IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Volume-3, Issue-1 E-ISSN: 2347-2693

A Comparitive Analysis of EAP Authentication Mechanism for WLAN

Yogesh Singare[1*] and Manish Tembhurkar[2]

[1,2]*Department of Computer Science and Engineering G.H.R.C.E. , Nagpur, India*

www.ijcaonline.org

Received: 07January2015 Revised: 15 January2015 Accepted: 26 January2015 Published: 31 January2015

***Abstract*—** In recent years, WLANs have been developing rapidly and are increasingly being used in many applications. The extensive application of WLAN has been using an authentication framework widely called as Extensible Authentication Protocol (EAP). The requirements for EAP methods (i.e. Authentication mechanisms built on EAP) in WLAN authentication have been defined in RFC 4017 are issues also increasingly receiving widespread attention. To achieve user efficiency and robust security, lightweight computation and forward secrecy, not included in RFC 4017, are also desired in WLAN authentication. However, all EAP methods and authentication protocols designed for WLANs so far do not satisfy all of the above properties. With detailed analysis of all EAP Methods and authentication protocols designed for WLANs, this article pointed out properties of all EAP method.

***Keywords*—** EAP Method, Authentication, WLAN

I. INTRODUCTION

The Authentication is the process of verifying user's identities when they want to access resources from networks. Typically, a user provides his authentication factors to a server, and then the server verifies them. If the factors are correct, the user is authorized to gain the access right to the resources provided by the server, and the server generates a session-key material that is shared with the user. Similarly, it is also crucial for Wireless Local Area Networks (WLANs) to authenticate users and build secure channels with them. Presently, using IEEES02.lx authentication mechanism, the communication between client, authenticator and authentication server is accomplished via Extensible Authentication Protocol (EAP) [13]. EAP supports multiple authentication protocols, such as: Message Digest 5 (MD5), Transport Layer Security (TLS), Tunneled Transport Layer Security (TTLS), Lightweight Extensible Authentication Protocol (LEAP), Protected Extensible Authentication Protocol (PEAP), Secure Remote Password protocol (SRP) Privacy-preserving aggregation scheme (PARK) and Complete EAP Method, etc.

This paper analyzed the authentication process of all EAP Method and its comparison by properties of each EAP Method.

II. EAP PROTOCOLS

A. Message Digest 5 Protocol (EAP-MD5)[4][6]:

The RADIUS server conducts a simple authentication on the user's name and password encrypted by the MD5 algorithm. In this way, the server just checks the user names and passwords, without verification of the certificates or other information, and there is no need for key management and dynamic key generation. This authentication method is only able to verify the client not the server.

MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^{64}.

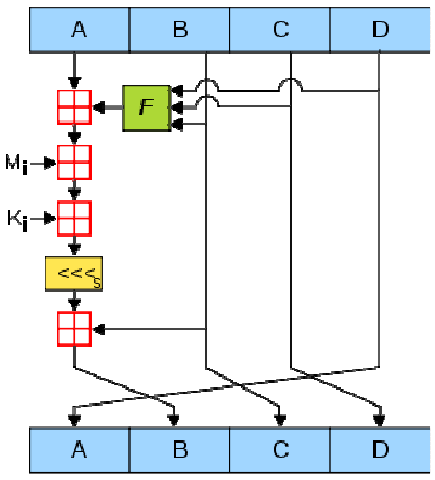

Figure 1: MD5 operation

Where:

F is a nonlinear function, is used in each round.
M_i denotes a 32-bit block of the message input.
K_i denotes a 32-bit constant, different for each operation.

$\lll_s$ denotes a left bit rotation by s places; s varies for each operation.
$\boxplus$ denotes addition modulo 2^{32}.

The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted *A*, *B*, *C*, and *D*. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function *F*, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions *F*; a different one is used in each round:

$$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B, C, D) = (B \wedge D) \vee = (C \wedge \neg D)$$
$$H(B, C, D) = B \oplus C \oplus D$$

$\oplus$, $\wedge$, $\vee$, $\neg$ denote the XOR, AND, OR and NOT operations respectively.

B. *Transport Layer Security Protocol (EAP-TLS) [15]:*

EAP-TLS [4] [10] was developed by Microsoft. It requests that both the client side and the server side install digital certificate based on X.S09 to provide dynamic session key distribution. During Certification, the client and the authentication server exchange certificate, carrying out mutual authentication, and then negotiate a session encryption key; the server will pass the key to AP, and notify AP to allow the client to access the network(Figure 2). EAP-TLS is of high safety, but requires the certificate must be installed in both the client and server side, thus requires higher management costs.

