Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

IJMTER

ISSN (ONLINE) : 2349 - 9745

ISSN (PRINT) : 2393 - 8161

Wireless Network Security: A review

Manojkumar P. Parmar[1]

[1]IT Department, Government Polytechnic, Himatnagar

Abstract- Awareness to the security risks of wireless computer networks is very much important in today era. Here a discussion on Wireless Network Security Position provides some general information on wireless networks and wireless network security. This gives detail information for Wireless Local Area Networks (WLANs) using IEEE 802.11. An organizations who are planning to use wireless networked computing devices in their systems and implement wireless networks System and network administrators who administer, here it is assumed that each users have at least some operating system, networking, and security expertise. Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to these technologies, it is strongly encouraged to take advantage of other resources for more current and detailed information. Wireless network is required to be secured enough from the outer attacks (intruders / hackers) and it should be capable to secure the information in this network.

Keywords— Wireless network, Adhoc network, Adhoc mode, Infrastructure mode, wired equivalent privacy (WAP), WLAN, SSID

I. INTRODUCTION

Traditional wired networks are using cables to transfer information, and these are protected by physical controls, such as buildings, that enclose them. To gain unauthorized access to a wired network, you must bypass the physical security of the building or breach network perimeter security devices, such as firewalls. While wireless networks are exposed to many of the same risks as wired networks, they are also vulnerable to additional risks. Wireless networks transmit data through the air using radio frequencies. These wireless signals can travel through the walls, ceilings and windows of buildings up to hundreds of meters outside of the building walls, and are accessible by anyone in range thus providing a network access point that is beyond the physical security controls of the wired network. Once they have accessed systems, intruders can launch denial of service attacks, steal identities, violate the privacy of users, insert viruses and disable operations. Private information which is being transmitted between two wireless devices can be identified and disclosed if it is not secured by strong encryption. Despite the additional security risks to networks, the use of wireless devices and WLANs is growing rapidly. Wireless communications give great flexibility in information delivery and in responding to changes in ICT infrastructure needs. Wireless connectivity also creates new security risks that agencies need to understand and factor into their business decisions.

II. OVERVIEW OF WIRELESS TECHNOLOGIES.

A. Wireless Networks

Wireless networks allow devices to be moved about with varying degrees of freedom and still maintain communication with each other. They also offer greater flexibility than cabled networks and significantly reduce the time and resources needed to set up new networks and allow for ad hoc networks to be easily created, modified or torn down. There are many forms of wireless networks. One way of categorizing wireless networks is to consider the relative range and complexity of each type of network.

Wireless Personal Area Network (WPAN) – a small-scale wireless network that requires little or no infrastructure and operates within a short range. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables.

Wireless Local Area Networks (WLANs) are groups of wireless networking nodes within a limited geographic area, such as an office building or campus that are capable of radio communications.

Wireless Metropolitan Area Networks (WMANs) can provide connectivity to users located in multiple facilities generally within a few miles of each other. Many WMAN implementations provide wireless broadband access to customers in metropolitan areas.

Wireless Wide Area Networks (WWANs) connect individuals and devices over large geographic areas. WWANs are typically used for mobile voice and data communications.

B. Wireless Network Components and Architectural Models

The IEEE 802.11 standard defines the following two WLAN design structures as follows:

Ad Hoc Mode. The ad hoc mode does not use APs(Access Points). Ad hoc mode is sometimes referred to as infrastructure less because only peer-to-peer STAs are involved in the communications. This mode of operation is possible when two or more STAs are able to communicate directly to one another. Examples are laptops, mobile phones, PDAs, printers and scanners being able to communicate with each other without an AP. One of the key advantages of ad hoc WLANs is that theoretically they can be formed anytime and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance.

Infrastructure Mode. In infrastructure mode, an AP logically connects STAs to each other or to a distribution system (DS), which is typically an organization’s wired network.

