International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 5, Issue 6, June 2016)

Review on LAN Security

Monika[1], Savita Bisnoi[2]

[1]M. Tech Scholar, [2]Associate Professor, CSE Dept, RIEM, Rohtak, MDU University Rohtak, India

Abstract: - **Wireless Local Area Networks (WLANs) are cost effective and desirable gateways to mobile computing. They allow computers to be mobile, cable less and communicate with speeds close to the speeds of wired LANs but can't achieve same speed. So wired network is always best in case of speed of transfer data. These features came with expensive price to pay in areas of security of the network. The functions performed by a client and a server are complementary and can be implemented by a set of software modules, hardware components, or a combination thereof. Client and/or server runs on dedicated separate machines. This paper identifies and summarizes these security concerns and their solutions.**

Keyword: **LAN, Client-server, Security issue**

I. Introduction

An access point must authenticate a station before the station communicates with the network. The IEEE 802.11 standard defines two types of WEP authentication: Open System and Shared Key. There are two other mechanisms: the Service Set Identifier (SSID) and authentication by client Media Access Control (MAC) address—are also commonly used. Open System Authentication allows any device to join the network. The 802.11 client authentication process consists of the following transactions:

1. *Probe request:* Client broadcasts a probe request frame on every channel.
2. *Probe Response:* Access points within range respond with a probe response frame. Open and shared key Authentication: Once the client determines the optimal access point to connect to, it moves to the authentication phase of 802.11 network access which is of two types Open Authentication and Shared key Authentication.
3. *Authentication request:* The client decides which access point (AP) is the best for access and sends an authentication request
4. *Authentication Response:* The access point will send an authentication reply
5. *Association request:* Upon successful authentication, the client will send an association request frame to the access point
6. *Association response:* The access point will reply with an association response
7. The client is now able to pass traffic to the access point

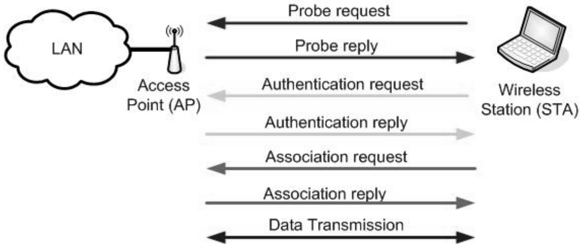

Fig. 1: The three phases undergone through LAN for the establishment of connections between STAs and AP.

II. Wired Equivalent Privacy

WEP-40(40-bit key) is defined as a means of protecting the confidentiality of data exchanged among authorized users of a WLAN from casual eavesdropping. The same algorithms have been widely used with a 104-bit key instead of a 40-bit key, this is called WEP-104. WEP security involves two parts, Authentication and Encryption. Authentication in WEP involves authenticating a device when it first joins the LAN. The authentication process in the wireless networks using WEP is to prevent devices/stations joining the network unless they know the WEP key [1].

Many Papers have been published relating to security methods of Pre-RSNA discussing the Wireless LAN 802.11 network security including the comparisons of SSIDs, MAC address filtering and the WEP key encryption. Various simulative platform of software and hardware is designed to crack WEP key based on these authentication methods and analyzing the weaknesses of WEP and RC4, It has been shown that WEP Key can be cracked including SSID enumeration, MAC address spoofing and WEP key cracking by FMS (Fluhrer, Mantin, Shamir) Attack [2].

III. Survey

The article describes how to apply the flaw in breaking WEP and concludes that the protocol also referred to as 802.11b WEP standard by the Institute of Electrical and Electronic Engineers Inc, is not secure.

Information from this article will help us support our research proposal that suggests current WEP problems which are still being experienced as WEP is still widely being applied by organizations and home users make the use of WEP a threat to the integrity of confidential data held on any network using it as their protocol [3].

The article suggests that it was for these reasons that the IEEE developed the 802.11i Standard in order to boost confidentiality, integrity, and mutual authentication between the keys and thus develop good key management practices. Information from this article will be used to support the research proposal that suggests current WEP protocol is inadequate to in maintaining the security of the wireless networks as it can be easily breached by unauthorized persons; [4].

Information from this article will help us produce a more credible research proposal as it objects to the common notion that the WEP protocol is not suitable for wireless technology. We noted that the journal dated back to 2002, which could have been a reason for their opinion, however the study will take on board what has been said [5].

