Chapter X
Vulnerability Analysis and Defenses in Wireless Networks

Lawan A. Mohammed
King Fahd University of Petroleum and Minerals, Saudi Arabia

Biju Issac
Swinburne University of Technology – Sarawak Campus, Malaysia

ABSTRACT

This chapter shows that the security challenges posed by the 802.11 wireless networks are manifold and it is therefore important to explore the various vulnerabilities that are present with such networks. Along with other security vulnerabilities, defense against denial of service attacks is a critical component of any security system. Unlike wired networks where denial of service attacks has been extensively studied, there is a lack of research for preventing such attacks in wireless networks. In addition to various vulnerabilities, some factors leading to different types of denial of service (DoS) attacks and some defense mechanisms are discussed in this chapter. This can help to better understand the wireless network vulnerabilities and subsequently more techniques and procedures to combat these attacks may be developed by researchers.

INTRODUCTION

Due to the increasing advancement in wireless technologies, wireless communication is becoming more prevalent as it is gaining more popularity in both public and private sectors. Wireless networks are based on a technology that uses radio waves or radio frequencies (RF) to transmit or send data along a communication path. Companies and individuals are using wireless technology for important communications that they want to keep private. A recent report by a market research firm Cahners In-Stat (In-Stat, 2006) predicts sales of 802.15.4 devices (using low powered network standard) could grow by a compound annual growth rate (CAGR) of 200% from 2004 to 2009. In a similar survey, the Infornetics projected that 57% of small, 62% of medium, and 72% of large organizations in North America will be using wireless LANs (WLANs) by 2009 (Richard, 2005).

Wired networks requires a physical setup (i.e., cable wiring) for a user to get access and a misbehaved network card can be tracked down and its switch port can be disconnected remotely using network management tools. But wireless users are not connected to any physical socket, and being in an unknown location, network access can be obtained almost spontaneously. Generally speaking, typical wireless networks are defenseless against individuals who can find unsecured networks. The wireless server dutifully grants the unauthorized computer or mobile device an IP address, and the attacker is able to launch a variety of attacks such as breaking into specific servers, eavesdropping on network packets, unleashing a worm, and denial of service (DoS) or distributed denial of service (DDoS) attacks, and so forth. In this chapter, we discuss some security threats along with DoS attacks in a typical wireless networks and survey some counter measures.

OVERVIEW OF SECURITY CHALLENGES IN WIRELESS NETWORKS

Security has traditionally consisted of ensuring confidentiality of data, the complete integrity of the data, and the availability of the data when ever needed—where service is not denied. Generally speaking, both wired and wireless network environments are complicated. Security solutions are most effective when they can be customized to a specific installation. Unfortunately, a high percentage of individuals involved in building and maintaining inter-networks and infrastructures for these environments have little knowledge of security protocols. As a result, many of today's systems are vulnerable. Recent reports indicated that the wireless networks are becoming more popular. As these networks deployments increase, so does the challenge to provide these networks with security. Wireless networks face more security challenges than their wired counterparts. This is partly due to the nature of the wireless medium as transmitted signals can travel through the walls, ceilings, and windows of buildings up to thousands of feet outside of the building walls. Moreover, since the wireless medium is airwaves, it is a shared medium that allows any one within certain distance or proximity to intrude into the network and sniff the traffic. Further, the risks of using a shared medium is increasing with the advent of available hacking tools that can be found freely from hacker's Web sites. Additionally, some default wireless access points (APs) come from the manufacturers in open access mode with all security features turned off by default. Therefore, insecure wireless devices such as APs and user stations, can seriously compromise wireless networks, making them popular targets for hackers.

Securing wireless networks requires at least three actions to be taken: first, authenticating users to ensure only legitimate users have access to the network; second, protecting the transmitted data by means of encryption; and third, preventing unauthorized connections by eliminating unauthorized transmitter or receiver. This emphasizes the need for a security framework with strong encryption and mutual authentication as explained later.

Specific Challenges and Key Issues

The security challenges in wireless networks can be roughly divided into two main categories, based on their scope and impact. The first category involves attacks targeting the entire network and its infrastructure. This may include the following:

- **Channel jamming:** This involves jamming the wireless channel in the physical layer thus denying network access to legitimate users. Typical example is the DoS attack.
- **Unauthorized access:** This involves gaining free access to the network and also using the AP to bypass the firewall and access the internal network. Once an attacker has access to the network, he/she can then launch additional attacks or just enjoy free network use. Although free network usage may not be a significant threat to many networks, however network access is a key step in address resolution protocol (ARP)-based man-in-the-middle (MITM) attacks.
- **Traffic analysis:** This attack enables gaining information about data transmission and network activity by monitoring and intercepting patterns of wireless communication. This involves analyzing the overhead wireless traffic to obtain useful information. There are three forms of information that an attacker can obtain. First, he/she can identify that there is