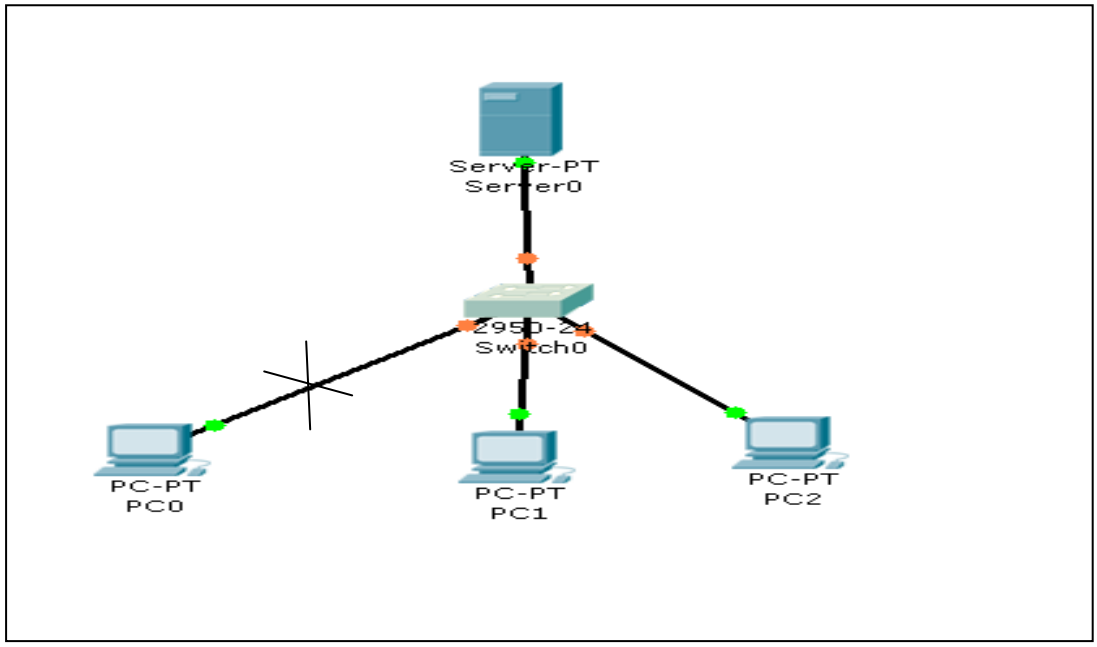

Figure 1.2: PC0 only can access the network if the machine fulfills the security requirement

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.

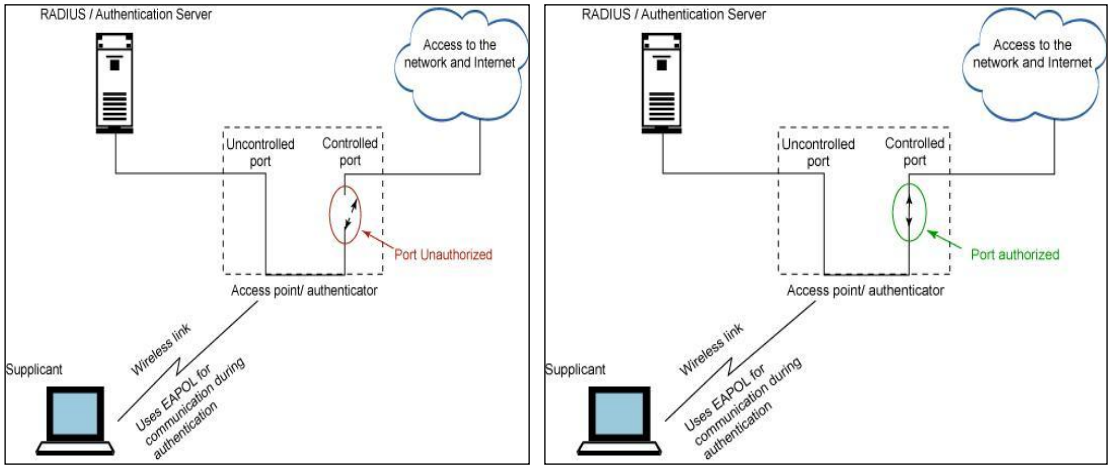

Figure 1.3: (a) unauthorized state port (b) authorized state port

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

Roberto Bell 2007, Remote Authentication Dial In User Service, Retrive 10 October 2008, from http://www.articledashboard.com/Article/Define-Radius-Server/443735

RADIUS 2008, retrieve 20 September 2008, from http://www.webopedia.com/TERM/R/RADIUS.html

Network Access Control Learning Guide 01 Jun 2006, retrieve October 4 2008, from http://searchsecurity.techtarget.com/generic/0,295582,sid14_gci1188421,00.html

Brien M. Posey Aug 11, 2004, *Windows Network Access Protection* (NAP) simplifies Quarantine Mode, retrieve 19 October 2008, from http://articles.techrepublic.com.com/5100-10878_11-5298997.html

Deb Shinder Published: May 26, 2004 Updated: Apr 06, 2005, *Authentication, Access Control & Encryption* , retirive October 3 2008, from http://www.windowsecurity.com/articles/Server-2003-Network-Access-Quarantine-Control-Security.html

Tony Bailey Published: November 4, 2005, *Virtual Private Network Quarantine*, retrieve October 12 2008, from http://technet.microsoft.com/en-us/library/cc512645.aspx

By Richard Langston, *Network Access Control Technologies*, retrieve October 10,2008 from http://www.bizforum.org/whitepapers/sygate-4.htm

Laura Taylor 11/10/2003, *access control*, Retrieved October 15, 2008, from http://www.intranetjournal.com/articles/200311/ij_11_10_03a.html
.

