November 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

GUIDE TO SECURING COMPUTERS USING WINDOWS XP HOME EDITION

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

Users of home computers must deal with many threats to the security of their systems, including sophisticated attacks by people who deliberately attempt to cause mischief, disrupt operations, commit fraud, and steal identities. Remotely launched attacks can spread malicious code and software, known as malware, through e-mail, malicious Web sites, and file downloads. These attacks may result in the insertion of viruses, worms, and spyware into home systems.

People attacking home computer systems can easily find information on the Internet to assist them in their activities. Information is readily available about vulnerabilities that are found in information technology (IT) products on a daily basis. Information about ready-to-use exploits and attacks can also be located readily. Since many IT products serve a wide range of users and systems, restrictive security controls are usually not enabled in systems by default. The available controls must be selected and installed appropriately for the individual systems. If the controls are not installed, the IT products are vulnerable. Therefore, many IT products are immediately vulnerable when they are installed out-of-the-box. Even experienced system administrators find that it is a complicated, arduous, and time-consuming task to identify a reasonable set of security settings for many IT products. But without the proper protection, home computer users are vulnerable to threats and risks.

The security issues that challenge home computer users are of paramount concern to federal agency staff members who telecommute, using laptop computers, mobile devices, and home computers. Unless these systems are specifically protected, they can be less secure than those that are used within the federal organizational setting. The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) has developed general guidance for securing workstations and small computer installations, with a focus on specific guidance applicable to those systems running Windows XP Home Edition.

NIST Special Publication (SP) 800-69, *Guidance for Securing Windows XP Home Edition: A NIST Security Configuration Checklist*

Issued in September 2006, NIST SP 800-69, *Guidance for Securing Windows XP Home Edition: A NIST Security Configuration Checklist, Recommendations of the National Institute of Standards and Technology (NIST)*, was written by Karen Kent and Murugiah Souppaya of NIST and John Connors of Booz Allen Hamilton. The publication is designed to alert home computer users to the threats to their systems and to make them aware of the security measures that are available for protecting systems. The information presented in the guide draws on extensive vendor knowledge and on the experience of government and security community experts. The Department of Homeland Security supported the development of the publication.

The guide explains the need to secure Windows XP Home Edition computers and the security protections that are available to reduce weaknesses, protect privacy, stop attacks, and preserve data. NIST SP 800-69 provides practical guidance on how to install Windows XP

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 December 2005:

- *Preventing and Handling Malware Incidents: How to Protect Information Technology Systems from Malicious Code and Software, December 2005*
- *Testing and Validation of Personal Identity Verification (PIV) Components and Subsystems for Conformance to Federal Information Processing Standard 201, January 2006*
- *Creating a Program to Manage Security Patches and Vulnerabilities: NIST Recommendations for Improving System Security, February 2006*
- *Minimum Security Requirements for Federal Information and Information Systems: Federal Information Processing Standard (FIPS) 200 Approved by the Secretary of Commerce, March 2006*
- *Protecting Sensitive Information Transmitted in Public Networks, April 2006*
- *An Update on Cryptographic Standards, Guidelines, and Testing Requirements, May 2006*
- *Domain Name System (DNS) Services: NIST Recommendations for Secure Deployment, June 2006*
- *Protecting Sensitive Information Processed and Stored in Information Technology (IT) Systems, August 2006*
- *Forensic Techniques: Helping Organizations Improve Their Responses to Information Security Incidents, September 2006*
- *Log Management: Using Computer and Network Records to Improve Information Security, October 2006*

Home Edition, how to secure new and existing installations, how to secure user accounts and settings, and how to maintain and monitor the security settings. The guidance applies generally to home desktop and laptop systems that run Windows XP Home Edition as the operating system.

In addition, the appendices contain step-by-step instructions for implementing additional security recommendations for computers with Windows XP Home Edition operating systems running Service Pack 2. Instructions are provided for securing certain applications, such as antivirus software, antispyware software, personal firewalls, e-mail clients, Web browsers, instant messaging clients, and office productivity suites.

The appendices also provide useful information about various tools, which are discussed in the publication, and which can be used to configure, manage, and monitor Windows XP Home Edition security settings. Other features include a glossary of terms used in the guide, a listing of acronyms, and a listing of in-print and online resources that should be helpful to people who want to learn more about Windows XP Home Edition and how to secure it.

The guide is available on NIST's Web pages at:

http://csrc.nist.gov/publications/nistpubs/index.html.

NIST Security Configuration Checklists

NIST SP 800-69 supports the NIST Security Configuration Checklists Program for IT Products. Checklists of security settings, such as NIST SP 800-69, are useful tools that have been developed to guide IT administrators and security personnel in selecting effective security settings that will reduce the risks of Internet connections and protect systems from attacks. A checklist, sometimes called a security configuration guide, lockdown guide, hardening guide, security technical implementation guide, or benchmark, is basically a series of instructions for configuring an IT product to an operational environment. Checklists can be effective in reducing vulnerabilities in systems, especially for small organizations with limited resources. IT vendors often create checklists for their own products, but other organizations such as consortia, academic groups, and government agencies also develop them.

NIST's checklists program provides a structure for the development and sharing of security configuration checklists. A central repository has been established for checklists that have been developed by organizations and submitted to NIST. This enables users to find checklists easily. NIST assists developers in making checklists that conform to common operational environments and associated baseline levels of security, and that are well documented and easy to use. A managed process provides for the review, update, and maintenance of the checklists.

Information about NIST's checklist program is available at:

http://csrc.nist.gov/checklists/index.html.

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.

