IDEA GROUP PUBLISHING ITB12237

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter XV

Wireless Security

Erik Graham, General Dynamics Corporation, USA

Paul John Steinbart, Arizona State University, USA

Abstract

The introduction of wireless networking provides many benefits, but it also creates new security threats and alters the organization's overall information security risk profile. Although responding to wireless security threats and vulnerabilities often involves implementation of technological solutions, wireless security is primarily a management issue. Effective management of the threats associated with wireless technology requires a sound and thorough assessment of risk given the environment and development of a plan to mitigate identified threats. This chapter presents a framework to help managers understand and assess the various threats associated with the use of wireless technology. We also discuss a number of available measures for countering those threats.

Introduction

Wireless networking provides a number of benefits. Productivity improves because of increased accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also

creates new threats and alters the existing information security risk profile. For example, because communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. If the attacker can alter the intercepted message and then forward it to its intended destination, integrity is lost. If the attacker prevents the message from reaching its intended destination, availability is compromised. Wireless networking also alters physical security risks. For example, wireless clients (e.g., laptops, PDAs, etc.) are smaller than desktop workstations and, therefore, more easily stolen. In addition, the low cost and ease of installation of wireless access points increases the risk of unauthorized, insecure, wireless access points on the network.

Nevertheless, although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. Moreover, the fundamental economic constraint on security also remains unchanged: most organizations do not have the resources to attempt to totally eliminate all risk. Consequently, wireless security involves risk management. Managers need to evaluate the likelihood that a particular threat might be successfully employed against their organization and estimate the impact of such an attack. They can then choose to invest in and deploy the set of control procedures that most cost-effectively manages risk at an acceptable level. The objective of this chapter is to assist managers in making such decisions by providing them with a basic understanding of the nature of the various threats associated with wireless networking and available countermeasures.

Wireless Threats, Vulnerabilities and Countermeasures

Figure 1 shows that wireless networks consist of four basic components:

1. The transmission of data using radio frequencies;
2. Access points that provide a connection to the organizational network and/or the Internet;
3. Client devices (laptops, PDAs, etc.); and
4. Users.

Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability. This section discusses the various security threats associated with each component and describes countermeasures that can be employed to mitigate those threats.