ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY OF ELECTRONIC MAIL

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

Electronic mail (email) is an essential communications tool for many industry, government, and academic organizations. Email is popular and convenient for exchanging messages, data files, images, and sound clips over computer networks and especially over the Internet. Two principal components, mail servers and mail clients, support the email processes. The mail server is the computer host that delivers, forwards, and stores the mail. Users interface with the mail client software to read, compose, send, and store email messages.

Because they are vulnerable targets for attack by malicious intruders, both mail servers and mail clients must be protected. In September 2002, the National Institute of Standards and Technology (NIST) issued NIST Special Publication (SP) 800-45, *Guidelines on Electronic Mail Security*, by Miles Tracy, Wayne Jansen, and Scott Bisker, to help federal agencies improve the secure design, implementation, and operation of their electronic mail servers and clients.

NIST SP 800-45 describes secure practices for the installation, configuration, and maintenance of mail servers and clients. Topics discussed in the guidelines include the security aspects of email standards, use of encryption standards, the security of the underlying operating systems, and the filtering of email content. The publication gives details on the use of devices such as firewalls, routers, switches, and intrusion detection systems to protect networks, and offers recommendations for managing the mail server in a secure manner using backups, tests, updates, patches, log reviews and records management practices. The appendices provide a glossary and information on mail-related standards and security tools. Also included in the appendices are discussions of the secure use of Microsoft, UNIX, and LINUX mail systems, references that are available in print and electronic format about protecting email systems, and a security checklist.

Along with other guidelines and recommendations, NIST SP 800-45 provides agencies with comprehensive information about protecting the computer and network systems that interact with and serve the public. NIST publications are developed primarily for the federal community, but should be useful to individuals, the private sector, and other public sector organizations. Other recent publications covering the security of publicly accessible systems include NIST SP 800-44, *Security of Public Web Servers*, and NIST SP 800-46, *Security for Telecommuting and Broadband Communications*. Summaries of these publications were featured in the November and December bulletins in this series. Information technology security publications and ITL bulletins are available in electronic format from the NIST website: http://csrc.nist.gov/publications/

Vulnerabilities of Mail Servers and Clients

After web servers, an organization's mail servers are typically the most frequent targets of attack as both mail servers and public web servers communicate to some degree with unknown parties, who may or may not be trustworthy. Attackers, with their thorough understanding of the supporting computing and networking technologies, have been successful in exploiting weaknesses in mail servers and clients.

Continued on page 2

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 8901, Gaithersburg, MD 20899-8901, 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 July 2001

- *A Comparison of The Security Requirements for Cryptographic Modules In FIPS 140-1 and FIPS 140-2*, July 2001
- *Security Self-assessment Guide For Information Technology Systems*, September 2001
- *Computer Forensics Guidance*, November 2001
- *Guidelines on Firewalls and Firewall Policy*, January 2002
- *Risk Management Guidance for Information Technology Systems,* February 2002
- *Techniques for System and Data Recovery,* April 2002
- *Contingency Planning Guide for Information Technology Systems*, June 2002
- *Overview: The Government Smart Card Interoperability Specification,* July 2002
- *Cryptographic Standards and Guidelines: A Status Report*, September 2002
- *Security Patches and the CVE Vulnerability Naming Scheme: Tools to Address Computer System Vulnerabilities*, October 2002
- *Security for Telecommuting and Broadband Communications*, November 2002
- *Security of Public Web Servers*, December 2002

Mail servers and clients can be vulnerable to events such as:

- Denial of service (DoS) attacks that are directed to the mail server or its supporting network which can deny or hinder access to the mail server by valid users.
- Sensitive information on the mail server may be disclosed or changed in an unauthorized manner.
- Sensitive information that is transmitted unencrypted between mail server and email client may be intercepted. For example, the email software may default to sending usernames, passwords, and the email message itself without the protection of encryption.
- Information within the email message may be altered at some point between the sender and recipient.
- A successful attack on a mail server can be used to gain unauthorized access to resources elsewhere in the organization's computer network, including user passwords and other computers on the network.
- A mail server that has been attacked can be used to attack another organization's network, perhaps creating liability for damages to the sending organization.
- Attackers may use the organization's mail server to send email-based advertisements (commonly referred to as spam).
- Viruses and other types of malicious code may be distributed to computers throughout an organization via email.
- Users may send inappropriate, proprietary, or other sensitive information via email. This could expose the organization to legal actions.

What Can Be Done to Improve Email Security

Mail servers, mail clients, and the network infrastructure that supports them must be protected to avoid the conditions that can lead to damage, compromise of information, and inconvenience. With good planning and rigorous implementation of secure configurations and operational procedures, organizations can operate successful electronic mail operations while protecting their networks and information resources.

