January 2008

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURE WEB SERVERS: PROTECTING WEB SITES THAT ARE ACCESSED BY THE PUBLIC

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Many organizations rely upon the World Wide Web (Web) to publish information, to exchange information with Internet users, and to conduct electronic transactions with their customers and their suppliers. The Web's system of interlinked text, images, videos, and other information makes vast amounts of information available to organizations and individuals. With the many advances in computer efficiency, programming techniques, and entry points to network systems, however, public Web sites have become vulnerable to frequent security threats.

The safe operation of public Web sites depends upon the safe and secure operation of two principal components of the networking infrastructure: the organization's Web servers, the software applications that make information available over the Internet; and Web browsers, the programs that enable users to access and display the information from the Web servers.

Guidelines developed by the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) help organizations manage the secure operation of both their Web servers and their Web browsers. This bulletin summarizes a recently updated NIST Special Publication (SP) 800-44, *Guidelines on Securing Public Web Servers*, which focuses on the design, implementation, and operation of publicly accessible and secure Web servers. See the *More Information* section at the end of the bulletin for references to other publications that deal with the security of both Web servers and browsers, and with the basic processes for planning, implementing, and operating secure systems.

NIST Special Publication (SP) 800-44, Version 2, *Guidelines on Securing Public Web Servers: Recommendations of the National Institute of Standards and Technology*

NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, details the steps that organizations should take to plan, install, and maintain secure Web server software and their underlying operating systems. The authors of NIST SP 800-44, Version 2, are Miles Tracy of Federal Reserve Information Technology, Wayne Jansen of NIST, Karen Scarfone of NIST, and Theodore Winograd of Booz Allen Hamilton.

Issues covered in the guide include how to secure, install, and configure the operating system that supports the Web server; how to secure, install, and configure Web server software; how to deploy appropriate network protection mechanisms, such as firewalls, routers, switches, and intrusion detection and intrusion prevention systems; the steps for maintaining the secure configuration of the operating system and server software through the application of appropriate patches and upgrades; the requirements for security testing; the methods for monitoring logs, and for managing backups of data and operating system files; and how to use, publicize, and protect information and data on Web servers in a careful and systematic manner.

The appendices to the guide provide useful supplemental information: a list of online Web security resources, definitions of the

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since December 2006:

- *Maintaining Effective Information Technology (IT) Security Through Test, Training, and Exercise Programs, December 2006*
- *Security Controls for Information Systems: Revised Guidelines Issued by NIST, January 2007*
- *Intrusion Detection and Prevention Systems, February 2007*
- *Improving the Security of Electronic Mail: Updated Guidelines Issued by NIST, March 2007*
- *Securing Wireless Networks, April 2007*
- *Securing Radio Frequency Identification (RFID) Systems, May 2007*
- *Forensic Techniques for Cell Phones, June 2007*
- *Border Gateway Protocol Security, July 2007*
- *Secure Web Services, August 2007*
- *The Common Vulnerability Scoring System, October 2007*
- *Using Storage Encryption Technologies to Protect End User Devices, November 2007*
- *Securing External Computers and Other Devices Used by Teleworkers, December 2007*

terms used in the guide, and a list of commonly used Web server security tools and applications. Other practical resources in the appendices are a list of in-print and online references, an extensive checklist of actions needed for Web server security, and an acronym list.

NIST SP 800-44, Version 2, is available on the NIST Web site: http://csrc.nist.gov/publications/PubsSPs.html.

Who We Are
The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

The Need for Security

The World Wide Web is a widely used system for exchanging information over the Internet. Both Web servers and Web browsers can be vulnerable to attacks that destroy or change information, and disrupt operations. Web servers are frequently targeted for attack and are subject to many security threats, such as:

- **Malicious attacks that exploit software bugs in the Web server, the underlying operating system, or the active content of information.** These attacks allow the intruder to gain unauthorized access to the Web server and to information that was not meant to be publicly accessible. Then, sensitive information on the Web server may be read or modified. These attacks can also result in giving the intruder unauthorized capabilities to execute commands and to install software on the Web server.

- **Denial of service (DoS) attacks that are directed to the Web server or its supporting network infrastructure.** These attacks can result in denying or hindering authorized users from making use of the Web server's services.

- **The compromise of sensitive information on backend databases that are used to support interactive elements of a Web application.** The attacker injects commands that are run on the server. Using Structured Query Language (SQL) and Lightweight Directory Access Protocol (LDAP), the attacker submits input that will be passed to a database and then processed. In cross-site scripting (XSS) attacks, the intruder manipulates the application to store scripting language commands that are activated when another user accesses the Web page.

