DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5928

ISSN No. 0976-5697

Volume 9, No. 2, March-April 2018

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# ISSUES AND CONCERNS IN ENTITY AUTHENTICATION IN WIRELESS LOCAL AREA NETWORKS (WLANS)

Pawan Kumar
Research Scholar I.K.G. P.T.U. Jalandhar (Punjab)
Assistant Professor, P.G. Deptt. of Computer Sc.,
D.A.V. College, Bathinda (Punjab)

***Abstract*:** Networking technologies have made the various computer services accessible and convenient for their users. In last one decade, the usage of sophisticated personal gadgets and Internet have increased manifolds, which in turn have changed the way of doing the official as well as personal activities. These gadgets are highly powerful and portable, and can be used for activities like communication, entertainment, business and banking etc. When the users access the personal or financial information via networks then various security issues may arise, so it is necessary for every online information system to provide its users certain security services like confidentiality, integrity, authenticity and availability. Authentication is a core component of every security model. As the security needs for accessing various online accounts are different and there exists different transmission technologies also, so a variety of authentication methods exists to provide the authentication services.

There exists no single authentication technology that can meet the diverse authentication requirements. The broadcasting nature of wireless networks makes them entirely different from their wired counterparts so, the authentication methods used in the wired networks can't be deployed directly in wireless networks. There are many authentication technologies, which have been devised and developed specifically for WLANs. In this paper study of various authentication methods used in WLANs have been done.

***Keywords***: WLAN Authentication, WEP, WPA, WPA2, 802.1X

## I. INTRODUCTION

The ICT (Information & Communication Technology) has facilitated its users with tremendous online services over the Internet. It has become an indispensable part in the life of every individual. The applications of ICT are augmenting in every sphere of our life. Companies are using the internet for transferring information faster and they are also coordinating their activities to achieve the speed and accuracy. E-commerce companies are using the internet to sell services and products online. There are a variety of online applications which facilitate the users to avail the services remotely, e-business, banking, governance, education, communication and many other sectors are the examples of it. On the other hand, these online services provided by the ICT have raised many security issues.

The key security aspects of any security sensitive include availability, authentication, authorization, data privacy and integrity. In an online system it becomes extremely important to verify the identity of an individual, who is requesting for the access to services. Authentication is a process of providing credentials to a system before getting access to the services offered by it. The credentials provided by the user are verified against the database of authorized users which resides either on a local system or in an authentication server. If the credential matches, the process is completed and the user is granted access. There is variety of authentication techniques which are used in WLANs to authenticate its users, ranging from very simple user-id and password to X.509 certificates. User-id and password based authentication is one of the most commonly deployed authentication technique, which is very simple and easy to deploy, but on the other hand if passwords are weak then it can be easily guessed by the adversary for getting illegal access to a system.

However, heavy flow of personal as well as financial information over the Internet leads to the need of more sophisticated and reliable entity authentication techniques. To avoid the attacks on the information a variety authentication techniques have been developed and are in use for providing the secure access to the legitimate users.
The structure of this paper is as: Section 2 describes the importance of Authentication, Authorization and Accounting (AAA) system in computer networks. Section 3 is about various commonly used authentication models. In section 4 we have described various authentication technologies and standard developed for the WLANs. Section 5covers the issues and attacks on WLANs. In section 6 we have listed the properties and features of EAP methods and section 7 draws the conclusions.

## II. IMPORTANCE OF AUTHENTICATION, AUTHORIZATION AND ACCOUNTING (AAA) SYSTEM

In the computer networking world, the term authentication means, the process of identifying a person or machine or some other device based on the credentials provided by it

[1]. As Internet has enabled its users to access all types of information and perform financial transactions online by initiating the request remotely. In this situation it becomes necessary for this system to provide Authentication, Authorization and Accounting services to its users, so that only legitimate users have access to the permitted resources only. An authentication mechanism prompts the user to provide its credentials, before providing the access to the requested data or information available in the system. After this these credentials are checked and verified against the database of legitimate users, if the credentials are found correct then user is provided access to the requested resources, otherwise the request is declined. The authorization system ensures that the users can access or perform operations only according to the access privileges granted to it by the system administrator. On the other hand the accounting subsystem is there to log each and every activity performed by the users in sufficient detail for handling the discrepancies and failures [1]. An intact AAA sub-system makes an online information system more reliable and secure.

## III. MODELS OF USER AUTHENTICATION

All the user authentication methods can be broadly divided into three categories, based on something you have, something you know and something you are [2].Token-based authentication, which is based on something you have normally uses some physical device such as a USB dongle or a smart card. Knowledge-based authentication, which is based on something you know, often uses a password, or it could involve a fact related to the user's life. Many users, who have used online banking system has likely been asked to set up the security questions such as Name of city where you were born or what is your father's middle name. Biometrics authentication is based on something you are, which can be further divided into physiological traits, like a fingerprint or retinal/iris scan, and behavioral traits, such as signature or a voice sample [3].

