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

Analysis of the Protected Extensible Authentication Protocol

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

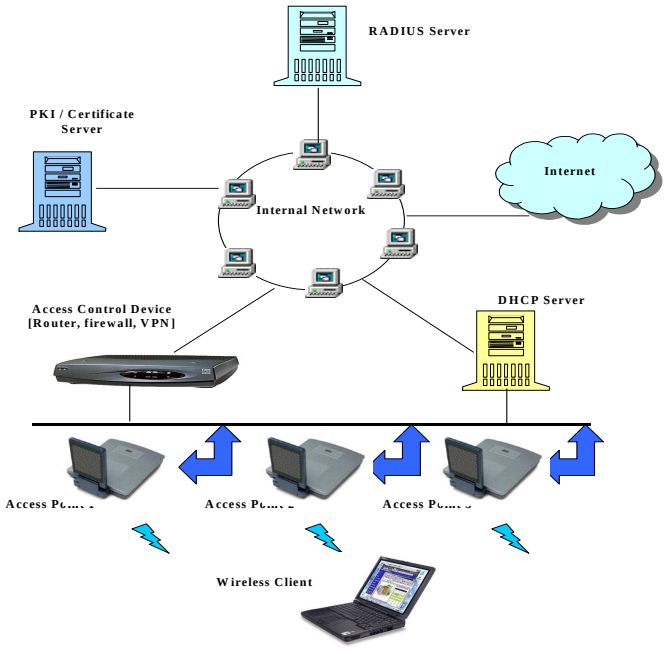
The Internet Engineering Task Force (IETF) has proposed new protocols for highly secured wireless networking. The purpose of this paper is to implement one such proposed security protocol - PEAP (Protected Extensible Authentication Protocol) [1]. PEAP was jointly developed by Microsoft, Cisco and RSA security. 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 activities.

Keywords: *Wireless LAN, Authentication Protocol.*

1. Wireless LAN Standards

Wireless networks have exhibited significant growth within the last few years in both home and corporate world because of lost cost with high hardware quality. The reliability and compatibility of WLANs increase its acceptance. Security on WLANs is a requirement in today's rapid deployment of this technology. There are several wireless LAN standards available today. As the globally recognized LAN authority, The Institute of Electrical and Electronics Engineers (IEEE) has established the standards that have driven the LAN industry for the past two decades. These standards provide the basis for wireless network products.

The IEEE 802 standards committee formed the first internationally recognized WLANs Standards Working Group – 802.11 in 1990. It developed a global standard in Jun 1997, for radio equipment and networks operating for data rates of 1 and 2 Mbps transmission in the 2.4 GHz unlicensed frequency band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). The new IEEE 802.11b extension (also



popularly referred to as 802.11 High Rate or Wi-Fi) in Sep1999, defines a standard for products of wireless networks working at 11 Mbps transmission in the 2.4 GHz band.

The 802.11 standard provides only limited support for confidentiality through the wired equivalent privacy (WEP)

Figure1: Wireless LAN topology

protocol, which has been discovered to contain significant flaws in the design. The IEEE 802.11 in response to the security flaws of 802.11 standards employed a task group in July 2001, which published the 802.1x standard. The use of the new standard offered an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and support multiple authentication methods.

2. Wireless Network Security

Security is a main concern for any network especially for wireless networks. With wireless LAN radio waves propagating throughout--and even outside--the enterprise, wireless LANs obviously present unique challenges like user security, data rate enhancements, lowering costs and roaming user challenges of which security considerations continue to be a major consideration. While fundamentals of wireless security are largely similar to those of the wired Internet, wireless data networks present a more constrained communication environment compared to wired networks. Because of fundamental limitations of power, available spectrum and mobility, wireless data networks tend to have less bandwidth, more latency, less connection stability, and less predictable availability. Similarly, handheld wireless devices tend to have limited battery life, less powerful CPUs, less memory, restricted power consumption, smaller displays, and different input presenting a more constrained computing environment compared to desktop computers [2].

Wireless networks are more vulnerable as compared to wired networks. In wireless networks, the communication medium is air. The transmitted data via the radio frequency can be accessed by equipment that is readily available in the market for a cheap rate. As a result, it's very important to use effective wireless security that guard against unauthorized access to important resources or data. WLAN security, involves concern in three separate issues:

1. Authentication,
2. User Privacy and
3. Authorization.

Focusing too much on any one of the above without adequately addressing the other issues will not help in reduce the security risks inherent in the wireless system.

