November 2002

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY FOR TELECOMMUTING AND BROADBAND COMMUNICATIONS

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

Both organizations and their employees can benefit when staff members are able to access office networks from home or while they are traveling. Today, broadband communications provide fast data transfer rates, making remote connections practical and productive. There are risks associated with remote access to information resources in general, and broadband communications, if not properly protected, can be especially vulnerable to intruder attacks. However, with good planning and careful implementation of sensible guidelines, organizations can support the popular practice of telecommuting, while protecting their networks and information resources.

The National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), recently issued new recommendations to help federal agencies make their telecommuting applications, broadband connections, and information resources more secure. NIST Special Publication 800-46, *Security for Telecommuting and Broadband Communications*, by D. Richard Kuhn, Miles C. Tracy, and Sheila E. Frankel, should be useful to federal agencies, individuals, the private sector, and other public sector organizations. The report discusses both technical and policy issues, and provides guidance on using personal firewalls, strengthening the security of personal computers and web browsers, protecting home networks, and using virtual private networks. The appendices include useful checklists for security, software update procedures, and pointers to additional resources available on the Internet. The recommendations are available in electronic format from the website http://csrc.nist.gov/publications/nistpubs/index.html.

The Risks of Broadband Communications

Employees working from home and while on the road often need access to long documents, spreadsheets, streaming video, and other large files. Dial-up access to organizational systems may be too slow to carry out many of these applications conveniently. Broadband connections, which supply essentially the same services as dial-up connections to an Internet service provider (ISP), are much faster. The data transfer rates of broadband communications can be ten to one hundred times faster than those provided by dial-up access.

While this speed is a definite advantage, broadband communications generally represent a greater threat to system security than dial-up connections. Some of the same features that attract telecommuters to broadband communications also attract intruders. Broadband connections are easier for attackers to exploit because they are always (or usually) on, and may not be protected as well as other information and computer resources.

When the broadband connection is on, the system is capable of sending and receiving data. It is exposed to potential intruders for much longer periods than is the case with dial-up connections. If the computer is turned on in the morning and off in the evening, the connection time may be 10 - 14 hours a day. Even though the user may be using the system only a few hours each day, it remains connected to the Internet and vulnerable to attack.

Because broadband connections are so much faster than dial-up, intruders can download information from a

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 May 2001

system in seconds, and the intrusion is not likely to be noticed. Similarly, intruders can transmit viruses or other types of Trojan horse programs without the user detecting the activity.

Intruders gaining access to a user's system can steal private information stored on the system, launch denial-of-service attacks, or cause the system to distribute pirated software. The protection of sensitive information on home systems is a serious security concern. Almost all users face a risk that intruders can read, modify, or delete files on their personal computers. If the intruder takes over control of the computer, it can be used whenever the device is online. Intruders have placed programs on computers operated by both organizations and home users with high-speed Internet connections and relatively little security. The planted programs have mounted denial-of-service attacks against other sites, sending messages at a rate too high for the sites to handle, and thus disrupting the organization's communications.

What Can Be Done

Federal agencies and their employees can take a variety of actions to protect the networks and computers that are used for telecommuting. NIST recommends that:

All home networks connected to the Internet via a broadband connection should have some firewall device installed. The first line of defense for the home broadband user is a good network firewall. Home users may be aware of highly publicized Internet break-ins and denial-of-service attacks, but may not realize that their systems are vulnerable to such attacks. Many large organizations use firewalls to reduce the risk of unauthorized access to their networks. A firewall is a filter that allows certain types of packets, or message fragments, to enter and exit a network, while rejecting others. Firewalls have now been developed for home use. Personal firewalls available for home systems are software add-ins that filter packets going to and from the communications connection.

All home networks connected to the Internet via a broadband connection should have some firewall device installed. Personal software firewalls installed on each computer are useful and effective, but separate, dedicated, and relatively inexpensive hardware firewalls that connect between the broadband connection and the telecommuter's computer or network can provide even greater protection. Routers with built-in firewall features are available at most computer and electronics stores for $50 to $100. NIST strongly recommends that organizations use both personal and hardware firewall devices for high-speed connections. When both a software personal firewall and a separate device are in operation, the organization can generally screen out intruders and identify most rogue software that attempts to transmit messages from the user's computer to an external system.

Section 3 of the report provides technical details and information on the features and availability of software personal firewalls.

Web browsers should be configured to limit vulnerability to intrusion. Web browsers also represent a threat of security compromise and require additional configuration beyond the default installation. Web browsers should be configured to reduce vulnerability to intrusions. Browser plug-ins should be limited only to those required by the end user. A browser plugin is a software application that handles a particular type of file or content, such as display of documents and video. Each plugin is a potential source of attack. Active code should be disabled or used only in conjunction with trusted sites. The browser should always be updated to the latest or most secure version. Privacy is always a concern with web browsers. The two greatest threats to this privacy are the use of cookies and monitoring of web browsing habits of users by third parties. Cookies can be disabled or selectively removed using a variety of built-in web browser features or third-party applications.

Section 4 of the report provides details on disabling features in browser software.