- **Transfer-of-Trust(ToT ) Model of Authentication:**

In this system Certificate Authority (CA) is an important entity that issues digital certificates to the communicating parties. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This makes other users to trust on the signatures and affirmations made about the private key that corresponds to the certified public key. A certificate authority acts as a trusted third party, which is trusted by both the owner of the certificate and by the party relying on the certificate. The format of these certificates is specified by the X.509 standard.

Main use for certificate authorities is to sign certificates used in HTTPS, which is the secure browsing protocol for the World Wide Web. Other important application of CA is in issuing certificates to devices that wish to access a secure enterprise WLAN that implements 802.1X authentication.

- **Third Party Authentication Model:**

In this fast-paced and busy world, sometimes user wish to surf a website for very short span of time, in this case asking a user who intends to spend only a few minutes on the website to sign up and create an account will not pleasurable experience for him. The user might just leave such a website and will find some other that doesn't require him to sign up for doing the same task. Now most of the websites have understood the reluctance of such users to create the new accounts. Keeping in mind the importance of such users, websites have started implementing the OAuth standard in their websites for getting their users authenticated.

OAuth is an open standard for the secure access delegation, which means it is a service that allows web giants like Facebook, Twitter, Google or Microsoft to permit its users to share their selected portion of information with third-party application and websites, while protecting the confidentiality of their information at the same time.

## IV. WLAN AUTHENTICATION TECHNOLOGIES AND STANDARDS

The WLAN technologies have developed gradually in last two decades. In the year 1997 IEEE ratified the original 802.11 standard. The Wireless Local Area Networks (WLANs) are based on the IEEE 802.11 series of MAC and Physical layer standards. These standards offers different data speed over the different range and uses different frequency bands. The most popular WLAN security standards are WEP, WPA and WPA2, all these security standards deploys one of the following authentication types to provide the authentication service to the network users.

- Open/ Null Authentication
- Shared Key Authentication
- Port based Authentication using EAP methods

The open authentication method is the simplest of all the methods and only requires that the end client device to be aware of the Service-Set Identifier (SSID) of the network. The SSID is a sequence of characters that uniquely identify a wireless local area network (WLAN). As long as the SSID is known to the client device, it will be allowed access to the network. The weak point of this method is that the SSID is broadcasted by the access points to show the presence of a network and if it is not, it is very easy to find it out with passive capturing techniques. This type of authentication is also known as null authentication, as it enables any client to authenticate to an access point. However, by enforcing it, it becomes possible for the access point to impose policy decisions, for example to impose the load constraint or to turn down particular client from using open authentication. This kind of authentication can be deployed for public WLANs like in hotels, coffee shops, airport lounges, and conference halls. Generally, the users use IPSec/VPN as solutions to connect to their corporate network. Hence, the open authentication in a WLAN is perfectly suitable as a connectivity mechanism.

Shared key authentication verifies that an authentication-initiating client has knowledge of a shared secret, assuming that the shared secret is delivered to the participating wireless clients by means of a secure channel that is other than the IEEE 802.11, but in practice, this shared secret is manually entered at the wireless access point and the

wireless clients [4]. The following messages are exchanged in the under given sequence when two devices use Shared Key Authentication:

- Client device sends an authentication request to the access point.
- Access point sends challenge text to the client station.
- Client device uses its shared key to encrypt the challenge text, and then it sends back the encrypted text to the access point.
- Access point decrypts the received encrypted text using its key that is configured corresponding to the client's key. After this access point compares the decrypted text with the original challenge text. Then after performing the comparison, if the decrypted text matches the original challenge text, then it means the access point and the client device possesses the same key, and the access point has successfully authenticated client device.
- Client device is granted access to the network.

The third authentication technique uses a three party authentication model by deploying the 802.1X authentication framework, which is an IEEE standard designed to provide port-based network access control. As described in [5], any authentication mechanism that involves a separate authentication server for client authentication is called 802.1X authentication. In this framework the three parties involved in the entire authentication process are: the supplicant, which is requesting access; the authenticator, which grants access and the authentication server, which grants permission.

802.1X operates by combining the two secure networking protocols Extensible Authentication Protocol (EAP) and Remote Authentication Dial-In User Service (RADIUS). This makes 802.1X more secure than the Pre Shared Key (PSK) based protocols, which require all users to share a password for getting access to the network [4][6]. EAP refers to the method or a type of 802.1X authentication, which is used by the authentication server and the wireless client for accomplishing the authentication process. An authentication server can authenticate a wireless client by using various EAP methods. These methods use different types of credentials to provide the one-way or mutual authentication. Some of the popular EAP methods includes: LEAP, PEAP, EAP-FAST, EAP-TLS and EAP-TTLS. These EAP methods uses different authentication mechanisms, such as user-id password, token cards, smart cards, X.509 certificates, one-time passwords, and public key encryption authentication. This is the most commonly deployed authentication protocol in enterprise WLANs [7].