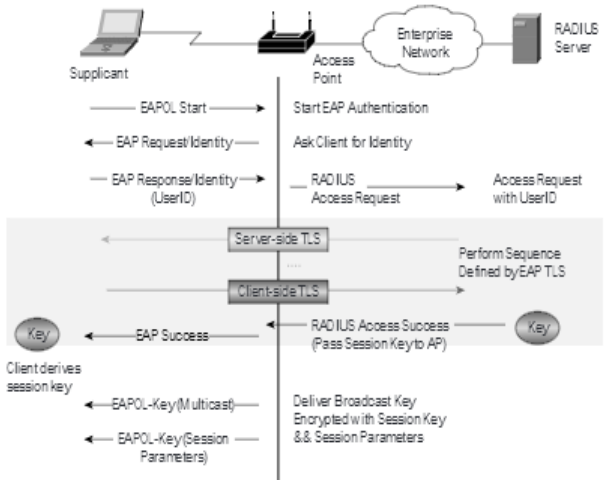

Figure 2: EAP-TLS Authentication

C. *Tunneled Transport Layer Security Protocol (EAP-TTLS) [4]:*

EAP-TTLS is a secure authentication method developed by Funk Company to solve the EAP-TLS certificate problem. The basic principle of EAP-TTLS is to provide authentication that is as strong as EAP-TLS, but it does not require that each user be issued a certificate. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel established based upon the server certificates.

1. After the authentication server determines that the user has made an authentication request, it sends its certificate to the user's system (Figure 3).

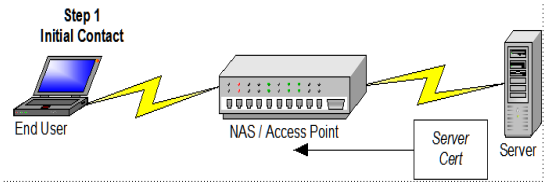

Figure 3: TTLS Server Certificate Sent to NAD

2. The authentication server's certificate is used to establish a tunnel between the user and the server (Figure 4).

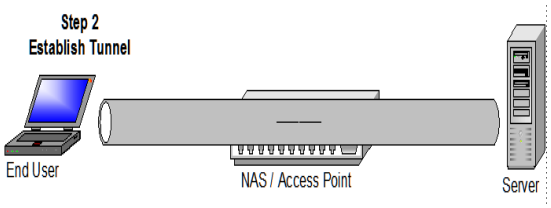

Figure 4: TTLS Tunnel Established

3. After the tunnel is established, credentials can be exchanged safely between the server and the user because tunnels encrypt all data in a secure fashion. This stage is called inner authentication (Figure 5).

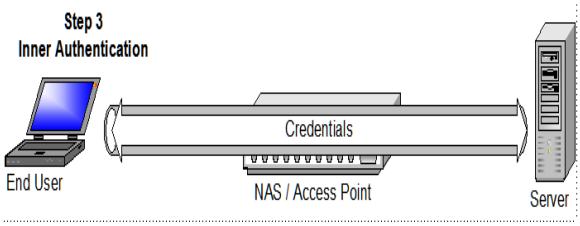

Figure 5: TTLS Inner Authentication

D. *Protected Extensible Authentication Protocol (EAP-PEAP)[14]:*

PEAP [4] is also through the "tunnel" between the client and the authentication server to achieve a two-step authentication process. Just like TTLS, PEAP only requires that the server side install digital certificates.

PEAP is of wide range of applications; Cisco, Microsoft, and RSA Security developed their own PEAP products.

E. Lightweight Extensible Authentication Protocol (LEAP)[4]:

LEAP, also known as the Cisco Wireless scalable protocol, is a new security technology based on WEP by the world's leading network equipment manufacturer Cisco. It is mainly used in the Cisco Aironet WLAN, and it enhances data encryption level by the use of dynamic WEP key, and achieves mutual authentication. Also LEAP is essentially an enhanced version of EAP-MD5 (since in the EAP authentication the EAP-MDS certification is the weakest in security, because it has only one-way authentication, and only supports static passwords). only adding a Dynamic Key Rotation and a mutual authentication. LEAP has its inherent weakness, and its password [5] has been proven to be broken within a few minutes; Compared with other authentication methods, EAP-TLS authentication, which requires installation of certificates both on the client and the server side, is much safer.

