February 1998

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

INFORMATION SECURITY AND THE WORLD WIDE WEB (WWW)

The Internet provides access to an ever-expanding storehouse of electronic information via the World Wide Web. Many people use the Web to browse, explore, and search for information. Organizations find the Web invaluable in providing information about their services and products. Web technology has been successful in linking homes, businesses, and governments together, and new applications involving connection to the Internet are appearing daily.

This bulletin on the World Wide Web and security contains information from a draft report, Internet Security Policy: A Technical Guide (http://csrc.nist.gov/isptg/) which NIST plans to publish this year. Trusted Information Systems, Inc., was a contributor to the draft guide, including the material in this bulletin and in our November 1997 bulletin on Electronic Mail.

The Internet

The Internet is a network of networks, providing the infrastructure for communication and sharing of information. The Internet makes possible a number of services including e-mail, file transfer, login from remote systems, interactive conferences, news groups, and access to the World Wide Web.

The World Wide Web (known as "WWW," "Web," or "W3") is the universe of Internet-accessible information. The World Wide Web began as a networked information project at CERN, the European Laboratory for Particle Physics. The Web has a body of software and a set of protocols and conventions which are used to traverse and find information over the Internet. Users can browse through information without being concerned about where the information is actually stored.

Web clients, also called Web browsers, enable a user to navigate through information by pointing and clicking. Web servers deliver HTML (HyperText Markup Language) and other media to browsers through the HyperText Transfer Protocol (HTTP). The browsers interpret, format, and present the documents to users. The end result is a multimedia view of the Internet.

The Web: Threats and Vulnerabilities

Computer systems are at risk when a threat takes advantage of a vulnerability and causes harm. A threat is any circumstance or event with the potential to cause harm to an organization through the disclosure, modification, or destruction of information, or by the denial of services. Organizations have different levels of sensitivity to risk, and they should develop and adopt security policies that reflect their particular sensitivities.

Vulnerabilities stemming from the use of the World Wide Web are associated with browser software and server software. While browser software can introduce vulnerabilities to an organization, these vulnerabilities are generally less severe than the threat posed by servers. A number of risks related to the use of WWW browsers to search for and retrieve information over the Internet exist. Web browsing programs are very complicated and are getting more complicated all the time. The more complicated a program is, the less secure it generally is. Flaws may then be exploited by network-based attacks.

Web pages often include forms. As with e-mail, data sent from a Web browser to a Web server may pass through many interconnecting computers and networks before reaching its final destination. Users should be

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 April 1996:

- *Guidance on the Selection of Low Level Assurance Evaluated Products,* April 1996
- *The World Wide Web: Managing Security Risks,* May 1996
- *Information Security Policies for Changing Information Technology Environments,* June 1996
- *Implementation Issues for Cryptography,* August 1996
- *Generally Accepted System Security Principles (GSSPs): Guidance On Securing Information Technology (IT) Systems,* October 1996
- *Federal Computer Incident Response Capability (FEDCIRC),* November 1996
- *Security Issues for Telecommuting,* January 1997
- *Advanced Encryption Standard,* February 1997
- *Audit Trails,* March 1997
- *Security Considerations in Computer Support and Operations,* April 1997
- *Public Key Infrastructure Technology,* July 1997
- *Cryptography Standards and Supporting Infrastructures: A Status Report,* September 1997
- *Internet Electronic Mail,* November 1997

aware that the privacy of personal or valuable information sent using a Web page entry cannot be assured.

Web servers are vulnerable to threats, especially to malicious threats. Web servers can be attacked directly, or they can be used as jumping off points to attack an organization's internal networks. Organizations should examine the underlying operating system of their Web server, the Web server software, server scripts and other software for vulnerabilities.

Many organizations now support an external Web site describing their products and services. For security reasons, these servers are usually posted outside the organization's firewall. The offerings of Web sites range from simple notices to carefully developed and designed marketing vehicles. Organizations may spend a considerable amount of money and effort in developing a Web site that is informational, easily accessible to users, and creates the right company logo or style. This effort is focused on making the Web site a component of the organization's image and reputation.

