IJCSMS International Journal of Computer Science and Management Studies, Vol. 12, Issue 03, Sept 2012
ISSN (Online): 2231-5268
www.ijcsms.com

Implementation of PEAP on Microsoft Window's

Anita Rana[1], Dr. Rajender Singh Chhillar [2]

[1]M.tech Student, Department Of Computer Science and Application,
M.D University, Rohtak-124001, Haryana, India
anita21rana@gmail.com

[2]Professor, Department Of Computer Science and Application,
M.D University, Rohtak-124001, Haryana, India
Chhillar02@gmail.com

Abstract

In today's world most organizations are moving from wire-connected LAN's to wireless LAN's. WLANs are changing the landscape of computer networking. Wireless communications are inherently more open to attack than wired data transfer, as its physical layer is not contained in the wire. Wireless LANs require strict user authentication, data privacy and data integrity to prevent unauthorized access to network resources and protect data from modification or destruction. Many standard setting bodies are working on the problem of wireless security. Recently new protocols have been proposed by the Internet Engineering Task Force (IETF) for protecting client authentication by running the protocols in a secure tunnel wherein all data required for authenticating the user is well encrypted. The purpose of this thesis is to implement one such proposed security protocol - PEAP (Protected Extensible Authentication Protocol) on Microsoft Windows.

Keywords: *PEAP, MS-chap, RADIUS Server, NAP.*

Introduction

In today's world most organizations are moving from wire-connected LAN's to wireless LAN's. Wireless local area networks are changing the landscape of computer networking. In recent years, the proliferation of mobile computing devices, such as laptops and personal digital assistants (PDA's), coupled with the demand for continual network connections without having to "plug in," are resulting in an explosive growth in enterprise WLANs [1]. Wireless LANs are finding their way into a wide variety of markets including financial sectors, corporations, health care, and education. Wireless networks offer the benefits of increased productivity, easier network expansion, flexibility, and lower the cost of ownership. In addition Wireless LAN systems can be configured in a variety of topologies to meet the needs of specific applications and installations. Following the increasing demand for wireless data access, different kind of wireless communication technologies are being developed continually.

On the other hand, security considerations continue to be a major challenge in the wireless network set-ups. Lack of security and inflexible authentication is often cited as a major barrier to the growth of e-commerce (electronic commerce) into m-commerce (mobile commerce). Wireless LANs, unlike the relative simplicity of wired Ethernet deployments, broadcast radio-frequency (RF) data for the Client stations to hear. This presents new and complex security issues requiring additional policies to be incorporated in every WLAN deployment. Wireless LANs require strict User authentication, Data privacy and Data Integrity to prevent unauthorized access to network resources and protect data from modification or destruction.

The Internet Engineering Task Force (IETF) has proposed new protocols for protecting Client authentication by running the protocols in a secure tunnel wherein all data required for authenticating the user is well encrypted. The purpose of this thesis is to implement one such proposed security protocol - PEAP (Protected Extensible Authentication Protocol)[2] . PEAP was developed by Microsoft, Cisco and RSA security and is currently an Internet draft. The protocol implementation is done on the server end of a Client/Server network model on a RADIUS server (Remote Authentication Dial-in User Service). The proposed protocol - PEAP provides for Client identity protection and key generation thus preventing unauthorized user access and protecting or encrypting the data against malicious manipulation.

Network Access Protection (NAP)

Network Access Protection (NAP) is a client health policy creation, enforcement, and remediation technology that is included in Windows Vista and Windows Server 2003. With NAP, you can establish health policies that define such things as software requirements, security update requirements, and required configuration settings for computers that connect to your network.

When you deploy NAP, a server running Network Policy Server (NPS) serves as a health policy server. You create health policies in NPS that specify the required configuration of NAP-capable computers that connect to your network, and then configure one or more network policies with the health policy. NPS then performs health checks while processing the network policy and performing authorization.

In Windows Server 2003, network policies were named remote access policies.NAP enforces health policies by inspecting and assessing the health of client computers, restricting network access when client computers are noncompliant with health policy, and remediating noncompliant client computers to bring them into compliance with health policy before they are granted full network access. NAP enforces health policies on client computers that are attempting to connect to a network; NAP also provides ongoing health compliance enforcement while a client computer is connected to a network.