4. Literature Survey

The emerging theory which goes by the name of Wireless Network Security using EAP-PEAP on RADIUS server. EAP was first used in the Point-to-Point protocol (PPP). Extensible Authentication Protocol (EAP) defines a standard message exchange between the Supplicant and an *Authenticator* before the *Supplicant* is granted access to the LAN. It allows an *Authentication Server* to authenticate the Client based on an authentication protocol agreed upon by both parties. EAP protocol uses the link layer and does not require the IP protocol to transport messages between devices and hence is effective in networks that rely on the Dynamic Host Configuration Protocol (DHCP) for assigning Client their IP addresses. The Clients can communicate with the access points without requiring a valid IP address and use the EAP over LAN (EAPoL) protocol to transmit messages. It is to be noted that in the context of WLANs the term EAPoW is used instead. EAPoW doesn't officially exist in any technical standard. EAP by itself cannot protect the authentication message exchange between the Client, Authenticator and the Authentication server. It makes use of some higher-level authentication mechanism to validate the user's login credentials. There are several EAP authentication schemes that can be used each with its own strengths and weaknesses. Some of the most commonly deployed EAP authentication types include EAP-MD-5, EAP-TLS, EAP-PEAP, and EAP-TTLS. However in practice, it has been noted that only methods based on the IETF's well-known Transport Layer Security (TLS) standard can satisfy strict encryption and authentication requirements [3].

EAP Transport Layer Security

EAP provides extensible authentication for accessing the network. EAP Transport Layer Security (TLS) (RFC2716) is an EAP type that is used in certificate-based authentication. The EAP-TLS offers very good protection because of its mutual authentication of Client and server with both parties mutually validating each other through the use of PKI (Public Key Infrastructure) certificates and per session WEP keys. TLS is designed to provide secure authentication and encryption of data by making use of the reliable Transport Layer like a TCP/IP connection. It provides security to any application protocol layered on top of it. TLS authentication is split into two methods:

1. Server side authentication and
2. Client side authentication.

The server presents a certificate to the Client, and, after validating the server's certificate; the Client presents a Client certificate. Naturally, the certificate may be protected on the Client by a pass phrase, PIN, or stored on a smart card, depending on the implementation. Thus the certificates on both the Certificate Authority and the Client must be valid in order for a connection to be established.

Protected Extensible Authentication Protocol (PEAP)

PEAP was developed jointly by Microsoft, Cisco and RSA security. Like its competing standard TTLS, PEAP makes it possible to authenticate wireless Clients without requiring them to have PKI certificates. PEAP uses Transport Layer Security (TLS) to create an encrypted channel between an authenticating EAP Client and an EAP Authenticator. It then uses the resulting TLS session as a secure wrapper for other EAP authentication protocols.

PEAP is based on server-side EAP-TLS and for Client-side it can use any non-mutually authenticating EAP-types, thus providing for a mutual authentication. In this way PEAP attempts to fix the problems found in EAP–TLS that of having to install digital certificates on every Client machine.

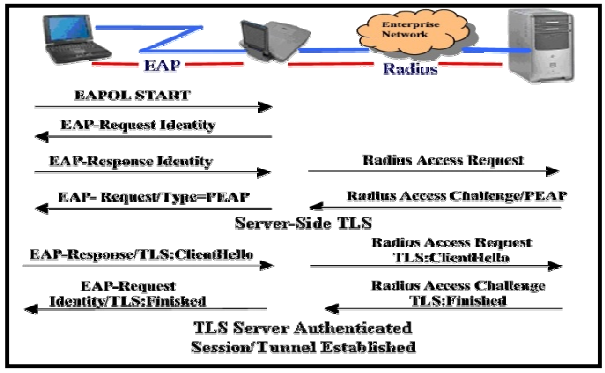


Figure 2: PEAP Phase 1 – Perform TLS handshake & Establish TLS Tunnel

PEAP performs authentication in two phases. In the first phase the Authentication Server is authenticated to the Supplicant using a PKI certificate. Using TLS, a secure channel is established through which any other EAP-Type can be used to authenticate the Supplicant to the Authentication Server during the second Phase. The Client and Server exchange a sequence of EAP messages encapsulated within the TLS messages, and the TLS messages are authenticated and encrypted using TLS session keys negotiated by the Client and the server.

There are two versions of the PEAP draft – Microsoft PEAP and Cisco PEAP

- Microsoft PEAP: This version of PEAP supports Client authentication by only MS-CHAPv2, which limits user database to those that support MS-CHAPv2, such as Windows NT domains and Active Directory.
- Cisco PEAP: This version supports Client Authentication by One-Time Password (OTP) support and logon passwords. This allows support for OTP databases from vendors such as RSA security and Secure Computing Corporation, and also supports logon password databases like LDAP, Novell NDS, and Microsoft databases.

