March 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

IMPROVING THE SECURITY OF ELECTRONIC MAIL: UPDATED GUIDELINES ISSUED BY NIST

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

Electronic mail (email) has become a widely accepted method for people to communicate with each other. Today, more than a billion people in the world use the Internet, according to Internet World Stats, an organization that collects information on Internet usage in over 230 countries. Electronic mail, a very popular Internet application, is used on a regular basis by individuals, government, and business organizations throughout the world to exchange personal and business information.

The popularity and widespread use of electronic mail systems make them tempting targets for malicious attacks, and all users and organizations should be concerned about protecting the security of their systems and their email communications. Attacks on email systems have taken different approaches. Some attackers with extensive knowledge of the workings of these systems have been able to exploit their weaknesses and use the systems to distribute viruses and other malware throughout an organization. Some sophisticated attacks have used email to compromise user workstations within an organization's internal network, and to influence users to provide information to the attackers or to unknowingly extend the attacks to other systems. Flaws in systems have enabled unauthorized users to gain access to and to change information not meant to be publicly accessible, and to execute commands and install software on the organization's mail server. Denial of service (DoS) attacks can harm an organization by preventing legitimate users from accessing systems. Attackers have also penetrated email systems to disable other organizational systems and to send false messages to others from the organization.

Revised Guidelines on Electronic Mail Security

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently updated its guidelines on protecting electronic mail systems. NIST Special Publication (SP) 800-45, Version 2, *Guidelines on Electronic Mail Security: Recommendations of the National Institute of Standards and Technology*, was written by Miles Tracy of Federal Reserve Information Technology, by Wayne Jansen and Karen Scarfone of NIST, and by Jason Butterfield of Booz Allen Hamilton. The publication revises NIST's original guidelines on electronic mail security that were issued in 2002, and recommends strengthened security practices for designing, implementing, and operating email systems on the public and private networks that are in use today.

The guide explains the structure of electronic mail systems and the standards that govern the composition, delivery, and storage of messages. One section is devoted to a discussion of the use of cryptography for signing and encrypting email messages to protect the confidentiality and integrity of information. Other topics covered in the publication include planning and managing mail servers, securing the operating system, and safeguarding the mail server application by filtering the messages that pass through the server and securing access to mailboxes. Additional sections of the publication provide assistance on using network protection mechanisms such as firewalls and

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 April 2006:

intrusion detection and prevention systems, securing the mail client, and maintaining server security on a daily basis.

The appendices in NIST SP 800-45, Version 2, provide extensive supplemental information on the terms used in the guide, and supply listings of in-print and online resources for further exploration. Other useful listings offer sources for available email security tools and applications. Comprehensive checklists are provided to help organizations carry out actions that are recommended in the guidelines: protecting the security of electronic mail systems; planning and managing mail servers; securing the mail server operating system; securing mail servers and their content; implementing a secure network infrastructure; securing mail clients; and administering the mail server.

NIST SP 800-45, Version 2, is available from NIST's website at http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf.

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 Components of Electronic Mail Systems

Electronic mail systems consist of two principal components: mail clients and mail servers. Users read, compose, send, and store their email using mail clients. Mail is formatted and sent from the mail client via the network infrastructure to a mail server. The latter is the computer host that delivers, forwards, and stores mail. All components - the mail servers, the mail clients, and the network infrastructure that connects and supports them - must be protected.

Voluntary industry standards have been developed for formatting, processing, transmitting, delivering, and displaying mail. Cryptography is used to protect the confidentiality and integrity of email. Cryptographic methods can be applied to sign a message to ensure the integrity of information that is sent and to confirm the identity of the sender of the message. Cryptography can also be used to encrypt the message itself to protect the confidentiality of information that is sent.

Federal government organizations are required to use the cryptography standards that have been approved as Federal Information Processing Standards (FIPS). NIST SP 800-45 includes references to the FIPS for security and to NIST's programs for validating the conformance of cryptographic modules to FIPS. Appendix B of the guide contains a listing of the voluntary standards that are related to email and email security.

To improve and maintain the security of their electronic mail systems, organizations should apply the principles of good planning and management that provide for the security of all of their other information and information systems. Comprehensive security plans enable organizations to identify the security requirements for each information system, and to put into place appropriate security controls. With continuous monitoring and management of systems, organizations can assess and maintain effective security.

NIST'S Recommendations for Electronic Mail Security

NIST recommends that organizations follow these guidelines in planning, implementing, and maintaining secure electronic mail systems:

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

Careful planning is critical to the efficient implementation of a secure mail server. It is more difficult and costly to address security issues once the mail server is deployed. With careful planning, organizations can make sure that their mail servers meet their security requirements and are in compliance with all relevant organizational policies prior to installation, configuration, and deployment. Management controls are especially important in organizations where the information technology support structure is highly fragmented. This fragmentation can lead to inconsistencies in managing systems, and these inconsistencies often result in security vulnerabilities.

Organizations are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. The development of such a plan will support mail server administrators in making the inevitable trade-off decisions between usability, performance, and risk.