NAP is an extensible platform that provides an infrastructure and an application programming interface (API) set for adding components to NAP clients and NPS servers that check a computer's health, enforce network health policy, and remediate noncompliant computers to bring them into compliance with health policy. By itself, NAP does not provide components to verify or remediate a computer's health. Other components, known as system health agents (SHAs) and system health validators (SHVs), provide client computer health state inspection and reporting, validation of client computer health state compared to health policy, and configuration settings to help the client computer become compliant with health policy. The Windows Security Health Agent (WSHA) is included in Windows Vista as part of the operating system. The corresponding Windows Security Health Validator (WSHV) is included in Windows Server 2003 as part of the operating system. By using the NAP API set, other products can also implement SHAs and SHVs to integrate with NAP. For example, an antivirus software vendor can use the API set to create a custom SHA and SHV. These components can then be integrated into the NAP solutions that customers of the software vendor deploy. If you are a network or system administrator planning to deploy NAP, you can deploy NAP with the WSHA and WSHV that are included with the operating system. You can also check with other software vendors to find out if they provide SHAs and SHVs for their products.

NPS Protocols

Authentication protocols are used to transmit user or computer logon credentials. If you configure NPS to process some or all of the connection requests that it receives from RADIUS clients, the authentication protocols that you have configured in network policy or connection request policy are used to transmit user or computer credentials so that NPS can verify the identity of the user or computer that is attempting to access the network.NPS uses the RADIUS protocol to communicate with RADIUS clients and other RADIUS servers.

These protocols are detailed in the following sections-

Authentication Protocols

When users attempt to connect to your network through network access servers, NPS authenticates and authorizes the connection request before allowing or denying access.

Because authentication is the process of verifying the identity of the user or computer attempting to connect to the network, NPS must receive proof-of-identity from the user or computer in the form of credentials.

Authentication protocols allow the transmission of these credentials from the computer or user who is proving their identity to the authenticator that is verifying their identity. Authentication methods typically use an authentication protocol that is negotiated by the Remote Authentication Dial-In User Service (RADIUS) server and the access client during the connection establishment process.

Each authentication protocol has advantages and disadvantages in terms of security, usability, and breadth of support. The authentication protocol used to transmit credentials is determined by the configuration of the following RADIUS infrastructure components: the access client, the RADIUS client, and the RADIUS server. You can configure NPS to accept the use of multiple authentication protocols. You can also configure your RADIUS clients to attempt to negotiate a connection by using the most secure protocol first, and then the next most secure, and so on down to the least secure. For example, the Routing and Remote Access service tries to negotiate a connection by using Extensible Authentication Protocol (EAP) first, then MS-CHAP v2, then MS-CHAP v1, then CHAP, and then PAP. When EAP is chosen as the authentication method, the negotiation of the EAP type occurs between the access client and the NPS server.

In addition, you can use network policies to implement different authentication methods depending on the type of access client that is being authenticated. For example, you can create two network policies, one for VPN clients and one for wireless clients—each of which uses a different authentication method. The network policy for VPN clients can be configured to use EAP-TLS with smart cards or certificates as the authentication method and authentication type, while the network policy for wireless clients can be configured to use PEAP-MS-CHAP v2, which provides secure password authentication.

Authentication methods

Some authentication methods implement the use of password-based credentials. For example, Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) requires that users type in a user name and password. These credentials are then passed to the NPS server by the network access server, and then NPS verifies the credentials against the user accounts database.

Other authentication methods implement the use of certificate-based credentials for the user, the client computer, the NPS server, or some combination of these types of certificates. Certificate-based authentication methods provide stronger security than password-based authentication methods. When you deploy NPS, you can specify the authentication method that is required for access to your network.

The following sections provide additional information on the authentication methods and protocols available for use with NPS.

Certificate-based Authentication Protocols

Certificates are digital documents that are issued by certification authorities (CAs), such as Active Directory Certificate Services (AD CS) or the VeriSign public CA. Certificates can be used for many purposes, such as code signing and securing e-mail communication, but with Network Policy Server (NPS), certificates are used for network access authentication.

Certificates are used for network access authentication because they provide strong security for authenticating users and computers and eliminate the need for less secure password-based authentication methods. Two authentication methods, when configured with certificate-based authentication types, use certificates: Extensible Authentication Protocol (EAP) and Protected EAP (PEAP). By using EAP, you can configure the authentication type Transport Layer Security (EAP-TLS), and with PEAP you can configure the authentication types TLS (PEAP-TLS) and Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAP v2). These authentication methods always use certificates for server authentication. Depending on the authentication type configured with the authentication method, certificates might also be used for user authentication and client computer authentication.

