International Journal of Latest Trends in Engineering and Technology
Vol.(10)Issue(1), pp.207-211
DOI: http://dx.doi.org/10.21172/1.101.36
e-ISSN:2278-621X

A REVIEW OF 802.1X-EAP AUTHENTICATION FOR ENTERPRISE WLANS

Pawan Kumar[1]

Abstract: With the availability and popularity of lightweight, multifunctional, portable and highly efficient electronic gadgets, the use of wireless local area networks is increasing very rapidly. The need of availability and accessibility to the fresh information, always and everywhere irrespective of the geographic location has increased the demand and hence the development of network based applications. The wireless networking technologies provide its users mobility, flexibility, connectivity and scalability etc. Although wireless networking technologies have many advantages over its wired counterpart, on the other side these technologies have certain security issues also. One of the major security issues in the WLANs is user authentication, which is the main concern of the work presented in this paper. Many authentication and access control protocols for WLANs are available and are in use. In this work most recent and secure 802.1X authentication framework and its associated EAP methods are been studied. The analysis of popular EAP authentication methods used in WLANs have been done to understand the working mechanism, strengths and weaknesses of each method.
Keywords: Authentication, 802.1X, EAP, WLAN Security

1. INTRODUCTION

The market of Wi-Fi enabled gadgets has increased manifolds in the current decade and this trend seems to be continued in the years to come. Every network is supposed to provide certain security services to its users. The primary security services that any networking technology must provide to its users are the authentication, confidentiality, availability and integrity of information flowing over it. Despite the availability of many tools and technologies meant to achieve these security services, various security breaches have been reported time to time, which demands more focused investigation and hence improvements in these security mechanisms. Authentication is the core component of any network security system, it provides a way to get ensure the legitimacy of the user and/or device trying to access the services offered by the network. In the case of wireless networks the importance authentication becomes more vital, due to open and broadcasting nature of the channel. As it is not possible to physically restrict the signals from spreading in the vicinity of a wireless network, so the use of strong authentication mechanism is the only way to control the access to the network. The features and requirements of the authentication mechanisms that can be deployed in a WLAN environment are different from the authentication technologies used in wired counterpart.

2. AUTHENTICATION VULNERABILITIES IN WLANs

The security vulnerabilities associated with the WLANs can be broadly divided into three categories, which are Denial of Services (DoS) attacks, Unauthorized Access and Passive Monitoring. Many tools and techniques have been developed and are available to tackle these vulnerabilities. As this paper is mainly concerned with the authentication issues, so authentication vulnerabilities are covered in more detail here.

Denial of Service (DoS) Attack: The most recent WLAN security standard 802.11i addresses most of the issues related with the user authentication and data encryption. However, it does not protect the WLANs against Denial of Service (DoS) attacks. Major DoS attacks on WLANs include authentication request flooding, association request flooding, de-authentication flooding and disassociation flooding [4, 5]. These DoS attacks cause the entire WLAN or some of its wireless nodes to get out of service.

Authentication Spoofing: To understand this vulnerability, it is necessary to understand the shared key authentication (SKA) process. The client sends an authentication request to the Access Point. Then the Access Point sends the challenge text to client. Now the client encrypts the received challenge text using its pre-configured WEP key and sends it back to the Access Point as challenge response. The Access Point uses its stored WEP key to validate the response of challenge received from the client and then determine whether the client knows the shared secret key or not. After the validation step is over, the Access Point informs back to the client with a success or failure message.

The issue with Shared Key Authentication (SKA) authentication is that an adversary can sniff the entire negotiation process, he can get the challenge/plain text and its associated challenge response /cipher text. Then the adversary can derive the key

[1] Research Scholar, I.K.G.P.T.U. Jalandhar, Assistant Professor, M.G.D.A.V. College, Bathinda(Pb.)

stream, get authenticated with the Access Point, and can use the same key on the challenge text to prepare a valid challenge response. In this way, attacker can get the access to the network resources in an illegal way.

MAC Address Spoofing: Various Access Points have feature called MAC based access control, which allows or deny the client stations trying to get connected with the network based on their MAC address. This approach has two major flaws. It is very time-consuming process to configure or maintain the list of legitimate MAC addresses, thus can't be preferred method for big or middle size organizations. Another major issue with this method is the ease with which attackers can spoof their MAC addresses. Several 802.11 NIC drivers allow users to change their MAC address, so an attacker can easily steal and use a valid MAC addresses by the active network by sniffing.