- **The interception of sensitive information that is transmitted unencrypted between the Web server and the browser.**

* **The modification of the information on the Web server for malicious purposes, such as the defacement of Web sites.**

- **Malicious entities that gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the Web server.**

- **Malicious entities that attack external entities after compromising a Web server host.** These attacks can be launched directly, from the compromised host against an external server, or indirectly, through the placement of malicious content on the compromised Web server in order to exploit vulnerabilities in the Web browsers of the users visiting the site.

- **Use of the Web server as a distribution point for attack tools, pornography, or illegally copied software.**

- **Attackers that use indirect methods to extract personal information from users.** Phishing attacks trick the user into logging into a fake site and giving personal information, which is then stolen. In another type of indirect attack known as pharming, Domain Name System (DNS) servers or users' host files are compromised to redirect users to a malicious site instead of to the legitimate site. The information that is collected in phishing and pharming attacks can be used to access the user's Web site or to carry out an identity theft scheme.

NIST'S Recommendations for Installing, Configuring, and Maintaining Secure Public Web Servers

To address the many sophisticated security threats, NIST recommends that organizations adopt the following practices to maintain a secure Web presence:

- **Carefully plan and address the security aspects for the deployment of a public Web server.**

Security issues should be considered when an organization begins to plan for the deployment of a public Web server since it is much more difficult to address security once deployment and implementation have taken place. Sound decisions about the appropriate configuration of systems are more likely to be made when organizations develop and use a detailed, well-designed deployment plan. The deployment plan will also support the organization's Web server administrators when they have to make the necessary trade-off decisions regarding usability, performance, and risk.

Human resource requirements are essential components of planning, deployment, and operational phases of the Web server and its supporting infrastructure. Human resource issues that need to be addressed in a deployment plan include:

- Types of personnel required: system and Web server administrators, Webmasters, network administrators, information systems security officers (ISSOs);
- Skills and training required by assigned personnel; and
- Required levels of effort for individuals and the overall level of effort required for the staff as a whole.

- **Implement appropriate security management practices and controls when maintaining and operating a secure Web server.**

Organizations should identify their information system assets and the

development, documentation, and implementation of policies, standards, procedures, and guidelines that help to ensure the confidentiality, integrity, and availability of information system resources. The following security management practices will help to strengthen the security of the Web server and the supporting network infrastructure:

- Develop an organization-wide information system security policy.
- Use configuration/change control and management practices.
- Conduct risk assessment and management processes.
- Adopt standardized software configurations that satisfy the information system security policy.
- Conduct security awareness and training activities.
- Adopt contingency planning, continuity of operations, and disaster recovery planning procedures.
- Apply certification and accreditation methods.

▪ **Ensure that Web server operating systems are deployed, configured, and managed to meet the security requirements of the organization.**

The security of a Web server depends upon the security of its underlying operating system. Most commonly available Web servers operate on a general-purpose operating system, which should be configured appropriately to circumvent security problems. Default hardware and software configurations are typically set by manufacturers to emphasize features, functions, and ease of use, and may not focus on security issues. Because every organization's security needs are different, Web server administrators should configure new servers to reflect their organization's security requirements and then reconfigure the servers as those requirements change. Security configuration guides or checklists can assist administrators in securing systems consistently and efficiently. Steps for securing the operating system include:

- Patch and upgrade the operating system.
- Remove or disable unnecessary services and applications.
- Configure operating system user authentication.
- Configure resource controls.
- Install and configure additional security controls.
- Perform security testing of the operating system.

▪ **Ensure that the Web server application is deployed, configured, and managed to meet the security requirements of the organization.**

The steps for the secure installation and configuration of the Web server application parallel the steps for securing the operating system. Administrators should install the minimal amount of Web server services required and eliminate any known vulnerabilities through patches or upgrades. Any unnecessary applications, services, or scripts resulting from the server installation program should be removed immediately after the conclusion of the installation process. Steps for securing the Web server application include:

- Patch and upgrade the Web server application.
- Remove or disable unnecessary services, applications, and sample content.
- Configure Web server user authentication and access controls.
- Configure Web server resource controls.
- Test the security of the Web server application and Web content.

Organizations should develop a Web publishing process or policy that determines what type of information will be published openly, what information will be published with restricted access, and what information **should not** be published to any publicly accessible repository. Some generally accepted examples of what **should not be published** or that at least should be carefully examined and reviewed before publication on a public Web site include:

- Classified or proprietary information;
- Information on the composition or preparation of hazardous materials or toxins;
- Sensitive information relating to homeland security;
- Medical records;
- An organization's detailed physical and information security safeguards;
- Details about an organization's network and information system infrastructure, such as address ranges, naming conventions, and access numbers;
- Information that specifies or implies physical security vulnerabilities;
- Detailed plans, maps, diagrams, aerial photographs, and architectural drawings of organizational buildings, properties, or installations; and
- Any sensitive information about individuals, such as personally identifiable information (PII), that might be subject to federal, state or, in some instances, international privacy laws.