The following actions will help organizations to improve their email security:

- **Plan carefully and address the security aspects of the deployment of a mail server.**

  Careful planning is the essential first step to assuring that mail servers have been installed, configured, and implemented in a secure manner. It is more difficult to address security issues once deployment and implementation have been completed. A detailed and well-designed deployment plan enables the organization to make prudent decisions regarding the tradeoffs between usability, performance, and risks. A deployment plan makes it possible to maintain secure configurations and identify security vulnerabilities.

  All mail server activities should be carried out in compliance with the organization's plans and policies. Plans and policies should support the application of consistent management controls across the entire organization. This is essential in order to avoid variations in controls that can result when the information technology support staff becomes fragmented within the organization.

  The following items should be considered when planning a mail server:

  - Identify the purpose of the mail server and the information to be processed on or transmitted through the mail server.
  - Identify the security requirements of the information.
  - Identify other services to be provided by the mail server and their security requirements.
  - Identify the location of the mail server, the network services to be provided, and the network service software on both the clients and the server.
  - Identify the users or categories of users of the mail server and any support hosts.
  - Determine the privileges that each category of user will have on the mail server and support hosts.
  - Consider issues such as authentication methods, enforcement of access rules, cost, and compatibility with the existing infrastructure, employee skills, and vulnerabilities.
  - Work closely with vendors in the planning stage.

  The deployment plan should address the human resource requirements for both the deployment and the operational phases of the mail server and its supporting infrastructure. The following issues should be covered in the deployment plan:

  - The types of personnel required, including the system and mail server administrators, network administrators, and information systems security officers (ISSOs).
  - The skills and training required by assigned personnel.
  - The levels of effort required of specific individuals and of the entire staff involved in deploying and operating the mail server.

- **Implement appropriate security management practices and controls to assure that the mail server is maintained and operated securely.**

  Protecting the operating system helps to protect the mail server from exposure to danger. Appropriate management practices are essential

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.

to operating and maintaining a secure mail server. Security practices include the identification of an organization's information system assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines. The goal is to ensure the confidentiality, integrity, and availability of information system resources.

The following practices are recommended.

- ❑ Create an organizational-wide information system security policy that states the basic policy and outlines responsibilities within the organization for carrying out the policy.
- ❑ Control and manage the modifications to a system's design, hardware, firmware, and software to assure consistency in handling changes and protection against improper modifications.
- ❑ Establish risk assessment and management procedures to collect and analyze data about assets, threats, and vulnerabilities. Based on the analysis of risks, select and implement controls to reduce risks to a level acceptable to the organization.
- ❑ Develop standardized software configurations for widely used systems and applications. This will provide guidance to mail server and network administrators on secure configurations that satisfy the information system security policy of the organization.
- ❑ Use security awareness and training programs to make users and administrators aware of their security responsibilities, correct practices, and individual accountability.
- ❑ Carry out contingency planning, continuity of operations, and disaster recovery planning to maintain operations if there are disruptions.
- ❑ Apply certification and accreditation techniques to analyze how well a system meets its security requirements. Document management acceptance of the analysis and the extent to which the system meets the technical requirements for security.

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

The operating system that supports the mail servers must be secure. It is important to check the hardware and software configurations, which may have been set originally to emphasize features, functions, and ease of use, rather than the security of the system. Since each organization has unique security needs, the mail server administrator should configure new servers to meet the organization's requirements. As requirements change, systems should be reconfigured. NIST SP 800-45 provides references and information about automated tools to help mail server administrators develop and maintain operating system security. To secure the operating system, follow these steps:

- ❑ Patch and upgrade the operating system to correct known vulnerabilities.
- ❑ Remove or disable all unnecessary services and applications, and enable only those services that are required by the mail server.
- ❑ Configure the operating system to authenticate users.
- ❑ Configure access controls to specify access privileges to files, directories, devices, and other resources.
- ❑ Test the security of the operating system periodically to identify vulnerabilities and to validate the effectiveness of security measures.

■ **Be sure that the mail server application is deployed, configured, and managed to meet the security requirements of the organization.**

In general, the same steps that are recommended for protecting the operating system also apply to the secure installation and configuration of the mail server application. The goal is to install the minimal amount of mail server services required and to eliminate any known vulnerabilities through patches or upgrades. The following steps should be followed to secure the mail server application:

- ❑ Patch and upgrade the mail server application to correct for any known vulnerabilities.
- ❑ Remove or disable unnecessary services, scripts, applications, and sample content.
- ❑ Configure mail servers to require authentication of users.
- ❑ Configure mail servers to implement the same or more restrictive controls on access to resources as those enforced by the operating system.
- ❑ Test the security of the mail server application.

