KEEPING INFORMATION TECHNOLOGY (IT) SYSTEM SERVERS SECURE: A GENERAL GUIDE TO GOOD PRACTICES

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

Organizations rely on the servers in their IT networks to provide a wide variety of services to internal and external users, including email, database, infrastructure management, and file server functions. Servers are the software applications that make information available over the Internet and other networks. A file server, for example, provides file sharing services enabling users to access, modify, store, and delete files. A database server provides database services for web applications on web servers. Many servers also store or process sensitive information for the organization's internal users.

Since their servers perform so many basic functions, organizations have a fundamental interest in implementing and maintaining secure server operations. The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued a new publication that addresses the general security issues related to typical organizational servers.

NIST Special Publication (SP) 800-123, *Guide to General Server Security: Recommendations of the National Institute of Standards and Technology*

Issued in July 2008, NIST SP 800-123, *Guide to General Server Security: Recommendations of the National Institute of Standards and Technology*, was written by Karen Scarfone and Wayne Jansen of NIST and by Miles Tracy of Federal Reserve Information Technology. The guide helps organizations select, implement, and maintain security controls for their servers, such as those that provide web and email services.

The guide concentrates on needed activities for implementing and maintaining the security of servers that provide services over network communications as their main function. Topics covered in the guide include common server vulnerabilities and threats, and the different environments in which servers are deployed. Also discussed are requirements to protect servers, how those requirements can be categorized, and how appropriate security controls can be determined. One section provides an overview of the basic steps that an organization should take to ensure the security of a server and explains the fundamental principles of server security.

The focus of the guide is on general security issues for both servers that are accessible to the public and servers that provide internal services to the organization's staff. These servers mostly use general operating systems such as UNIX, Linux, and Windows. Host servers that incidentally provide one or a few services for maintenance or accessibility purposes, such as a remote access service for remote troubleshooting, are not covered. Specific issues related to web servers, email servers, and other specialized servers are

covered in other NIST publications, including NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, and NIST SP 800-45, Version 2, *Guidelines on Electronic Mail Security*. See the More Information section at the end of this bulletin for details about these and other guides and standards.

The appendices to the guide include a glossary of the terms and an explanation of the acronyms and abbreviations used in the publication. Another section of the appendices provides a list of NIST resources that help users to understand general server security.

NIST SP 800-123 is available at http://csrc.nist.gov/publications/PubsSPs.html.

Security of Servers

Servers are frequently targeted for attack because of the value of their data and services, such as personally identifiable information that could be used in identity theft. Some of the common security threats to servers include:

- Malicious attackers may exploit software bugs in the server or its underlying operating system to gain unauthorized access to the server;
- Denial of service (DoS) attacks may be directed to the server or its supporting network infrastructure, denying or hindering valid users from making use of its services;
- Sensitive information on the server may be read by unauthorized individuals or changed in an unauthorized manner;
- Sensitive information transmitted unencrypted or weakly encrypted between the server and the client may be intercepted;
- Malicious attackers may gain unauthorized access to resources elsewhere in the organization's network via a successful attack on the server; and
- Malicious attackers may attack other entities after compromising a server. These attacks can be launched directly, such as from the compromised host against an external server, or indirectly, such as through the placement of malicious content on the compromised server in order to exploit vulnerabilities in the clients of the users accessing the server.

How to Install, Configure, and Maintain Secure Servers

To implement and maintain secure servers, organizations should:

* secure, install, and configure the underlying operating system;
* secure, install, and configure the server software; and

* maintain the secure configuration through application of appropriate patches and upgrades, security testing, monitoring of logs, and backups of data and operating system files.

NIST recommends that organizations follow these guidelines for installing, configuring, and maintaining secure servers:

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

Because it is much more difficult to address security once deployment and implementation have occurred, security should be carefully considered from the initial planning stage. Organizations are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support server administrators in making the inevitable trade-off decisions between usability, performance, and risk.

Organizations often fail to consider the human resource requirements for both the deployment and operational phases of the server and supporting infrastructure, and should address the following points in their deployment plan:

* the types of personnel required, such as system and server administrators, network administrators, and information systems security officers (ISSOs);
* the skills and training required by assigned personnel; and
* the individual level of effort required of specific staff members and the collective staffing or overall level of effort required of all staff members.

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

Appropriate management practices are essential to operating and maintaining a secure server. Good security practices involve identifying an organization's information system assets and developing, documenting, and implementing policies, standards, procedures, and guidelines that help to ensure the confidentiality, integrity, and availability of information system resources. Essential components for ensuring the security of servers and supporting network infrastructures include:

* an organization-wide information system security policy;
* configuration/change control and management;
* risk assessment and management practices;
* standardized software configurations that satisfy the organization's information system security policy;
* security awareness and training activities;
* contingency planning, continuity of operations planning, and disaster recovery planning; and
* certification and accreditation.

