INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURING MICROSOFT WINDOWS XP SYSTEMS: NIST RECOMMENDATIONS FOR USING A SECURITY CONFIGURATION CHECKLIST

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

Organizations can strengthen the security of their local Windows XP workstations, mobile computers, and telecommuter systems when their system administrators apply information technology (IT) security configuration checklists as part of an established security program. NIST's Information Technology Laboratory has issued guidance to assist the trained and experienced system administrators who are responsible for the administration and security of Windows XP systems that are used in a variety of environments including the small office, the home office, and managed enterprise settings.

Checklists of security settings 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 to 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 have also developed them.

The NIST Checklist Program

Working with other government agencies, with IT product vendors, and with private industry, NIST is managing a program to make checklists readily available and to encourage the exchange of information about checklists. The Cyber Security Research and Development Act of 2002 designated NIST "to develop and revise, as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer

hardware or software system that is, or is likely to become, widely used within the Federal Government." NIST's checklist program supports the development, test, review, and dissemination of information about security configuration checklists for IT products, such as operating systems, database systems, web servers, e-mail servers, firewalls, routers, intrusion detection systems, virtual private networks servers, biometric devices, smart cards, telecommunication switching devices, and web browsers. For more information about this effort, see NIST Special Publication (SP) 800-70, *Security Configuration Checklists Program for IT Products*, the June 2005 bulletin in the ITL bulletin series, and the checklists website:
http://csrc.nist.gov/checklists/index.html.

Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist

NIST's Information Technology Laboratory has published Special Publication (SP) 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist: Recommendations of the National Institute of Standards and Technology*. The guide assists IT professionals, and particularly Windows XP system administrators and information security personnel, in securing Windows XP Professional systems running Service Pack 2 (SP2). Released in August 2004, Service Pack 2 contains changes that affect the security of Windows XP Professional systems and is considered a major upgrade to those systems. The recommendations in the guide do not apply to Windows XP Home systems running Service Pack 2. NIST plans to develop separate guidance for these systems.

Written by Murugiah Souppaya, Karen Kent, and Paul M. Johnson, NIST SP 800-68

NIST National Institute of Standards and Technology • Technology Administration • U.S. Department of Commerce

discusses the security components offered by Windows XP Professional SP2 and provides guidance on installing, backing up, and patching Windows XP systems. It also discusses security policy configurations, presents an overview of the settings in accompanying security templates, and provides information on how to apply additional security settings that are not included in the security templates. Tested and secure settings are recommended for popular office productivity applications, web browsers, e-mail clients, personal firewalls, anti-virus software, and spyware detection and removal utilities on Windows XP systems to protect these systems against viruses, worms, Trojan horses, and other types of malicious code.

The Windows XP checklist guide is available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/itsec/. Also available from this web page is NIST SP 800-43, *The Systems Administration Guidance for Windows 2000 Professional*, which recommends tested secure settings and includes configuration templates and security checklists for Windows 2000 Professional systems. NIST SP 800-43 provides detailed information about the security features of the Windows 2000 Professional system, security configuration guidelines for popular applications, and security configuration guidelines for the operating system.

Operational Environments

NIST has identified four types of operational environments to help developers to target their checklists to the security baselines that are associated with the different environments. Users can select the checklists that are most appropriate for their operating environments. NIST SP 800-68 recommends secure settings for Windows XP workstations in these four types of operational environments.

- **Small Office/Home Office (SOHO)**, sometimes called Standalone, describes small, informal computer installations that are used for home or business purposes. SOHO encompasses a variety of small-scale environments and devices, ranging from laptops, mobile devices, or home computers, to telecommuting systems located on broadband networks, to small businesses and small branch offices of a company. These environments, which generally focus on functionality and ease of use, may be less secure than the others, and may be supported by less experienced system administrators.

- **Enterprise** environments are sometimes referred to as managed environments that are structured in terms of hardware and software configurations. These environments, consisting of centrally managed workstations and servers, are usually protected from Internet threats by firewalls and other network security devices. Generally, a skilled staff supports users and provides security from initial system deployment through system maintenance. The structure and the staff contribute to the implementation and maintenance of consistent security practices.

- **Specialized Security-Limited Functionality** environments are at high risk of attack or data exposure, and therefore security takes precedence over usability. These environments include computers that are usually limited in their functionality to specific specialized purposes and that may contain highly confidential information, such as personnel records, medical records, and financial information. These computers also may perform vital organizational functions such as accounting and payroll processing. Providing sufficiently strong protection for these systems often involves a substantial tradeoff between security and functionality based on the premise that more than strictly necessary functionality provides more opportunity for exploitation. This can result in a significant reduction in system functionality and a higher risk of applications breaking, thus causing increased costs for system support. Because of the tradeoffs and complexities, a security-limited environment is not recommended for most SOHO users who are managing their own systems but may want better security. In most cases, the specialized security-limited functionality environment is not suitable for widespread enterprise usage.

- **Legacy** environments contain older systems or applications that often use older, less secure communication mechanisms. Other systems operating in a legacy environment may need less restrictive security settings so that they can communicate with legacy systems and applications. Using legacy services increases the potential risk of security breaches, as does lowering the security profile of other systems that need to interact with legacy systems. Legacy environments may exist within the SOHO and the enterprise environments, and in rare cases, within specialized security-limited functionality environments as well.

