International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 08, August 2017
www.ijarse.com

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

A Brief Review of Wireless LANs for How To Prevent The Intrusions in the Networking Protocols

Prof. Pavithra G[1], Pratheekshasetty M[2],

Treza Mary[3], Dr. T.C.Manjunath[#4]

[1]Research Scholar pursuing Full Time Ph.D. in VTU Research Centre (RRC), Belagavi, Karnataka

[2, 3]Ex HKBKCE Students, ECE Dept., HKBKCE, Bangalore, Karnataka

[4]Prof. & HOD, ECE Dept., Dayananda Sagar College of Engg., Bangalore, Karnataka

ABSTRACT

In this paper, a brief review of the wireless LAN w.r.t. the intrusion is being presented in greater detail.

Keywords –WLAN, authentication, Ad-hoc network.

I. INTRODUCTION

Wired networks, at their most basic level, send data between two points, A and B, which are connected by a network cable. Wireless networks, on the other hand, broadcast data in every direction to every device that happens to be listening, within a limited range. Hackers/intruders have found wireless networks relatively easy to break into, and even use wireless technology to hack into wired networks. A WLAN consists of a set of wireless stations (STx), called a *Basic Service Set* (BSS), and a *Point Coordinator*(PC) which arbitrates the access of the wireless stations (figure **Wireless security** is the prevention of unauthorized access or damage to computers using wireless networks.

Types of unauthorized access:

1. Accidental association/ mis-association
2. Malicious association/ Trojans/VPNs/802.1/ MAC spoofing
3. Ad-hoc networks/ peer-to-peer networks
4. Non-traditional networks/ Bluetooth/ barcode readers.

II. WLAN CHARACTERISTICS

WLAN characteristics that are pertinent to security protocols design.

1. *Roaming*: It is the ability to deliver services to wireless stations outside of the basic service area. When a wireless station is roaming, new authentication through the wireless medium must be performed to ensure the new origination of communication and the new session key from unauthorized access and use. In this case it is desirable that the new security mechanisms performed in the new service area should be kept minimal to assure seamless transfer between the areas.

2. *Reduce power consumption*: Since the WLANs are intended for portable battery operated wireless stations, low power consumption is a very important consideration. Therefore, the security mechanisms developed should use relatively low complexity cryptographic algorithms.
3. *Limited bandwidth*: The limited ISM frequency band allocated by the FCC and the requirement to use spread spectrum communication limit the data rate. For example in the IEEE 802.11 standard the data rate is up to 2 Mbps. This characteristic will require security protocol design that minimizes the number of messages exchanged over the wireless medium.
4. *Noisy channel*: In WLANs the bit error rate is high relatively to wired transmission medium. This characteristic will dictate security protocols that incorporate appropriate provisions for erroneous messages and retransmission procedures.

III. WIRELESS INTRUSION PREVENTION SYSTEMS (WIPS)

A Wireless Intrusion Prevention System (WIPS) is a concept for the most robust way to counteract wireless security risks.

1. For closed networks (like home users and organizations) the most common way is to configure access restrictions in the access points. Those restrictions may include encryption and checks on MAC address.
2. **SSID hiding**: A simple but ineffective method to attempt to secure a wireless network is to hide the SSID (Service Set Identifier).This provides very little protection against anything but the most casual intrusion efforts.
3. **MAC ID filtering:** One of the simplest techniques is to only allow access from known, pre-approved MAC addresses. Most wireless access points contain some type of MAC ID filtering.
4. **Static IP addressing:** Typical wireless access points provide IP addresses to clients via DHCP. Requiring clients to set their own addresses makes it more difficult for a casual or unsophisticated intruder to log onto the network, but provides little protection against a sophisticated attacker.
5. **802.11 security***:* IEEE 802.1X is the IEEE Standard authentication mechanisms to devices wishing to attach to a Wireless LAN.
6. **Wi-Fi Protected Setup (WPS):** In 2007, a new security method – Wi-Fi Protected Setup (WPS) – began to show up on wireless access points. With this type of security, a user is able to add new devices to their network by simply pushing a button (within administration software or physically on the router) and then typing in an 8-digit PIN number on the client device. The PIN feature acts as a sort of shortcut for entering in a longer WPA (Wi-Fi Protected Access) key. The basic idea behind WPS is that having physical access to the AP to hit a button and reading a sticker would provide a more secure implementation of Wi-Fi authentication.
7. **Wired Equivalent Privacy (WEP):** When a client (like your laptop or iPad) connects to a WEP-protected network, the WEP key is added to some data to create an "initialization vector", or "IV" for short. For example, a 128-bit hexadecimal key is comprised of 26 characters from the keyboard (totaling 104 bits) combined with a 24-bit IV. When a client goes to connect to an AP, it sends a request to authenticate, which is met with a challenge reply from the AP. The client encrypts the challenge with the key, the AP decrypts it, and if the challenge it receives matches the original one it sent, the AP will authenticate the client. The

original encryption protocol developed for wireless networks. As its name implies, WEP was designed to provide the same level of security as wired networks. However, WEP has many well-known security flaws, is difficult to configure, and is easily broken.

8. **Wi-Fi Protected Access (WPA):** Introduced as an interim security enhancement over WEP while the 802.11i wireless security standard was being developed. Most current WPA implementations use a pre shared key (PSK), commonly referred to as *WPA Personal*, and the Temporal Key Integrity Protocol (TKIP), for encryption. *WPA Enterprise* uses an authentication server to generate keys or certificates
9. **Restricted access networks:** Solutions include a newer system for authentication, IEEE 802.1x, that promises to enhance security on both wired and wireless networks. Wireless access points that incorporate technologies like these often also have routers built in, thus becoming wireless gateways.

IV. CONCLUSION

Basic list ranking the current Wi-Fi security methods available on any modern (post-2006) router, ordered from best to worst is presented in this paper along with a review.

1. WPA2 + AES
2. WPA + AES
3. WPA + TKIP/AES (TKIP is there as a fallback method)
4. WPA + TKIP
5. WEP
6. Open Network (no security at all)

REFERENCES

[1] "Network Security Tips". *Cisco*. Retrieved 2011-04-19.

[2] "The Hidden Downside Of Wireless Networking".

[3] "How to: Define Wireless Network Security Policies".

[4] "Wireless Security Primer (Part II)". windowsecurity.com.

[5] "Fitting the WLAN Security pieces together". pcworld.com.

[6] "Top reasons why corporate WiFi clients connect to unauthorized networks". InfoSecurity..

[7] "SMAC 2.0 MAC Address Changer". klcconsulting.com.

[8] "Caffé Latte with a Free Topping of Cracked WEP" airtightnetworks.com.

[9] PCI Security Standards Council "PCI DSS Wireless Guidelines".

[10] "Simple Wireless Security For Home".

[11] "The six dumbest ways to secure a wireless LAN", George Ou, March 2005, ZDNet

[12] "What is a WEP key?". lirent.net .

[13] “Weaknesses in the Key Scheduling Algorithm of RC4” by Fluhrer, Mantin and Shami

[14] "FBI Teaches Lesson In How To Break Into Wi-Fi Networks", informationweek.com.

[15] "Analyzing the TJ Maxx Data Security Fiasco", New York State Society of CPAs, PCI DSS 1.2

[16] Hacking Wireless Networks for Dummies, Robert McMillan. "Once thought safe, WPA Wi-Fi encryption is cracked"