International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 2 145 - 148

Classification of EAP methods and Some Major Attacks on EAP

Meenu Katoch
Computer Science Department
Shoolini University (H.P), India
Katochmeenu66@gmail.com

Randhir Bhandari
Computer Science Department
Shoolini University (H.P),India
jobrandhir@gmail.com

***Abstract*—** This paper presents an overview of authentication protocol and analysis of Extensible Authentication Protocol (EAP) and its place in securing network. In general, authentication procedure adds extra messages to the original message flow and results in throughput reduction/ increase in processing time. Extensible Authentication Protocol (EAP) is a framework which aims to provide a flexible authentication for wireless networks. A number of specific widely used EAP methods are examined and evaluated for their advantages and susceptibility to types of attack. In addition, we evaluate how we communicate between two entities over the network.

Keywords- *Authentication protocol, EAP, Wireless network, Extensible authentication protocol, Authentication server.*

*****

I. INTRODUCTION

An authentication protocol is a type of computer communications protocol or cryptographic protocol that specially designed for transfer of authentication data between two entities. This allows to authenticate the connecting entity i.e. Client connecting to a Server as well as authenticate itself to the connecting entity i.e. Server to a client by declaring the type of information that ca be needed for authentication It is also the very important layer of protection that can be needed for securely communicate with computer networks.EAP or Extensible Authentication Protocol is used between a dial-in client and server to determine what authentication protocol will be used. EAP is an authentication framework frequently used in wireless network and point to point connections.

II. CLASSIFICATION OF COMMON AUTHENTICATION PROTOCOL

A. CHAP

Challenge Handshake Authentication Protocol is a three way handshake protocol which is as compared to B PAP Authentication Protocol be more secure than PAP.

B. EAP

Extensible Authentication Protocol is a protocol used between a dial-in client and server to determine what authentication protocol will be used. EAP is an authentication framework frequently used in wireless network and point to point connections

C. PAP

Password Authentication Protocol is a two way handshake protocol, it starts when the link is established.
Authentication Protocol Password Authentication Protocol is a plain text password used on older SLIP systems and it is also not secure.

D. Kerberos

Kerberos is a centralized network authentication system developed at MIT and available as a free implementation from MIT but also in many commercial products

III. TYPES OF AUTHENTICATION PROTOCOL

A. Authentication protocols are designed to transfer the authenticated data between two entities.

There are some common protocols that are mainly used by point to point servers to verify the identity of remote clients before granting them to the authenticated server data.[15] Then out of which mostly are using a password as the cornerstone of the verification. Then shared the password between the communicating entities in advance.

A.I PAP - Password Authentication Protocol

PAP is password authentication protocol and is one of the oldest protocol for the verification of packet. The verification of the packet is initialized by client or user by sending packet with credentials (username and password) at the beginning of the establishment.[6] Now it is highly insecure because the credentials are being transfer to the network in plain ASCII text thus PAP is vulnerable to the attacks like Eavesdropping and man-in-the-middle based attacks. [15]

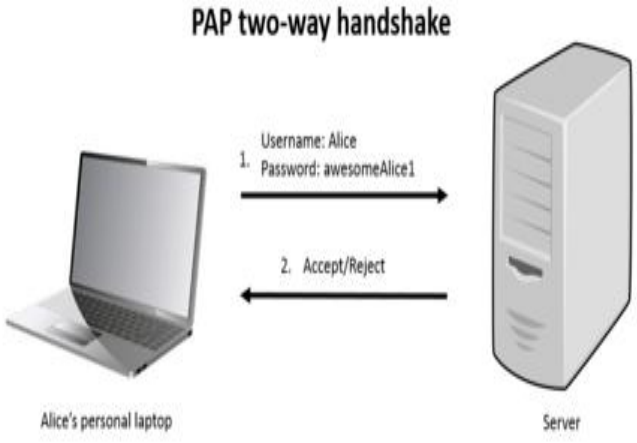

Figure 1. PAP 2-way handshake scheme

A.II. CHAP - Challenge-handshake authentication protocol

In this protocol the authentication process is always initialized by the host or server and anytime that can be performed during the session, also repeatedly. Server can sends a random string (usually 128B long). Client can use the string and password received as parameters for MD5 hash function and then result sends together with username in plain text .To apply the same function server can use the same username and then compares the calculated and receive hash. An authentication is successful or unsuccessful.

