ITL BULLETIN FOR MAY 2011

USING SECURITY CONFIGURATION CHECKLISTS AND THE NATIONAL CHECKLIST PROGRAM

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

The secure management of information systems is a difficult challenge for both private sector and government organizations. We depend upon the Internet to carry out essential services in many areas, including finance, healthcare, transportation, energy, homeland security, and protection of critical infrastructures. With the increasing complexity of systems and networks, organizations must devote significant staff and resources to maintain reliable, accurate, safe, and secure operations. Cyber attacks have become more frequent, widespread, and potentially damaging in today's highly interconnected networks. Vulnerabilities in information technology (IT) products are discovered frequently, and techniques for exploiting weaknesses are readily available on the Internet.

While the solutions to these security challenges are complex, the use of automated tools and methods can help organizations to manage security risks more effectively and avoid costly security breaches. One useful and effective tool is the security configuration checklist. A security configuration checklist (also called a lockdown, hardening guide, or benchmark) helps organizations to automatically set and verify the appropriate security settings for different IT products.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) supports the users and developers of checklists through its National Checklist Program (NCP) and with publications that recommend practices for the use and development of checklists. A revised publication, NIST Special Publication (SP) 800-70 Rev. 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers: Recommendations of the National Institute of Standards and Technology,* was issued earlier this year.

The Contents of Checklists

A checklist contains a series of instructions for configuring a product to a particular operational environment. Some checklists also contain instructions or procedures for verifying that the product has been configured properly. Checklists can include templates or automated scripts, patches or patch descriptions, Extensible Markup Language (XML) files, and other procedures.

Checklists can also provide administrative practices that improve the security of an IT product. Often, successful attacks on systems result from poor administrative practices,

such as not changing default passwords or not applying vendor patches. Checklists can be tailored by organizations to meet their specific local security, operational, and compliance requirements.

Frequently, checklists are created by IT vendors for their own products; however, checklists are also created by other organizations, such as academia, consortia, and government agencies. The use of well-written, standardized checklists can reduce the security risks of IT products and services. Checklists can be particularly helpful to small organizations and to individuals with limited resources for securing their systems.

Uses and Benefits of Checklists

System administrators and end users can follow the instructions in the checklist to configure a product or system to the level of security implemented in the checklist or to verify that a product or system has been configured properly. The system administrator may need to modify the checklist to incorporate the organization's security policy.

Checklists can be applied to a wide range of devices and software: general-purpose operating systems; desktop applications such as email clients, Web browsers, word processors, personal firewalls, and antivirus software; infrastructure devices such as routers, firewalls, virtual private network (VPN) gateways, intrusion detection systems (IDSs), wireless access points, and telecommunication systems; application servers such as Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Web, mail, and database servers; and other network devices such as mobile devices, scanners, printers, copiers, and faxes.

Since many IT products are developed for general use, checklists can help an organization to apply the appropriate security settings to meet its specific needs. Using checklists helps to reduce system vulnerabilities and to improve the consistency and predictability of system security, particularly when used in conjunction with user training and awareness activities and other supporting security controls as part of a risk management process. The use of checklists reduces the time required to research, develop, and test appropriate security configurations for installed IT products, helping organizations make more efficient use of their resources.

Federal government agencies can use checklists to meet the requirements of the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. FISMA requires each agency to determine minimally acceptable system configuration requirements and to ensure compliance with them. Checklists can also map specific technical control settings to the corresponding security controls, which federal organizations select and specify in accordance with Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems;* FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems;* and NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations.*

While security configuration checklists cannot guarantee total security for information systems, their use can significantly improve overall levels of security. Checklists that emphasize hardening of systems against the hidden software flaws can lead to greater levels of product security and protection from future threats. Federal agencies using FISMA-related checklists can achieve more consistent and cost-effective configuration settings.

NIST's National Checklist Program (NCP)

The Cyber Security Research and Development Act of 2002, P.L. 107-305, specifies that NIST "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 maintains the National Checklist Repository (NCR), a publicly available resource that contains information on a variety of security configuration checklists for specific IT products or categories of IT products. The repository contains metadata that describes each checklist. The repository also contains copies of some checklists, primarily those developed by the federal government, and has pointers to the locations of other checklists.

NIST is moving toward the conformance of the checklist repository to the Security Content Automation Protocol (SCAP), which enables standards-based security tools to automatically perform configuration checking using NCP checklists. For example, the repository contains checklists (and pointers to tools) for performing configuration checking of systems implementing the United States Government Configuration Baseline (USGCB), and the Federal Desktop Core Configuration (FDCC), both using SCAP. The NCR also hosts pointers to other SCAP-enabled checklists produced by IT product vendors and government organizations.