■ **Consider implementing and using cryptography to protect user authentication and mail data.**

Cryptographic functions have been added to standard email protocols to allow for encryption of the message, authentication of sending party, non-repudiation of the message, and integrity of the message. Mail protocols can be attacked when they default to unencrypted user authentication and send email data in the

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/.

clear (unencrypted). Attackers can intercept this data, compromise a user's account, and alter unencrypted messages. At a minimum, organizations should consider encrypting the user authentication information even if they do not encrypt the email message. Encrypted user authentication is now supported by most standard and proprietary mailbox protocols.

There are many issues to be considered regarding the encryption of email. Encrypting email places a greater load on the user's computer and on the organization's network infrastructure. Encryption may complicate virus scanning and mail content filtering, and usually entails significant administrative overhead. However, for many organizations, the benefits of email encryption will outweigh the costs.

- **Use the network infrastructure to protect the mail servers.**

  The network infrastructure, including the firewalls, routers, and intrusion detection systems that support the mail server, plays a critical role in maintaining the security of the mail server. In most configurations, the network infrastructure will be the first line of defense between potential attackers using the Internet and the mail server. Network design alone, however, cannot protect a mail server. Attacks have been too frequent, sophisticated, and varied. The best defense is through the application of diverse and layered protection mechanisms.

- **Continue to maintain the security of mail servers in an ongoing process.**

  Maintaining a secure mail server requires continued effort, resources, and vigilance from an organization. Daily attention to the administration of a mail server is essential. The following steps are recommended for maintaining the security of mail servers:

  - Configure, protect, and analyze the log files of information about access and use of the mail server.
  - Back up the data on the mail server frequently.
  - Analyze intrusions and protect against malicious code (e.g., viruses, worms, Trojan horses).
  - Establish and follow procedures for recovering from compromise.
  - Test and apply patches in a timely manner.
  - Test the security of the system periodically.

About Standards for Secure Electronic Mail

Standards are critical to the successful exchange of email. Standards for electronic mail have been developed by the Internet Engineering Task Force (IETF), a large open international community of network designers, operators, vendors, and researchers, who are concerned with the evolution and operation of the Internet architecture. The standards cover the composition, formatting, transmission, delivery, and storage of email, and they often reference other standards issued by the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU). The handling of an email message involves many complex steps, and the use of standards makes it possible for different systems to interchange messages. The relevant IETF documents for standard electronic mail are listed in Appendix B of NIST SP 800-45.

- **Standards for Encryption**

  Pretty Good Privacy (PGP) and the Secure Multipurpose Internet Mail Extensions (S/MIME) are the principal mechanisms used to secure email content from end to end. Both techniques are based, in general, on public key cryptography processes. A user has a pair of related keys: a public key that is available openly and a private key that is held exclusively by its owner. The recipient's public key is used to send encrypted information that can be decrypted only with the private key. The sender's private key is used to send digitally signed information that can be verified for authenticity by anyone holding the corresponding public key. Digital signature techniques use a cryptographic hash function to create a digest of the message being sent. This digest can be signed more efficiently than the entire message.

  PGP and S/MIME differ in their approach to key management. Some versions of PGP have no central key issuing or approving authority, and its users exercise management and control. S/MIME and newer versions of PGP use a hierarchical model involving a master registration and approving authority, and subordinate local registration authorities. This Public Key Infrastructure (PKI) provides a mechanism to authenticate users and protect the confidentiality of email. See Chapter 3 of NIST SP 800-45 for details about the advantages and disadvantages of PGP and S/MIME systems.

  NIST SP 800-49, *Federal S/MIME V3 Client Profile*, issued in September 2002, provides specifications for adding cryptographic security services to the standard mail protocol. Based on the Multipurpose Internet Mail Extensions (MIME) standard, S/MIME allows for the addition of services, such as authentication, non-repudiation of origin, message integrity, and message privacy.

- **Federal Information Processing Standards**

  Standards for the cryptographic techniques used for encryption, key management, and digital signatures within the secure email end-to-end process include the following Federal Information Processing Standards (FIPS):

  - FIPS 46-3, *Data Encryption Standard (DES)*, in triple DES mode (3DES) for data encryption.
  - FIPS 197, *Advanced Encryption Standard (AES)*, for data encryption.
  - FIPS 186-2, *Digital Signature Standard (DSS)*, for digital signatures. The DSS specifies the Digital Signature Algorithm (DSA) and allows the use of digital signature techniques specified in American National Standards

Institute (ANSI) X9.31, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* and ANSI X9.62, *Elliptic Curve Digital Signature Algorithm (ECDSA)*.

- FIPS 180-2, *Secure Hash Algorithm (SHA-1)*, for hashing (effective February 2003).

Information about these and related FIPS is available at: http://csrc.nist.gov/publications/fips/index.html

Summary

Organizations and individuals benefit when electronic mail and mail systems are protected. Mail systems available to public access can be vulnerable to misuse, unauthorized access, and denial of services. However, the risks of operating, implementing, and maintaining electronic mail systems can be managed through careful planning, secure configuration of systems, and continued attention to implementation and maintenance.

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.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900