Operating system configuration options should be selected to increase security. Since many computer tasks require passwords, users should select passwords that are not easily guessed or cracked. The default configuration of most home operating systems is generally inadequate from a security standpoint. File and printer sharing should almost always be disabled unless needed for home networking. The operating system and major applications should be updated to include the latest and most secure version or patch level.

All home computers should have an antivirus program installed and configured to scan all incoming files and electronic mail. The antivirus program should have its virus database updated on a regular basis. Another concern for many telecommuters is the threat to their privacy through the surreptitious installation of spyware by certain software applications. This spyware, while usually not intended to be malicious, reports information on users (generally without their knowledge) back to a third party. This information could be general information about the user's system or specifics on their web browsing habits. A variety of programs are available for detecting and removing this spyware.

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.

Encryption is an important and powerful method for protecting data in transmission and in storage. Encryption should be used when sensitive and critical data are subject to compromise. Commercial and freeware encryption products are readily available and easy to use. NIST maintains a list of cryptographic modules that have been validated to conform to Federal Information Processing Standard (FIPS) 140-2 (see http://csrc.nist.gov/cryptval/). This standard is applicable to all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems.

See Section 5 of the report for details on operating system security techniques, including the use of passwords, operating system updates, protection from viruses and worms, tools for spyware removal, and the use of encryption.

Selection of wireless and other home networking technologies should be in accordance with security goals. Several home networking technologies are available for telecommuters who wish to connect their home computers together to share resources. Some of these technologies are the same as their office counterparts (e.g., Ethernet), and others are designed specifically to meet the needs of telecommuters (e.g., phone- and power-line networking). While most of these technologies can be made relatively secure, some represent a threat to the security of the home network and, sometimes, of the office network. In particular, wireless networking has vulnerabilities that should be carefully considered before any installation. Wireless networking is a popular and fast-growing segment of the home networking market. It offers telecommuters the convenience of easy installation and the ability to stay connected when in their houses and close-by areas. Wireless networking broadcasts information that can be intercepted more easily than wired communications. Security concerns should be carefully considered before decisions are made to deploy wireless technology. To learn more about this technology, see NIST Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices* (http://csrc.nist.gov/publications/nistpubs/index.html).

Section 6 of the report covers the technologies that are available for home networking, including Ethernet, phone-line, power-line, and wireless networking.

Federal agencies should provide telecommuting users with guidance on selecting appropriate technologies, software, and tools that are consistent with the agency network and with agency security policies. Users have many approaches to choose from in establishing an off-site office. Organizations can support a range of solutions from low-cost techniques to highly sophisticated technologies such as virtual private networks (VPNs). VPNs can provide a high level of security, making it possible for secure communications to take place over public networks. However, they are more expensive and complex to implement than other solutions, and must be carefully configured on both the organization's central systems and the telecommuter's system. Because of the complexity of these systems, users must be informed and supported by their organizations to assure proper operation.

Whenever practical, agencies should provide telecommuting users with systems containing pre-configured security software and necessary hardware. If possible, agency security administrators should update and maintain the systems as well, to minimize reliance on users who are not specialists in security features. However, it may not always financially or logistically practical for agencies to provide users with pre-configured systems, and it is still possible to maintain an acceptable level of security with careful implementation of policies and technology. Many users, particularly if they do not require interactive access to agency databases, can obtain an adequate degree of security at very low cost and with little additional software, easing burdens on both the user and system administrators at the central computing system.

Sections 7 and 8 provide details on virtual private networks and telecommuting architectures for voice, electronic mail, and document exchange applications. Section 9 explores organizational considerations for telecommuting security.

Summary

Both organizations and their staff members benefit when access to computing resources and office networks is available to those on the road or working from home. While remote access to organizational resources always entails risks, most of these risks can be managed through careful planning and implementation. Although broadband connections generally represent a greater threat than dial-up connections, the threat can be reduced through careful configuration and the judicious use of the security tools and techniques. The benefits and risks of telecommuting will be important considerations for organizations in the years ahead.

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 web site is http://www.itl.nist.gov/.

Supplemental Information

Under the Computer Security Act of 1987 (P.L. 100-235), ITL's Computer Security Division develops computer security prototypes, tests, standards, and procedures to protect sensitive information from unauthorized access or modification. Focus areas include cryptographic technology and applications, advanced authentication, public key infrastructure, network security, criteria and assurance, and security management and support.

ITL issues publications covering research, guidance, standards, and the results of collaborative outreach efforts with industry, government, and academic organizations. Publications dealing with information security topics, including archived copies of bulletins, are available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications/.

Some publications of general interest covering network security topics include:

- NIST Special Publication 800-31, *Intrusion Detection Systems (IDS)*, November 2001.
- NIST Special Publication 800-40, *Recommendations for Applying Security Patches*, September 2002
- NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy* - a starting point on network security topics, January 2002.
- NIST Special Publication 800-44, *Guidelines on Securing Public Web Servers*, September 2002.
- NIST Special Publication 800-45, *Guidelines on Electronic Mail Security*, September 2002.
- NIST Special Publication 800-47, *Security Guide for Interconnecting Information Technology Systems*, September 2002.
- NIST Special Publication 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*, November 2002.
- NIST Special Publication 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, September 2002.

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

Official Business
Penalty for Private Use $300

Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195