Users can browse and search the repository's metadata to locate a particular checklist using a variety of criteria, including the product category, vendor name, and submitting organization. Organizations can use the centralized checklist repository to find the current, authoritative versions of security checklists and to determine which ones best meet their needs.

The NCP provides procedures and requirements for developers of checklists. After testing and documenting checklists according to the NCP guidelines, developers may submit checklists to NIST for inclusion in the NCP. NIST screens the submissions according to program requirements and addresses any issues with the developer. A public review of the checklist is conducted, usually taking 30 to 60 days. Any comments submitted are reviewed, and any issues raised are resolved. NIST posts the checklist with its metadata on the repository and announces its availability. NIST periodically asks checklist developers to review their checklists and to provide updates as necessary. NIST retires or archives checklists as they become outdated.

The repository is located at http://checklists.nist.gov/.

NIST Special Publication (SP) 800-70 Rev. 2, *National Checklist Program for IT Products—Guidelines for Checklist Users and Developers: Recommendations of the National Institute of Standards and Technology*

Recently revised by NIST, this publication helps both users and developers of security configuration checklists. It includes general information about threats and fundamental technical security practices for operational environments. Checklist users are advised how to select checklists from the NIST National Checklist Repository, how to evaluate and test checklists, and how apply them to IT products. Information of special interest to checklist developers includes the policies, procedures, and general requirements for participation in the NIST National Checklist Program (NCP).

NIST SP 800-70 Rev. 2 was written by Stephen D. Quinn and Murugiah Souppaya of NIST, and by Melanie Cook and Karen Scarfone of G2, Inc. One section of the report presents an overview of checklists and describes the contents and operations of the NIST NCP. This information is supplemented in a following section that includes additional details on predefined checklist operational environments, threats to systems, and fundamental technical security practices used in the NCP. These details help developers to create checklists that are consistent with security practices, and help checklist users to better understand the fundamental security practices and to select the checklists that best match their own operational environments.

Another section of the report contains specific information for potential checklist users. It describes how to use the NCP to find and retrieve checklists that best match the identified needs. Guidance is provided on how to implement checklists, to analyze the specific operating environment, and to tailor checklists to meet users' needs. Guidance is also provided for current and prospective checklist developers, advising on the procedures for preparing and submitting a checklist to NIST for inclusion in the checklist repository.

Extensive tables, figures, and appendices supplement the discussion of checklists. Included in the appendices are reference sources that were used to develop the report; the checklist description fields of the template used to catalogue checklists in the NIST repository; the programmatic and legal requirements that must be satisfied to participate in the NCP; the NCP participation and logo usage agreement form; additional requirements that USGCB checklists must meet; a list of acronyms; and a glossary of the terms used in the publication.

NIST SP 800-70 Rev.2 is available from the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

NIST Recommendations to Checklist Users and Developers

NIST recommends that organizations adopt the following practices:

Organizations should apply checklists to operating systems and applications to reduce the number of vulnerabilities that attackers can attempt to exploit and to lessen the impact of successful attacks.

The use of checklists can improve system security, but must be used in conjunction with ongoing security maintenance, such as patch installation. Using checklists that emphasize both hardening of systems against software flaws (e.g., by applying patches and eliminating unnecessary functionality) and configuring systems securely will typically reduce the number of ways in which the systems can be attacked, resulting in greater levels of product security and protection from future threats. Checklists can also be used to verify the configuration of some types of security controls for system assessments, such as confirming compliance with certain FISMA requirements and federal mandates or other security requirements.

Federal agencies are required to use appropriate security configuration checklists from the NCP when available. Paragraph (d) of section 39.101 of the Federal Acquisition Regulation (FAR), revised in February 2008, states: "In acquiring information technology, agencies shall include the appropriate IT security policies and requirements, including use of common security configurations available from the NIST Web site at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated."

Also, FISMA, section 3544(b)(2)(D)(iii), requires each federal agency to determine minimally acceptable system configuration requirements and to ensure compliance with them. Federal agencies, as well as vendors of products for the federal government, should acquire or implement and share such checklists using the NIST repository. NIST encourages checklist developers to assert mappings to the security controls delineated in NIST SP 800-53 to facilitate FISMA compliance checking for federal agencies.

Organizations should consider the availability of security configuration checklists when they select IT products.

When selecting checklists, checklist users should carefully consider the degree of automation and the source of each checklist.

NIST has defined four tiers of checklists to assist checklist users in identifying the major differences among checklists:

- Tier I checklists are prose-based with narrative descriptions of how a product's configuration can be altered.

- Tier II checklists document their recommended security settings in a machine-readable but nonstandard format, such as a proprietary format or a product-specific configuration script. These checklists may include some elements of SCAP.

