International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org

Review paper on 802.11 Wireless LAN Security

Neelima Saini & Sunita Mandal

Dronacharya college of engineering, Gurgaon
neelimasaini1994@gmail.com
,coolsunitamandal@gmail.com

Introduction

IEEE 802.11b standard in 1999, wireless LANs have become more prevalent. Today, wireless LANs are widely deployed in places such as corporate office conference rooms, industrial warehouses, Internet-ready classrooms, and even coffeehouses.

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. These features came with expensive price to pay in areas of security of the network. This paper identifies and summarizes these security concerns and their solutions. Broadly, security concerns in the WLAN world are classified into physical and logical. The paper overviews both physical and logical WLANs security problems followed by a review of the main technologies used to overcome them. It addresses logical security attacks like man- in-the-middle attack and Denial of Service attacks as well as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was the first logical solution to secure WLANs. However, WEP suffered many problems which were partially solved by IEEE802.1x protocol. Towards perfection in securing WLANs, IEEE802.11i emerged as a new MAC layer standard which permanently fixes most of the security problems found in WEP and other temporary WLANs security solutions.

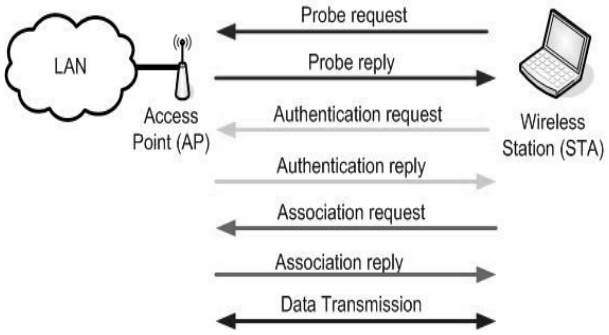
Abstract

Security in the IEEE 802.11 specification—which applies to 802.11b, 802.11a, and 802.11g—has come under intense scrutiny. Researchers have exposed several vulnerabilities in the authentication, data-privacy, and message-integrity mechanisms defined in the specification. This white paper:

- *Reviews the authentication and data-privacy functions described in Clause 8 of the IEEE 802.11 specification*
- *Describes the inherent security vulnerabilities and management issues of these functions*
- *Explains how security issues can be addressed effectively only by augmenting the 802.11 security standard*
- *Examines Cisco Systems architecture for enhanced security on wireless LANs—including the Cisco Wireless Security Suite*
- *Looks ahead to long-term security enhancements*

Wireless Local Area Networks (WLANs) succeeded in providing wireless network access at acceptable data rates. The Institute of Electrical and Electronics Engineering (IEEE) have set standards and specifications for data communications in wireless environment, IEEE802.11 is the driving technology standard for WLANs [1]. WLANs are deployed as an extension to the existing fixed/wired LANs and due to the fact that the nature of WLANs are different from their wired counterparts, it is important to raise the security of WLANs to levels closer or equal to the wired LANs. In general IEEE802.11 can operate in two network topology modes, Ad hoc and Infrastructure modes. This paper discusses WLANs in infrastructure mode. In the infrastructure topology, wireless stations (STAs) communicate wirelessly to a network access point (AP) which is connected to the wired network, this setup forms a WLAN. The establishment of connections between STAs and AP goes through three phases; probing, authentication and association [1]. In probing phase, the STA can either listen passively to AP signals and automatically attempts to join the AP or can actively request to join an AP. Next is the authentication phase, the STA here is authenticated by the AP using some authentication mechanisms described later in the paper. After successfully authenticating, the STA will send an association request to the AP, when approved, the AP adds the STA to its table of associated wireless devices. The AP can associate many STAs but an STA can be associated to one AP only at a time. Figure 1 shows the three phases in WLANs.

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org



3 Logical attacks

Attacks on WEP

Wired Equivalent Privacy (WEP) is a security protocol based on encryption algorithm called "RC4" that aims to provide security to the WLAN similar to the security provided in the wired LAN [1]. WEP has many drawbacks like the usage of small Initialization Vector (IV) and short RC4 encryption key as well as using XOR operation to cipher the key with the plain text to generate cipher text. Sending the MAC addresses and the IV in the clear in addition to the frequent use of a single IV and the fact that secret keys are actually shared between communications parties are WEPs major security problems [2]. WEP encrypted messages can be easily retrieved using publicly available tools like WEPCrack [3]and AirSnort . More discussion about WEP is addressed in later sections.

3.1 MAC Address Spoofing

MAC addresses are sent in the clear when a communication between STAs and AP takes place. A way to secure access to APs and hence to the network is to filter accesses based on MAC addresses of the STAs attempting to access the network [4]. Since MAC addresses are sent in the clear, an attacker can obtain the MAC address of authorized station by sniffing airwaves using tools like ethereal [5]or kismet to generate a database of legitimate wireless stations and their MAC addresses. The attacker can easily spoof the MAC address of a legitimate wireless station and use that MAC address to gain access to the WLAN. Stealing STAs with MAC addresses authorized by the AP is also possible. This can cause a major security violation. The network security administrator has to be notified of any stolen or lost STA to remove it from the list of STAs allowed to access the AP hence the WLAN.