Roger Needham, Access control 2008, Retrieve 3 October 2008, from http://www.cl.cam.ac.uk/~rja14/Papers/SE-04.pdf

Ralph Droms, November 22, 2003, *Dynamic Host Configuration*, retrieve 8 October 2008, from http://www.dhcp.org/

Marshall Brain 2008, *How Domain Name Servers Work*, retrieve 27 October 2008, from http://computer.howstuffworks.com/dns1.htm

Internet Authentication Service 24 March 2008, retrieves 20 September 2008, from http://en.wikipedia.org/wiki/Internet_Authentication_Service

Jonathan Hassell 2004-08-04, *Deploying Network Access Quarantine Control*, retrieve 6 October 2008, From http://www.securityfocus.com/infocus/1794

Jeff felinge July 2006, *network quarantine & IPsec*, retrieve October 2 2008, from http://windowsitpro.com/article/articleid/50253/market-watch-network-quarantine.html

Mike Fratto July 17,2007, *Network Computing*, Retrieved October 1, 2008.from http://en.wikipedia.org/wiki/Network_Access_Control

By Joern Wettern June 2005, Secure Network Access Control, retrieve 5 October 2008, from http://mcpmag.com/columns/article.asp?EditorialsID=987

Paul Rubens November 10, 2006, *All About Network Access Controls*, retrieve 9 October 2008, From http://webopedia.com/DidYouKnow/Computer_Science/2006/network_access_control.asp

Horizan data system 2008, Retrieved October, 2008, from http://www.horizondatasys.com/206483.ihtml

Computer network by Andrew S. Tanenbaum, 2003, retrieve 17 October 2008, from http://books.google.com.my/books?id=Pd-z64SJRBAC&dq=computer+network&pg=PP1&ots=RBOMLvY2eF&sig=PVZokW3AmO_9X0tqw4BBrJfrAww&hl=en&sa=X&oi=book_result&resnum=1&ct=result

The business of authentication 2006, retrieve 6 October 2008, from) http://www.authenticationworld.com/

Coordination Center 2006, Home Network Security, retrieve 6 October 2008, from http://www.cert.org/tech_tips/home_networks.html

Privacy Assurance and Systems Security Council (PASS Council) Kirk Bailey, UW Chief Information Security Officer, Chair 2006, *Minimum Data Security Standards*, Retrieve 29 September 2008, from

http://www.washington.edu/president/tacs/utac/meetings/2006-07/materials/01.09.min.data.security.standards.pdf

Computer and Network Usage Policy December 15, 2005. Retrieve 10 October 2008, from http://adminguide.stanford.edu/62.pdf

Bradley Mitchell, *What Are the Advantages and Benefits of a VPN*?, retrieve 10 September 2008, from http://compnetworking.about.com/od/vpn/f/vpn_benefits.htm

Network Access Quarantine Control in Windows Published: March 24, 2003 Updated: December 06, 2004, retrieve 16 september 2008 , from http://technet.microsoft.com/en-us/library/bb726973.aspx

Brien M. Posey Jun 23, 2005, *Control access to your network with Network Access Quarantine Control*, retrieve 14 September 2008, from http://articles.techrepublic.com.com/5100-22_11-5746439.html

Raleigh Stout, *What quarantine of computer files is?*, retrieve 17 September 2008, from http://www.helium.com/items/667557-what-quarantine-of-computer-files-is

Deb Shinder Jan 05, 2007, *NAP offers a network access control solution for SMBs*, retrieve 10 September 2008, from http://articles.techrepublic.com.com/5100-10878_11-6147167.html

Rick Vanover Nov 28, 2007, *Introducing Network Access Protection for Windows*, retrieve 18 September 2008, from http://articles.techrepublic.com.com/2415-1035_11-177853.html

Rob Whiteley 2008, *Success Takes Careful Consideration*, retrieve 7 September 2008 , from http://www.forrester.com/Research/Document/Excerpt/0,7211,47182,00.html

Nathan Einwechter 2002-06-19, Implementing Networks Taps with Network Intrusion Detection Systems, retrieve 8 September 2008, from http://www.securityfocus.com/infocus/1594

Robert Whiteley with Laura Koetzle, Benjamin Gray June 28, 2005, *How To Determine The Best Architecture For Securing LAN Access*, retrieve 10 September 2008 , from http://www.forrester.com/Research/Document/Excerpt/0,7211,36275,00.html

