International Journal of Latest Research in Engineering and Technology (IJLRET)
ISSN: 2454-5031
www.ijlret.com || Volume 02 - Issue 08 || August 2016 || PP. 94-99

A Survey on Wireless Security Standards and Future Scope

Nagesha AG[1], Gowri Shankar[2]

[1]*Research Scholar, Department of Computer Science & Engg., BMS College of Engg., & Associate Professor,*
Department of Computer Science &Engg.
Acharya Institute of Technology
Bangalore, INDIA
[2] *Professor & HoD, Department of Information Science & Engg.*
BMS College of Engineering
Bangalore, INDIA

Abstract: In today's unsecured IT world providing security over a network is very important, security plays a vital role as communication happens through internet and it is quite complicated. Unauthorized user may misuse or modify the network content and its configuration. Thus, providing security over the network is the main role of network Engineers. Therefore, providing security to wired and wireless networks are the two main concepts evolving from many decades. Henceforth, guaranteeing the security in communication is the main need of the network system. Therefore, the focus of this paper is to bring out the different categories of network, security standards, and security in wireless network, advantages, and disadvantages of wired and wireless networks. Also this paper gives an insight into Protocol for carrying Authentication for Network Access (PANA).

Keywords: Network, Communication, Protocol, PANA, Wired, Wireless

I. INTRODUCTION

Authentication policies are adopted to avoid unauthorized access, misuse, modification, denial of network services and other resources of network. Network administrator controls the authorization of access to data in a network. Network security plays an important role in daily life; bank transactions, communication in various fields, several agencies and individuals. Wireless networks allow the user to connect computer systems to network or the internet and it doesn't require network to be physically attached with computers. Since, it is necessary to have an access to network according to user convenience and process, security need to be tightened. In this direction several techniques were introduced to avoid the security threats, and those methods were re-placed by the advanced methods. This promoted the development of wireless network security.

The main intend of this paper is to give overall view of different methods used for security purpose and the protocols available in the market to avoid threats. This paper discusses; evolution of security standards in the wireless LANs, WAN 802.16 protocol and other security schemes. In addition to the above it is also noted that, the advantages and disadvantages of wired and wireless networks. Therefore, in order to provide security in today's networks, it is very important to have idea about both the wired and wireless networks. Recent works on wireless network security helps the developers to know the current position of the system. Wireless networks generally adopt the OSI protocol architecture [1] comprising the application layer, transport layer, network layer [2], MAC layer [3] and physical layer [4],[5].

II. OVERVIEW

This section presents detailed description on security and wireless communication.

Network security is protection of the access to files and Network security is protection of access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system. Thus, IMT-Advance is considered as the specificationfor4Gwireless and the objective of IMT Advance is that, 4G wireless technology must support the following:

- **Mobility support at high speeds**

Several broadband wireless access technologies have been developed however, only LTE developed by 3GPP and Wi MAX developed by IEEE 802.16 got the characteristics for 4G wireless technology [7].

- **Security aspects**

A. Authentication: Authentication is a process of providing network access to authorized users only. The goal of authentication is to compare the dataset of authorized users against the information stored in the systems. Further, the user is provided with the system access through key or other access methods as well authentication is part of security in which it is different from authorization. A uthorization is the process of providing permission to users based on privileges set during network setup.

B. Data Confidentiality: Data confidentiality is the property used in networks to maintain secrecy of data, communication and other information of users, as privacy of personal information is very crucial in business organization.

C. Data Integrity: Data integrity is the service provided, where unauthorized user cannot alter the transmitting data from sender to receiver knowing the origin of sender. Some of the examples for violation of integrity are; modification of w ebsite, e-commerce transactions etc., were altered or intercepted, therefore electronically stored records are modified using different methods.

D. Availability: The accessibility of the data for users can be measured using availability. Here is an example for the availability of the network data that is an unhandled exception error faced by the networked device when the providers end an improperly formatted data. The huge amount of traffic or requests is sent to network makes system accessibility more complex.

E. Non-Repudiation: The non-repudiation function implies that, both sender and the receiver cannot falsely deny claiming that, they have sent message. This will take two forms; with proof of origin of data and the recipient of data. The many schemes used for encryption constitute the area of study known as cryptography.

- **Security Mechanisms**:

A. Encipherment mechanism: An original message is known as the plain text, while the coded message is called as cipher text. The process of converting plain text to cipher text is known as enciphering or encryption; restoring the plain text from the cipher text is deciphering or decryption. Such a scheme is known as a cryptographic system or a cipher. Techniques used for deciphering a message without the knowledge of enciphering details fall into the area of crypt analysis. Crypt analysis is in terms of laymen view is breaking code. Theare as of cryptography and crypt analysis together are called cryptology.