Need to Secure Windows XP Home Edition

Users of Windows XP Home Edition need to be aware of the threats to the security of their systems and the security protections that will eliminate or reduce system vulnerabilities. The most common threat to these systems is malware, also known as malicious code, a computer program that is covertly placed onto a computer with the intent to compromise the privacy, accuracy, or reliability of the computer's data, applications, or operating system. Common types of malware threats are:

* Viruses - self-replicating code that makes copies of itself and distributes the copies to other files, programs, or computers.

* Worms - self-replicating programs that are completely self-contained and self-propagating.

* Malicious mobile code - malicious software that is transmitted from a remote system to be executed on a local system without the user's explicit instruction.

* Trojan horses - non-replicating programs that appear to be benign but that have hidden malicious purposes.

* Rootkits - collections of files that are installed onto computers to alter their functionality in a malicious and stealthy way, including installing and hiding other types of malware.

Security protections, also called security controls, are the measures used to thwart threats and to compensate for the computer's security weaknesses, or vulnerabilities. Threats are directed to take advantage of the vulnerabilities. Security protections can eliminate some of the vulnerabilities and also prevent attacks from taking advantage of vulnerabilities that cannot be eliminated. Security protections include the following:

* Technical protection - configuring a computer to restrict the actions that can be performed with the computer and to monitor the actions that are performed. Examples include the use of username and password to limit access to a computer or service, or the use of a feature in an application that automatically downloads and installs new versions of the application with previous errors corrected.

* Operational protection - the actions performed by computer users. Examples are the use of antivirus software to check a user's files, e-mails, and Web browsing for malware and to quarantine or delete any malware and prevent the malware from infecting the computer and causing damage. Other examples are making backup copies of users' files, keeping a computer and the computer's removable

media in a locked room, and users learning how to use a computer securely.

* Management protection - oversight of the security of computers. While taking place mostly within an organizational setting, management oversight also includes practices such as users performing periodic reviews of the security of their systems and identifying vulnerabilities.

Security protections cannot prevent all attacks, but they can greatly reduce the opportunities that attackers have to gain access to a computer or to damage the computer's software or information. A combination of security protections may be needed to secure a Windows XP Home Edition computer effectively and to maintain its security protection. Then, if one protection fails or is ineffective against a particular threat, other protections are likely to prevent the threat from succeeding. Windows XP Home Edition computers should be secured using a combination of technical and operational protections, such as antivirus software, Windows XP Home Edition configuration settings, and user education and security awareness activities. Security protections should be updated on a regular basis because new vulnerabilities in software are discovered on an ongoing basis.

NIST Recommendations for Securing Windows XP Home Edition

NIST recommends the following actions to improve the security of systems running Windows XP Home Edition:

Users should eliminate any known weaknesses in their Windows XP Home Edition computers because attackers will attempt to take advantage of them.

Known weaknesses should be eliminated through a combination of several methods, including the following:

* Install Windows XP Home Edition Service Pack 2 (SP2) and apply software updates to the computer on a regular basis, including Windows XP Home Edition and software applications.

* Limit access to the computer through separate password-protected user accounts for each person.

* Limit network access by disabling unneeded networking features, limiting the use of remote access utilities and configuring wireless networking securely.

* Disable services that are not needed.

Users should configure their Windows XP Home Edition computers to use a combination of software and software features that are designed specifically to stop attacks, particularly malware.

Every Windows XP Home Edition computer should use antivirus software, antispyware software, and a personal firewall at all times, and they should be kept up to date. Other helpful software performs the filtering of spam and Web content and carries out popup blocking. Users can also change settings on common applications such as e-mail clients, Web browsers, instant messaging clients, and office productivity suites to stop some attacks.

Users or administrators of Windows XP Home Edition computers should periodically perform backups that duplicate data from the computer onto another medium.

Performing regular backups helps to ensure that user data is available if an unfortunate event should occur, such as an attack against the computer, a hardware failure, a natural disaster, or human error. User data should be backed up periodically, on a weekly or monthly schedule, for example. Some of the options available for performing backups on Windows XP Home Edition computers are the use of utilities built into Windows XP Home Edition, as well as the use of third-party utilities and remote backup services.

Users or administrators of Windows XP Home Edition computers that connect to the Internet should ensure that they are protected properly from Internet-based threats.

The five most important protections that should be used for all Windows XP Home Edition computers connecting to the Internet are:

* Apply updates to the operating system and major applications, such as e-mail clients and Web browsers, regularly. The updates should be done through an automated process that checks for updates frequently.

* Use a limited user account for typical daily tasks on the computer. Full privileges should be used only when performing computer management tasks, such as installing updates and applications software, managing user accounts, and modifying software and settings.

* Run up-to-date antivirus software and antispyware software that is configured to monitor the computer and applications often used to spread malware, such as Web browsing and e-mail, and to quarantine or delete any identified malware.

* Use a personal firewall that is configured to restrict incoming network communications to only that which is required.

* Perform regular backups so that data can be restored in case an adverse event occurs.

For More Information

NIST SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist*, assists IT professionals, and particularly Windows XP system administrators and information security personnel, in securing Windows XP Professional systems running Service Pack 2.

NIST SP 800-70, *Security Configuration Checklists Program for IT Products: Guidance for Checklist Users and Developers*, discusses the development and dissemination of security configuration checklists to help users and developers of IT products secure their IT products and systems.

NIST SP 800-83, *Guide to Malware Incident Handling and Prevention: Recommendations of the National Institute of Standards and Technology*, assists

organizations and users in planning and implementing security programs to prevent malware incidents as much as possible and to limit damage from any incidents that might occur.

NIST publications assist organizations in planning and implementing a comprehensive approach to IT security. For information about NIST standards and guidelines that are referenced in the Windows XP guide, as well as other security-related publications, see NIST's Web page:

http://csrc.nist.gov/publications/index.html

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.