3. WLAN AUTHENTICATION TECHNOLOGIES

It is important to understand that there is a distinction between being authenticated onto a wireless network and then having the traffic passed be encrypted. It is also possible to get authenticated in a network and then communicate using the open unencrypted traffic. In this section the commonly used authentication methods are discussed.

There are three main methods of authentication that are used in wireless LANs:

- Open Authentication
- Pre Shared Key (PSK) Authentication
- Port-Based Network Access Control or EAP Authentication

Open Authentication: This method is the most simple method and only requires that the end user device be aware of the Service-Set Identifier (SSID) used on the network, as long as the SSID is known then the device will be allowed onto the network. The problem with this method is that the SSID is generally broadcasted and if it is not so, it is easy to find this with the help of passive capturing techniques.

Shared Key Authentication: This method is commonly used by individual and small organization WLAN implementation, it uses a Pre-Shared Key (PSK) that is configured at both sides of the connection and if it matches then the device is allowed to access the services of the network.

Extensible Authentication Protocol (EAP): This method is the most popular method used by large enterprises, which is given in more detail in the next section. The EAP methods utilize the services of authentication servers for user authentication by using a variety of credential options.

4. 802.1x AUTHENTICATION FRAMEWORK

To enhance the security in IEEE 802.11 WLAN networks, the IEEE802.11i has been proposed, which uses 802.1x framework using EAP methods for providing the most secure means of user authentication in a flexible manner.802.1x provides a network access model, whereas EAP adds the various authentication methods to access the network.802.1x is a link layer protocol for providing the user authentication services in wireless networks. It protects the wireless network by denying access to the network until a user requesting access to the network is not successfully authenticated. The IEEE 802.1x is used in enterprise WLANs to guarantee authentication at the link level i.e. layer 2. In this way the port with which the client device is connected will stay in blocking state until the authentication is successfully completed. The 802.1x port access control prevents full access to the network services until authentication process completes successfully.

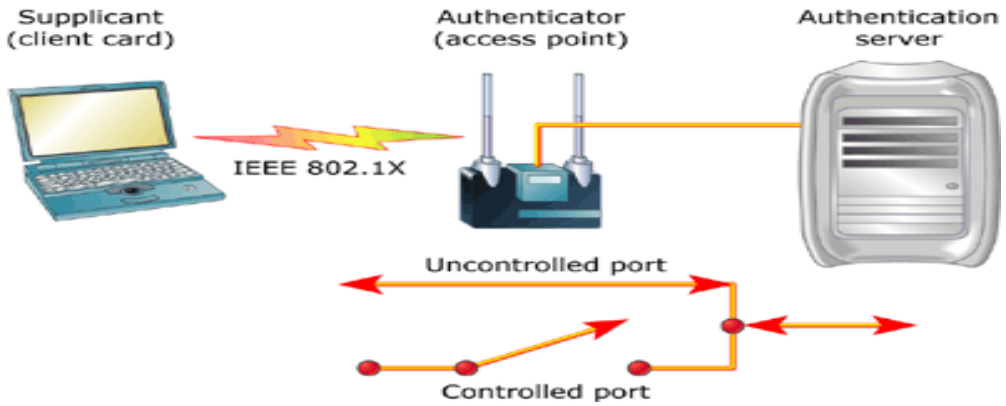

Figure 1.Communication through Uncontrolled Port during the Authentication Process.

The 802.1x authentication is a three party model for accomplishing the authentication process. These three parties involved in the authentication process are a supplicant (a client which is to be authenticated), Authenticator (an access point) and Authentication Server (a central decision making entity). This architecture provides a scalable solution with different encryption type support for supplicants, while centralizing the access control functionality to a few authentication servers. This feature makes 802.1x authentication manageable in big organizations.

