Chapter 2
Wireless Security

Faisal Kaleem
Florida International University, USA

Kang K. Yen
Florida International University, USA

ABSTRACT

As the portability and accessibility of mobile devices have grown over the last decade, applications of wireless communication technologies have become more prevalent. Mature technologies such as Wi-Fi, Bluetooth, and GSM (Global System for Mobile Communication) cellular wireless and emerging technologies such as WiMax are becoming commonplace in both the business and consumer world. As such, it is extremely important to understand the security considerations and vulnerabilities in order to ensure that these technologies are as reliable and secure as possible.

Since the communication medium in wireless technologies, as compared to the wired medium, are "invisible airwaves", the security vulnerabilities and threats may be less obvious, resulting in individuals and organizations with no or low awareness of the associated risk of their wireless infrastructure and technology.

The purpose of this chapter is to educate individuals about the inherent security risks and vulnerabilities of common and emerging wireless technologies and to provide them with some of the best practices used in securing or minimizing these associated risks.

INTRODUCTION

The immense popularity of wireless technology has significantly changed the way we access information, browse the Internet and read our emails. Whether you are busy doing research at a college campus, enjoying latte at a coffee store while chatting with your friends, using Skype talking to your Facebook contact, while waiting to board a plane at the airport, video conferencing with your loved one during a business trip while staying at a hotel, or using Google on your Smartphone to find driving directions; you cannot ignore the importance of wireless technology,

DOI: 10.4018/978-1-61350-507-6.ch002

which is now a must-have for businesses and individuals. The degree to which different wireless technologies can be found across a broad spectrum of industries is truly astounding as they have given rise to innovative means of communication and greater convenience.

Despite their added convenience, capabilities and affordable cost, securing different types of wireless technologies is one major concern that cannot be simply ignored. In fact, to most large corporations, wireless is one of the most essential yet a very frustrating technology to secure, and manage. By offering new features and services and allowing for distributed functionality across geographically dispersed systems, threats against the nodes attached to wireless networks have increased. Relying on out-of-the box settings, the ease with which an ignorant corporate employee or a home user can plug-in an unsecure wireless device into their existing network, thus extending its signal beyond the secure perimeter, completely violates the basic principles of network security and reduces their overall security posture. This is one of the reasons why attacks to wireless networks are growing at a higher rate.

The term wireless technology encompasses many things: AM/FM radio, IEEE 802.11 and 802.16 based communications, cell phones networks, Global Positioning System (GPS), Satellite TV, Bluetooth, RFIDs, Infrared, and any other devices that are capable of establishing communication without any physical or wired connections. In this chapter we will only discuss the security issues associated with the most commonly used wireless technologies as follows:

- Wireless Local Area Network (WLAN) or Wi-Fi based on IEEE 802.11 protocol.
- Wireless Personal Area Network (WPAN) or Bluetooth based on IEEE 802.15 protocol.

The major objective behind this chapter is to assist individuals to improve their overall security awareness in the aforementioned areas of wireless technologies by exposing them to the common threats associated with these technologies and providing them with some best practices and countermeasures to use them in a more secure fashion.

For each of these wireless technologies, the chapter will provide:

- An overview of the technology and the associated terminologies,
- An overview of different types of associated threats and vulnerabilities,
- Recommendations and best practices to mitigate the associated risks.

A BRIEF HISTORY OF WIRELESS TECHNOLOGIES

Wireless communication, a branch of telecommunication, is a method to accomplish transfer of information over both short and long distances without using a guided media, like electrical wires or optical cables. Instead, different forms of electromagnetic emissions like, Radio Frequencies (RF), microwave, and infrared are used as a medium to establish communication between the sending and receiving stations.

It was around 1864 when James Clerk Maxwell theoretically conceptualized electromagnetic wave, followed by Guglielmo Marconi, who, in 1897 demonstrated their usage by transmitting Morse Code over wireless links. The year 1928 marks the beginning of the first electronic television broadcast when the visual image of "Felix the Cat" was sent on-air. Since then, wireless communications have come a long way. Satellite based communication for Radios and TVs, GPS navigation, cellular based voice and data networks, and wireless based local and personal area networks are all based on wireless technologies. The wireless technologies that will be discussed throughout the remainder of this chapter are based on RF.