You can deploy certificates for use with NPS by installing and configuring the Active Directory Certificate Services (AD CS) server role.

Certificate types

When you use certificate-based authentication methods, it is important to understand the following types of certificates and how they are used -

CA certificate

When present on client and server computers, tells the client or server that it can trust other certificates, such as certificates used for client or server authentication, that are issued by this CA. This certificate is required for all deployments of certificate-based authentication methods.

Client computer certificate

Issued to client computers by a CA and used when the client computer needs to prove its identity to a server running NPS during the authentication process.

Server certificate

Issued to NPS servers by a CA and used when the NPS server needs to prove its identity to client computers during the authentication process

User certificate

Issued to individuals by a CA and typically distributed as a certificate that is embedded on a smart card. The certificate on the smart card is used, along with a smart card reader that is attached to the client computer, when individuals need to prove their identity to NPS servers during the authentication process.

Certificate deployments and Active Directory replication

Some authentication methods, such as PEAP and EAP, can use certificates for authentication of computers and users. Latency in Active Directory replication might temporarily affect the ability of a client or server to obtain a certificate from a certification authority (CA). If a computer configured to use certificates for authentication cannot enroll a certificate, authentication fails.

This latency in Active Directory replication can affect your network access authentication infrastructure because the certificates used for client and server authentication are issued by CAs to domain member computers. In the moments after you have joined a client or server computer to the domain, it is possible that the only Active Directory global catalog server that has a record of the client or server computer's domain membership is the domain controller that handled the join request.

After a computer is joined to the domain, a restart of the computer is required. After the computer restarts and you log on to the domain, Group Policy is applied. If you have previously configured the auto-enrollment of client computer certificates or, for NPS servers, server certificates, this is the moment at which the new domain member computer requests a certificate from a CA.

The CA in turn checks Active Directory to determine whether or not to issue a certificate to the client or server that has requested it. If Active Directory replication of the computer account has replicated across the domain, the CA can determine whether the client or server has the security permissions required to enroll a certificate. If Active Directory replication of the computer account has not replicated across the domain, however, the CA might not be able to verify that the client or server has the security permissions to enroll a certificate.

If this occurs, the CA does not enroll a certificate to the client or server computer. This circumstance has the following effect:

If a domain member client computer cannot enroll a client computer certificate, the client computer cannot be successfully authenticated by NPS servers when attempting to connect to the network by using any network access servers that are configured as RADIUS clients in NPS where the required authentication method is either EAP-TLS or PEAP-EAP-TLS. For example, if you have deployed RADIUS clients that are 802.1X wireless access points and you are using PEAP-EAP-TLS as your authentication method, client computers that do not have a client computer certificate cannot be authenticated and cannot access network resources. If a domain member NPS server cannot enroll a server certificate, the NPS server cannot be successfully authenticated by client computers when they are attempting to connect to the network by using any network access servers that are configured as RADIUS clients in NPS where the required authentication method is EAP-TLS, PEAP-EAP-TLS, or PEAP-MS-CHAP v2, and where clients have the Validate server certificate setting enabled. These authentication methods provide mutual authentication, where both the access client and the NPS server authenticate each other, and the NPS server must have a server certificate to be successfully authenticated by client computers. If the NPS server does not have a server certificate, all connection requests that it receives where these authentication methods are required will fail, because client computers are unable to authenticate the NPS server.

For this reason, when you deploy certificate-based authentication methods, it is recommended that you design Active Directory replication times and the deployment of subordinate CAs in such a manner that you diminish the possibility that slow replication might negatively impact your network access authentication infrastructure.

Extensible Authentication Protocol

Extensible Authentication Protocol (EAP) extends Point-to-Point Protocol (PPP) by allowing arbitrary authentication methods that use credential and information exchanges of arbitrary lengths. EAP was developed in response to demand for authentication methods that use security devices, such as smart cards, token cards, and crypto calculators. EAP provides an industry-standard architecture for supporting additional authentication methods within PPP.

EAP allows for an open-ended conversation between the remote access client and the authenticator. The conversation consists of authenticator requests for authentication information and the responses by the remote access client. For example, when EAP is used with security token cards, the authenticator can separately query the remote access client for a name, PIN, and card token value. As each query is asked and answered, the remote access client passes through another level of authentication. When all questions have been answered satisfactorily, the remote access client is authenticated.