EAP-LEAP works like this:

1. The client sends a connection request message to an access point
2. The access point sends an EAP request for the client's identity.
3. The client sends an EAP response with identity information. The access point forwards the client's identity information in a RADIUS access request message to the RADIUS server.
4. The RADIUS server sends back a RADIUS access challenge, which is forwarded by the access point to the client as an EAP request.
5. The client returns an EAP response containing a hash of a password or other credentials with the challenge value to the access point. The access point forwards the information to the RADIUS server as a RADIUS access request.
6. The RADIUS server validates the client's credentials by generating a hash of the challenge value and the client's password and compares the results to the value forwarded by the client. If they match, the RADIUS server returns a success message to the access point, which relays the message to the client.
7. The client sends a challenge to the access point to authenticate the network. The access point sends back a hash of its credentials and the client's challenge value.
8. If the network is successfully authenticated, the client passes a success message through the access point to the RADIUS server, which sends an access-accept message to the access point.
9. The access point opens a connection for the client

F. Secure Remote Password Protocol (EAP-SRP) [12]:

It is one of the most used password-based authentication protocol. It provides a way to strongly authenticate a user without the usual risks of dictionary attacks faced by other password-based authentication schemes. In this protocol the password is neither stored as a plain text nor in a ciphered way. Instead, a verifier, obtained from the password through a one-way hash function, is stored. Another important characteristic of this authentication scheme is that the password is never sent across the network, thus avoiding that an intruder spoofs the network and retrieve the password or some information that could make possible a password reconstruction. During the authentication process, ephemeral public keys are exchanged between the server and the client and these keys are different for each authentication session. Another important SRP assumption is that a user can choose a "weak" password without impacting the strength of the authentication scheme. To perform the authentication a set of handshakes, between the server and the client must be accomplished.

G. Privacy-preserving aggregation scheme (PARK) [2]:

A privacy-preserving aggregation scheme (PARK) with the efficient and adaptive key management and revocation for smart grid. The PARK enables the aggregator to extract the statistical information from the aggregated data without learning anything else about the individual user. Furthermore, the encryption key for each user can be automatically updated according to the pre established bi-directional Hash chains. During the revocation, only the aggregators receive update keys from the control center so that the revocation cost is considerably reduced. The security analysis demonstrates that the PARK can extract the aggregated statistical data and preserve user privacy, while achieving forward and backward secrecy. PARK has a more efficient key management compared with other schemes.

H. Secure Services Client Protocol(EAP-SSC)[1]:

It was designed especially for the smart card environment in 2004. The method builds an EAP secured channel between a smart card and an authentication server in both asymmetric and symmetric key-exchange models. The computation is efficient, but it does not provide provable security and the security of forward secrecy.

I. Flexible Authentication via Secure Tunneling(EAP-FAST) [9]:

It is Cisco‘s response to LEAP‘s weaknesses and vulnerabilities. FAST is a hybrid authentication methods like TTLS and PEAP. While TTLS and PEAP require digital certificate for server authentication, the use of server certificates is optional in EAP-FAST. EAP-FAST employs a protected access credential (PAC). The PAC can be provisioned manually or dynamically in Phase 0 of EAP-FAST. EAP-FAST has three phases. Phase 0 is an optional phase. While in Phase 1 using the PAC, the client and the RADIUS server establish TLS tunnel, In Phase 2, the user information is sent by the client across the established

tunnel. The security provided by FAST basically depends on its implementation. If it is poorly implemented, the security level provided by FAST could be comparable to LEAP or even MD5 Although by using digital certificates at clients' machines, FAST provides maximum security but the problem will be the difficulty in the implementation and in this case FAST will not be easier to use than PEAP, TTLS or even TLS.

J. EAP-SPEKE, EAP-TLS-SEM, EAP-double-TLS, EAP-SRP [1]:

Table 1: The Comparison Table

EAP Methods	Mutual Authentication	Generation Of Session Key	Resistance To Dictionary Attacks	Resistance To Man-In-The-Middle Attacks	End-Reconnect	Fast Reconnect	Forward Secrecy	No Requirement For Certificate Maintenance	Provable Security	The Number Of EAP Request/Response Round Trips
MD5[4] [6]	N	N	N	N	N	N	N	Y	N	2
TLS[4] [10][15]	Y	Y	Y	Y	Y	Y	Y	N	N	4
TTLS[4]	Y	Y	Y	Y	Y	Y	Y	Y	N	5
PEAP[4][14]	Y	Y	Y	Y	Y	Y	Y	Y	N	7
LEAP[4] [5]	Y	Y	N	Y	N	N	Y	Y	N	4
FAST[9]	Y	Y	Y	Y	Y	Y	Y	Y	N	5
SPEKE[1]	Y	Y	Y	Y	N	N	Y	Y	N	3
TLS-SEM[1]	Y	Y	Y	Y	Y	Y	Y	Y	N	2
double-TLS[1]	Y	Y	Y	Y	Y	Y	Y	Y	N	6
SRP[12]	Y	Y	Y	Y	Y	Y	Y	Y	N	4
SSC[1]	Y	Y	Y	Y	N	N	N	N	N	2
Park[2]	Y	Y	Y	Y	N	N	N	Y	N	-
Complete EAP Method[1]	Y	Y	Y	Y	Y	Y	Y	Y	Y	2