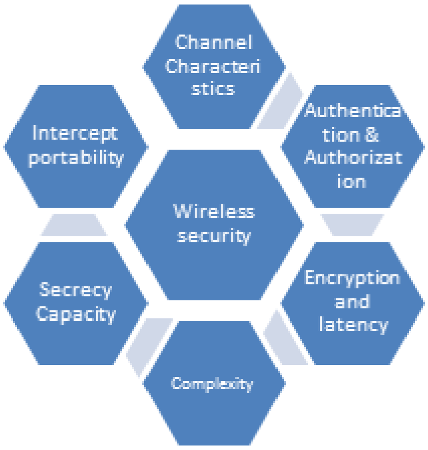

Figure.1: Wireless security methodology and design

B. Digital Signature: Digital signature is the electronic code which is generated and authenticated by public key encryption. To verify the content of the transmitted document and the sender’s identity, digital signature is attached to the electronically transmitted document.

C. Access Control Mechanism: The firewalls and operating system access privileges are access control mechanism in corporated to provide services in regard to access user information.

D. Traffic Padding Mechanism: The exchanged communication is protected by security mechanisms and many protocols in which individuals padding mechanism provides protection from traffic analysis attacks.
E. The Routing and Control Mechanism: The communication data is allowed with selection of specific route. The routes may be dynamic or static in nature.

F. Notarization Mechanism: The integrity of data for source and destination in transmission process are assured in notarization mechanism. Security of Wireless network design depends on number of factors as depicted as in Figure.1.

III. 802.11STANDARDANDSECURITY

The set of security features are involved to provide security to a wireless network. In order to control the access an AP (Access Point) and SSID (Service Set Identifier) are used. Therefore, to prevent unauthorized users from network access ACL (Access Control List) and to provide data security WEP (Wired Equivalent Privacy) is used.

Service Set Identifier (SSID) It is a name given to wireless local area network (WLAN). SSID is a 32 bit alphanumeric characters used to set identifiers and it is unique in its nature and attached to the header of packets that transmits over a WAN. Sometimes SSID is referred as network name and it is difficult to connect a particular network when numbers of independent networks are operated in the same physical area.

The SSID makes the station easy to connect with specific network. BSS (Basic Services Set), BSS is used to communicate directly with wireless devices. The logical WLAN called as an ESS (Extended Service Set) is formed of number of BSS, each ESS is provided with SSID name. Every access point (AP) broadcasts beacon frames several times per second that contains the SSID , by these frames stations can discover the APs of particular network and the stations can send probe frames to search AP of desired SSID. In this way communication takes place between APs and network stations. The broadcast SSID are permitted with a null or zero length SSID. An access to an access point (AP) is denied if the wireless network station doesn't know the SSID value. The security is provided through SSID as a password when a computer is connected to the access point.

Appropriate SSID can be set by an external user, because SSID can be easily shared. Any client in a broadcast be enabled to access to the access point without having SSID. Thus for hackers it is easy to obtain an access points SSID and accesses the network through different software tools with no hurdles. Using the configured SSID, an SSID has any i.e., even blank SSID access points that can be connected by the clients if a non-secure access WLAN mode exists.

ACL (Access Control List): A set of commands combined together by a number or name are called Access Control List. In order to control the signals over an interface an Access Control List is required. However, to control the signals on an interface, one must specify the direction also of which the traffic should be controlled. The traffic that comes into an interface is called Inbound and the traffic that exists from an interface is called Outbound. , As in the definition, Access control lists might of numbers or names. There are two types of filtering in ACL such as standard filtering and extended filtering. Source IP address in a packet can be filtered by standard IP ACLs. Both source and destination. However, IP address in a packet can also be filtered by extended IP by permitting or denying. Permitting and denying actions of ACLs needs an order of statements and it is essential because when a match is found, next statements is not processed. The implicit deny statement is placed at the end of the ACL and drops the packet, if there were no matches. Explicitly denying statement leads to traffic and packet get dropped, therefore, at least one permit should present at an ACL.

Vulnerabilities of ACL : On the basis of MAC address filtering the process of restricting the access for authorized users through ACL is an optional feature. The attacker can identify the authorized MAC address because packet sniffer are visible to MAC address. By using one of the MAC address the attacker will come to know the authorization to access the network.