The study also suggests that by disposing interface identifiers a user's location is kept secret and gave example of how an experiment using an analysis of a public WLAN has already shown this theory to be true. The study supports what was said earlier by [6] and also suggests that using MAC is not sufficient and that mechanisms should be rebuilt for privacy. Information from this article will help us support our research proposal that suggests current location of Wi-Fi access cold be used to secure access points and levels for users working with confidential data [7].

The information in this article will help support our research proposal which suggests that WLANs data transmitted by radio waves exposes the organization to security risks such that the integrity of confidential data held on any of their networks using the known standards such as 802.11 protocols is not reliable [8].

It was suggested that the Radio Frequency Identification Prototype (RFID) be used to solve these problems and an RFID compiler was used to develop and implement and test different groups of standards or proprietary needs of a company in order to rank the severity of potential threats [9].

"A firm can build more effective security strategies by identifying and ranking the severity of potential threats to its information systems efforts" [10]. This study by a Security researcher warned of the inherent dangers facing financial organizations and what the cost to the financial industry was going to be.

The study used historical cybercrime data collected from the intelligence services to show that computer security breaches had continued to increase every year, with the internet and wireless networks a frequent point of attack.

Cisco, netgear devices are available for such conformity one can create scenario and can check the security practically as per requirement. Besides the security methods may include the simulator such as NS2, Matlab, Qualnet and/or Opnet for evaluation purpose. The specific aspects of this paper is to investigate earlier security aspect called pre-RSNA within the framework of main objectives i.e. RSNA in order to develop a Secure Model for Wireless Local Area Network.

IV. Conclusion

There are many levels at which we can do the bandwidth sharing. Bandwidth distribution is among users within a single organization, bandwidth sharing among several cooperative organizations and bandwidth allocation at the ISP level for its customers. Each organization likes to have their own policy to share their own bandwidth. IPBNS is developed for an environment of loosely coupled independent organizations. Here the IPBNS implementation assumes the possibility of having independent bandwidth sharing policies at individual organizations. Even though there are many possible ways for bandwidth monitoring the best selection must be done which gives accurate results. At the same time it should be responsive i.e. the monitoring system should reflect the change in bandwidth usage immediately when the IPBNS shares bandwidth with a neighbor. The monitoring system should be light weight having a small memory footprint.

REFERENCES

[1] Shivaputrappa Vibhuti, "IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability", San Jose State University, CA, USA, CS265 Spring 2005 (26.03.2005)

[2] NETGEAR, Inc. "Wireless Networking Basics", October 2005.

[3] Stubblefield, A; et al, 'A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)' in ACM Transactions on Information and System Security, Vol. 7, No. 2, May 2004, pg 319–332.

[4] He, C. et al, 'A Modular Correctness Proof of IEEE 802.11i and TLS' in A formal analysis of Crypto Protocols; Proceedings of the 12th ACM conference on Computer and communications security CCS '05, pg 2

[5] Xu, K, 'TCP Behaviour across Multi-hop Wireless Networks and the Wired Internet' in Mobile Ad hoc Networks; Proceedings of the 5th ACM international workshop on Wireless mobile multimedia WOWMOM '02, pg 41- 45

[6] Mahajan, R, ‘Analyzing the MAC-level Behaviour of Wireless Networks in the Wild’ in ACM SIGCOMM Computer Communication Review , Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications SIGCOMM '06, 36(4) pg75- 79

[7] Gruteser, M. and Grunwald, D. (2005) ‘Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers: a Quantitative Analysis’ Mobile Networks and Applications, 10(3) pg 315-325

[8] Bhagyavati et al. ‘Securing Wireless Data: System Architecture Challenges’ in Proceedings of the 1st annual conference on Information security curriculum development InfoSecCD '04; pg 82-87

[9] Jones, A., S. Dontharaju, et al (2008) "Radio Frequency Identification Prototyping" ACM 13(2).

[10] Whitman, M. (2003) "Enemy at the gate: Threats to Information Security" Communications of the ACM 46(8): 91-95.

[11] http://www.cisco.com/c/en/us/products/collateral/wireless/aironet-1200-access-int/prod_white_paper09186a00800b469f.html

[12] Anthony C. Ijeh, Allan J. Brimicombe, David S. Preston, Chris .O. Imafidon “Security Measures in Wired and Wireless Networks”.

[13] Mohd Izhar et. al, “International Journal of Scientific and Research Publications, Volume 3, Issue 11, ISSN 2250-3153 “Enhanced Security Evaluation and Analysis of Wireless Network based on MAC Protocol”, November 2013.