November 1997

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

INTERNET ELECTRONIC MAIL

Electronic mail (email) is one of the most popular uses of the Internet. With access to Internet email, one can potentially correspond with any one of millions of people worldwide. Proprietary email systems can be gatewayed to Internet email, which expands the connectivity of email manyfold. This bulletin summarizes a chapter of the draft *Internet Security Policy: A Technical Guide* (http://csrc.nist.gov/isptg) which NIST plans to publish next year. Trusted Information Systems, Inc. is a contributor to that draft document including the material in this bulletin.

Organizational Email Policy

Electronic mail is increasingly critical to the normal conduct of business. Organizations need policies for email to help employees use electronic mail properly, to reduce the risk of intentional or inadvertent misuse, and to assure that official records transferred via electronic mail are properly handled. Organizational polices are needed to establish general guidance in such areas as:

- the use of email to conduct official business,
- the use of email for personal business,
- access control and confidential protection of messages, and
- the management and retention of email messages.

In addition to one-to-one communication, email can support email address lists, so that a single individual or organization can send email to a list of addresses of individuals or organizations. Email-based discussion groups are another use of email lists. Participants send email to a central mailing list server, and the messages are broadcast to the other participants. This allows subscribers, who may be in different time zones or different continents, to have useful discussions. USENET newsgroups are an elaboration of the email discussion group.

Email Protocols

The principal Internet email protocols (not including proprietary protocols which are tunneled or gatewayed to the Internet) are:

- SMTP (Simple Mail Transport Protocol) - a host-to-host email protocol. An SMTP server accepts email messages from other systems and stores them for the addressees.
- POP (Post Office Protocol) - the most popular email retrieval protocol. A POP server allows a POP client to download email that has been received via another email server.
- IMAP (Internet Mail Access Protocol) - a newer and less popular email retrieval protocol. IMAP is more convenient for reading email while traveling than POP, since the messages can be left on the server, without having to keep the local list and server list of read email messages in sync.

MIME stands for Multipurpose Internet Mail Extensions; it redefines the format of email messages. It can be used to support security

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, Room 562, Building 820, Gaithersburg, MD 20899, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and address to this office.

Bulletins issued since March 1996:

features like digital signatures and encrypted messages. But MIME also has been used to mail virus-infected executables and dangerous messages and attachments.

Potential Email Problems

Accidents

It is easy to have email accidents. An email message can be sent instantly with no hope of retrieval. A single keystroke or mouse-click can misroute the message. Email messages may be archived for years, so that an ill-considered remark can return to haunt the sender later. Email folders can grow until the email system crashes. Misconfigured discussion group software can send messages to the wrong groups. Errors in email lists can flood the subscribers with hundreds of error messages. Sometimes error messages will bounce back and forth between email servers, multiplying until they crash the servers. When an organization's internal email system is connected to the Internet, the effect of accidents can be increased a thousandfold.

Ways to prevent accidents include:

- train users what to do when things go wrong, as well as how to do it right,
- configure email software so that the default behavior is the safest behavior, and
- use software that follows Internet email protocols and conventions rigorously.

Personal Use

Since email is usually provided as an organizational tool, like a telephone, facsimile machine, or photocopier, non-business use would normally be limited or forbidden (depending on the organization). While it is tempting to simply state that all use of email must be for business purposes only, it is generally recognized that this type of policy is difficult to enforce. It is more effective to define policy that places clear limits on personal use of email, in the same manner as personal use limits are defined for telephones and fax machines.

Note that sending email from the organization's address is like sending a letter on company letterhead, using the company's postage meter. If senders use their company account to send email to an email discussion list, it may appear as though the company endorses whatever opinions the sender put in their last message.

Marketing

When the major online services gatewayed their email systems to the Internet, suddenly there was a convenient means to reach a large affluent audience. Unsolicited direct email marketing on the Internet was born. Since the cost of sending email is nominal compared to paper mail, there is little incentive to be selective about the list of addresses sent to, the size of the message, or the frequency of the mailings. There is a bill in the U.S. Congress to put direct email marketing under rules similar to those for bulk mail, so that email marketers would be required to keep lists of addresses which do not wish to receive mailings.

Email Threats

The most common Internet email transfer protocols (SMTP, POP3, IMAP4) do not typically include provisions for reliable authentication as part of the core protocol, allowing email messages to be easily forged. Nor do these protocols require the use of encryption which could ensure the privacy of email messages. Although extensions to these basic protocols exist, the decision to use them needs to be established as part of the mail server administration policy. Some of the extensions use a previously established means of authentication while others allow the client and server to negotiate a type of authentication that is supported by both ends.

