chapter 3

Security

System security vulnerability and the corresponding impact of a security lapse on the organization and its customers are significant.

Ensuring the security of a Web system is a difficult task. Given the open nature and original intent of the Internet as a data-sharing medium among research scientists worldwide, many aspects of the Internet work against the security interests of a Web site. A user anywhere in the world can connect to a Web site in a fairly anonymous fashion. Although many Internet services and operating systems include auditing mechanisms for tracking users, a knowledgeable attacker will know how to trick or avoid these mechanisms, and tracking down an Internet intruder is a very complicated and laborsome task.

Because they handle sensitive and personal information, e-commerce Web systems have particular security concerns. Electronic payment is generally a necessary function of an e-commerce Web system, and this type of transaction requires the system to gather a customer's payment information, which usually includes a credit card number and some personal data. Most e-commerce systems retain this information in order to support the processing of future transactions or to enhance a user's future browsing experience. In addition, merchants usually retain customer credit information for the duration of a dispute period, for the purpose of linking the payment information to the transaction. It is critical that this data be safeguarded against retrieval by unauthorized users.

This chapter covers the following aspects of Web system security:

- *Overview:* The threats and aspects of the Internet that make all sites inherently insecure.
- *Web and application servers:* A detailed examination of Web components on these servers to ensure that they do not provide ways for an attacker to enter the system.
- *Database server:* The safeguarding of site data and user confidential information to protect it from being accessed by unauthorized users.
- *Client computers and browsers:* User components can host a variety of site-specific code and data storage, such as ActiveX controls and cookies, and can also, unfortunately, provide an opportunity for exploits and loss of user privacy.
- *Secure communications:* Transmission of critical user data, such as payment and other private information, via a secure protocol, such as SSL, to protect user information from network eavesdroppers.
- *Network:* The use of firewalls and other mechanisms to hide and to restrict access to the Web system's servers, thereby preventing intruders from probing for entry points into the site's network.
- *Security evaluation:* Step-by-step strategies for testing the security of the site. These strategies can be used as the basis for security test case development.

This chapter is concerned primarily with the security of software and components developed by an organization, as well as some large-scale site design considerations. Therefore, coverage of file permissions, operating system and Web server configurations, and other such issues is limited. However, many books and Internet resources on those subjects are available, and many are specific to the operating system and software in use by the site.

The material in this chapter references two types of utilities that are useful in the evaluation of Web site security:

- A *port-scanning tool* allows the user to scan a host or range of hosts to determine whether they are exposing services (server processes) on some or all ports. Because some of these services contain known security problems, a port scanner allows an outside user to determine whether a potential entry point on a server may be used to gain access to the system. Several port-scanning tools are available as shareware or as freeware; it is best to use a few different port scanners, as they each offer different feature sets.
- A network monitor, or *sniffer,* is a tool that supports the detailed examination of packets being transmitted across a network.

3.1 Overview

This section describes the Internet security issues that Web sites must be aware of, owing to the nature of the Internet. In addition, a brief discussion of operating system and service security is presented, as well as the need to consider security risks and outsourcing.

Internet Security Issues

Many things working against the security of a Web system are unavoidable facts of the Internet. Therefore, a few fundamental principles must be understood to successfully approach the task of securing the Web system.

The Internet and the machines that connect to it are inherently insecure. The Internet was not built on a secure foundation. For much of the Internet's history, data traveled between hosts in an unencrypted, plaintext form. This data could readily be intercepted and read by a third party, potentially compromising passwords or important content. For electronic commerce, transmitting information in plaintext format was clearly not acceptable, given the transmission of private, financial, and other sensitive data. With the advent of security protocols, such as the Secure Sockets Layer (SSL), this problem of insecure data transmission has been largely remedied since data can now travel over the Internet in an encrypted form. Nonetheless, other Internet security concerns remain.

The modern Internet was built primarily on the use of servers running the UNIX operating system. Although some security controls were necessary to enable the Internet's use as a multiuser system, it was not long before holes were discovered that allowed unscrupulous users to penetrate system security. Although the security of UNIX systems has been vastly improved over the years, and other secure operating systems, such as Windows NT/2000, have been developed, the host security problem still exists. In fact, as more users and computers continue to be connected to the Internet and as additional vulnerabilities are discovered and exploited, the host security problem may never be completely resolved.