A.III. EAP-Extensible Authentication Protocol

EAP was originally developed for PPP (Point-to-Point Protocol) and it is widely used in IEEE 802.3, IEEE 802.11(Wi-Fi) standard or IEEE 802.16[15]as the place of 802.1x authentication framework and the latest version is standardized in RFC 5247.[15] There is also an advantage of EAP that for client-server authentication method it is general authentication framework –there are some various versions called EAP-methods. Most commonly used methods of EAP are as follows:

i. EAP-MD5
ii. EAP-TLS
iii. EAP-TTLS
iv. EAP-FAST
v. EAP-PEAP

A.IV. Kerberos (protocol)

Kerberos is a centralized network authentication system developed at MIT and available as a free implementation from MIT but also in many commercial products. Kerberos is the default authentication method in Windows 2000 and later. The process of authentication is more complicated itself than in the previous protocols - Kerberos uses symmetric key cryptography, requires a trusted third party and that can be use public-key cryptography during certain phases of authentication if needed.

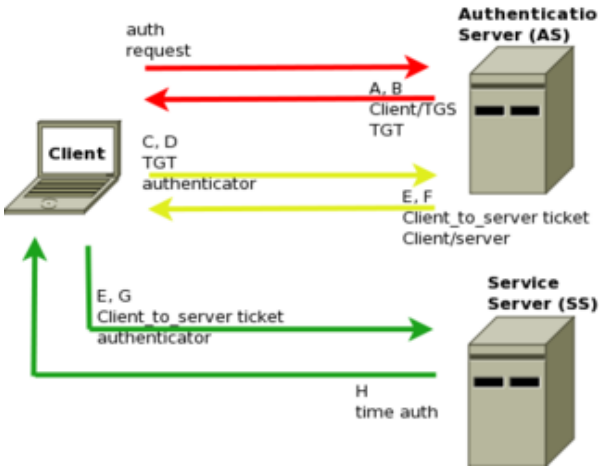

Figure 2. Kerberos authentication process

IV. Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) is a protocol for wireless networks that expands on authentication methods and used by the Point-to-Point Protocol (PPP), an EAP is used when computer connecting to the Internet. EAP can support multiple authentication mechanisms, such as token cards, smart cards, certificates, one-time passwords, and public key encryption authentication. EAP is defined in RFC 3748, which is made by RFC 2284 obsolete, and that was updated by RFC 5247.

EAP is in wide use. There are some examples, in IEEE 802.11 (Wi-Fi) the WPA and WPA2 standards have adopted IEEE 802.1X with one-hundred EAP Types as the official authentication mechanisms.

A. Working of EAP when communicating between two parties:

In communications using EAP, a user can requests connection to a wireless network through an access point (an access point is station that transmits and receives data, sometimes known as a transceiver). The access point requests for identification (ID) data from the user and transmits that data to an authentication server. The authentication server asks the access point for proof of the validity of the ID. After the access point obtains that verification from the user and sends it back to the authentication server, the user is connected to the network as requested.