Dangerous Attachments

An attacker can attach files to email messages that contain Trojan executables, virus-infected files, or documents that contain dangerous macros.

Impersonation

The sender address on Internet email cannot be trusted, since the sender can create a false return address, or the header could have been modified in transit, or the sender could have connected directly to the SMTP port on the target machine to enter the email.

Eavesdropping

Email headers and contents are transmitted in the clear. As a result, the contents of a message can be read or altered in transit. The header can be modified to hide or change the sender, or to redirect the message.

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.

Mailbombing

Mailbombing is an email-based attack. The attacked system is flooded with email until it fails. A system will fail in different ways, depending on the type of server and how it is configured. Some Internet service providers (ISPs) give temporary accounts to anyone who signs up for a trial subscription, and those accounts can be used to launch email attacks.

Junk and Harassing Email

Since anyone in the world can send you email, it can be difficult to stop someone from sending it to you. People can get your address from company email directories, subscriber lists, or USENET postings. If you give your email address to any Web site, they can resell your address to junk mailers. Some Web browsers volunteer your email address when you visit a Web site.

Most mail systems have some provision for filtering email, that is, searching the email header or body for particular words or patterns, and then filing or deleting the email. However, many users don't know how to use the filtering mechanism. Also, client-side filtering usually takes place only after the email has been received or downloaded, so large messages or large numbers of messages can't be discarded. There are several bills in Congress to restrict junk email.

Email Safeguards

Preventing Dangerous Content

Attachments to email messages or the messages themselves can be scanned for executables, viruses, macros, etc. However, not all dangerous content can be detected or prevented. Depending on the ingenuity of the attacker and the gullibility of the recipient, dangerous content can still be hidden or encrypted in an email message. Users should be warned to treat unusual email messages the same way they treat unusual parcels, with all due caution.

Preventing Modification and Impersonation

Email messages are the electronic equivalent to a postcard written in pencil. Anyone along the way can alter or forge a message. Digital signatures can be used to authenticate the sender of a message and to protect the integrity of its contents. A digital signature is a string of digits produced by cryptographic algorithms that is transmitted with the message. Digital signature methods generally use a one-way hash or message digest algorithm to detect changes in the contents of a message, and a cryptographic algorithm to protect the hash. A message digest is a relatively short string of digits that corresponds to the longer message. A good message digest algorithm makes it computationally infeasible to create a message with different content but the same digest value.

Various cryptographic algorithms may be used to protect the message digest. For example, Federal Information Processing Standard (FIPS) 46-2, the Data Encryption Standard (DES), could be used to encrypt the message digest, but the sender and receiver would need to already have a secret key in common. On the other hand, using public key encryption and a public repository of public keys allows strangers to securely exchange email (depending on the trustworthiness of the repository). FIPS 186, Digital Signature Standard (DSS), and FIPS 180-1, Secure Hash Standard, provide guidance on cryptographic techniques for federal government applications requiring authentication of email messages using public key cryptography. Most commercial secure Internet email systems support both the FIPS algorithms and those of RSA Data Security, whose patented public key encryption and message digest algorithms are in widespread use.

Unfortunately, although standards exist for the cryptographic algorithms and the means for exchanging keys, the infrastructure for trustworthy public repositories is still under development. Organizations and networks of organizations can still create key exchange infrastructures for their own use now using commercial products.

Preventing Eavesdropping

Eavesdropping can be prevented by encrypting the contents of the message or the channel over which it is transmitted. In a typical email system, where mail is sent and received via a central server, if just the channel is encrypted, system administrators at the sending or receiving ends could still read or alter the messages. To provide the highest degree of confidentiality, either a secure channel must be used from sender desktop to receiver desktop or the contents of the message must be encrypted.

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 to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper 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 @ 301-975-2832.

Various Internet email encryption schemes have been proposed, but none has reached a critical mass of use. Most use a symmetric or secret key cipher to encrypt the contents of the message. This requires that the sender and receiver already have a secret key distribution mechanism in place. Other encryption methods use public key encryption to encrypt a secret one-time session key that is used to encrypt the contents of the message. The receiver then uses their private key to decrypt the session key, and that is used to decrypt the message. Semi-automated encryption add-on software is available for most popular email packages.