- Tier III checklists use SCAP to document their recommended security settings in machine-readable standardized SCAP formats. Tier III checklists can be processed by SCAP-validated tools, which are products that have been validated by an accredited independent testing laboratory as conforming to applicable SCAP specifications and requirements.

- Tier IV checklists include all properties of Tier III checklists, and have been validated by NIST or a NIST-recognized authority for interoperability with SCAP-validated products. Tier IV checklists also provide a complete mapping of low-level security settings and high-level security requirements in accordance with FISMA requirements and the selection and implementation of security controls.

When multiple checklists are available for a particular product, organizations should consider the tier of each checklist. Generally, checklists from higher tiers can be used more consistently and efficiently than checklists at lower tiers. There may be other significant differences among checklists that are not indicated by the tier; for example, one checklist may include software bundled with an operating system (e.g., Web browser, email client) while another checklist addresses that operating system only. Also checklist users identify the assumptions on which the checklists are based (e.g., environment, threat model) and determine the checklists that may be appropriate for further analysis.

Users in civilian agencies of the federal government should search first for government-authorized or mandated checklists. In general, users should search for NIST-produced checklists, which are tailored for civilian agency use. If a NIST-produced checklist is not available, agency-produced checklists from the Defense Information Systems Agency (DISA) or the National Security Agency (NSA) should be used if available. If formal government-authored checklists do not exist, then organizations are encouraged to use vendor-produced checklists. If vendor-produced checklists are not available, then other checklists that are posted on the NCP Web site may be used.

Checklist users should customize and test checklists before applying them to production systems.

Organizations should consider customizing checklists that are not mandatory for the organization to adopt. The configuration settings are based on sound knowledge of security threats and vulnerabilities, but may not support organization-specific security and operational requirements, existing security controls, and other factors that may necessitate changes. Organizations should carefully evaluate the checklist settings and give them considerable weight, and then make any changes necessary to adapt the settings to the organization’s environment, requirements, policies, and security objectives. This is particularly true for checklists intended for an environment with significantly different security needs. All deviations from the checklist settings should be documented for future reference, and include the reason behind each deviation and the impact of deviating from the setting.

Before applying a checklist that will be used to alter product settings, users should first test it on noncritical systems, preferably in a controlled non-operational environment. Each checklist in the NIST repository has been tested by its developer, but there are often significant differences between a developer's testing environment and an organization's operational environment, and some of these differences may affect checklist deployment. In some cases, a security control modification can have a negative impact on a product's functionality and usability, or on other products or security controls. Consequently, it is important to perform testing to determine the impact on system security, functionality, and usability; to document the results of testing; and to take appropriate steps to address any significant issues.

Checklist users should take their operational environments into account when selecting checklists, and checklist developers should target their checklists to one or more operational environments.

Checklists are significantly more useful when they can run in common operational environments. The NCP has identified several broad and specialized operational environments. The two broad operational environments are referred to as Standalone (or Small Office/Home Office [SOHO]) and Managed (or Enterprise). Three typical Custom environments, which could be subsets of the broader environments, are Specialized Security-Limited Functionality (SSLF), Legacy, and United States Government. One of the environments should be common for most users. By thoroughly identifying and describing these environments, users will be able to select the checklists that are most appropriate for their particular operating environments, and developers will be able to better target their checklists to the general security characteristics associated with their operating environments.

NIST strongly encourages IT product vendors to develop security configuration checklists for their products and contribute them to the NIST National Checklist Repository.

NIST encourages IT product vendors to develop security configuration checklists for their products, since the vendors have the most expertise on the possible security configuration settings and the best understanding of how the settings relate to and affect each other and impact the system functionality and usability. Vendors that create security configuration checklists should submit them for inclusion in the National Checklist Repository through the NCP, following the process and guidance provided.

For More Information

The **National Vulnerability Database (NVD)** is the U.S. government repository of standards-based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. NVD includes databases of SP 800-53 security controls, security checklists, security-related software flaws,

misconfigurations, product names, and impact metrics. The NVD is available at http://nvd.nist.gov/home.cfm.

The NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the **United States Government Configuration Baseline (USGCB)** using the Security Content Automation Protocol (SCAP). USGCB information is available at http://usgcb.nist.gov.

The **Security Content Automation Protocol (SCAP)** is a suite of specifications for organizing, expressing, and measuring security-related information in standardized ways, as well as related reference data such as unique identifiers for vulnerabilities. Information about SCAP is available at http://scap.nist.gov.

For information about NIST standards and guidelines referenced in this bulletin, as well as other security-related publications, see the NIST Web page http://csrc.nist.gov/publications/index.html.

Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.gov.

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