As shown in the Figure 1 above, 802.1x uses the concept of two logical ports, uncontrolled port and controlled port. Prior to the successful authentication, the supplicant is allowed to interact by using only the uncontrolled port, and this port allows only the authentication request related traffic to pass through it. After the successful authentication of the supplicant, the controlled port is opened for the normal traffic. The services provided by the WLAN are accessible only through the controlled port, which only get opened after the successful authentication of client device i.e. supplicant completes successfully.
When EAP is run over a LAN, EAP packets are encapsulated by EAP over LAN (EAPOL) messages. The format of EAPOL packets is defined in the 802.1x specification. EAPOL communication occurs between the end-user station (supplicant) and the wireless access point (authenticator). The RADIUS protocol is used for communication between the authenticator and the RADIUS server as shown in the Figure 2 given under.

Figure 2. Protocols between Supplicant, Authenticator and Authentication Server during Authentication Process.

The authentication process begins when the end user attempts to connect to the WLAN. The authenticator receives the request and creates a virtual port with the supplicant. The authenticator acts as a proxy for the end user passing authentication information to and from the authentication server on its behalf. Authenticator passes the authentication credentials received from the supplicant to the authentication server. The authentication server refers to the user database stored on it to check and verify the validity of the authentication credentials and to determine the network access level of a valid user.
The authenticator limits traffic to authentication data to the server. A negotiation takes place between the client and the authentication server, which includes the following flow of messages:

- Client may send an EAP-start message.
- Access Point sends an EAP-request identity message back to the Client.
- Client's EAP-response packet with the client's identity is forwarded to the Authentication Server by the Authenticator.
- Authentication Server challenges the Client to prove itself and may send its own credentials to prove its identity to the client (when operating in mutual authentication mode).
- Client verifies the server's credentials (when operating in mutual authentication mode) and then sends its credentials to the Authentication Server for proving own identity.
- Authentication Server accepts or rejects the client's request for connection depending upon the authentication process results is failed or passed.
- If the Client is accepted, Authenticator changes the state of the virtual port for the Client to an authorized state by allowing network access to that end user.
- At the log-off, the Client virtual port is again changed back to the unauthorized state.

4.1 Extensible Authentication Protocol (EAP):
EAP was developed long back and primarily used in the point to point authentication (PPP), where clients were authenticated to a network using some EAP method. Today, EAP is commonly used in wireless networks for authentication. EAP is basically an authentication framework which supports multiple authentication methods. The EAP methods plug-in at both the client and the server, which provides the messaging system i.e. format in which authentication mechanisms like EAP-PEAP, EAP-TTLS, EAP-FAST, EAP-LEAP may operate.
For EAP clients and authentication server to support a novel EAP method the same EAP scheme library files needs to be installed and configured at both EAP client as well as at authenticating server. This extensibility feature of EAP to allow plug-ins that enables vendors to create the new authentication schemes as per the security requirements of the application. Therefore EAP provides the highest flexibility as compared to other authentication schemes.
EAP also allows two parties to exchange information that is specific to the authentication method they want to use. The content of these authentication-specific methods is not defined in EAP. In fact, they can be completely proprietary

authentication methods or newly invented ones. EAP's ability to handle part of the communication in a standardized way and part in a specific way, which is the key to its extensibility
IEEE 802.1x specifies a protocol called EAP over LAN (EAPoL) for transferring the EAP messages between the supplicant and the authenticator and another protocol named RADIUS (Remote Authentication User Dial-In Services) for the messages exchange between the authenticator and the authentication server.

5. WLAN STANDARDS & AUTHENTICATION TECHNOLOGIES

Authentication Mechanism in WEP: An access point must authenticate the client station before it can get associated with the access point or use services of the network. IEEE 802.11 standard defines two types of WEP authentication namely Open System Authentication and Shared Key Authentication.
•Open System Authentication allows the client device to access the network, by assuming that the client device's SSID (Service Set Identifier) matches the access point's SSID. Alternatively, client can use the "ANY" SSID option to associate with any available access point within range, irrespective of its SSID.
• Pre Shared Key (PSK) Authentication requires that client stations and access point have the same WEP key configured on both of these in advance for later authentication process.
WEP was the first form of authentication used with 802.11 WLAN. It proved easy to crack, hence other systems are now preferred more.
Authentication Mechanism in WPA/WPA2: In order to improve the flawed WEP system, the WPA access methodology was devised. In WPA standards user authentication is implemented using 802.1x and the EAP (Extensible Authentication Protocol) methods. Support for 802.1x authentication is required in WPA and WPA2. Which is the most secure, extensible, flexible and strong mechanism of mutual authentication.
The pre-shared key (PSK) which is also known as personal mode of WPA/WPA2 security is easier to configure than the enterprise mode. On the other hand enterprise mode of WPA/WPA2 security is more complex to set up and involves setting up a RADIUS (Remote Authentication Dial-In User Service) authentication server. This server is required for the 802.1X authentication. But it enables you to set unique usernames and passwords for WLAN users.