These three authentication technologies are implemented in the various security protocols for providing the authentication services to users.

**WLAN Security Standards:**

The most popular WLAN security standards are WEP, WPA and WPA2.WEP was introduced as part of the original 802.11 standard ratified in 1997, with the goal to provide security services equivalent to that of a traditional wired network. It uses RC4 stream cipher for the encryption, CRC-32 checksum to provide the message integrity and a shared secret key for the user authentication.WEP is a least secure security standard, WEP broadcasts messages are much easier to crack, because every data packet is encrypted by using the same encryption key. If enough data packets are captured and analyzed by an eavesdropper, the key can be cracked with easily with the help of specialized software. WEP provides one way authentication, where only an access point authenticates a wireless client but reverse is not possible.

The WPA was released as an interim protocol due to the delay in the standardization process of IEEE 802.11i. It is a specialized security standard for WLANs, which implemented a subset of the draft of 802.11i. However, WPA2 is a complete and approved implementation of the 802.11i standard [8].

WPA uses TKIP (Temporal Key Integrity Protocol) as encryption standard, which in turn deploys the same encryption engine and RC4 algorithm used in the WEP. However, the key used for encryption in TKIP is 128 bits long, in comparison to the 64 bit static key used in the WEP. Another important strength of TKIP is that its changes the key after encrypting the each packet. TKIP encrypts each data packet using a unique encryption key [9]. To solve the message integrity issues with WEP, WPA uses an algorithm Michael, to calculate the message integrity check called MIC. Michael was better than the CRC method used in WEP for providing the message integrity. Michael implements a frame counter which helps to protect against replay attacks [10].

On the other hand WPA2 uses the most advanced AES-CCMP encryption, 802.1X as the authentication mechanism and CBC-MAC (Cipher Block Chaining Counter and Message Authenticity Check) technology for providing the data integrity

**Modes of WPA and WPA2:**

WPA and WPA2 standards can be deployed in two different modes as given under:

- **WPA/WPA2-Pre Shared Key (PSK):** This mode uses Pre-Shared Key for authentication and is mainly used for the small office or home WLANs.
- **WPA/WPA2–Enterprise:** In this mode, authentication is implemented by using the 802.1x framework and EAP methods for providing the one-way or mutual authentication.

## V. ISSUES AND ATTACKS ON WLANs

The ability to get connected with a network while roaming has great benefits. However, the risks to users of wireless technology have increased exponentially as these services have become more popular in financial and business sectors. As in the wireless networks data is transmitted through the broadcast radio technology, hence these networks are susceptible to some special type of attacks in addition to the security threats to the traditional wired network. The nature of radio signals makes them highly vulnerable and insecure, hence specialized defensive techniques need to be deployed

for implementing the confidentiality and integrity services in these networks.

**Common Attacks on WLANs:**

Various attacks against 802.11 WLAN and 802.1X can be categorized into four major groups:

- **Confidentiality Attacks:** These are the attacks launched by the adversary on the personal/secret information of the communicating parties with certain wrong intentions.
- **Integrity Attacks:** While performing such type of attacks, the adversary either tampers the contents of the original message or delays the message.
- **Authentication Attacks:** These types of attacks are carried out by stealing the credentials, keys, MAC address or IP address of the legitimate users/devices and later on at some other point of time adversary pretends to be the legitimate user to get access to the system. Examples of such attacks include spoofing, masquerading and session hijacking etc.
- **Availability Attacks*:*** Under this category of attacks, the adversary makes the network services unavailable to the legitimate users. Examples of such attacks are Denial-of-Services (DoS) and Flood attack.
- **Access Control Attacks:** An attacker performs such attacks `to gain entry into the network by exploiting some weakness or security hole in the network. Once the access is gained, adversary can launch several other types of attacks against the network.

In this paper, brief discussion of only authentication attacks is presented.

***WPA/WPA2 Pre-Shared Key Cracking:*** Attacker performs this attack by recovering the pre-shared key by capturing the handshake frames.

***Shared Key Cracking:*** This type of attack can be performed either by guessing the shared key or by using the vendor default WEP keys.

***Password Guessing***: Such attack is performed by stealing the user's identity and then by repeatedly trying the 802.1x authentication to get the user's correct credentials.

***Domain Login Cracking:*** Adversary launches such attack by recovering the user credentials by cracking the NetBIOS password hashes by applying either the brute-force or dictionary tool.

***Application Login Cracking:*** This kind of attack is made by stealing the user credentials by using certain sniffing tools.

