ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

NIST'S SECURITY CONFIGURATION CHECKLISTS PROGRAM FOR IT PRODUCTS

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

The National Institute of Standards and Technology (NIST) is cooperating with other federal agencies, IT vendors, and with industry to advance the development and use of security configuration checklists. A security configuration 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 information technology (IT) product to an operational environment. Checklists can be useful tools for 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.

Checklists can be used to counter threats to computers, such as remotely launched attacks through networks and the spread of malicious code through e-mails, malicious websites, and file downloads. Vulnerabilities in IT products are discovered almost daily. Because many IT products are designed to serve a wide variety of users, they may not provide needed restrictive security controls routinely. As a result, computers can be vulnerable to threats when the products are installed. Even experienced system administrators may find it difficult and time-consuming to identify the right set of security settings for many IT products.

The NIST checklists program, described in this ITL Bulletin, serves both checklists developers, e.g., vendors, and users, e.g., federal agencies. NIST provides checklist developers with guidance for developing standardized, high-quality checklists to secure IT products. Checklist developers are invited to submit their well-documented and usable checklists to NIST for review and for listing in an easy-to-use repository of checklists. NIST has developed a formal process to review, update, and maintain the checklists in the repository. Users are invited to browse through the descriptions in the repository to locate a particular checklist. The checklists repository is organized by product category, vendor, and submitting organization, and currently includes over fifty checklists. Information about the program and access to the checklist repository is available from the NIST web page: http://csrc.nist.gov/checklists/.

Why Checklists Are Needed

The Cyber Security Research and Development Act of 2002 (Public Law 107-305) designates 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."

Checklists provide a baseline of security to protect against common and dangerous threats, and they provide a consistent approach to securing systems. This is especially important for small organizations, which may not have the resources to investigate and develop their own security settings for installed products. Checklists alone cannot

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 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 April 2004

- *Selecting Information Technology Security Products*, April 2004
- *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004
- *Information Technology Security Services: How to Select, Implement, and Manage*, June 2004
- *Guide for Mapping Types of Information and Information Systems to Security Categories*, July 2004
- *Electronic Authentication: Guidance For Selecting Secure Techniques*, August 2004
- *Information Security Within The System Development Life Cycle*, September 2004
- *Securing Voice Over Internet Protocol (IP) Networks*, October 2004
- *Understanding the New NIST Standards and Guidelines Required by FISMA*, November 2004
- *Integrating IT Security into the Capital Planning and Investment Control Process*, January 2005
- *Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201 Approved by the Secretary of Commerce*, March 2005
- *Implementing The Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, April 2005
- *Recommended Security Controls for Federal Information Systems: Guidance for Selecting Cost-effective Controls Using a Risk-based Process*, May 2005

guarantee complete security, but they can reduce an organization's vulnerabilities when used with well-developed guidance, leveraged with high-quality security expertise, vendor product knowledge, operational experience, and accompanied with tools.

What are Checklists

A security checklist in its simplest form can be a document that contains instructions or procedures for configuring an IT product to a baseline level of security. Checklists are also commonly referred to as lockdown guides, hardening guides, security technical implementation guides (STIGs), or benchmarks. A checklist could contain scripts, templates, and pointers to patches, or updates or firmware upgrades that can be applied to a product. A checklist might include any of the following:

- Configuration files that automatically set various security settings (e.g., executables, security templates that modify settings, scripts);
- Documentation (e.g., text file) that guides the checklist user to configure software manually;
- Documents that explain the recommended methods for the secure installation and configuration of a device; and/or
- Policy documents that set forth guidelines for activities such as audits, authentication security (e.g., passwords), and perimeter security.

The instructions in a security configuration checklist can apply to administrative practices as well as security settings for an IT product to support improvements to the product's security. Often, successful attacks on systems are the direct result of poor administrative practices such as not changing default passwords or failure to apply new patches.

While many checklists have been developed, they vary in quality, usability, and documentation, and they may not be kept current with software updates. The NIST program provides a consistent process for the development, review, and use of checklists. Examples of IT product technology areas that are included are: operating systems, database systems, web servers, e-mail servers, firewalls, routers, intrusion detection systems, virtual private networks, biometric devices, smart cards, telecommunication switching devices, and web browsers.

The NIST Checklists Program

NIST is currently working with other checklist-producing organizations including the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and the Center for Internet Security (CIS), as well as IT product vendors and vendors of configuration and management products.

Ideally, product vendors create checklists as they release new products. The vendor is often in the best position to create the checklists; however, in some cases, third-party checklists may be submitted, such as from recognized security groups, state governments, and corporations. After testing their checklists and documenting them according to the guidelines of the program, checklist developers can submit a checklist package to NIST.

NIST screens the checklist package for adherence to the development criteria and format. After addressing any identified issues with the checklist submitter, NIST posts the checklist for public review. Issues that are raised during the review will be referred to the checklist developer. After all issues have been addressed satisfactorily, the checklist or checklist description will be posted on the NIST checklist repository (http://csrc.nist.gov/checklists/repository/index.html).

Checklist submitters are responsible for maintaining their checklists when new versions of the products appear. When the final checklist is listed, NIST will set up a periodic review schedule with the developer. The review will take place in one year, or sooner, depending upon factors such as the discovery of new vulnerabilities. If the developer decides to update the checklist, NIST will announce that the checklist is in the process of being updated. If the checklist contains major changes, it will be accepted as if it were a new submission; it must undergo the same reviews as a new submission. Outdated or incorrect checklists will be retired or archived.

