Chapter 6.2
Six Keys to Improving Wireless Security

Erik Graham
General Dynamics C4 Systems, USA

Paul John Steinbart
Arizona State University, USA

ABSTRACT

This chapter presents a step-by-step approach to improving the security of wireless networks. It describes the basic threats to achieving the security objectives of confidentiality, integrity, and availability when using wireless networking. It also explains various countermeasures that can be used to reduce the risks associated with wireless networks. This chapter has two main objectives. The first is to provide managers with practical guidance for improving the security of their organization's wireless networks. The second objective is to summarize the issues and concerns associated with the use of wireless networking so that researchers can identify fruitful areas in need of further investigation.

INTRODUCTION

Organizations implement wireless networking in the hopes of cutting costs and improving productivity. The use of wireless technologies enables network connectivity to be extended faster, and at less cost, than would be associated with having to install additional infrastructure. It can also increase productivity by providing workers with access to computing resources wherever they happen to be working, rather than only from fixed locations thereby potentially improving employee productivity. Wireless networking, however, also poses new and different threats to the confidentiality, integrity, and availability of information resources. Fortunately, with proper planning, organizations can mitigate many of those threats and achieve a reasonable level of protection to justify the use of wireless networking. This chapter presents a step-by-step approach to guide managers in that process. Keep in mind, however, that wireless technology has evolved dramatically during the

DOI: 10.4018/978-1-61350-323-2.ch6.2

past ten years. For example, transmission speeds that used to be measured in kilobits per second now approach 100 megabits per second. This pace of change is likely to continue for the foreseeable future. Nevertheless, many security issues, such as the inherent susceptibility of wireless transmissions to unauthorized interception, will continue to exist and must be addressed by management. Consequently, the discussion in this chapter is necessarily at a high level, with the objective being to concisely summarize the critical issues associated with the use of wireless networks and the corresponding countermeasures for reducing those risks. Readers desiring more detailed technical information about wireless security are referred to the NIST publications SP800-48 (Karygiannis & Owens, 2002) and SP800-97 (Frankel, Eydt, Owens, & Scarfone, 2007). In addition, other chapters in this handbook provide more detailed information about many of the specific countermeasures discussed here (e.g., encryption, firewalls, user authentication, and VPNs).

Our approach focuses on the three basic objectives of information security: preserving the confidentiality, integrity, and availability of information resources. Table 1 shows that wireless networking poses two types of threats to each of those objectives. Confidentiality can be compromised either by intercepting wireless transmissions or by unauthorized access to the network holding sensitive information. The integrity of information can be destroyed by altering it either during transmission or when it is at rest. The availability of information resources can be removed either by disrupting the wireless transmissions or by the loss, theft, or destruction of the wireless networking devices.

Table 1 also lists some of the countermeasures that effectively can mitigate the risks associated with wireless networking. Notice that many of the countermeasures address threats associated with more than one information security objective. Encryption can protect the confidentiality of information both during transmission and at rest. Strong authentication not only protects confidentiality by preventing unauthorized access to sensitive information, but also makes it more difficult to make undetected changes to information. Proper network design and configuration protects confidentiality by making it more difficult to intercept information and improves availability by making it more difficult to disrupt wireless communications. Thus, managers can significantly improve the security of wireless networking by focusing on these six key items:

1. Encrypt all sensitive information, both during transmission and at rest on mobile devices
2. Employ strong authentication and access controls

Table 1. Wireless security objectives, threats, and countermeasures

Security Objective	Threats	Countermeasures
Confidentiality	Interception of wireless signals	Encryption Network Design/Configuration
	Unauthorized access	Strong Authentication Encryption Network Design/Configuration Policies and audits
Integrity	Alteration of wireless signals	Strong authentication Encryption
	Alteration of stored data	Strong authentication Encryption
Availability	Disruption of wireless signals	Network Design/Configuration
	Theft of wireless devices	Physical Security