3.2 Denial of Service attack

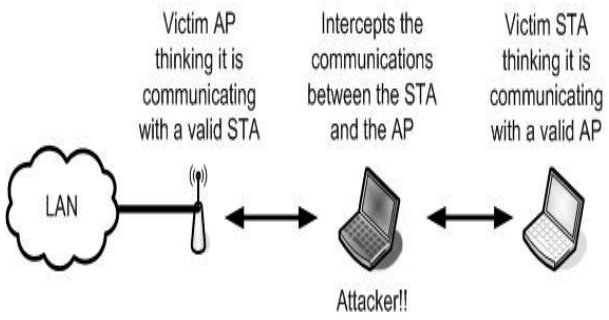
Denial of Service attacks or DoS is a serious threat on both wired and wireless networks. This attack aims to disable the availability of the network and the services it provides [6]. In WLANs, DoS is conducted in several ways like interfering the frequency spectrum by external RF sources hence denying access to the WLAN or, in best cases, granting access with lower data rates [7]. Another way is sending failed association messages to AP and overloads the AP with connections till it collapses which, as a result, will deny other STAs from associating with the AP. Attempts are maid by researchers to overcome such attack by introducing new network elements like Admission Controller (AC) and Global Monitor (GM) [8]. AC and GM allocates specific bandwidth to be utilized by STAs and in the case of heavy traffic on AP, they can de-route some packets to neighboring AP to deter DoS attacks on APs. Also attackers try to exploit the authentication scheme used by APs; this will force the AP to refuse all legitimate connections initiated by valid STAs. Little is done so far to counter DoS attacks the fact that DoS attacks are serious and tools to counter them are minimum attracted attackers to vandalize WLANs using such attacks.

3.3 Man-in-the-middle attack

This is a famous attack in both wired and wireless networks. An illicit STA intercepts the communication between legitimate STAs and the AP. The illegal STA fools the AP and pretends to be a legitimate STA; on the other hand, it also fools the other end STA and pretends to be trusted AP. Using techniques like IEEE802.1x to achieve mutual authentications between APs and STAs as well as adopting an intelligent wireless Intrusion Detection System can help in preventing such attacks.

Figure 2 shows how this attack is conducted

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 05, May 2015
Available at http://internationaljournalofresearch.org



3.4 Bad network design

WLANs function as an extension to the wired LAN hence the security of the LAN depends highly on the security of the WLAN. The vulnerability of WLANs means that the wired LAN is directly on risk. A proper WLAN design should be implemented by trying to separate the WLAN

3.5 Default AP configurations

Most APs are shipped with minimum or no security configuration by default. This is true because shipping them with all security features enabled will make usage and operation difficult for normal users. The aim of AP suppliers is to deliver high data rate, out of the box installation APs with-out sincere commitment to security. Network security administrators should configure these AP according to the organizations security policy [9]. Some of the default unsecured setting in APs shipped today are default passwords which happens to be weak or blank.

Service Set Identifier (SSID) is the name given to a certain WLAN and it is announced by the AP, the knowledge of SSID is important and works like the first security defense. Unfortunately, by default, some APs disable SSID request which means users can access the WLAN without proving the knowledge of SSID . On the other hand, Some APs don't disable SSID request, in fact the SSID request is enabled but the SSID name itself is broadcasted in the air. This is another security problem because it advertises the existence of the WLAN. SSID requests should be enabled and SSID names shouldn't be broadcasted so users have to prove the knowledge of WLAN's SSID prior establishing communication. Another default configuration in APs is that Dynamic Host Configuration Protocol (DHCP) is ON so users can obtain IP addresses automatically and hence access the WLAN easily. Simple Network Management Protocol

(SNMP) parameters are also set to unsecured values [10]. Network security administrators have the responsibility to change these configurations to maximize APs security.

4 Physical attacks

4.1 Rogue Access Points

In normal situations, AP authenticates STAs to grant access to the WLAN. The AP is never asked for authentication, this raises a security concern, what if the AP is installed without IT center's awareness? These APs are called "Rogue APs" and they form a security hole in the network . An attacker can install a Rogue AP with security features disabled causing a mass security threat. There is a need for mutual authentication between STAs and APs to ensure that both parties are legitimate. Technologies like IEEE802.1x can be used to overcome this problem . Network security administrators can discover Rogue APs by using wireless analyzing tools to search and audit the network.

4.2 Physical placement of APs

The installation location of APs is another security issue because placing APs inappropriately will expose it to physical attacks. Attackers can easily reset the APs once found causing the AP to switch to its default settings which is totally insecure. It is very important for network security administrators to carefully choose appropriate places to mount APs.