***VPN Login Cracking:*** Attacker launches such kind of attacks by recovering the user credentials i.e. IPSec-PSK by using the brute-force attack on the VPN authentication protocols.

***User-Identity Stealing***: Under this attack the attacker steals the user identity from clear text 802.1X identity response packets.

***LEAP Cracking***: Adversary launches such attack by recovering the user's credentials from the captured LEAP packets and then by using the dictionary attack tool to crack the password.

***EAP Downgrading***: In this attack an adversary makes the RADIUS sever to offer weak type of authentication by forging the EAP response packets.

## VI. DESIRED PROPERTIES AND FEATURES OF WLAN AUTHENTICATION PROTOCOLS

For providing the strong authentication services to the enterprise WLAN users 802.1X authentication framework with EAP methods was developed and standardized by the IEEE workgroup.EAP authentication methods must possess certain desirable properties and features. For providing the secure and efficient authentication services to its users some important properties and features are being identified by the researchers. These properties and features are categorized into three major groups. In the first group, properties which are mandatory for the EAP authentication methods are kept. Second group contains the properties which are recommended for authentication methods and the third group is having the additional operational requirements [11].

**Group I: Mandatory Requirements**

*(i)Support for Mutual Authentication*
*(ii) Credential Protection*
*(iii) Resistant to Man- in- the- Middle Attack*
*(iv)Protection against Dictionary attack*
*(v)Resistant to Replay Attack*
*(vi)Resistant to Forgery Attack*
*(vii)Strong Session Keys Generation Capability*

**Group II: Recommended Requirements**
*(i)User Authentication*
*(ii) Public Verifiability*
*(iii)Channel Authentication*

**Group III: Desired operational Properties and features**
*(i)Less Computational Overhead*
*(ii)Easy to Implement*
*(iii)Rapid Reconnection*

Different EAP methods like EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-FAST and EAP-PSK etc., which fulfills almost all the mandatory requirements mentioned in group one but they partially fulfills the properties and features recommended in group 2 and 3, for balancing the tradeoff among the application security and efficiency requirements.

## VII.CONCLUSIONS

Which authentication method is best? It depends upon the primary security concerns and requirements of an

organization. Carefully selecting a solution is an important part of strategy. Like any other important decisions one has to choose among flexibility, simplicity, efficiency and security needs of the organization. There exists no single authentication approach which fits all the applications running in the WLAN environment [12]. There is a tradeoff among the, what is needed and what is to be paid for it. Some important points are identified and given under, keeping which in mind one can choose the most suitable alternative out of the available ones.

- Level of security needed for the application in question.
- Available hardware and software.
- Additional resources required for implementing the better and secure authentication technology.
- Availability of Technical support required for implementing and maintaining the better secure solutions.
- Cost of moving from existing to better alternative solution.

By doing the cost -benefit analysis of the available alternatives the decision can be made regarding which alternative will be most suitable for the organization.

## VIII. REFERENCES

[1]. R. Havighurst, "User identification and authentication concepts." ,pp. 2-45, (2007)

[2]. D.Gibson, "Understanding the three factors of authentication." Pearson IT certification, (2011)

[3]. A. Babich, "Biometric Authentication. Types of biometric identifiers", pp. 6- 49(2012).

[4]. J.Vollbrecht and R. Moskowitz "Wireless LAN access control and authentication", Ann Arbor,1001, p.48108 (2002).

[5]. J. Snyder, "What is 802.1 x?" Network World Fusion 6, (2002)

[6]. A. Sari and M. Karay , "Comparative analysis of wireless security protocols: WEP vs WPA", International Journal of Communications, Network and System Sciences 8 no.12, p.483(2015).

[7]. J.C. Chen and Y.P. Wang "Extensible authentication protocol (EAP) and IEEE 802.1 x: tutorial and empirical experience", IEEE communications magazine 43 no.12, supl-26, (2005)

[8]. V. Kumkar, A. Tiwari, P. Tiwari, A. Gupta and S. Shrawne, "Vulnerabilities of wireless security protocols (WEP and WPA2)", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) 1 no. 2, pp.34-38, (2012)

[9]. S. Malgaonkar, R. Patil, A. Rai and A. Singh, "Research on Wi-Fi Security Protocols" International Journal of Computer Applications 164 no.3, pp.30-36, (2017).

[10]. R. Lindemann. "The evolution of authentication." ISSE 2013 Securing Electronic Business Processes. Springer Fachmedien Wiesbaden, pp. 11-19,( 2013)

[11]. D. Stanley, J. Walke & B. Aboba, "Extensible authentication protocol (EAP) method requirements for wireless LANs ",No. RFC 4017, (2005).

[12]. Y. Zou, J. Zhu, X.Wang and L. Hanzo," A survey on wireless security: technical challenges, recent advances and future trends", Proceedings of the IEEE 104.9 pp. 1727-1765 , (2016)