Y: Yes
N: No

This EAP Methods are used the Diffie-Hellman key exchange to generate session keys, which provide mutual authentication and are also immune to man-in-the-middle attacks and dictionary attacks.

K. The complete EAP method [1]:

Its utilizes passwords and stored secrets to verify users, also use secure symmetric encryption schemes and hash functions to avoid exponentiation computations and to achieve security requirements without maintaining certificates. So that it can fully meet the requirements of RFC 4017, along with lightweight computation, and forward secrecy.

III. COMPARATIVE ANALYSIS

All EAP methods [1] [9] and authentication protocols designed for WLANs and its satisfied properties as shown in following table1 [8].

The comparison of all previous EAP methods authentication mechanisms for WLANs from the[1] viewpoints of the EAP method requirements defined in RFC 4017 and other key properties, including forward secrecy, and maintenance of certificates in Table 1, and also show the number of request/response trip comparison among the methods achieving all efficiency authentication properties.

The mandatory requirements: EAP-MD5 doesn't achieve both mutual authentication and session key generation. Besides, it is vulnerable to dictionary attacks and man-in-the-middle attacks [1] [11]. EAP-TLS, EAP-TTLS, EAP-PEAP,

and EAP-FAST are Certificate-based EAP methods; provide mutual authentication and session-key generation. These methods can withstand dictionary attacks and man-in-the-middle attacks.

EAP-LEAP has been shown to be vulnerable to dictionary attacks [7]. In addition, the symmetric-based methods, such as EAPSPEKE, EAP-TLS-SEM, EAP-double-TLS, EAP-SRP use the Diffie-Hellman key exchange to generate session keys, which is used to provide mutual authentication and are also immune to man-in-the-middle attacks and dictionary attacks. Besides, EAP-SSC, and the protocols of Park et al. are compliant with the mandatory requirements. Complete EAP method also satisfies the mandatory requirements defined in RFC 4017. End-user identity hiding, End-user identity hiding means that a user's identity is encrypted during the authentication processes. EAP-TTLS, EAP-PEAP, and EAP-FAST all create or establish secure tunnels after the server is authenticated by the client. After that the client is authenticated by the server using a legacy method via the secure tunnel. Because the user's identity is transmitted in the secure tunnel before any person is authenticated by the server, the user's identity is protected by encryption. Therefore, these EAP methods are able to hide the end-user identities. The user identities in EAP-SEM and EAP-double-TLS are also protected because they use TLS tunnels. EAP-MD5, EAPLEAP, EAP-SPEKE, and EAP-SSC don't provide identity privacy due to the lack of establishing secure tunnels. Complete EAP method provides identity privacy because the user identity UID is encrypted in the communication.

Fast reconnect; [1] certificate-based EAP methods support fast reconnections to improve performance. These methods quickly establish a connection between a client and a server. This capability can reduce the number of exchanged messages or trips. EAP-FAST, EAP-SEM, EAP-double TLS, and EAP-SRP are able to support fast reconnections and Complete EAP method also achieves this.

Forward secrecy [1], the protocols of Park et al. only support half forward secrecy. If adversaries know the long-term keying material on the side of client, the adversaries can compute the past session keys. Therefore, they only provide half forward secrecy. In addition, EAP-MD5 and EAP-SSC don't support forward secrecy. Maintenance of certificate, all of the certificate-based EAP methods rely on certificate authorities issuing certificates to the servers, but only EAP-TLS requires that all clients must apply the certificates. Each client must install a certificate on its device. This will greatly increase the cost of administration, and maintaining certificate revocation lists adds an additional heavy load. In symmetric-key based methods, AS can simply revoke the users by discarding the shared secrets. The number of EAP request/response round trips**,** EAP-MD5 only requires two EAP request/response round trips for authentication, but it does not achieve mutual authentication. EAP-TLS takes four EAP request/response round trips for authentication, but it requires that the certificates should be installed on the server and the clients. In EAP-TTLS and EAP-PEAP, it's unnecessary to install certificates on the clients, and after finishing server authentication using a TLS handshake, legacy EAP methods, such as EAP-MD5, is used to authenticate the clients. Therefore, EAP-TTLS and EAP-PEAP require five and seven EAP request/response round trips for authentication, respectively. EAP-LEAP performs the Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) twice for mutual authentication. Therefore, it requires four EAP request/response round trips. EAP-FAST adopts the TLS handshake to establish a tunnel key. Then the actual authentication uses MS-CHAP or One-Time Password (OTP). Therefore, EAP-FAST needs at least five EAP request/response round trips for authentication. EAPSPEKE contains three EAP request/response round trips. The protocol of Park et al. is not based on the EAP format. The Complete EAP method satisfies all of the properties with only two EAP request/response round trip.