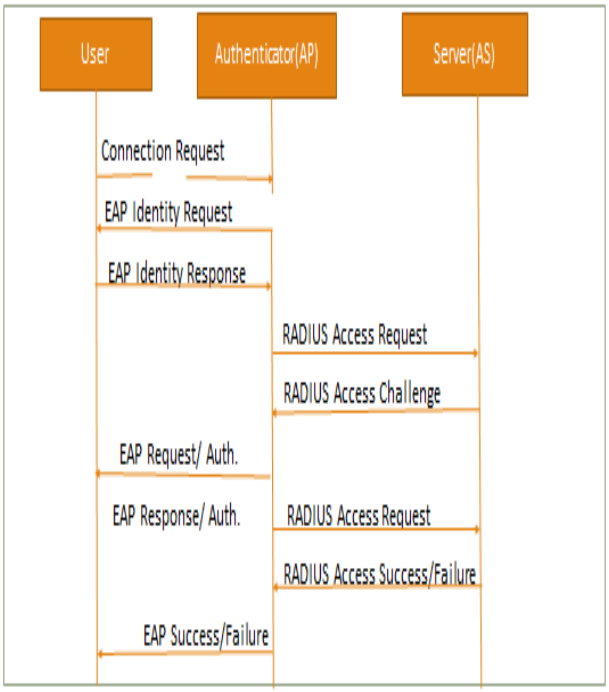

Figure3. Message flow

B. EAP methods

Modern wireless networks secured with the 802.11i standard and it is also referred to asWPA2 and Wi–Fi Protected Access (WPA) or in enterprise mode use authentication techniques that are based on the IEEE802.1X standard. EAP main meaning in 802.1X does not specify the main method, procedure, algorithm, or for the authentication but rather it specifies a framework into which a particular method that can be plugged.[2] There are some EAP methods that specially developed for wireless networks in addition to EAP methods that are existing for wired networks.

B.I. EAP–TLS

EAP–TLS (Transport Level Security) is an EAP method that based on RFC 2716 using a public key certificate authentication steps in the EAP framework. This gives a means for mutual authentication between the client and the authenticator and between the authenticator and the client. [9] For this reason it is more costly to implement the password based methods. There is also some issues under this, one of them the issue of distributing the certificates to all the objects on the network. The main features provided by EAP–TLS are key exchange and establishment, mutual authentication, support for the fragmentation and reassembly, and fast reconnect.

B.II. EAP–MD5

The mechanism of EAP–MD5 is to collect a username and password from the user to be authenticated, encrypted by the MD5 message hashing algorithm, or pass that data on to a RADIUS server. However, it has significant flaws and also it is a simple EAP method. It offers no description to which the change keys over time so that the same issue of constant keys which WEP faces is an issue with MD5.[7] In addition to this the requirement for symmetric authentication cannot fulfil by the MD5 between client and access point. Pertaining to EAP, access point and client as specified in RFC over wireless networks. There are no good arguments due to these vulnerabilities and no significant advantages over WEB.

B.III. EAP–TTLS

TTLS (tunnel- TLS) is an expanded form of transport layer security. To this EAP methods, a secure tunnel is established between the server and the client using a certificates issued by mutually trusted certificate authority and public key algorithm.[8] Once this tunnel is established, another authentication method is employed and that transaction is communicate via the secure tunnel because by the secure tunnel the authentication exchange now takes place, a less secure authentication method can be used.[2]This method is a less secure EAP method, such as another legacy method of authentication or MD5, such as PAP or CHAP.

B.IV. EAP- PEAP

PEAP (Protected EAP) [2] is one of the EAP method which is mostly similar in behavior to that of TTLS. However, as compared to TTLS, PEAP verified the authenticator to the client, but not in the other direction. [10] So, it reduces the cost and complexity by only requiring certificates to be present on the authenticator, not on the clients. Some of the benefits of PEAP are the message authentication and encryption, fragmentation and reassembly ability, secure key exchange and fast reconnect. [11]

B.V. LEAP

Lightweight EAP is also known as Cisco-EAP. It is a method defined by Cisco Systems. It uses a Username or password pair to authenticate both the client and the authentication server LEAP, that is based on mutual authentication between server and client and using the username or password scheme [2]. However, it is password based method and the challenge and response dialog is not an encrypted tunnel. LEAP is vulnerable to dictionary attacks. [12] LEAP promotes the session means that it is independent by restarting keys for each session, thereby leaving the prior and subsequent sessions secure even if a single session is attacked. [13]

B.VI. EAP –AKA

Under the consideration of EAP-AKA, there is slightly variation on EAP-SIM or authentication and key agreement. [14] The procedures and methods are similar between EAP–AKA and EAP–SIM, EAP–AKA presents a stronger level of security as compared to EAP–SIM due to the use of stable keys for mutual authentication [12] This standard is developed by the 3GPP and can be replaces the SIM cards used on GSM networks and in EAP–SIM with identity of user modules or USIMs that are used in UMTS networks.

C. EAP SECURITY ISSUES

EAP is a standard protocol which provide an infrastructure for network access to clients and authentication servers. It does not specify the mechanism of authentication itself but the way that it is negotiated by the communicating parties. Consequently, EAP has no security issues itself. There are some attacks under the EAP methods:

C.I. Dictionary Attacks

A dictionary attack is a technique for defeating a process of authentication or code by trying each of the word from a dictionary as like list of common words and encoding. [1] This attack is differ from brute-force attack in the way that only the most likely words are tried. It the same way of the original pass phrase was encoded.