Checklist producers can use the special checklist program logo on their product literature or websites to show participation in the NIST program and ownership of a checklist on the repository. To use the logo, the producer must provide checklist-related assistance to users. The logo, which is reproduced on page 1 of this bulletin, does not convey NIST endorsement of the checklist or IT product.

Using Checklists

Organizations usually conduct a requirements analysis before selecting and purchasing IT products. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, provides useful guidance for federal agencies on conducting the requirements analysis and the subsequent risk assessment. Users should identify their functional needs to determine what functions an IT product must perform and what security controls should be used. Next, threats related to particular products and vulnerabilities that could be exploited in the product should be identified. Then the needed security controls should be determined to minimize or eliminate the likelihood of threats exploiting system vulnerabilities. After determining local operational product requirements, users can research and retrieve the checklists that match their operational environment and security requirements. Users are able to modify and document the checklist to take into account local policies and needs, test the checklist, and provide any feedback to NIST and the checklist developers after applying the checklist in their systems.

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.

Users can browse a database of checklist descriptions to locate and retrieve a particular checklist using a variety of different fields, including the following:

- Checklist Summary: Summarizes the purpose of the checklist and its settings.
- Status: Whether Candidate, Final, or Archived.
- Version: Indicates the version or release number of the checklist.
- Revision Date: States the date when the checklist was last revised.
- Vendor: Contains the name of the manufacturer of the IT product.
- Point of Contact: Provides the e-mail address where questions, comments, suggestions, and problem reports can be sent in reference to the checklist. The point of contact should be an e-mail address that the checklist developer monitors for checklist problem reports.
- Product Category: The main product category of the IT product, e.g., firewall, Intrusion Detection System (IDS), operating system, web server, etc.
- Product Name: The official IT product name.
- Product Role: Specifies the primary use or function of the IT product as described by the checklist, e.g., Client Desktop Host, Web Server, Bastion Host, Network Border Protection, Intrusion Detection, etc.
- Product Version: The specific software or firmware released version number of the IT product, including service pack or patch level as appropriate.
- Rollback Capability: Whether the changes in product configuration made by applying the checklist can be rolled back, and if so, how to roll back the changes.
- Target Audience: Intended audience that should be able to install, test, and use the checklist, including suggested minimum skills and knowledge required to correctly use the checklist.
- Target Operational Environment: The IT product's operational environment, e.g., SOHO, Managed, Custom (with description such as Specialized Security-Limited Functionality or Legacy).
- Testing Information: Platforms on which checklist was tested. Can include any additional testing-related information such as summary of testing procedures used.
- Product Support: Vendor will accept support calls from users who have applied the checklist on their IT product; warranty for the IT product has not been affected. This support is required for participation in the Checklist Program and use of the Checklist Program logo.

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.

- **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 may be less secure than the others and may be supported by less experienced system administrators.
- **Managed or Enterprise** environments are environments that are structured in terms of hardware and software configurations, usually consisting of centrally managed workstations and servers protected from the Internet 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.
- **Custom** environments contain systems in which the functionality and degree of security do not fit into the other two environments. There are two typical custom environments:
  - **Specialized Security-Limited Functionality** environments contain systems and networks at high risk of attack or data exposure. Protecting the security of these systems may be a higher priority than the usability of the systems or their interoperability with other systems. These systems have limited or specialized functionality in a highly threatened environment such as an outward facing firewall or public web server. Checklists for this environment are not recommended for home users or for large-scale, general purpose systems. A Specialized Security-Limited Functionality environment could be a subset of a SOHO or an enterprise environment.
  - **Legacy** environments contain older systems or applications that use older, less-secure communication mechanisms. Other machines operating in a legacy environment may need less restrictive security settings so that they can communicate with legacy systems and applications. These environments could exist within a SOHO or an enterprise environment.

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/.

NIST Special Publication 800-70, Security Configuration Checklists Program for IT Products

NIST recently issued NIST Special Publication 800-70, *Security Configuration Checklists Program for IT Products*. Written by Murugiah Souppaya, John Wack, and Karen Kent, this guide was developed with the sponsorship of the Department of Homeland Security (DHS) and is available on NIST's web pages (http://csrc.nist.gov/checklists). The publication discusses checklists and their benefits, and explains the operation of the checklists program. It describes the policies, procedures, and general requirements for participation in the program, and explains how to retrieve checklists from NIST's repository. It also provides general information about threat models and baseline technical security policies for associated operational environments.

NIST has developed checklists for Microsoft Windows™ 2000 and for Microsoft Windows XP systems. Draft 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*, and NIST SP 800-43, *The Systems Administration Guidance for Windows 2000 Professional*, are both available at: http://checklists.nist.gov/repository/.

How Checklists Will Help Federal organizations

Checklists will help federal organizations carry out the requirements of the Federal Information Security Management Act (FISMA) of 2002 (Public Law 107-347). Section 3534(b) (2) (D) (iii) of this Act requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them. Accordingly, federal agencies, as well as vendors of products for the federal government, are encouraged to acquire or develop and share such checklists using the NIST repository.

For More Information

The NIST website (http://csrc.nist.gov/checklists/) provides links to the checklist repository, announcements, answers to frequently asked questions, and to documents and forms for participation in the checklists program. Information is available about a workshop held by NIST in 2003 to identify federal government checklist activities and needs, voluntary efforts for building security checklists, and industry capabilities for developing checklists for IT products widely used by the federal government. Also available is information about XCCDF, a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. XCCDF provides a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, to help foster more widespread application of good security practices.

NIST welcomes comments on all aspects of the checklists program. Comments may be submitted to checklists@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.*

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