ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SELECTING INFORMATION TECHNOLOGY SECURITY PRODUCTS

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

Information technology security products are essential to better secure information technology (IT) systems, and many products to protect IT systems are available in the marketplace today. But IT security products alone will not guarantee that an organization's IT systems are secure. Security products should be selected and used within the organization's overall program to manage the design, development, and maintenance of its IT security infrastructure, and to protect the confidentiality, integrity, and availability of its mission-critical information.

The foundation for the selection of IT security products is a comprehensive information security management program, including risk management procedures that are applied throughout the System Development Life Cycle (SDLC). The risk management process enables organizations to analyze their systems for security, to identify appropriate and cost-effective controls, to select and use security products that will protect their information and information systems, and to monitor the effectiveness of the controls. Management, operational, and technical controls are needed to support security objectives and to protect information.

Guide to Selecting Information Technology Security Products

NIST's Information Technology Laboratory published Special Publication (SP) 800-36, *Guide to Selecting Information Technology Security Products*, to help organizations select cost-effective and useful products for their systems. Written by Timothy Grance, Marc Stevens, and Marissa Myers, NIST SP 800-36 defines broad security product categories and specifies product types, product characteristics, and environment considerations within those categories. This *ITL Bulletin* summarizes the publication, which is available at http://csrc.nist.gov/publications.

The guide presents pertinent questions that an organization should ask when selecting a product from within the categories. As security products evolve and change, organizations can modify the questions to be asked to fit their particular needs. When used with other NIST publications, including those listed in the More Information section at the end of this bulletin, the guide will help organizations develop a comprehensive approach to managing their IT security and information assurance requirements.

In its March 2004 report, "Information Security: Technologies to Secure Federal Systems," the U.S. General Accounting Office (GAO) referred to the product selection guide, as well as other NIST publications. The GAO report discusses commercially available, state-of-the-practice cybersecurity technologies that federal agencies can use to secure their information systems, and states, "these technologies implement the technical controls that NIST recommends federal agencies deploy in order to effectively meet federal requirements." The GAO emphasizes the importance of developing a framework and a continuing cycle of activity to assess risks, implement effective security procedures, and monitor the effectiveness of the procedures. GAO 04-467 is available at http://www.gao.gov/.

Who Selects Security Products for an Organization

People throughout the organization may be involved in product selection at both the individual and the group

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 December 2002

- *Security of Public Web Servers*, December 2002
- *Security of Electronic Mail*, January 2003
- *Secure Interconnections for Information Technology Systems*, February 2003
- *Security for Wireless Networks and Devices*, March 2003
- *ASSET: Security Assessment Tool for Federal Agencies*, June 2003
- *Testing Intrusion Detection Systems*, July 2003
- *IT Security Metrics*, August 2003
- *Information Technology Security Awareness, Training, Education, and Certification*, October 2003
- *Network Security Testing,* November 2003
- *Security Considerations in the Information System Development Life Cycle*, December 2003
- *Computer Security Incidents: Assessing, Managing, and Controlling the Risks*, January 2004
- *Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems*, March 2004

level. All should be aware of the importance of security in the organization's information infrastructure and the security impacts of their decisions. People involved include the following:

- IT Security Program Manager, who is responsible for developing enterprise standards for IT security;
- Chief Information Officer, who is responsible for the organization's IT planning, budgeting, investment, performance, and acquisition;
- IT Investment Board (or equivalent), which is responsible for planning and managing the capital planning and investment control process for federal agencies, as specified in the Information Technology Management Reform Act of 1996 (Clinger-Cohen Act);
- Program Manager, who owns the data, initiates the procurement, is involved in strategic planning, and is aware of functional system requirements;
- Acquisition Team, which is composed of representatives from program, technical, and contracting areas of the organization and which provides a balanced perspective of cost and schedule considerations;
- Contracting Officer, who has authority to enter into, administer, and terminate contracts;
- Contracting Officer's Technical Representative, who is appointed by the Contracting Officer to manage the technical aspects of a particular contract;
- IT System Security Officer, who is responsible for ensuring the security of an information system throughout its life cycle; and
- Other participants, who may include the system certifier and accreditor, system users, and people representing information technology, configuration management, design, engineering, and facilities groups.

Using the Risk Management Process in Product Selection

Before selecting specific products, organizations should review the current status of their security programs and the security controls planned or in place to protect their information and information systems. Organizations should use the risk management process to identify the effective mix of management, operational, and technical security controls that will mitigate risk to an acceptable level.

The Secretary of Commerce recently approved Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, for use by federal government organizations (available at http://csrc.nist.gov/publications/fips/). The new standard helps federal agencies identify and prioritize their most important information and information systems by defining the maximum impact that a breach in confidentiality, integrity, or availability could have on the agency's operations, assets, and/or individuals. The security categorization serves as the starting point for the selection of security controls that are commensurate with the importance of the information and information system to the agency, and then for the selection of appropriate security products. Draft NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides recommendations for minimum-security controls associated with the various security categories defined in FIPS 199. Organizations may adjust the set of recommended controls based on local risk assessments.