Levels of Protection of Electronic Mail

The protection provided for electronic mail messages, systems, and software should be consistent with the value of the information that will be transmitted over networks. In general, there should be centralized control of electronic mail services. Policies should be defined to specify the level of protection to be implemented. The following guidelines may be helpful, but are not intended to be rigid categories.

- **Low**

User

Use of electronic mail services for purposes constituting clear conflict of COMPANY interests or in violation of company information security policies is expressly prohibited, as is excessive personal use of email.

Use of COMPANY email to participate in chain letters or moonlighting is not acceptable.

The COMPANY provides electronic mail to employees for business purposes. Limited personal use is acceptable as long as it doesn't hurt the COMPANY.

The use of email in any way to facilitate the conduct of a private commercial purpose is forbidden.

Manager

Use of electronic mail services for purposes constituting clear conflict of COMPANY interests or in violation of company information security policies is expressly prohibited, as is excessive personal use of email.

All employees must read and sign the email user policy.

Email address directories can be made available for public access.

If the COMPANY provides access to electronic mail to external users such as consultants, temporary employees, or partners, they must read and sign the email policy statement.

The contents of email messages will be considered confidential, except in the case of criminal investigations.

Technical

The POP server will be configured to accept plaintext passwords from local machines.

- **Medium**

User

Electronic mail is provided by the COMPANY for employees to conduct COMPANY business. The use of email for personal business is not allowed.

Confidential or company proprietary information will not be sent by email.

Only authorized email software may be used.

Anonymous remailer software cannot be installed.

Employees may not use anonymous remailers for any purpose.

Manager

Confidential or company proprietary information will not be sent by email.

Employees found to be deliberately misusing email will be disciplined appropriately.

Technical

The email system will provide a single externally accessible email address for employees. The address will not contain the name of internal systems or groups.

Only approved SMTP servers and configuration files will be installed.

The SMTP servers will be configured to reject attempts to forward email from non-COMPANY senders to non-COMPANY addresses via COMPANY mail servers.

A local archive of approved MIME-compatible viewers will be maintained and made available for internal use.

- **High**

User

Electronic mail is provided by the COMPANY for employees to conduct COMPANY business. No personal use is allowed.

All electronic messages created and stored on COMPANY computers or networks are property of the COMPANY and are not considered private.

The COMPANY retains the right to access employee electronic mail if it has reasonable grounds to do so. The contents of electronic mail will not be accessed

or disclosed other than for security purposes or as required by law.

Users must not allow anyone else to send email using their accounts. This includes their supervisors, secretaries, and assistants.

The COMPANY reserves the right to review all employee email communications. Email messages may be retrieved by the COMPANY even though they have been deleted by the sender and the reader. Such messages may be used in disciplinary actions.

Manager

Directories of employee email addresses will not be made available for public access.

If confidential or proprietary information must be sent via email, it must be encrypted so that it is only readable by the intended recipient using COMPANY-approved software and algorithms.

No visitors, contractors, or temporary employees may use COMPANY email.

Encryption shall be used for any information designated sensitive or confidential that will be transmitted over open networks such as the Internet.

Outbound messages will be spot-checked to ensure that this policy is being followed.

Technical

Incoming messages will be scanned for viruses and other dangerous content.

Email servers shall be configured to refuse email addressed to non-COMPANY systems.

Email server logs files will be scanned for unapproved versions of email client software, and the systems will be corrected.

Email clients will be configured so that every message is signed using the digital signature of the sender.

Email Retention Policy for Federal Agencies

The National Archives and Records Administration (NARA) has issued standards for the management of federal records created or received on electronic mail. These standards require agencies to manage such records in accordance with the provisions of the chapter pertaining to adequacy of documentation, record keeping requirements, agency record management responsibilities, and records disposition (36 CFR parts 1220,1222, and 1228). For more information, visit the NARA Web site at

gopher://gopher.nara.gov:70/00/about/cfr/records/1222.txt.

Additional Resources

For more information on email security, consult the list of resources listed in Appendix 1 of the *Internet Security Policy: A Technical Guide* (http://csrc.nist.gov/isptg).

Note: Reference to specific commercial products or brands is for information purposes only; no endorsement or recommendation by the National Institute of Standards and Technology, explicit or implicit, is intended or implied.

U.S. DEPARTMENT OF COMMERCE

National Institute of Standards and Technology
Building 820/562
Gaithersburg, MD 20899

Official Business
Penalty for Private Use $300

Forward and Address Correction

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NUMBER G195