Security Templates

The guide for Windows XP systems includes security templates to enable system administrators to apply the security recommendations rapidly. The templates are text-based configuration files that specify values for security-relevant system settings, and that involve Windows XP policy areas, including password policy, account lockout policy, auditing policy, user rights assignment, system security options, event log policy, system service settings, and file permissions. The NIST template for Specialized Security-Limited Functionality environments represents the consensus settings from the Center for Internet Security (CIS), Defense Information Systems Agency (DISA), Microsoft, NIST, the National Security Agency (NSA), and the United States Air Force (USAF). The other NIST templates are based on Microsoft's templates and recommendations.

The templates and additional settings have been tested for their impact on both security and functionality. The NIST Windows XP Security Templates were developed to strengthen the security of Windows XP workstation configurations. However, since every system and environment is unique, system administrators should perform their own

testing. Specific settings may have to be modified because they might reduce the functionality or usability of a system, interfere with legacy applications, or conflict with local policies.

The templates should be thoroughly tested on representative systems before widespread deployment, and a full system backup should be performed before the recommendations are applied. To apply the templates to systems, administrators can use the Security Configuration and Analysis Microsoft Management Console (MMC) snap-in for a local system, compare a template's settings to the existing settings on a system, and identify discrepancies. In a Windows XP domain environment, the Group Policy Editor can be used to distribute security settings quickly from templates to computers in an Active Directory Organizational Unit (OU). Also the Group Policy Management Console (GPMC) can be used to manage Group Policy for multiple domains, and to import, edit, and apply security templates to Windows systems throughout an enterprise.

NIST Recommendations

System administrators should begin the process of securing Windows XP workstations from a clean formatted state. The installation process should be performed on a secure network segment or off the organization's network until the security configuration is completed, all patches are applied, and strong passwords are set for all accounts. After systems have been installed and securely configured, they should be regularly monitored and patched when software vulnerabilities are identified, and when new patches, policies, and procedures are issued.

The recommendations include measures for testing and configuring common Windows applications, such as office productivity tools, web browsers, e-mail clients, personal firewalls, anti-virus software, and spy-ware detection and removal utilities. This list is not intended to be a complete list of applications to install on Windows XP, nor does NIST endorse particular products. The configuration settings for applications focus on deterring viruses, worms, Trojan horses, and other malicious code. The recommendations can help to protect Windows XP systems from malicious code when the applications are being used.

The settings and recommendations assist organizations in making their Windows XP systems more secure, and provide system administrators with the information necessary to modify the settings and to comply with local policy or special situations. The baseline recommendations and settings provide a high

level of security for Windows XP Professional systems when used in conjunction with a sound and comprehensive local security policy and other relevant security controls. The recommendations are also appropriate for managed environments that are configuring and deploying laptops for mobile users and desktop computers for telecommuters.

NIST recommends that the IT professionals using the Windows XP checklist review all of the material provided in the guide, as well as the recommended references. Decisions to install and patch the operating system, to use and modify the security templates, and to apply additional controls should be made in accordance with the principles of sound system administration.

Using Checklists as Security Controls

The Federal Information Security Management Act (FISMA) requires that federal agencies carry out a risk-based approach to information security. To support agencies in conducting their information security programs, FISMA called for NIST to develop federal standards for the security categorization of federal information and information systems according to risk levels, and for minimum security requirements for information and information systems in each security category. Two Federal Information Processing Standards (FIPS) have been developed. FIPS 199, *Standards for the Security Categorization of Federal Information and Information Systems*, issued in February 2004, assists agencies in categorizing their information and information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. Soon to be issued in final form, FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* helps agencies provide appropriate levels of information security based on levels of risk. In applying the provisions of FIPS 200, agencies will categorize their systems as required by FIPS 199, and then select an appropriate set of security controls from NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, to satisfy their minimum security requirements.

Organizations using the Windows XP security guide, its security templates, and its other general prescriptive recommendations should be able to meet the baseline system configuration requirements for Windows XP systems. The controls are consistent with the management, operational, and technical security controls described in NIST SP 800-53, and they provide a high level of security for Windows XP systems when used in conjunction with sound local security policies. Organizations should:

- Protect each system based on the potential impact to the system of a loss of confidentiality, integrity, or availability.

- Reduce the opportunities that attackers have to breach a system by limiting functionality according to the principle of least privilege and resolving security weaknesses.

- Select security controls that provide a reasonably secure solution while supporting the needed functionality and usability.

- Use multiple layers of security so that if one layer fails or otherwise cannot counteract a certain threat, other layers might prevent the threat from successfully breaching the system.

- Conduct risk assessments to identify threats against systems and determine the effectiveness of existing security controls in counteracting the threats. Perform risk mitigation to decide whether and what additional measures should be implemented.

- Document procedures for implementing and maintaining security controls, and maintain other security-related policies and documentation that affect the configuration, maintenance, and use of systems and applications, such as acceptable use policy, configuration management policy, and IT contingency plans.

- Test all security controls to determine what impact they have on system security, functionality, and usability, and address any significant issues.

- Monitor and maintain systems on a regular basis so that security issues can be identified and mitigated promptly. Actions that may be needed include acquiring and installing software updates; monitoring event logs; providing remote system administration and assistance; monitoring changes to operating system and software settings; protecting and sanitizing media; responding promptly to suspected incidents; performing vulnerability assessments; disabling and deleting unused user accounts; and maintaining hardware.

More Information

The NIST publications mentioned in this bulletin, as well as other publications needed for the secure management of systems, are available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendations or endorsements by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.