Web sites are continuously being scanned by attackers probing for potential entry points. On the Internet, no Web systems are exempt from examination by would-be intruders. One must assume that no host is safe and that all security mechanisms must be in place and active at all times to prevent intrusion. Any door left open has a high degree of probability of being exploited by an attacker. Even small security holes can lead to an attacker ultimately gaining administrative access to the system.

All server software and operating systems are inherently insecure. It has been said that the only secure computer is one that is physically inaccessible and not connected to any network. New security flaws are discovered nearly every day, even within the latest, most secured operating systems and software. Therefore, it must be assumed that a Web system's services and software are not without security flaws and are at risk of being compromised at any time.

Even the most thorough security preparations may miss a security flaw. Although this sounds quite disheartening, the basic principle that applies to Web system deployment is that the system cannot rely on any single security mechanism. For example, simply having a firewall to block unwanted traffic is not enough to ensure the security of a Web system and its data. It must be assumed that a knowledgeable attacker will find a way to bypass the firewall and to gain access to a computer residing on an internal network. In view of such grim odds, it is clear that each aspect of the system must be considered from a security point of view and that any applicable, and practical, security measures must be applied. The odds of an attacker's defeating one mechanism are high; the odds of an attacker's defeating multiple different mechanisms, however, are much lower.

Operating System and Service Security

As outlined in Chapter 1, most Web systems are built with an *n*-tier architectural pattern, whereby several types of servers work together to provide the functionality offered by the Web site. The most common types of servers in this scenario are the *Web server,* the *application server,* and the *database server.* Although these three server types perform vastly different functions, they still perform as servers in the general sense and must be secured at the operating system and service levels, meaning such aspects as file system permissions, user accounts, Web server functions, file transfer, and printing services.

Although the minute details of configuring the operating system and service security are beyond the scope of this book and are not discussed in depth, an overview is provided here, together with a listing of a few Internet resources for further information. Note that securing a server of any kind requires a multitude of configuration changes. A server can be attacked in many ways, so it is imperative that the server be thoroughly secured prior to being placed in a production environment with a connection to the Internet. Securing a server entails two steps. First, it is necessary to secure the base operating system. Second, services running on the server need to be secured.

The action to secure the operating system focuses on properly configuring the installation of the operating system in order to keep unauthorized users from being able to connect to the particular computer and accessing configuration or data files located on its file system. The following list highlights some of the major areas of security concern for the operating system configuration:

- Unnecessary user accounts
- File and directory permissions, especially critical configuration files
- Networked disk volumes, such as Network File Service (NFS) or Windows shared directories
- Log files
- Registry on Windows NT/2000 machines
- Unnecessary background processes
- Password policy

Services and other software running on the server are the most likely points of entry for an attacker. Many services, such as File Transfer Protocol (FTP) and Web servers, are provided with the operating system. In addition, a Web site may require other commercial software to be installed to provide additional or enhanced services. All must be properly configured to prevent unwanted intrusion. Although each service will have its own particular configuration issues, the following list illustrates some of the major areas of service security concern:

- Service user—the user the service is running as
- Configuration files—permissions
- Additional service settings that may allow access to other parts of the server

Many books deal with the intricacies of securing a server for use on the Internet. In addition, many Web sites provide detailed instructions for securing servers, including

- Microsoft Security: http://www.microsoft.com/security
- W3C Web security FAQ: http://www.w3.org/Security/Faq/

The discussion of security in this chapter assumes that the server has been secured from the base operating system and service perspectives. The focus of this chapter is on security concerns pertinent to the architecture, design, and implementation of a Web site's components and content, typically developed in-house by the organization.

Security Risk and Outsourcing

Each Web site needs to gauge the potential severity of a security problem, given the nature of the content and cost to the business should a security-related incident occur. For example, banks and e-commerce sites should regard security as a very high risk to their customers and to the image of the organizations, in addition to having possible legal ramifications. Other sites may have considerably fewer security-related risks, especially if the content is nonconfidential and a security-related incident would not result in much loss of business.

Given the proliferation of hacking and security tampering occurring on the Web, all sites should consider security to some extent. Following the practices outlined in this chapter when developing system components and designing the network configuration will greatly help ensure a secure site. However, some sites with high security-related risks, such as banks and other e-commerce sites, should also consider outsourcing the security evaluation of the site to a third-party security organization. Doing so will ensure that the latest and most thorough evaluation procedures are used to greatly reduce the possibility of a security breach.