4.3 AP's coverage

The main difference between WLANs and wired/fixed LANs is that WLANs relies on Radio Frequency (RF) signals as a communication medium. The signals broadcasted by the AP can propagate outside the perimeter of a room or a building, where an AP is placed, allowing users who are not physically in the building to gain access to the network. Attackers use special equipments and sniffing tools to find available WLANs and eavesdrop live communications while driving a car or roaming around CBD areas. Because RF signals obey no boundaries, attackers outside a building can receive such signals and

launch attacks on the WLAN. This kind of attack is called "war driving" . Publicly available tools are used for war driving like NetStumbler . Hobbyists also chalk buildings to indicate that signals are broadcasted from the building and the WLAN in it can be easily accessed. This marking is called "war chalking". In War chalking, information about the speed of the connection and whether the authentication scheme used is open or shared keys are mentioned in the form of special codes agreed upon between war-chalkers. There are a lot of doubts and debates in the wireless network community regarding the legality of war chalking and war driving activities. Network security administrators can test the propagation of APs by using special tools to verify to what extent the signals can reach. Accordingly they can control the propagation of APs by lowering the signal strength or by using smart type of antennas to control the direction of the signal or move the AP to a place where it is guaranteed that the signal will not travel beyond the building premises . Some work has been done in the area of smart antennas in APs to direct the propagation of traffic .Directing the propagation of traffic as well as managing the power of signals originating form the APs can be helpful in restricting the coverage of APs to specified regions.

Sometimes public and open access to the WLAN is preferable, such public WLANs are called "hot spots" [13]. Implementing hot spots is subject to many of the mentioned security problems. It is important to understand that breaking the security of a hot spot will result in breaking the security of wired network connected to that hot spot. The control and monitoring of APs is minimal because it is installed in a public area like hotel lobbies, coffee shops, and airport lounges so preventing physical access to AP is more difficult as the site has to be monitored all the time. In this case, there is a tradeoff between giving users the mobility and the flexibility to log in to the network in public areas versus the security of the network infrastructure. The network backbone can be highly secured but a breach in the security of the network access node (i.e. AP) can always lead to a breach in the security of the backbone behind the node.

References

[1] IEEE Standard for local and metropolitan area networks, “Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications”, ANSI/IEEE Std 802.11, 1999 Edition (R2003).

[2] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., “Wireless network security and interworking”, Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.

[3] Wang Shunman, TaoRan, WmgYue and ZhangJi,
"Wireless LAN and it's security problem". Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003.

[4] Matthew S. Gast, 802.11 Wireless Networks, O’REILLY, 2002.

[5] William Stallings, Cryptography and Network Security, Principles and Practices, 3rd Edition, Prentice Hall 2003.

[6] Matija Sorman, Tomislav Kovac and Damir Maurovic, "Implementing Improved WLAN security", 46th International Symposium Electronics in Marine. ELMAR-2004, Zadar. Croatia, 16-18 June 2004.

[7] Mohit Virendra, Shambhu Upadhyaya, “SWAN: A Secure Wireless LAN Architecture”. Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN’04) , 2004.

[8] Narendar Shankar, William A. Arbaugh and Kan Zhang, “A Transparent Key Management Scheme for Wireless LANs Using DHCP” September 2001. (online) HP
Website [Available:
http://www.hpl.hp.com/techreports/2001/HPL-2001-
227.pdf]

[9] Joseph M. Carey and Dirk Grunwald, “Enhancing WLAN Security with Smart Antennas, A Physical Layer Response for Information Assurance”. IEEE 60th Vehicular Technology Conference, VTC2004, Fall 2004.

[10] Neil Smyth, Máire McLoone and John V. McCanny, “Reconfigurable hardware acceleration of WLAN security”.IEEE Workshop on Signal Processing Systems SIPS, 2004.

[11] IEEE Standard for local and metropolitan area networks , “Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications, Medium Access Control (MAC) Security

Enhancements". ANSI/IEEE Std 802.11i, 2004 Edition.

[12] Tom Karygiannis and Les Owens, " Wireless Network Security: 802.11, Bluetooth and Handheld Devices", National Institute of Standard and Technology. November 2002.

[13] Jesse Walker, 2002. "802.11 Security Series Part I: The Wired Equivalent Privacy (WEP)". February 2002. (online) Intel Corporation. [Available: http://www.intel.com/cd/ids/developer/asmo-na/eng/technologies/mobile/20501.htm]

[14] Cisco Wireless LAN Security Web site

[15] http://www.cisco.com/go/aironet/security

[16] *Cisco Aironet Wireless LAN Security Overview*

[17] http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

[18] http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

[19] http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

[20] http://www.cs.umd.edu/%7Ewaa/wireless.pdf

[21] http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm

[22] http://www.cs.umd.edu/~waa/1x.pdf

[23] Cisco response to *An Initial Security Analysis of the IEEE 802.1x Standard*

[24] http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.htm

[25] *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*

[26] *Authentication with 802.1x and EAP Across Congested WAN Link*

[27] http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/authp_an.htm

[28] *Configuring the Cisco Wireless Security Suite*

[29] http://www.cisco.com/warp/public/cc/pd/witc/ao1200ap/prodlit/wrsec_an.htm

[30] http://grouper.ieee.org/groups/802/11/