IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

#ITB7886

CHAPTER TEN

Security: The Snake in the E-Commerce Garden

Raymond R. Panko
University of Hawaii, USA

Security is one of the fastest-growing concerns in e-commerce and intranets. This chapter describes a number of attacks that hackers may attempt against companies and the methods used to combat each attack. The chapter also describes integrated security systems (ISSs), which automatically secure communication between two parties, protecting them from a variety of network attacks. Finally, the chapter describes potential risks from lawsuits if a company fails to adequately secure its systems and losses result.

INTRODUCTION

Hackers have defaced e-commerce Web sites, brought major e-commerce sites to their knees, stolen passwords (and threatened to post them unless extortion money was paid) and engaged in many other types of criminal attacks on e-commerce sites and on corporate intranets.

Yet as bad as things have been, they will be much worse in the future. Managers of e-commerce sites and intranets are engaged in an arms race with attackers. Both the stakes and the required level of security knowledge will rise dramatically in coming years.

The purpose of this chapter is to lay out basic security threats, principles, implementations and issues for e-commerce and intranets today. Specifically, we will look at the following.

- First, we will look at security threats, including interception and reading, impersonation, message modification, login attacks and denial-of-service attacks. For each of these threats we'll look at some basic security principles used to defend against it, including encryption for confidentiality, authentication, digital certificates, message integrity, firewalls, client PC security and server security.

- Second, we will look at integrated security systems (ISSs) for implementing security in practical situations.
- Third, we will look at a number of unresolved issues regarding security, including potential liability if your computers are taken over and used to attack the computers of other companies.

BACKGROUND: THREATS AND PROTECTIONS

It is important to begin a discussion of security by listing some major threats to security and the general steps that can be taken to thwart each of these threats. This section will examine interception, impersonation, message content attacks, login attacks and denial-of-service (DOS) attacks.

Interception and Encryption for Confidentiality

Interception.

The most obvious danger in network transmission is that someone will intercept our messages en route and read them. This would allow them to learn confidential information, such as consumer credit card numbers and business trade secrets.

Encryption for confidentiality.

Fortunately, it is relatively easy to provide *confidentiality* for transmitted messages, that is, the assurance that even if someone *intercepts* your messages, he or she will not be able to read them. We simply *encrypt* each message before we send it out.

The original message to be sent out is called *plaintext*. This name is somewhat misleading, because we are not limited to encrypting text messages. Our plaintext can be any type of file, including graphics files or video files.

We encrypt this plaintext to produce *ciphertext*, which we then transmit across the network. To anyone intercepting the ciphertext, it will look like a random string of ones and zeros. The interceptor will not be able to read it.

The receiver, however, can *decrypt* the ciphertext back to the original plaintext message. He or she can then read it, as we had intended.

Encrytion methods and keys.

Encryption requires an *encryption method*. This is the mathematical algorithm used to transform the plaintext into ciphertext. There are only a few encryption algorithms, so we cannot change our encryption method every time someone discovers our method. Therefore, we yield to reality and do not even try to keep our encryption method secret from attackers.

Encryption requires both an encryption method and a *key*. A key is nothing more than a string of bits (ones and zeros). When we encrypt plaintext, the resulting