C. **Wireless Technologies and Standards**

Wireless computer networks are generally based on infrared, radio or microwave transmissions using various protocol suites. The most common of these are:

Infrared Data Association (IrDA), Bluetooth and IEEE 802.11 standard for Wireless Local Area Networks (WLANs).

II. WLAN SECURITY, THREATS AND COUNTERMEASURES

This section provides a high-level overview of general wireless network security. The information in this section is intended to apply to many types of wireless networks. It first lists the security objectives for wireless networks, the inherent characteristics of wireless technology, and the most common threats against the security objectives. It next discusses countermeasures to mitigate these risks from management, operational and technical perspectives.

A. Security Objectives

Wireless technologies typically need to support several security objectives, the most common being:

- Confidentiality – It ensure that communications cannot be read by unauthorized users.
- Integrity – It detect any intentional or unintentional changes to data that occur in transit
- Availability – It ensure that devices and individuals can access a network and its resources whenever required.
- Access Control – This restrict the powers of access of devices to access a network or resources within a network

B. Threats

Mainly threats against wireless networks involve an attacker with access to the radio link between wireless devices. This indicates the most significant difference between protecting wireless and wired networks: the relative ease of intercepting wireless network transmissions and inserting new or altered transmissions from what is presumed as the authentic source. For a wired network, an attacker would have to gain physical access to the network or remotely compromise systems on the network: for a wireless network, an attacker simply needs to be within range of the wireless transmissions, making eavesdropping a particularly prevalent threat. Another common threat against wireless networks is the deployment of rogue wireless devices. This provides a back door into the wired network, bypassing perimeter security mechanisms, such as firewalls. Attacks on wireless networks, either passive or active, are essentially on confidentiality, integrity and network availability.

a. Passive Attack - An attack in which an unauthorized party gains access to an asset and does not modify its content.
b. Active Attack - An attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible for these attacks to be detected but they may not always be preventable. Active attacks may take the form of one of four types (or combination thereof) listed below.
c. Masquerading - The attacker impersonates an authorized user and thereby gains certain unauthorized privileges.
d. Denial of Service - The attacker prevents or prohibits the normal use or management of communication facilities.

C. Countermeasures

Organizations can mitigate risks to WLANs by applying countermeasures to address specific threats and vulnerabilities. Countermeasures at the management, operational and technical levels can be effective in reducing the risks commonly associated with WLANs.

An effective WLAN security strategy involves documenting, deploying and enforcing WLAN security policies and practices.

A security policy and compliance therewith, is the foundation on which other operational and technical countermeasures are rationalized and implemented. A WLAN security policy should include the following:

Centralize the management of Access Points so that each Access Point must authenticate to the controller before it is allowed onto the network

- Identify who may use WLAN technology in an agency
- Identify whether Internet access is required
- Describe who can install and configure access points and other wireless equipment
- Provide limitations on the location and physical security for access points
- Describe conditions under which wireless devices are allowed to be used and operated
- Describe limitations on how the wireless device may be used, such as location
- Describe the hardware and software configuration of all wireless devices
- Provide guidelines on the use of encryption and key management

Organizations should ensure that all critical personnel are properly trained on the use of wireless technology. Network administrators need to be fully aware of the security risks that WLANs and wireless devices pose. They must work to ensure security policy compliance and to know what steps to take in the event of an attack. Finally, the most important countermeasure is trained and aware users.

WLAN Checklist

Here are some suggestions that may stop hackers compromising your WLAN. This is a suggested checklist only, and mainly covers design, usage and configuration for WLAN devices. It does not cover other more technically detailed areas such as cryptographic protection or user authorization features of IEEE 802.11. Agencies should have their own checklist tailored to their business needs.

Design for security: when placing wireless APs for strategic coverage, consider signal bleed into uncontrolled areas where transmissions may be intercepted.

Survey your site for other wireless networks in the vicinity using the same channel that may cause co-channel interference.

Segment the AP wired portion of your network on to a separate VLAN – this allows you to separate this traffic and may lessen the access that a hacker gets to your LAN.