- **Ensure that the server operating system is deployed, configured, and managed to meet the security requirements of the organization.**

The first step in securing a server is securing the underlying operating system. Most commonly available servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying the servers are configured appropriately. Default hardware and software configurations are often set by manufacturers to emphasize features, functions, and ease of use, at the expense of security. Because manufacturers are not aware of each organization's security needs, server administrators must configure new servers to reflect their organization's security requirements and reconfigure them as those requirements change. Using security configuration guides or checklists can assist administrators in securing servers consistently and efficiently. The following steps are important in securing an operating system:

* patch and upgrade the operating system;
* remove or disable unnecessary services, applications, and network protocols;
* configure operating system user authentication;
* configure resource controls;
* install and configure additional security controls, if needed; and
* perform security testing of the operating system.

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

In many respects, the steps for the secure installation and configuration of the server application will be very similar to the steps for securing the server's operating system. A fundamental principle for organizations is to install the minimal amount of services required and to eliminate any known vulnerabilities through patches or upgrades. Unnecessary applications, services, or scripts that may have been installed should be removed immediately after the installation process concludes. To secure the server application, organizations should:

* patch and upgrade the server application;
* remove or disable unnecessary services, applications, and sample content;
* configure server user authentication and access controls;
* configure server resource controls; and
* test the security of the server application and the server content, if applicable.

Many servers also use authentication and encryption technologies to restrict access to the server and to protect information transmitted between the server and its clients. Organizations should periodically examine the services and information accessible on the server and determine the necessary security requirements to protect the services and information. Organizations should also be prepared to implement stronger cryptographic techniques if weaknesses are identified in their servers' existing cryptographic

technologies. For example, NIST has recommended that use of the Secure Hash Algorithm 1 (SHA-1) be phased out by 2010 in favor of SHA-224, SHA-256, and other larger, stronger hash functions. For information about federal requirements for the implementation of cryptographic techniques, see the More Information section at the end of this bulletin.

- **Commit to an ongoing process of maintaining the security of servers so as to ensure continued security.**

The maintenance of a secure server requires constant effort, resources, and vigilance on the part of an organization. Essential activities that support the secure administration of servers include:

* configure, protect, and analyze log files on an ongoing and frequent basis;
* back up critical information frequently;
* establish and follow procedures for recovering from compromise;
* test and apply patches in a timely manner; and
* test security periodically.

More Information

Publications developed by NIST help information management and information security personnel in planning and implementing a comprehensive approach to information security. The general security of servers depends upon attention to basic issues such as security planning, certification and accreditation, risk management, categorization of systems, and use of security controls. Organizations can draw upon NIST standards and guidelines on these issues, including:

FIPS 180-2, *Secure Hash Standard*, specifies four secure hash algorithms - SHA-1, SHA-256, SHA-384, and SHA-512 - for computing a condensed representation of electronic data such as an electronic message. This standard has been proposed for revision. See the Federal Information Processing Standards (FIPS) tab on the web page noted below for more details.

FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, requires that agencies determine minimum security requirements after they have categorized their systems, and select an appropriate set of security controls to satisfy the minimum requirements. Security controls are specified in NIST SP 800-53.

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, provides guidance to organizations in identifying the risks to their missions brought about by the

use of information systems, assessing the risks, and taking steps to reduce the risks to an acceptable level.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, recommends procedures for the security certification and accreditation of information systems.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides guidance in selecting, specifying, and tailoring security controls that will provide an appropriate level of security, based on the organization's assessments of mission risk.

NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, recommends assessment methods and procedures that can be used to determine if the security controls selected by the organization are implemented correctly, operating as intended, and meeting the security requirements of the organization.

NIST SP 800-65, *Integrating IT Security into the Capital Planning and Investment Controls Process*, presents common criteria that organizations can use to prioritize security activities and ensure that identified corrective actions are incorporated into the capital planning process for cost-effective information security.

NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, reviews the components essential to establishing and implementing effective information security programs to help managers select and implement appropriate security controls.

For information about specific server security issues, see:

NIST SP 800-44, Version 2, *Guidelines on Securing Public Web Servers*, advises organizations on managing the secure operation of their web servers and their web browsers.

NIST SP 800-45, Version 2, *Guidelines on Electronic Mail Security*, recommends security practices for designing, implementing, and operating email systems on public and private networks.

NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, explains the secure deployment of DNS services in an organization and provides practical guidance on securing each aspect of DNS based on analysis of the operating environment and associated threats.

For information about NIST standards and guidelines that are listed above, as well as other security-related publications that support server security activities, see NIST's web page: 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.