WEP (Wired Equivalent Privacy): To encrypt the transmitted data, wireless network needs a security protocol called Wired Equivalent Privacy (WEP). In case of wireless LAN confidentiality , availability and integrity are achieved by WEP. There are several flaws in the WEP algorithm that affects the security of the system. The types of attacks occurring in wireless LAN are, Passive attacks and Active attacks.

Passive attack is used to decrypt traffic, and Active attacks are to decrypt traffic on the basis of tricking access point. Active attacks will generate huge traffic from unauthorized stations based on known plaintext. Dictionary-building attack, allows automated decryption of all traffic.

Encryption process is used to provide security by WEP. Further , client and the access point encryption process takes place only after packet transfers after the wired LAN (WLAN). In WEP packet encryption integrity check (IC) value is computed and it is attached to the payload. Subsequently, payload is get XORed with wired equivalent privacy key and initialization vector. Thereafter, the packet is moved with IV values sent in plain text. Wired equivalent privacy uses the cyclic redundancy checking (CRC) algorithm and RC4 algorithm for message integrity, the same process is inverted at the receiver side for the decryption of the message resulting a message decryption.

WEP Vulnerabilities: The major problem with wired equivalent privacy is authentication and encryption. The integrity check vector initialization and RC4 are faced with security problem. The secret keys shared for the encryption and decryption of the message cannot be changed. The RC4 algorithm can not applicable for all kinds of attacks. Henceforth, it is possible for the attackers to collect more information during the IV collision because two devices which are in the same network which are connecting at the same time may have the same value. Since the CRC-32 is a linear hash, attackers can easily correct the checksum value and can reach the destination.

- **802.1X**

802.1X is a protocol that provides security and it works in associated with 802.11g and 802.11b and wired devices in wireless networks. Extensible authentication protocol (EAP) is the extension protocol of point to point protocol (PPP) and 802.1X is the extension and works on the basis of EAP. Therefore without using any underlying protocols, 802.1X serves for the authenticating users to physical network. Other authentication techniques such as Token cards, one-time passwords certificates, Kerberos and public key authentications were also supported by 802.1X protocol.

- **802.11I**

This protocol is the improved version of 802.11 standards in authentication data transfer and integrity. There are mainly two security upgrades are available in this protocol. They are Wi-Fi Protocol Access (WPA) and Robust Security Network (RSN). In WEP protocol the process of adoption of wireless LANs in many corporations has been delayed. By considering security of the network exposed by WLANs must be treated as an access network instead of treating as core enterprise network. The network may or may not use a 802.1X protocol or RADIUS for additional authentication, because when a user connected to a LAN switch or hub, it assumes that they are the trusted users.

- **Wi-Fi Protected Access (WPA)**

The users of computers with wireless Wi-Fi connection use the security standard of WPA. WPA was released in April 2003. Further an algorithm was developed to fulfill the needs of huge demand of communication network enterprises. In this direction an algorithm called Michael was developed to calculate a 8-byte integrity check called Message Integrity code (MIC) which is different from cyclic Redundancy Check (CRC) method and it helps in security of replay attacks.

Furthermore, TKIP, CCMP and WRAP are the three protocols of 802.11i and were used to solve the integrity problems. TKIP (Temporal Key Integrity Management), In this protocol there is no need to update the hardware of the device to run. Hence it is called as a band aid solution per packet key mixing, message integrity check and re-keying mechanism are also provided by TKIP. Backward compatibility is the main feature of TKIP.

The research has progressed towards the development of WRAP (Wireless Robust Authenticated Protocol) to gain AES encryption features and enhance WRAP protocol. Although WRAP was popular some issues occurred in regard to intellectual property and to overcome this problem CCMP was introduced. With the introduction of CCMP (Counter with Cipher Block Chaining Message Authentication Code Protocol) secure protocol in 801.11i i.e., AES is upgraded to support the new encryption algorithm.

The first paragraph under each heading or subheading should be flush left, and subsequent paragraphs should have a five-space indentation. A colon is inserted before an equation is presented, but there is no punctuation following the equation. All equations are numbered and referred to in the text solely by a number enclosed in a round bracket (i.e., (3) reads as "equation 3"). Ensure that any miscellaneous numbering system you use in your paper cannot be confused with a reference [4] or an equation (3) designation.

IV. Robust Security Network (RSN)

The issues with mobile devices and access points is encryption, authentication and it can be negotiated using RSN. This is evolved for the reason of security and adding algorithms to new threats and provides security to WLANs information. RNS is very strongerthan WEP and WPA but it is not efficient to apply over legacy systems. Particular hardware is required to apply algorithms in clients and access points.