The public Web site can be subject to vandalism and break-ins, as documented by many well-publicized incidents over the past few years. These attackers exploited weaknesses in the base operating systems on which the Web servers ran, and broke into the sites with apparent ease. Attackers modified information, and, in some instances, added pornographic material. In one case, attackers inserted hateful language.

Public embarrassment to the organization may have been the only consequence in these cases. Had the attackers modified statements of services or falsified prices, the consequences might have been more severe.

Web sites that are inside the organization's firewall are often used for posting company information to employees. Information such as birthdays, organizational calendars, and phone directories are often posted. Internal Web sites are also used for internal information on the status of projects. Although internal Web sites do not carry the same visibility as external pages, they should be managed with system-specific guidance and procedures. The project leader generally takes on this responsibility.

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.

Security Policies

Security policies provide the foundation for implementing security controls to reduce vulnerabilities and reduce risks. The cost of security controls that are adopted should be appropriate for the risks involved. For Web users, organizational security policies should clearly state the terms and conditions for the use of the Web, and should assign roles and responsibilities for carrying out the policies.

Managers should assign specific responsibilities for the creation, management, and maintenance of an organization's external Web site. The assignment of roles helps to implement organizational policies. In smaller organizations, there may be only a Web site engineer or Webmaster who reports to a senior manager.

In larger organizations, Web site responsibilities may be spread across several different groups and managers. In general, managers are responsible for identifying and implementing new business opportunities using the Web. The Web site manager oversees the overall strategy of the Web site including coordinating content preparation, distribution, and budget monitoring. The technical staff or the Webmaster is responsible for Web site development, connection, intranet, e-mail, and firewall security. Programmers and graphic artists are responsible for the installation, design, coding, debugging, and documentation of the Web site.

The following guidelines give some examples (not an exhaustive list) that organizations might use to start thinking about policies to protect their Web sites. These policies are divided into situations involving low, medium, and high sensitivities to risks that could result from the use of the Web. User, manager and technical staff member responsibilities are identified where appropriate.

Example Policy Statements for Browsing

- **Low-Risk Situations**

User

Software for browsing the Internet is provided to employees primarily for business use.

Any personal use must not interfere with normal business activities, must not involve solicitation, must not be associated with any for-profit outside business activity, and must not embarrass the company.

Internet users are prohibited from transmitting or downloading material that is obscene, pornographic, threatening, or racially or sexually harassing.

Users of the WWW are reminded that Web browsers leave "footprints" providing a trail of all site visits.

Manager

Approved sources for licensed WWW software will be made available to users.

Technical

A local repository of useful WWW browsers, helper applications, and plug-ins will be maintained and made available for internal use.

- **Medium-Risk Situations**

User

Software for browsing the World Wide Web is provided to employees for business use only.

Only technical staff may download files over the WWW.

Manager

All software used to access the WWW must be approved by the Network Manager and must incorporate all vendor-provided security patches.

Technical

Any files downloaded over the WWW shall be scanned for viruses, using approved virus detection software.

Due to the non-secure state of the technology, all WWW browsers shall disable the use of Java, JavaScript, and ActiveX.

Only company-approved versions of browser software may be used or downloaded. Non-approved versions may contain viruses or other bugs.

All Web browsers shall be configured to use the firewall HTTP proxy.

When using a form, ensure that the SSL or Secure Sockets layer or other such mechanism is configured to encrypt the message as it is sent from the user's browser to the Web server.

- **High-Risk Situations**

User

Users may browse the Internet using approved software for the sole purpose of their research or job function.

No sites known to contain offensive material may be visited.

Any user suspected of misuse may have all transactions and material logged for further action.

URLs of offensive sites must be forwarded to the organization's Web security contact.

Manager

An organization-wide list of forbidden sites will be maintained. WWW software will be configured so that those sites cannot be accessed.

Internet sites containing offensive material will be immediately blocked by network administrators.

Contractors must follow this policy after explicit written authorization is given for access to the Internet.

