Fourth LACCEI International Latin American and Caribbean Conference for Engineering and Technology (LACCET'2006)
"Breaking Frontiers and Barriers in Engineering: Education, Research and Practice"21-23 June 2006, Mayagüez, Puerto Rico

Security in Wireless Local Area Network

Shamila Makki, Ph.D. Candidate,
Department of Electrical and Computer Engineering
Florida International University, Miami, FL, USA

Subbarao V. Wunnava, Ph.D, P.E.
Professor, Department of Electrical and Computer Engineering
Florida International University, Miami, FL, USA

Abstract

A new type of Local Area Network (LAN) called Wireless LAN (WLAN) provides an alternative to the wired or optical LANs. WLAN uses wireless access (Radio Frequency) technology for transmitting and receiving data over the air. It uses the same principle as LANs for transmission of information among the devices attached to the LAN, but with the lack of physical cabling, thus the network can be much more flexible and moving a wireless node is easy. Wireless LANs based on the 802.11 standard are the most likely candidate to become widespread in corporate environments. Wireless LANs provide flexibility and productivity growth for enterprises, but still they have not been extensively installed due to security concerns. Since mobile applications have special requirements and vulnerabilities against the hackers, therefore security is a critical issue in WLAN. This paper introduces the different technologies for WLAN and also addresses various methods for security in WLAN.

Key Words:

Flexibility**,** Hacker, Local Area Network (LAN), Security, Wireless LAN (WLAN)

1. Introduction

The concept of Wireless LAN was introduced in mid-1980s. Then 1997, the IEEE approved the 802.11 international interoperability standard and in 1999, IEEE verified the 802.11a and the 802.11b wireless networking [1]. Wireless LAN is similar to traditional LAN or Wide Area Network (WAN) which is a flexible data communication system and offers identical access and functionality as a wired LAN. Wirelesses LAN like wired LAN are being developed to provide high bandwidth to users in a limited geographical area [2]. The only difference is that users can access to a LAN or WAN from anywhere that there is a wireless access point. WLAN provides high-speed data communication in small area. It uses one of the transmission techniques; spread spectrum

radio, broadcast radio, microwave radio, or infrared light transmission to connect workstation together. [3].

Wireless LANs can be constructed with any of the host of the international networking standards, including IEEE 802.11, IEEE 802.11a, b, or g (Wi-Fi), Bluetooth, and various European-Specific Standards like HIPERLAN.

The term Wi-Fi (Wireless Fidelity) is often used to describe 802.11 wireless networks. Wi-Fi is easier to say and the popular marketing word, it comes from the testing and certification programs run by the Wi-Fi Alliance. Therefore, 802.11 products that receive Wi-Fi certification have been tested and found to be interoperable with other certified products [4].

Bluetooth is a very popular Ad hoc network standard. The Bluetooth is a computing and telecommunications industry specification that describes how wireless devices should interconnect with each other. Ad hoc networks enabled by Bluetooth, allow data synchronization with network systems and application sharing between devices [1].

HIPERLAN is ETSI's wireless broadband access standard, which defines the Media Access Control (MAC) sub- layer, the Channel Access Control (CAC) sub-layer and the physical layer. The MAC accesses the physical layer through the CAC, which allows easy adaptation for different physical layers [5].

Any network, including a wired LAN, is subject to considerable security risks as follow:

- Threats to the physical security of a network
- Unauthorized access and eavesdropping
- Authorized attacks from the network's user community

Wireless network are more exposed to hackers than wired networks, because a hacker could tap into a network with a laptop and a wireless network card. Also the source and the destination address are not encrypted, even if the data is encrypted. Therefore network security requires continuous review to guarantee that current measures are adequate for safety against new threats.

The wireless network standards concentrating on the security functions are HIPERLAN and IEEE 802.11. HIPERLAN specification defines an encryption decryption scheme for optional use.

Large corporate networks generally approach security in three faces [2]:

- Creating security policy
  The security goals are developed based on a list of resources and applications that need to be protected and the type of access a given individual might need to different areas of the network.
- Implementing network security

Good security is to build layers of barriers that discourage challenges to damage the network and its resources. These layers include the implementation of encryption, passwords and firewalls. Also, we must be very careful to change the default settings that come with the wireless equipment and wireless applications.