Routing protocols should be filtered to the APs – this can eliminate network injection attacks.
Secure all user accounts with complex hard to guess passwords.
Monitor your network traffic. Deny by default, and only allow specific IP ranges.
Audit your authorized wireless networks, and proactively look for rogue wireless networks.

Use WPA2 in WPA2 Only Mode.
Alter the SSID name to other that cannot be easily guessed and that does not identify your network. Default SSIDs alert hackers to vulnerable WLANs.
Disable the SSID broadcast option where the AP constantly broadcasts its SSID as an icon in the search of stations with which it is to be connected.
Alter any fixed passwords on wireless devices. Default passwords are set by the manufacturer and are known by hackers. By changing our password we can prevent hackers from going in and changing your network settings.
Enable MAC address filtering.
Make sure that APs are turned off when they are not used.

III. RECOMMENDATIONS

Implementing the recommendations presented here for a new or existing WLAN will ensure that accepted wireless networking best practice is met, and will provide reasonable assurance that an agency is protected against most currently known WLAN security threats.

- Develop a Strategy
- Develop Policies and Ensure Compliance
- Monitor for Wireless Devices

Service Set Identifier (SSID)

The SSID acts as a WLAN identifier; it allows STAs to distinguish one WLAN from another. All devices trying to connect to a WLAN must use the same SSID. A client device cannot communicate with an established wireless network unless it is configured with the correct SSID. Because the SSID is broadcast in plaintext by the AP by default, an attacking node can read the SSID from beacon frames and use it to join the network as a legitimate node. Even if the APs beacon frames are disabled, since the SSID is transmitted in clear text in the message headers, any node listening to the traffic can sniff it.

Media Access Control (MAC) Address Filters

A MAC address is a unique 48-bit value that is assigned to a particular wireless network interface by the network card's vendor. Many WLAN implementations allow administrators to specify a list of authorized MAC addresses; the AP will permit devices with those MAC addresses only to use the WLAN. This is known as MAC address filtering. However, since the MAC address is not encrypted, it is simple to intercept traffic and identify MAC addresses that are allowed past the MAC filter. Unfortunately, almost all WLAN adapters allow applications to set the MAC address, so it is relatively trivial to spoof a MAC address, meaning attackers can gain unauthorized access easily.

Wired Equivalent Privacy (WEP)

According to the IEEE802.11 standard, WEP was supposed "to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network". WEP was plagued with security issues in relation to the actual implementation of the encryption algorithm, the key lengths, poor key management, authentication and message integrity. WEP has now been proven to be easily breached and cannot be relied upon to secure WLANs.

IV. CONCLUSION

The deployment of insecure wireless networks poses new security threats to agencies' existing connected wired network environments by providing network access points that bypass existing security controls and mechanisms in place. IEEE 802.11i WLANs which is rely on WEP have several defined security issues that can be exploited to circumvent impact network access control and authentication, confidentiality, integrity and availability. It is also recommended that organizations using such wireless networks use a secure Extensible Authentication Protocol for key management rather than pre-shared keys.

REFERENCES

[1]. Defense Signals Directorate (Australian Department of Defense). Australian Government Information and Communications Technology Security Manual (ACSI 33). September 2007

[2]. Frankel, S et al. Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. NIST Special Publication 800-97

[3]. Ossman, M. WEP: Dead again. SecurityFocus Infocus, 14 December 2004. Part 1. [Online] Available: http://www.securityfocus.com/infocus/1814

[4]. Trusted Information Sharing Network for Critical Infrastructure Protection (Australian Government). Wireless Security – Information for CIOs. February 2006

[5]. IEEE Standard 802.11, 1999 Edition. Also available at http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[6]. IEEE Standard 802.11i, 2004 Edition. Also available at http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[7]. IEEE Standard 802.1X, 2004 Edition. Also available at http://standards.ieee.org/getieee/download/802.1X-2004.pdf