▪ **Take appropriate steps to protect Web content from unauthorized access or modification.**

After organizations carefully review the information that is made available to the public on their Web sites, the organizations should ensure that the information cannot be modified without proper authorization. Users rely on the integrity of the publicly available information. Because of the public accessibility of Web content, the information is vulnerable to modification. Organizations should protect public Web content through practices for the appropriate configuration of Web server resource controls, such as:

- Install or enable only necessary services.
- Install Web content on a dedicated hard drive or logical partition.
- Limit uploads to directories that are not readable by the Web server.
- Define a single directory for all external scripts or programs executed as part of Web content.
- Disable the use of hard or symbolic links.
- Define a complete Web content access matrix that identifies which folders and files within the Web server document directory are restricted, which are accessible, and to whom.
- Disable directory listings.
- Use user authentication, digital signatures, and other cryptographic mechanisms as appropriate.

- Use host-based intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and/or file integrity checkers to detect intrusions and to verify Web content.
- Protect the backend server from command injection attacks directed to both the Web server and the backend server.

▪ **Use active content judiciously after balancing the benefits gained against the associated risks.**

Early Web sites usually presented static information such as text-based documents that were on the Web server. Today, interactive elements are available, making possible new ways for users to interact with a Web site. These interactive elements have introduced new Web-related vulnerabilities because they involve dynamically executing code on either the Web server or the client using a large number of inputs, from Universal Resource Locator (URL) parameters to Hypertext Transfer Protocol (HTTP) POST content and, more recently, Extensible Markup Language (XML) content in the form of Web service messages. Different active content technologies have different vulnerabilities associated with them, and their risks should be weighed against their benefits. Although most Web sites use some form of active content generators, many also deliver some or all of their content in a non-active form.

▪ **Use appropriate authentication and cryptographic technologies to protect certain types of sensitive data.**

Public Web servers often support a range of technologies for identifying and authenticating users with different privileges for accessing information. Some of these technologies are based on cryptographic functions that can provide an encrypted channel between a Web browser client and a Web server. Web servers may be configured to use different cryptographic algorithms, providing varying levels of security and performance.

Without proper user authentication processes, organizations cannot selectively restrict access to specific information. All of the information that is available on a public Web server would be within reach of anyone with access to the server. Also, a process to authenticate the server to the user helps users of the public Web server to determine whether the server is the "authentic" Web server or a counterfeit version operated by a malicious entity.

Despite the employment of an encrypted channel and an authentication mechanism, attackers may still attempt to access the Web site via a brute force attack. Improper authentication techniques can allow attackers to gather valid usernames or potentially gain access to the Web site. Strong authentication mechanisms can also protect against phishing and pharming attacks. Therefore, an appropriate level of authentication should be implemented based on the sensitivity of the Web server's users and content.

▪ **Employ the network infrastructure to help protect public Web servers.**

The network infrastructure, which includes firewalls, routers, and IDSs, supports the Web server and plays a critical role in the security of the Web server. In most configurations, the network infrastructure will be the first line of defense between a public Web server and the Internet. Network design alone, however, cannot protect a Web server. Web server attacks are frequent, sophisticated, and varied. Web server security must be implemented through layered and diverse protection mechanisms that provide defense-in-depth.

▪ **Commit to an ongoing process for maintaining the security of public Web servers to ensure continued security.**

Organizations should apply constant effort, resources, and vigilance to maintain secure Web servers. The following steps should be performed on a daily basis to maintain the security of Web servers:

* Configure, protect, and analyze log files.
- Back up critical information frequently.
- Maintain a protected authoritative copy of the organization's Web content.
- Establish and follow procedures for recovering from compromise.
- Test and apply patches in a timely manner.
- Test server security periodically.

More Information

Federal agencies will find information about protecting sensitive information in the following directives:

White House Memorandum dated March 19, 2002, *Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security* (http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm).

OMB Memorandum M-06-16, dated June 23, 2006, *Protection of Sensitive Agency Information*; and OMB Memorandum M-07-16, dated May 22, 2007, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, at http://www.whitehouse.gov/omb/memoranda/.

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. NIST publications that support the secure installation, configuration, and maintenance of Web servers and browsers include:

NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*.

NIST SP 800-28, *Guidelines on Active Content and Mobile Active Code*.

NIST SP 800-40, Version 2.0, *Creating a Patch and Vulnerability Management Program*.

NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*.

NIST SP 800-42, *Guideline on Network Security Testing*.

NIST SP 800-45, Version 2, *Guidelines on Electronic Mail Security*.

NIST SP 800-46, *Security for Telecommuting and Broadband Communications*.

NIST SP 800-92, *Guide to Computer Security Log Management*.

NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*.

NIST SP 800-95, *Guide to Secure Web Services*.

For information about NIST standards and guidelines that are referenced in the Web server security guide, as well as other security-related publications, see NIST's Web page at http://csrc.nist.gov/publications/index.html

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.