Microsoft TechNet 2007. Security administration. Last accessed at 5 March 2007, Available at http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsecad.mspx

Microsoft Corporation Published: March 2003 Updated: October 2004, 2003 *Network Access Quarantine Control*, retrieve 12 September 2008, from http://technet.microsoft.com/en-us/network/bb545879.aspx

Schneier B. (2007). *A 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

Bai, C. (2004). Enhancing network security via error-correcting codes. University of Louisiana at Lafayette: Ph. D thesis

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

SANS (2007). Definition of Network Security, Last accessed at 21 March 2007, Available at http://www.sans.org/network_security.php

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

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

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

Schmidt, M. (2006). Deployement and analysis of a model for assessing perceived security threats and characteristics of innovating for wireless networks. Mississippi State University: Ph. D thesis

Wikipedia (2007a). Definition of authentication. Last accessed at 22 March 2007, Available at http://en.wikipedia.org/wiki/Authentication

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

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

Phifer, L. (2002). *Understanding network vulnerabilities*. Business Communication Review. September 2003. 26-32. Last accessed at 22 March 2007, Available at: http://www.corecom.com/external/bcrmag/bcrmag-wlansec-sep02.pdf

Hernández, H. (2005). Security *Enhancement for IEEE 802.11 network LANs*. University Of Puerto Rico: Msc. Thesis

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

Wirelessdefense.org (2007). Rouge Access Point: HOWTOs. Last accessed at 26 March 2007, Available at: http://www.wirelessdefence.org/Contents/RougeAPHowtoMain.htm

Barken, L., Bermel, E., Eder, J., Fanady, M., Mee, M., Palumbo, M. Koebrick, A. (2004). Hacking – Projects for Wi-Fi Enthusiasts. Rockland, MA02370: Syngress Publishing Inc.

Earl, A. (2006). Security Handbook. Boca Raton, New York: Auerbach Publications – Taylor and Francis Group

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)

Brawn, S., Koan, R., Caye, K. (2004). *Staying secure in an insecure world: 802.1x secure computer network 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

Zahur, Y. (2004). Local Area Networks – Security & performance. The University of Houston Clear Lake: Msc. Thesis

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

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

Ali, K. (2007*). Selection of EAP authentication method for network.* Int. J. Information and computer security. 1(2): 210-233

Wikipedia (2007c). Definition of Dictionary attack. Last accessed at 5 April 2007,

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

IEC – International Engineering Consortium (2007). EAP methods for 802.11 network security. Last accessed at 5 April 2007, Available at: http://www.iec.org/online/tutorials/eap_methods/topic03.html

Ennis, D. (2005). network tightrope: an economical, secure, and user friendly approach for the campus. Proceedings of the 33rd annual ACM SIGUCCS conference on User services table of contents. Monterey, CA, USA: 62 - 67

Microsoft TechNet (2007b). PEAP with MS-CHAP V2 for secure password-based network access. Last accessed at 6 April 2007, Available at:

http://www.microsoft.com/technet/community/columns/cableguy/cg0702.mspx

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

Danto, R., Clothier, G., and Atri A. (2007). EAP methods for wireless networks. Computer Standards & Interfaces. 29(3): 289-301

He, C. (2005). *Analysis of Security Protocol for Wireless Networks*. Stanford University: Ph. D thesis

Steve. (2005-08-24). An Illustrated Guide to IPsec last access 20 November 2008, available at: http://unixwiz.net/techtips/iguide-ipsec.html
Microsoft (2005-Decmber-07) update (2006 –April-16), Internet Protocol Security and Packet Filtering available at : http://technet.microsoft.com/en-us/library/bb727017.aspx

Ausif mahmood (2006-April-09), Securing Networks Using IPSEC VPN and 802.1x, available at:

http://www.bridgeport.edu/sed/projects/cs597/Fall_2002/nasirnizami/nasirnizami.pdf

András Salamon (2006-jan-23), DNS Resources Directory, available at: http://www.dns.net/dnsrd/

D. J. Bernstein (2007), *Costs and benefits of third-party DNS service available* at: http://cr.yp.to/djbdns/third-party.html

Barken, L., Bermel, E., Eder, J., Fanady, M., Mee, M., Palumbo, M. Koebrick, A. (2004). Network Hacking – Projects for Wi-Fi Enthusiasts. Rockland, MA02370: Syngress Publishing Inc.

Regan Kevin (2003). Network Security: Things you should know about security. Network Security. 2003(1): 7-9.

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

Rick Vanover (April 21st, 2008), network administrator available at

http://static.ppurl.com/addison_wesley/p/protect_your_windows_network_from_perimeter_to_data/preview/0321336437/ch10lev1sec5.html

Pietro Nicoletti (2008-01-20), Authentication and Security:IEEE 802.1x and protocols
EAP based, available at : http://www.netscire.it/CourseMaterial/802-1-X-2008-Eng.pdf

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

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

Bradley Mitchell, Network Topology, available at:

http://compnetworking.about.com/od/networkdesign/a/topologies.htm