Windows Server 2008 includes an EAP infrastructure, two EAP types, and the ability to pass EAP messages to a RADIUS server (EAP-RADIUS).

EAP infrastructure

EAP is a set of internal components that provide architectural support for any EAP type in the form of a plug-in module. For successful authentication, both the remote access client and authenticator must have the same EAP authentication module installed. You can also install additional EAP types. The components for an EAP type must be installed on every network access client and every authenticator.

EAP types

By using EAP, you can support additional authentication schemes, known as *EAP types*. These schemes include token cards, one-time passwords, public key authentication using smart cards, and certificates. EAP, in conjunction with strong EAP types, is a critical technology component for secure virtual private network (VPN) connections, 802.1X wired connections, and 802.1X wireless connections. Both the network access client and the authenticator, such as the NPS server, must support the same EAP type for successful authentication to occur.

Strong EAP types, such as those based on certificates, offer better security against brute-force or dictionary attacks and password guessing than password-based authentication protocols, such as CHAP or MS-CHAP.

With EAP, an arbitrary authentication mechanism authenticates a remote access connection. The authentication scheme to be used is negotiated by the remote access client and the authenticator (either the network access server or the Remote Authentication Dial-In User Service [RADIUS] server). Routing and Remote Access includes support for EAP-TLS and PEAP-MS-CHAP v2 by default. You can plug in other EAP modules to the server running Routing and Remote Access to provide other EAP types.

EAP-TLS

EAP-Transport Layer Security (EAP-TLS) is an EAP type that is used in certificate-based security environments. If you are using smart cards for remote access authentication, you must use the EAP-TLS authentication method. The EAP-TLS exchange of messages provides mutual authentication, negotiation of the encryption method, and encrypted key determination between the remote access client and the authenticator. EAP-TLS provides the strongest authentication and key determination method.

EAP-TLS is supported only on servers that are running Routing and Remote Access, that are configured to use Windows Authentication or RADIUS, and that are members of a domain. A network access server running as a stand-alone server or as a member of a workgroup does not support EAP-TLS.

Using RADIUS as a transport for EAP

Using RADIUS as a transport for EAP is the passing of EAP messages of any EAP type by a RADIUS client to a RADIUS server for authentication. For example, EAP messages are sent by a remote access client to a network access server that is configured as a RADIUS client. The network access server encapsulates and formats the EAP messages as RADIUS messages, and then sends them to the RADIUS server. When you use EAP over RADIUS, it is called EAP-RADIUS.

EAP-RADIUS is used in environments where RADIUS is used as the authentication provider. An advantage of using EAP-RADIUS is that EAP types do not need to be installed at each network access server, only at the RADIUS server. In the case of an NPS server, you only need to install EAP types on the NPS server.

In a typical use of EAP-RADIUS, a server running Routing and Remote Access is configured to use EAP and to use an NPS server for authentication. When a connection is made, the remote access client negotiates the use of EAP with the network access server. When the client sends an EAP message to the network access server, the network access server encapsulates the EAP message as a RADIUS message, and then sends it to its configured NPS server. The NPS server processes the EAP message and sends a RADIUS-encapsulated EAP message back to the network access server. The network access server then forwards the EAP message to the remote access client. In this configuration, the network access server is only a pass-through device. All processing of EAP messages occurs at the remote access client and the NPS server.

Routing and Remote Access can be configured to authenticate locally, or to a RADIUS server. If Routing and Remote Access is configured to authenticate locally, all EAP methods will be authenticated locally. If Routing and Remote Access is configured to authenticate to a RADIUS server, all

EAP messages will be forwarded to the RADIUS server with EAP-RADIUS

Enabling EAP

To enable EAP-based authentication

1. Enable EAP as an authentication protocol on the network access server. For more information, see your network access server documentation.
2. In NPS, on the Constraints tab of the appropriate network policy, enable EAP and configure the EAP type.
3. Enable and configure EAP on the access client. For more information, see your access client documentation.