WIRELESS SECURITY VS WIRED SECURITY

Wired and wireless are the two different methods of security system.

Advantages of wired security method are,
(i) Requires less cost for configuration of system.
(ii)No batteries required in wired security system.

Disadvantages of wired security method are,
(i) Not portable, hence it is difficult to use outside.
(ii) Good knowledge is mandatory to configure and install the system.

Advantages of Wireless security system.
(i) The installation of the system is very easy and quick.
(ii) This system is portable.

Disadvantages of Wireless security system.
(i)Wireless security systems need costly equipment than the wired security.

V. RECENT PROPOSALS

This section provides recent work in the field of wireless network security protocol. The PANA (Protocol for Carrying Authentication of Network Security) is a protocol used to provide authorization between client and AAA servers.

PANA is an IP based protocol and provides access to network through own authentication, EAP will be used for authentication of new protocol, key distribution, key agreement or key derivation of protocols. EAP payload was carried by PANA. PANA is independent from the link layer mechanisms and it allows the process of service provider selection, allows different authentication methods.

ELEMENTS of PANA are,

i) PaC(PANA client) is located in the node and it is the client part of the protocol.

ii) PAA(PANA Authentication Agent), this is the server part of the protocol. The communication in the network with PaC is the main work of this agent. Addition to this, message exchange takes place between the AAA server.

iii) iii)AS(Authentication server),To check the credentials of PaC ,AS is used, through PAA it receives PaCs credential. This contains the information about the IP configuration and access parameters.

iv) EP(Enforcement Point),it acts as a filter to the packets as an authentication PaC. If the authentication features doesn't match the packets then packets will be dropped. It acts as a access point or a router. If the parameters matched with the authentication values, a key is installed in EP and PaC and established a session between Pac an EP.

VI. CONCLUSION

Security is the basic need of network communication. Wired and Wireless security are two types of the network security, where wireless security over a network is more flexible and efficient. Security involves several goals for network communication to satisfy users, which involves several security mechanisms. To protect the computer system from unauthorized users network security is needed. Security standards of 802.11, 802.1x, 802.11i are discussed in detail with the concepts involved. Therefore, for authenticated data transfer and integrity of data TKIP, WRAP and CCMP are the best protocols in 802.11i standard. There are several pros and cons associated with wired and wireless security communication. Hence, by considering disadvantages and recent works on wireless security more works need to be done in future to provide the user with secure network.

REFERENCES

[1]. Y. Leo, M. Kai, and A. Liu, ”A comparative study of WiMAX and LTE as the next generation mobile enterprise network,” in Advanced Communication Technology (ICACT), 2011 13th International Conference on, 2011, pp. 654-658.

[2]. H. Chin-Tser and J. M. Chang ”Responding to Security Issues in MAX Networks,” IT Professional. 10, no. 5, pp. 15-21, 2008.

[3]. M. M. Rashid, E. Hossain, and V. K. Bhargava, Cross-layer analysis of downlink V-BLAST MIMO transmission exploiting multiuser diversity, IEEE Trans. Wireless Commun., vol. 8, no. 9, pp. 45684579, Sep. 2009.

[4]. F. Foukalas, V. Gazis, and N. Alonistioti, Cross-layer design pro- posals for wireless mobile networks: A survey and taxonomy, IEEE Commun. Surv. Tut., vol. 10, no. 1, pp. 7085, Apr. 2008.

[5]. R. Jurdak, C. Lopes, and P. Baldi, A survey,classification and com- parative analysis of medium access control protocols for ad hoc networks, IEEE Commun. Surv. Tut.,vol. 6, no. 1, pp. 216, Apr. 2004.

[6]. M. Takai, J. Martin, and R. Bagrodia,Effects of wireless physical layer modeling in mobile ad hoc networks, in Proc. 2nd ACM Int. Symp. Mobile Ad Hoc Netw.Comput., Long Beach, CA, USA, Sep.2001, pp. 8794.

[7]. C. Saradhi and S. Subramaniam, Physical layer impairment aware routing (PLIAR) in WDM optical networks: Issues and challenges, IEEE Commun. Surv. Tut., vol. 11, no. 4, pp. 109130, Dec. 2009.

[8]. Y. Leo, M. Kai, and A. Liu, ”A comparative study of WiMAX and LTE as the next generation mobile enterprise network,” in Advanced Communication Technology (ICACT), 2011 13th International Conference on, 2011, pp. 654-658.

[9]. H. Chin-Tser and J. M. Chang ”Responding to Security Issues in WiMAX Networks,” IT Professional. 10, no. 5, pp. 15-21, 2008.