IV. CONCLUSION

In this paper we presented all EAP Methods which are used on EAP framework, to provide authentication between client and server. All EAP Methods do not fulfill all requirements of RFC 4017 along with user efficiency, robust security, lightweight computation and forward secrecy, except Complete EAP Method. This paper also presents a solution on the basis of properties of each EAP Method to get an effective EAP Method on EAP, to provide authentication between client and server according to suitable environment.

REFERENCES

[1] Chun-I Fan, Yi-Hui Lin, and Ruei-Hau Hsu "*Complete EAP Method: User Efficient and Forward Secure Authentication Protocol for IEEE 802.11 Wireless LANs*" Ieee Transactions On Parallel And Distributed Systems, Vol. 24, No. 4, April 2013.

[2] Liang, Jian Qiao, and Xuemin (Sherman) Shen*," PARK: A Privacy-preserving Aggregation Scheme with Adaptive Key Management for Smart Grid",* 2nd IEEE/CIC International Conference on Communications in China (ICCC): QRS: QoS, Reliability and Security, 2013.

[3] Kamal Ali Alezabi, Fazirulhisyam Hashim, Shaiful Jahari Hashim and Borhanuddin M. Ali*," A New Tunnelled EAP based Authentication Method for WiMAX Networks",* IEEE 11th Malaysia International Conference on Communications, November 2013.

[4] Ling-wei Zhou, Sheng-ju Sang*," Analysis and Improvements of PEAP Protocol in WLAN",*

International Symposium On Information Technology IN Medicine and Education,2012.

[5] Ahmed M. El- Nagar, Dr. Ahmed A. Abd El-Hafez and Prof.Dr. Adel Elhna Wy*," A Novel EAP-Moderate Weight Extensible Authentication Protocol",*IEEE,2012.

[6] Xiaoling Zheng, Jidong Jin*," Research for the Application and Safety of MD5 Algorithm in Password Authentication",* 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD 2012),2012.

[7] DictionaryAttackonCiscoLEAP,http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml, 2012.

[8] Khidir M. Ali and Ali Al-Khalifah*," A Comparative Study of Authentication Methods for Wi-Fi Networks",* Third International Conference on Computational Intelligence, Communication Systems and Networks,2011.

[9] Alexandra Chiornita, Laura Gheorghe, Daniel Rosner*," A Practical Analysis of EAP Authentication Methods",* 9th RoEduNet IEEE International Conference ,2010.

[10] D. Simon, B. Aboba, and R. Hurst, *"The EAP-TLS Authentication Protocol",*RFC 5216, March 2008.

[11] H. Hwang, G. Jung, K. Sohn, and S. Park, "*A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using802.1X and EAP,*"Proc. Int'l Conf. Information Systems Security, pp. 164-170, 2008.

[12] Flávio O. Silva, João A. A. Pacheco, Pedro F. Rosa, Ph.D.*," A SRP Based Handler for Web Service Access Control"* IEEE International Conference on Services Computing (SCC'04),2004.

[13] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, *"Extensible Authentication Protocol (EAP)"*, RFC 3748, June 2004.

[14] A. Palekar, D. Simon, G. Zorn, J. SaloweY,H. Zhou, and S. Josefsson, *"Protected EAP Protocol (PEAP) Version 2",* work in progress, October 2004.

[15] Ma. Y. and Cao, X., (2003), *"How to use EAP-TLS Authentication in PWLAN Environment*", IEEE, Proceedings of the 2003 International conference on neural networks and signal processing, Volume 2, 14-17 Dec, Pages 1677-1680.

[16] Jitesh Zade,Manish Tembhurkar,"Voice Capacity Over wi-fi network",IJETED-2014.