- Auditing the network

  The integrity of the network, the policies, tools, and applications that implement security are frequently reviewed to guarantee that the network is not subject to threats.

This paper is organized as follows, in section two we introduce the security in wireless network. In section three, we describe the security of wireless LAN. In section four, we conclude our paper.

2. Security in Wireless Network

Security is serious problem in all communication systems both for users and providers. Network security refers to the safety of data and recourses from loss, changed, and inappropriate use. Emerging wireless networks share many common characteristics with traditional wired-line networks. Though, the combination of security features into wireless communication must consider restrictions that may apply to their use such as small packet size, low bandwidth, high transmission costs, limited processing, storage recourses and real time constraints.

Security risks in wireless LANs are, RF signal limiting, Interference and RF disruption, network detection, and unauthorized network access, Denial of Service, insider threat, compromised devices, illicit access point deployment [6]. The major security problem with wireless networks, generally radio networks, is that they intentionally propagate data over an area that may exceed the limits of the area that the organization physically controls. This problem also exists with wired Ethernet networks, but to a lesser degree.

3. Security in Wireless LAN

The IEEE 802.11 contains several security features [7], such as open system and shared key authentication modes, the Service Set Identifier (SSID), Wired Equivalent Privacy (WEP). Originally, Wireless LAN equipments are distributed with a WEP security mechanism. WEP implement the confidentiality and integrity of the traffic in a network. It has weak key management and weak authentication, and provides a limited level of security. WEP used at the station-to-station level and does not offer any end-to-end security [8]. Therefore, organizations should plan to move to Wi-Fi Protected Access (WPA).

Hacker-proofing Techniques are as follow [3]:

- Change default parameters, such as SSID and password for administration, when implementing the network.
- Enable WEP.
- Use the filter capabilities of the access point.

- Disable remote access point administration.
- Implementing strict password guidelines for the administration of the access point configuration.

3.1 Wired Equivalent Privacy (WEP)

Early deployments of Wireless LANs offered no reliable method of authorization and authentication to the network. Wireless LANs are depending on superfluous monitoring. Therefore IEEE 802.11 specifies an optional MAC layer security system known as Wired Equivalent Privacy (WEP). MAC address lists were implemented with obvious scalability and management issues. WEP is the security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11, it provides a wireless LAN with a level of security and privacy equal to a wired LAN. WEP makes available confidentiality and authentication services to 802.11 networks. WEP uses shared (symmetric) static keys, which have to be distributed manually to all clients and access points on a network. This shared secret-key to encrypt data at the link-layer (MAC layer) where key size is different for each manufacturer. WEP supports cryptography key size of up to 128 bits [7].

The IEEE defines three basic security services which are provided by WEP [8], these are;

- Authentication
  The WLAN specification for WEP describes two common ways in which a user that is trying to connect to a LAN can be authenticated.

  - First method uses cryptography which is based on rudimentary cryptographic technique that does not provide mutual authentication. That means, that the client does not authenticate the access point and, therefore, has no way of ensuring it is communicating with an access point.

  - The second method of authentication does not use cryptography and we disable WEP on the access point. Therefore by using this method, a wireless client can be authenticated through one of the two methods called Open System and Closed System Authentication.

- Privacy
  For privacy or confidentiality WEP uses cryptography techniques. It uses the RC4 symmetric-key, stream cipher algorithm. It uses the 128-bit of WEP option, which must be supported by all Wi-Fi devices.

- Integrity
  The goal of the integrity service is to identify and reject any message that could have been interfered with during transit. This service uses an encrypted Cyclic Redundancy Check (CRC) or Frame Check Sequence (FCS).

WEP presents a major cryptography weakness [9] and its disadvantages are as follow:
- Station identification relies on hardware addresses that can be easily captured and

copied.
- Static keys are rarely changed by users.
- Keys are duplicated on client stations.
- A weak implementation of the RC4 algorithm is used.
- An Initialization Vector (IV) sequence is too short and therefore repeats during the timeframe calculation of the key.

3.2 Service Set Identifier (SSID)

SSID is another security mechanism, which it is introduced by IEEE 802.11b. SSID is a network name that identifies the area covered by one or more access points (APs). In a commonly used mode, the access point (AP) periodically broadcasts its SSID in a signal. A wireless station wishing to associate with AP can listen for these broadcasts and can choose an AP to associate with based upon its SSID [7].