Technical

All sites visited are logged.

Web browsers shall be configured with the following rules:

They will only access the Internet through the firewall HTTP proxy.

They will scan every file downloaded for viruses or other malign content.

Only ActiveX controls signed by the organization may be downloaded.

Only Java signed by the organization may be downloaded.

Only JavaScript signed by the organization may be downloaded.

Example Policy Statements for Web Servers

- **Low-Risk Situations**

User

No offensive or harassing material may be made available via the organization's Web sites.

No personal commercial advertising may be made available via the organization's Web sites.

Manager

Managers and users are permitted to have a Web site.

The personal material on or accessible from the Web site is to be minimal.

No offensive or harassing material may be made available via the organization's Web sites.

No organization confidential material will be made available.

Technical

A local archive of Web server software and authoring tools will be maintained and made available for internal use.

- **Medium-Risk Situations**

User

Users are not permitted to install or run Web servers.

Web pages must follow existing approval procedures regarding company documents, reports, memos, marketing information, etc.

Manager

Managers and users are permitted to have Web pages for a business-related project or function.

Technical

The Web server and any data to be accessed by the general public must be located external to the organization's firewall.

Web servers shall be configured so users cannot install CGI scripts.

All network applications other than HTTP should be disabled (e.g., SMTP, ftp).

Information servers shall be located on a screened subnet to isolate itself from other systems on the site. This reduces the chance that an information server could be compromised and then used to attack these systems.

If using a Web administrative tool, access is restricted to only authorized systems (via IP address, rather than hostname). Default passwords must always be changed.

- **High-Risk Situations**

User

Users are forbidden to download, install, or run Web server software.

Network traffic will be monitored for unapproved Web servers, and operators of those servers will be subject to disciplinary action.

Manager

The Chief Information Officer (CIO) must approve the operation of any other Web server to be connected to the Internet in writing.

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.

All content on the organization's WWW servers connected to the Internet must be approved by and installed by the WebMaster.

No confidential material may be made available on the Web site.

Information placed on the Web site is subject to the same Privacy Act restrictions as when releasing non-electronic information. Accordingly, before information is placed on the Internet, it must be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information. Copyrights must be protected and permission obtained before placing copyrighted information on the Web site. Public affairs offices or legal authorities should be contacted for advice and assistance.

All publicly accessible Web sites must be thoroughly tested to ensure all links work as designed and are not "under construction" when the site is opened to the public. Under construction areas are not to appear on publicly accessible Web sites.

Technical

Remote control of the Web server (i.e., from other than the console) is not allowed. All administrator operations (e.g., security changes) shall be done from the console. Supervisor-level logon shall not be done at any device other than the console.

The Web server software, and the software of the underlying operating system, shall contain all manufacturer-recommended patches for the version in use.

Incoming HTTP traffic will be scanned, and connections to unapproved Web sites will be reported.

Restricting user access to addresses ending in .GOV or .COM provides a minimal level of protection for information not cleared for release to the public. A separate server or partition may be used to separate restricted use information (internal information or internal Web site) from information released to the public.

All Web sites may be monitored as part of the organization's network administration function. Any user suspected of misuse may have all their transactions logged for possible disciplinary action.

On UNIX systems, Web servers shall not be run as root.

The implementation and use of CGI scripts shall be monitored and controlled. CGI scripts shall not accept unchecked input. Any programs that run externally with arguments should not contain metacharacters. The developer is responsible for devising the proper regular expression to scan for shell metacharacters and shall strip out special characters before passing external input to the server software or the underlying operating system.

All WWW servers connected to the Internet will have a firewall between the Web server and internal company networks. Any internal WWW servers supporting critical company applications must be protected by internal firewalls. Sensitive, confidential, and private information should never be stored on an external WWW server.

Forward and Address Correction

Official Business
Penalty for Private Use $300

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

U.S. DEPARTMENT OF COMMERCE

BULK RATE
POSTAGE & FEES
PAID
NIST
PERMIT NUMBER G195