Protected Extensible Authentication Protocol

Protected Extensible Authentication Protocol (PEAP) uses Transport Layer Security (TLS) to create an encrypted channel between an authenticating PEAP client, such as a wireless computer, and a PEAP authenticator, such as a server running Network Policy Server (NPS) or other Remote Authentication Dial-In User Service (RADIUS) server. PEAP is part of the Extensible Authentication Protocol (EAP) protocols. PEAP does not specify an authentication method, but provides additional security for other EAP authentication protocols, such as EAP-Microsoft Challenge Handshake Protocol version 2 (MS-CHAP v2), that can operate through the TLS-encrypted channel provided by PEAP. PEAP is used as an authentication method for access clients connecting to your organization network through the following types of network access servers:
802.1X wireless access points
802.1X-capable switches
Computers running Windows Server 2003 and Routing and Remote Access configured as virtual private network (VPN) servers
Computers running Windows Server 2003 and Terminal Services Gateway (TS Gateway)
To enhance both the EAP protocols and network security, PEAP provides:

A TLS channel that provides protection for the EAP method negotiation that occurs between client and server. This TLS channel helps prevent an attacker from sending packets between the client and the network access server to cause the negotiation of a less secure EAP type. The encrypted TLS channel also helps prevent denial-of-service attacks against the NPS server.
Support for the fragmentation and reassembly of messages, allowing the use of EAP types that do not provide this functionality.
Clients with the ability to authenticate an NPS server or other RADIUS server. Because the server also authenticates the client, mutual authentication occurs.
Protection against the deployment of an unauthorized wireless access point at the moment when the EAP client authenticates the certificate provided by the NPS server. In addition, the TLS master secret created by the PEAP authenticator and client is not shared with the access point. Because of this, the access point cannot decrypt the messages protected by PEAP.
PEAP fast reconnect, which reduces the delay between an authentication request by a client and the response by the NPS server or other RADIUS server. Fast reconnect also allows wireless clients to move between access points that are configured as RADIUS clients to the same RADIUS server without repeated requests authentication. This reduces resource requirements for both client and server, and minimizes the number of times that users are prompted for credentials.

Steps to configure MS-CHAPv2

We will concentrate on the peer authentication using MS-CHAPv2. This stage takes place after a PPTP tunnel is established and the setup for the PPP connection has started. The client requests an authenticator challenge from the server. The server sends back a 16-bytes random authenticator challenge.

The client generates the response

(a) The client generates 16-bytes random peer challenge.
(b) The client generates the challenge by hashing the authenticator challenge, the peer challenge, and the user's login using SHA.
(c) The client generates the NT password hash from the user's password.
(d) The 16-byte NT password hash from step (c) is padded with 5 bytes of zero. From these 21 bytes three 7-byte DES keys are derived.
(e) The _rst 8 bytes of the hash generated in step (b) (these 8 bytes are later revered to as the challenge)

are encrypted using DES with each of the three keys generated in step (d).

(f) The 24 bytes resulting from step (e), the 16-byte random peer challenge, and the user's login are sent back to the server as response.

The server decrypts the response with the hashed password of the client that is stored in a database. If the decrypted response matches the challenge, the server sends a positive.

Authenticator response:

(a) The server hashes the NT password hash using MD4 to generate a password-hash-hash.

(b) The server generates a hash using SHA from the client’s response, the password-hash-hash, and the literal constant Magic server to client signing constant".

Configuring MSCHAP V2 Authentication

To configure the NAS to accept MSCHAP V2 authentication for local or RADIUS authentication and to allow proper interpretation of authentication failure attributes and vendor-specific RADIUS attributes for RADIUS authentication, use the following commands beginning in global configuration mode.

Steps

1. Enable
2. Configure terminal
3. radius-server vsa send authentication
4. Interface type number
5. ppp max-bad-auth number
6. ppp authentication ms-chap-v2
7. End

Verifying MSCHAP V2 Configuration

To verify that the MSCHAP Version 2 feature is configured properly, perform the following steps

Steps

1. Show running-config interface type number
2. Debug ppp negotiation
3. Debug ppp authentication
4. Verifying MS-CHAP V2 Configuration
5. How to Configure MS-CHAP Version 2

The following table compares MS-CHAP v2 to PEAP-MS-CHAP v2.

Function	**MS-CHAP v2**	**PEAP-MS-CHAP v2**
Provides client authentication by using passwords	Yes	Yes
Ensures that the server has access to credentials	Yes	Yes
Authenticates the server	Yes	Yes
Prevents wireless access point spoofing	No	Yes
Prevents an unauthorized server from negotiating the least secure authentication method	No	Yes
Uses TLS keys generated with a public key	No	Yes
Provides end-to-end encryption	No	Yes
Prevents dictionary or brute force attacks	No	Yes
Prevents replay attacks	No	Yes
Allows chaining of authentication methods	No	Yes
Requires client trust of certificates provided by the server	No	Yes

Conclusion:

The proposed security protocol - PEAP (Protected Extensible Authentication Protocol) is implemented on the Microsoft Windows. This protocol protects client authentication by running the protocols in a secure tunnel wherein all data required for authenticating the user is well encrypted.