3.3 Firewalls

Firewalls are used as a barrier to keep critical attacks away from the network and provide protection from various kinds of IP spoofing and routing attacks [10]. Firewalls provide a location for monitoring security-related events. They are essential for security of Wireless LAN. Firewalls can be applied as a dedicated hardware/software or completely in software, as in the case in an AP. Firewalls are usually placed at the point of entry to the network or between the segments of the network that need protection .

In general, firewalls use one or more of the following three methods to control the flow of traffic in and out of the network [11].

- Packet Filtering Router
  Filtering rule related to a variety of factors, conditions, and elements of the packets. Common elements for filtering include the following;
  - IP Address
  - Domain Names
  - Protocols
  - Ports
  - Content filtering

- Proxy Service
- State full Inspection

Firewalls have their limitations, including the following [10]:
- The firewall cannot protect against attacks that bypass the firewall.
- The firewall does not protect against internal threats.
- The firewall cannot protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, e-mail, and messages for viruses.

3.4 Access Control

Access Control and authentication are key aspects of a wireless network. It nearly impossible to make a security policy that relay only on WEP for authentication and access control. Thus we need to set supplementary parameters [12].

- Service Set ID (SSID): It is a 32-character-long identifier, which is similar in function to a network identifier and is used to differentiate between wireless LANs.
- Access Control List (ACL) sets in most access points. ACL is the technical name for the list of rules to be used for the packet filtering.

Conclusions:

Wireless LAN is an extension of LAN that uses high frequency radio waves rather than cables and wires to communicate between networking devices. Wireless LAN promises high mobility, and convenience. Also Physical and environmental requirement is the most important factor in using the wireless LAN.

In a wired network, the transmission medium can be physically secured, and access to the network is easily controlled. In a wireless network the transmission medium is open to anyone within the geographical range of a transmitter. Therefore the security threats in wireless network are the technology's underlying communications medium, the airwave that causes Wireless LANs are vulnerable to attackers and eavesdropping.

Wireless LANs can use all the security features of wired LAN, and also add additional security features for wireless LAN. Therefore IEEE 802.11 wireless communications have a function called WEP, a form of encryption which provides privacy comparable to that of a traditional wired network. WEP has several weaknesses. Because of the way WEP keys are initialized between the client and access point, WEP keys can be broken very simply, WEP Keys are difficult to manage effectively. They are static and must be distributed to an entire group of users and once distributed they are difficult to change. Also traditional Virtual Private Networking (VPN) techniques will work over wireless networks in the same way as traditional wired networks. Generally data privacy is possible over a radio medium using encryption. But it causes encryption of wireless traffic. Therefore, it generally reduces performance and increases the cost.

References:

[1] T. Karygiannis, L. Owens, "Wireless Network Security 802.11, Bluetooth and Handheld Devices", National Institute of Standards and Technology (NIST), November 2002.

[2] B.P.Crow, I.Widjaja, J.G. Kim, P.T.Sakai, "IEEE 802.11 Wireless Local Area Networks", IEEE Communication Magazine, Sep 1997.

[3] D.C.Yen, D.C.Chou, " Wireless Communication: the Next Wave of Internet Technology", Technology In Society, 2001.

[4] Becta Technical paper, "Wireless Local Area Networks (WLAN)", 2005.

[5] ETS 300 652., "High Performance Radio Local Area Network (HIPERLAN) Type1; Functional specification", ETSI, 1996.

[6] K. Pahlavan, A. Zahedi, P. Krishnamurthy, “Evolving Wireless LAN Industry - Products and Standards. Invited paper PIMRC’97, Worcester Polytechnic Institute, 1997.
[7] J. S. King, “ An IEEE 802.11 Wireless LAN Security ”, October 22, 2001.
[8] S. Uskela, “Security in Wireless Local Area Networks,” Helsinki University of Technology, 1997.
[9] Wireless Local Area Network, http://www.assureconsulting.com/articles/wlan.shtml.
[10] W. Stallings, “Cryptography and Network Security Principles and Practices”, Third Edition, Prentice Hall, New Jersey, pp. 616-628, 2003.
[11] J. Chen, T. Zhang, “IP- Based Next- Generation Wireless networks”, Wiley, 2004.
[12] R.D. Vines, “Wireless Security Essentials”, Wiley, 2002.