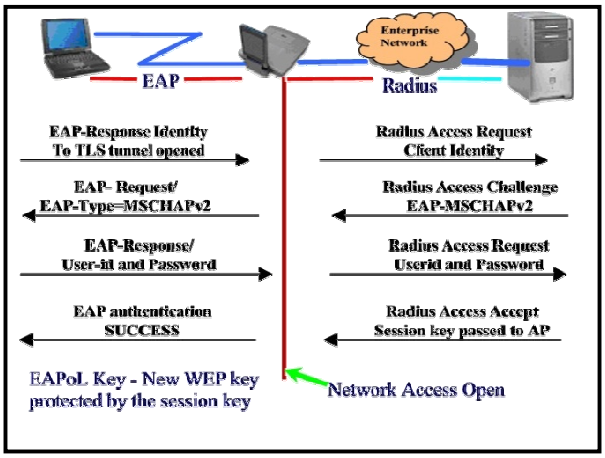


Figure 3: PEAP Phase 2 – Authenticate Client in the generated TLS tunnel

Figures 2 and 3 depict the message exchanges that take place during the process of authentication. As PEAP adds a TLS layer on top of EAP, the message exchange starts and server side TLS is done.In figure 2 TLS session/tunnel is established. The Client and server negotiate and create an encrypted tunnel. This tunnel provides a secure data path for Client authentication that shown in figure 3. The RADIUS server sends the access point a RADIUS ACCEPT message, including the Client's WEP key, indicating successful authentication.

3. Problem Statement

Problem Statement

There can be various problems occurred during the purposed implementation of PEAP. The first problem can be encountered in setting up the test-bed based on the open sources available.

There can be number of compiling errors that needed to be corrected initially. The next problem is in generating the PKI certificates because of different versions of the OpenSSL package that were needed. The HOW-TO presented by Raymond McKay [4] helped solve the problem. The next problem is to debug why the access point did not relay messages to the RADIUS server.

The problems can be encountered in compiling the code. Changes made to the Make files in the source directories to include the path for the new Kerberos location. The next problem faced was trying to get the EAP-TTLS code working. It failed to authenticate in the second Phase of the protocol. Finally debugging the PEAP code was difficult particular problem that had held me for a long time was the eap-header length field. PEAP version 0 does not provide EAP headers in the inner request hence they need to be removed before tunneling the EAP-message packet back to the Client.

4. Objective

The main goal of this is to study the server side implementation of the Protected Extensible Authentication Protocol (PEAP) on RADIUS Server. RADIUS Server is used for both wired as well as wireless networking. RADIUS Server is used because it provides security on both layer link layer as well as network layer. PEAP is an 802.1x EAP authentication protocol designed typically for access control in wireless LANs. It makes use of two very well known protocols Extensible Authentication Protocol (EAP) and EAP- Transport Layer Security (TLS) for highly secured wireless communication.

5. Conclusion

We have discussed purposed PEAP (Protected Extensible Authentication Protocol) for the Free Radius Server. A comparative analysis between the implemented protocol PEAP and its competing standard TTLS (Tunneled Transport Layer Security) are presented. This paper has given a deeper insight in some of the issues faced in the design of protocol standards.

Four groups of test scenarios have been conducted for both PEAP and TTLS. In all the tests both TTLS and PEAP had similar behavioral pattern. The distance tests indicate that the wireless Client's performance slows down as it goes farther away from the access point irrespective of the authentication method it is using. The resilience tests indicate that the Client performance degraded as the network interface uptime gets shorter irrespective of the authentication protocol it was using.

Also beyond 3.8 sec network uptime both PEAP and TTLS failed to recover. On an average in all the tests the TTLS protocol has shown a higher performance rate of 10% in terms of the time taken in handling requests as compared to PEAP. Also from the tests it can be observed that relatively PEAP has been more influenced by the Client's processor speeds, the distance ranges and the network transitive nature as compared to TTLS. Although the better performance shown by TTLS over PEAP is negligible, it is worth noting that TTLS was outperforming PEAP consistently in all the tests.

Finally a MAC address-spoofing test has been performed to see if an attacker could gain access to the wireless network that is using the TTLS/PEAP protocols as its authentication mechanism. The test results clearly indicate that by MAC address spoofing an attacker could not masquerade his identity and break into the network. The attacker in addition to the MAC address and IP address required user credentials and they were relayed across the network in encrypted format that could not be decrypted.

References:

[1] Yang 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] Cisco/Aironet driver for Linux (4500/4800/340/350 series), URL: http://airo-linux.sourceforge.net/
[3] Wireless LAN analyzer tools, WildPackets Inc., URL: http://www.wildpackets.com/
[4] N.Asokan, Valtteri Niemi, Kaisa Nyberg. Man-in-the-Middle in Tunneled Authentication. Nokia Research Center, Finland, 2002
[5] Wireless LANs: The 802.1X Revolution http://www.drizzle.com/~aboba/IEEE/BAWUG.ppt
[6] AirSnort Tool. The Shmoo group. URL: http://airsnort.shmoo.com/
[7] Intercepting Mobile Communications: The Insecurity of 802.11. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf
[8] Comprehensive Review of 802.11 Wireless LAN Security and URL: www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf
[9] Cisco Wireless LAN Security Bulletin /www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm
[10] Authentication with 802.1x and EAP Across Congested WAN Links www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp_an.htm