References

[1] Syang Xiao Jon Rosdahl. Performance analysis and enhancement for the current and future IEEE 802.11 MAC protocols. ACM SIGMOBILE Mobile Computing and Communications Review

[2] Wireless LAN analyzer tools, WildPackets Inc., URL: http://www.wildpackets.com/

[3] N.Asokan, Valtteri Niemi, Kaisa Nyberg. Man-in-the-Middle in Tunneled Authentication. Nokia Research Center, Finland, 2002

[4] Wireless LANs: The 802.1X Revolution http://www.drizzle.com/~aboba/IEEE/BAWUG.ppt

[5] AirSnort Tool. The Shmoo group. URL: http://airsnort.shmoo.com/

[6] Intercepting Mobile Communications: The Insecurity of 802.11. URL:http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

[7] A comprehensive Review of 802.11 Wireless LAN Security URL:www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf

[8] Cisco Wireless LAN Security Bulletin www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm

[9] Authentication with 802.1x and EAP Across Congested WAN Links www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp_an.htm

[10] Configuring the Cisco Wireless Security Suite

[11] Cisco Aironet Wireless LAN Security Overview

[12] Carter, Brian, CISSP and Russell Shumway. Wireless security: end to end c2002.

[13] The Unofficial 802.11 Security Web Page http://www.drizzle.com/~aboba/IEEE/

[14] Wireless LAN: Issues and Challenges R. Chandramouli and K.P. Subbalakshmi URL: www.ece.stevens-tech.edu/~suba

[15] Free network protocol analyzer for Unix and Windows, URL: http://www.ethereal.com/

[16] Stubblefield, A., Ioannidis, J., Rubin, A. “Using the Fluhrer, Mantin, and Shamir. Attack to Break WEP” URL: http://www.cs.rice.edu/~astubble/wep/wep attack.pdf

[17] Alan Curry, RLM Module Interface (for developers), April 2003,

[18] Free Radius, Open Source implementation of the RADIUS Server http://www.freeradius.org/

[19] Frost & Sullivan analyst briefings URL: http://www.frost.com/prod/servlet/analyst-briefings.pag

[20] Mathew Gast, TTLS and PEAP Comparison, Wireless LAN Security Interoperability Lab URL: www.ilabs.interop.net/WLAN_Sec/TTLS-PEAP-lv03.pdf

[21] Geier, James T.Wireless LANs / Jim Geier 2001.

[22] Geoff Marshall, Odyssey, August 2002. URL: http://www.scmagazine.com/scmagazine/sc-online/2002/review/28/product.html

[23] Redder, Greg. “Implementation of a Secure Wireless Network on a University Campus” October 29, 2001. URL: http://rr.sans.org/wireless/wireless_univ.php

[24] Web ProForumTutorials. URL: http://www.iec.org

[25] IEEE 802.11 Working Group Web site. URL: http://grouper.ieee.org/groups/802/11/

[26] IEEE Standard 802-11, IEEE standard for wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification June 1999) URL: http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[27] Bernard Aboba, Tim Moore, Paul Congdon, IEEE 802.1X For Wireless LANs, IEEE Plenary Submission, March 2000. URL: www.ieee802.org/1/files/public/docs2000/ieee_plenary.PDF

[28] IEEE 802.1X Committee. “IEEE Std 802.1X, 2001 Edition, IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control”. July, 2001. URL: http://standards.ieee.org/reading/ieee/std/lanman/802.1X-2001.pdf

[29] Paul Congdon, IEEE Plenary, March 2000 “IEEE 802.1X Overview Port Based Network Access Control” URL: www.ieee802.org/1/files/public/docs2000/P8021XOverview.pdf

[30] Andersson, H., Josefsson, S., Zorn, G., and B. Aboba, “Protected Extensible Authentication Protocol (PEAP)”, IETF Work in progress, October 2001. URL: http://ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-xx.txt

[31] Andersson, H, “Protected EAP Protocol (PEAP)”, IETF Internet Draft. 23 February, 2002. URL: http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tlseap-02.txt

[32] Paul Funk and Simon Blake-Wilson. EAP tunneled TLS Authentication Protocol (EAP-TTLS), Nov 2002. IETF *pppext* working group draft. URL: http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-02.txt