6. FEATURES OF 802.1X-EAP AUTHENTION FRAMEWORK

802.1x framework which can be used with a variety of EAP methods has many advantages as it posses many good and desired features. Some of the main features of it are given under:

- Flexible: Supports a variety of authentication mechanism ranging from simple passwords to the most sophisticated digital certificate, hence it provides flexibility in choice to the network administrators.
- Extensible: Better authentication schemes can be developed and added to the existing systems.
- Automatic Key Generation: Keys are derived and configured automatically after the authentication process is over successfully over.
- Centralized Policy Enforcement: This method is based on the management of the user database, which makes it manageable in big organizations.
- Mutual Authentication support between the Client and Network: It provides the mutual authentication between Client and Authentication Server. Software, which is required on the client to participate in the authentication process is called a supplicant and similarly software on the authentication server is referred as RADIUS (Remote User Dial-In User Services)
- Works with Variety of Encryption Algorithms: 802.1X can be deployed with multiple encryption algorithms, like WEP, WPA, TKIP or AES.

7. ISSUES IN EAP AUTHENTICATION

Presently 802.1x is strongest available authentication framework based on the port authentication. Though it has many features and advantages as described in the previous section, but on the other hand it has some security vulnerabilities associated with it. Some of the weaknesses of this framework are as under:

- Brute Force Attack on User Passwords: The enterprise mode of 802.1X is still susceptible to certain attacks. An attacker could potentially connect to enterprise-secured wireless network is by cracking the user passwords by launching the brute force dictionary attacks. Though not as simple as cracking WPA/WPA2 PSKs, but it is still possible with sophisticated tools.
- Incompatible and Weak Client Configuration: Some client devices don't support for configuring the strong authentication and validation settings at the authentication server. For providing the network access to employees having such kind of devices, sometimes it is required to lower the level authentication at the authentication server. But same action becomes an opportunity for an attacker for getting access to the network resources in an illegal way.

8. CONCLUSIONS

Presently 802.1x in association with EAP is the strongest authentication framework for deployment in WLAN. It provides a highly flexible mechanism for hosting authentication plug-in modules for current and future authentication methods. It supports a variety of EAP methods for varying level of application needs, which provides both flexibility as well as security. It needs continues improvements in order to handle the ongoing security concerns. Manufactures of modern Wi-Fi based client terminals must keep all authentication vulnerabilities in mind and should provide support for strong authentication methods in their devices.

9. REFERENCES

[1] Y. Zou, J. Zhu, X.Wang, L. Hanzo," A Survey on Wireless Security: Technical Challenges, Recent Advances and Future Trends",IEEE

[2] G. Raju and R. Akbani, "Authentication in wireless networks," Proceedings of the 40th Annual Hawaii International Conference on System Sciences, Hawaii, USA, January 2007.

[3] Lindemann, Rolf. "The evolution of authentication." ISSE 2013 Securing Electronic Business Processes. Springer Fachmedien Wiesbaden, 2013. 11-19.

[4] C. Liu, J. T.Yu, "Review and Analysis of Wireless LAN Security Attacks and Solutions", Journal of International Engineering Consortium, vol. 59, 2006.

[5] C. Liu, J. T.Yu, "An Analysis of DoS Attacks on Wireless LAN", IASTED International Conferences on Wireless Networks and Emerging Technologies (WNET2006), Banff, Canada, 2006.

[6] Ajah, Ifeyinwa Angela. "Evaluation of enhanced security solutions in 802.11-based networks." arXiv preprint arXiv:1409.2261 (2014).

[7] Ali, Khidir M., and Ali Al-Khlifa. "A comparative study of authentication methods for wi-fi networks." Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on. IEEE, 2011.

[8] Lei, Jun, et al. "Comparative studies on authentication and key exchange methods for 802.11 wireless LAN." computers & security 26.5 (2007): 401-409.