C.II. Plaintext Attacks

EAP implementations depend on clear-text authentication by using the RADIUS even within protected tunnel are susceptible to known plaintext attacks. In this known-plaintext attack (KPA) [1], the attacker can uses the samples of both the plaintext and its encrypted form to reveal further important information such as the secret encryption key.

C.III. Man-in-the-middle Attacks

Tunneling protocols such as TLS and TTLS offer a server-authentic tunnel that secures both the authentication method or the user's identity .The original implementations of EAP that are based on those protocols which may also be vulnerable to man-in-the-middle attacks. [1] With this attack, client can assumes the characteristics of both the client and the server in order to catch communication from one device and send one to the other device.

C.IV. Cipher text attacks

EAP-SIM improves the original GSM security model—that based on a challenge-response mechanism and pre-shared key. The original GSM standard uses A5/1 and A5/2 stream ciphers with key length of 64 bits. EAP-SIM can improves the original GSM standard by increase the length of key to 128 bits.[1] Unfortunately, the way the new 128-bit key is generated has been shown to be defective. Even other than

being 128-bit long, then the resulting key has an effective key length of 64 bits only.

V. CONCLUSION

With the increase in its use security problems of confidentiality, integrity and authentication are also increasing. The mechanism to solve these problems has changed to public key cryptography from symmetric key cryptography .The proposed EAP method satisfies the requirements defined in RFC 4017. Other important features, such as forward secrecy, were also included in our proposed EAP method. In addition, we took advantage of secure symmetric encryption schemes and hash functions to avoid exponentiation computations and to achieve security requirements without maintaining certificates. Finally, we have also provided formal security proofs to demonstrate that our EAP method is truly secure.

VI. REFERENCE

[1] Dr. S.P. Anandaraj, S. Poornima, Sougandhika Reddy, Sindhuja Manchala, "Semantic Analysis On Communication And Security Issues Of EAP On Wireless Network": International Journal Of Advanced Computing And Electronics Technology (IJACET), Volume-2, Issue-1,2015.

[2] Ram Dantu ,Gabriel Clothier, Anuj Atri Ram Dantu , Gabriel Clothier, Anuj Atri: **"**EAP methods for wireless networks" Computer Standards & Interfaces 29 (2007) 289–301 , 27 September 2007

[3] D. Stanley, J. Walker, B. Aboba, EAPMethod requirements for Wireless LANs, RFC 4017, March 2005.

[4] L. Blunk, J. Vollbrecht, PPP ExtensibleAuthentication Protocol (EAP), RFC2284, March 1998.

[5] IEEE Computer Society, IEEE MicrowaveTheory and Techniques Society, IEEE Standard for Local and Metropolitan Area Networks:Part

[6] Air Interface for Fixed Broadband Wireless Access Systems,IEEE Std 802 16-2004. 1 October 2004.

[7] L. Blunk, J. Vollbrecht, PPP Extensible Authentication Protocol (EAP), RFC 2284, March 1998

[8] B. Aboba, D. Simon, PPP EAP TLS Authentication Protocol, RFC 2716,October 1999.

[9] P. Funk, S. Blake-Wilson, EAP Tunneled TLS Authentication protocol version 1, February 2005.

[10] H. Andersson, S. Josefsson, G. Zorn, D. Simon, A. Parlekar, I-D ACTION: draft-josefsson-pppext-eap-tls-eap-tls-eap-04.txt: Protected EAP, IETF Draft, , September 2002.

[11] Securing Wireless LANs with PEAP and Passwords, Introduction:Choosing a Strategy for Wireless LAN Security, www.microsoft.com., April 2004.

[12] S. Convery, D. Miller, S. Sundaralingam: Cisco Systems, Cisco SAFE: WLAN security in Depth, White Paper.

[13] Interlink Networks, EAP Methods for Wireless Authentication, April 2003.

[14] J. Arrko, H. Haverinen, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key agreement (EAP–AKA), IETF Draft, June 2005.

[15] https://en.wikipedia.org/wiki/Authentication_protocol.