Some of the issues that should be addressed in the organization's deployment plan include:

* Purpose of the server and the services to be provided;

* Software to be installed;

* Users and their privileges;

* Security and privacy issues;

* Management practices and procedures to assure secure systems;

* Types of personnel required for deployment and operational phases of the mail server and the supporting infrastructure. Personnel types that should be considered include system and mail server administrators, network administrators, and information systems security officers;

* Skills and training required by assigned personnel; and

* Availability of personnel.

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

Appropriate management practices are essential to operating and maintaining a secure mail server. As part of their comprehensive planning and management practices, organizations should identify their systems and information to be

protected, and then develop, document, and implement the policies, standards, procedures, and guidelines that will help to ensure the confidentiality, integrity, and availability of information system resources.

To ensure the security of a mail server and the supporting network infrastructure, the following practices should be implemented:

* Organization-wide information system security policy;

* Configuration/change control and management;

* Risk assessment and management;

* Standardized software configurations that satisfy the information system security policy;

* Security awareness and training;

* Contingency, continuity of operations, and disaster recovery planning; and

* Certification and accreditation.

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

The first step in securing a mail server is to secure the underlying operating system. Most commonly available mail servers operate on a general-purpose operating system. Many security issues can be avoided if the operating system's underlying mail servers are configured appropriately. Default hardware and software configurations are typically 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, each mail server administrator 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 systems consistently and efficiently. To secure the operating system, organizations should carry out the following steps:

* Patch and update the operating system;

* Remove or disable unnecessary services and applications;

* Configure operating system user authentication;

* Configure resource controls;

* Install and configure additional security controls if needed; and

* Perform security tests on the operating system.

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

Many of the steps outlined for the security of the operating system apply also to the secure installation and configuration of the mail server application. The basic recommendation is that organizations install the minimal mail server services required and eliminate any known vulnerabilities through patches or upgrades. If an installation program installs unnecessary applications, services, or scripts, they should be removed immediately after the installation process has been completed. The following steps should be performed in securing the mail server application:

* Patch and upgrade the mail server application;

* Remove or disable unnecessary services, applications, and sample content;

* Configure mail server user authentication and access controls;

* Configure mail server resource controls; and

* Test the security of the mail server applications.

▪ **Consider the implementation of cryptographic technologies to protect user authentication and mail data.**

Most standard mail protocols default to unencrypted user authentication and send email data unencrypted through the network. When unprotected data is sent, an attacker may be able to easily compromise a user account and to intercept or alter unencrypted email messages. Most organizations should consider encrypting the user authentication session even if they do not encrypt the email data itself. Encrypted user authentication is now supported by most standard and proprietary mailbox protocols.

Organizations should examine closely the decision about whether to encrypt and sign email data. Encrypting and signing email places a greater load on the user's computer and the organization's network infrastructure, and this practice may complicate malware scanning and email content filtering. Encrypting and signing messages may also result in significant administrative overhead and may increase the costs of managing email systems. However, for many organizations, the benefits of email encryption and signatures will outweigh the costs.

▪ **Employ the network infrastructure to protect mail servers.**

The network infrastructure includes the firewalls, routers, and the intrusion detection and prevention systems that support the mail server. These systems play a critical role in the security of the mail server. In most configurations, the network infrastructure will be the first line of defense between the Internet and a mail server. Network design alone, however, cannot protect a mail server. Because of the frequency, sophistication, and variety of mail server attacks that occur today, organizations should consider protecting their mail servers through layered and diverse protection mechanisms.

▪ **Ensure that the mail clients are deployed, configured, and used properly to meet the security requirements of the organization.**

The client side of the electronic mail process may represent a greater risk to the security of the mail system than the mail server functions. Organizations must address numerous issues in order to provide an appropriate level of security for email clients. The following steps will help organizations with the secure installation, configuration, and implementation of mail client applications:

* Patch and upgrade the mail client applications;

* Configure mail client security features, such as disabling automatic opening of messages and enabling antispam and anti-phishing features;

* Configure mailbox authentication and access; and

* Secure the client host's operating system.

▪ **Maintain the security of a mail server as an ongoing process.**

Organizations should devote constant effort, resources, and vigilance to maintain a secure mail server. The mail server should be monitored and maintained on a daily basis to assure mail security. To maintain the security of a mail server, organizations should take the following actions:

* Configure, protect, and analyze log files;

* Back up data frequently;

* Protect against malware (e.g., viruses, worms, Trojan horses);

* Establish and implement procedures for recovering from compromise;

* Test and apply patches in a timely manner; and

* Test the security of the system periodically.

More Information

NIST SP 800-45, Version 2, recommends that organizations follow effective practices for planning, implementing, and managing secure electronic mail systems as part of a comprehensive approach to information security. Many NIST publications assist organizations in developing that comprehensive approach. For information about the following publications that are linked to electronic mail security and to other security-related standards and guidelines issued by NIST, see the web page http://csrc.nist.gov/publications/index.html

FIPS 140-2, *Security Requirements for Cryptographic Modules*.

FIPS 197, *Advanced Encryption Standard (AES)*.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

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

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*.

NIST SP 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*.

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

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

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

NIST SP 800-63, *Electronic Authentication Guideline*.

NIST SP 800-83, *Guide to Malware Incident Prevention and Handling*.

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

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

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.