Chapter XI
Wireless Security and Privacy Issues

Joarder Kamruzzaman
Monash University, Australia

ABSTRACT

Security and privacy protection are very strong requirements for the widespread deployment of wireless technologies for commercial applications. The primary aim of this chapter is to present an overview of the security and privacy issues by highlighting the need to secure access to wireless networks and the loss that might accrue from the breach of a network. The vulnerabilities of the IEEE 802.11 and Bluetooth networks are discussed, and a paradigm for secure wireless network is presented. The legal framework guiding the privacy issues in wireless communications is also presented.

INTRODUCTION

Wireless connectivity offers large organizations as well as individual users many advantages including mobility and flexibility, increased productivity, and low installation cost. The third generation wireless communications bring multimedia communication, mobile commerce, and many innovative applications and services in diverse areas including finance, industry, entertainment, and military. Wireless LAN (WLAN) allows users to move into an organization without losing network connectivity. This rapid development of technology and applications has created a diminishing boundary between wireless and wireline networks with an ease of access to the Internet through mobile devices. As the technology progresses towards maturity, new security problems arise that are specific to wireless environment. Wireless devices are usually portable and constrained by bandwidth, memory, and processing power. These constraints demand less computational complexity of encryption algorithms and fewer numbers of messages involved in security protocol.

Wireless access is inherently less secure, mainly due to the communication medium which

is open to the intruders, and mobility adds higher risk than those encountered by the fixed wired networks. The motivating idea of going wireless, being able to connect "anywhere anytime", has the potential to attract an increasing number of users and hence also intruders. Wireless devices, for example, cellular phone and personal digital assistance (PDA) with Internet access, were not initially designed with security as one of the highest consideration. Increasing use of wireless and mobile technology for data, voice, and video communication without the appropriate security mechanism in place has made it easy for attackers to intrude into a wireless network and potentially into other parts of the network placing enterprise data in jeopardy. In this chapter, we present an overview of security problems and privacy issues related to the wireless environment and the technologies available to enhance the security standard/feature in wireless network.

WIRELESS SECURITY THREATS

Risk and Challenges

Most conveniently, a wireless access point can be plugged into a wireline network and made available for use within a certain range. This easy installation of wireless connectivity often does not implement any security mechanism in place. The result is that, on the top of various types of attacks common in wireline networks, wireless communication is prone to many types of malicious attacks specifically targeted to wireless networks. In April 2002, a security flaw in wireless network forced a major telecommunication company in New Zealand to shut down its mobile e-mail services (Grifin, 2002). In many countries, wireless computer communications share the same frequency as many other applications, for example, garage door opener, cordless phones, and other short distance applications. This causes a main problem—interception of signals. A strong antenna, properly tuned, would be able to intercept this signal from a few kilometers away. Encryption on wireless data can improve this situation, but encryption is not always used in wireless communication and in many cases, the encryption implemented in wireless devices is not strong enough to prevent an attack. The three key threats to wireless security are discussed next.

Confidentiality

Confidentiality of data transmission is one of the fundamental security requirements for organizations as well as individuals. Since wireless transmission is of broadcast nature and easily interceptable, meeting this security requirement is more difficult in wireless network than wireline network. The physical security countermeasure is far less ineffective in this case. Interception of data means compromising proprietary information, network IDs and passwords, configuration data, and encryption keys. Most often, confidentiality features of wireless LAN technology are not enabled and the hackers exploit the numerous vulnerabilities in the IEEE 802.11 technology security (Cam-Winget, Housley, Wagner, & Walker, 2003; Housley & Arbaugh, 2003; Stubblefield, Ioannidis, & Rubin, 2002). This type of attack is further made easy by the use of easily available tools on the Internet, like wireless packet analyzers, such as AirSnort (2006) and WEPcrack (2006). Another risk to the loss of confidentiality through simple eavesdropping is broadcast monitoring. When an access point is connected to a hub, instead of a switch, it leaves all network traffic vulnerable to unauthorized monitoring. Wireless access point is just one of the entry points to a wireline network. In general, if an attacker is successful in intercepting transmission, he might gain further access to the wireline network and eventually launch further attack on servers, workstation, and other connected devices.