After systems and products are in place, the controls should be monitored for effectiveness throughout the system life cycle.

Products Discussed

NIST SP 800-36 provides information about the following IT security product categories, including the types of products in each category, the product characteristics, and the environment considerations for each category:

- Identification and Authentication products including security tokens, authentication protocols, and biometric control systems;
- Access Control products including access control lists and role based access control systems;
- Intrusion Detection products including network-based, host-based, and application-based systems;
- Firewall products that control the flow of network traffic between networks or between a host and a network;
- Public Key Infrastructure systems that manage cryptographic key pairs and associate key holders with their public keys;
- Malicious Code Protection systems including malicious code scanners, integrity checkers, vulnerability monitors, and improper behavior blockers;
- Vulnerability Scanners that examine servers, workstations, firewalls, and routers for known vulnerabilities;
- Forensic systems that identify, preserve, extract, and document computer-based evidence; and
- Media Sanitizing products that remove data from or modify storage media so that the data cannot be retrieved and reconstructed.

Organizational, Product, and Vendor Considerations

The guide discusses the characteristics of products in each of these categories and recommends that organizations consider organizational, product, and vendor issues when selecting IT security products. These issues are

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/.

presented as specific questions to be asked by organizations selecting information technology security products:

- Organizational considerations
  - Need for product to mitigate risk
  - Identification of user community
  - Relationship between product and organization's mission
  - Sensitivity of data to be protected
  - Support for security requirements in security plan, policies, and procedures
  - Identification of the organization's security requirements and comparison to product specifications
  - Consideration of threat environment and security functions needed to mitigate risks
  - Consideration of the use of tested products
  - Need for firewalls, intrusion detection systems, or other boundary controllers
  - Impact of product on operational environment, maintenance, and training
  - Requirements for support, plug-in components, or middleware
- Product considerations
  - Review of lists of validated products, including those products validated under the joint NIST/Communications Security Establishment of Canada Cryptographic Module Validation Program (CMVP) and the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), jointly managed by NIST and the National Security Agency
  - Review of product vulnerabilities
  - Test and implementation of patches
  - Review of protection profiles
  - Review of total life cycle costs, including acquisition and support
  - Ease of use, scalability, and interoperability requirements
  - Test requirements for acceptance and integration testing, and for configuration management
  - Known vulnerabilities of products
  - Implementation requirements for relevant patches
  - Requirements and methods for reviewing product specifications against existing and planned organizational programs, policies, procedures, and standards
  - Security critical dependencies with other products and interactions with the existing infrastructure
- Vendor considerations
  - Impact of the selection of a particular product on future security choices
  - Vendor experience with the product
  - Vendor history in responding to security flaws in its products

All of these considerations may not apply in all cases to all organizations. The questions posed in the guide can be modified to meet the specific conditions of organizations and help them reach decisions that support their requirements and that provide the appropriate level of protection.

More Information

For a list of references to publications and to web pages with information that can help you in planning and implementing a comprehensive approach to information technology security, consult Appendix A of NIST SP 800-36.

NIST Special Publications, including the following, are available in electronic format from ITL's Computer Security Resource Center at http://csrc.nist.gov/publications.

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides guidance on the fundamentals of information system security.

NIST SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, explains approaches and methods that can be used to secure information systems.

NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, discusses developing and updating security plans.

NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, provides guidance to federal agencies on selecting cryptographic controls to protect sensitive, unclassified information.

NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, discusses the concept of assurance in the acquisition and use of security products.

NIST SP 800-26, *Security Self Assessment Guide for Information Technology Systems*, helps organizations determine the status of their information security programs and establish targets for improvement.

NIST SP 800-27, *Engineering Principles for Information Technology Security: A Baseline for Achieving Security*, presents the system-level security principles that should be considered in the design, development, and operation of an information system (draft revision available at http://csrc.nist.gov/publications/drafts.html).

NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, discusses the risk-based approach to security and provides guidance on conducting risk assessments (draft revision available at http://csrc.nist.gov/publications/drafts.html).

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.

NIST SP 800-31, *Intrusion Detection Systems (IDSs)*, and NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy*, provide information on using and deploying IDSs and firewalls.

NIST SP 800-33, *Underlying Technical Models for Information Technology Security*, provides information on IT security engineering principles and concepts for IT systems.

NIST SP 800-35, *Guide to Information Technology Security Services*, covers evaluating, selecting, and managing security services throughout the system life cycle.

NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, describes the fundamental concepts of the certification and accreditation processes, and details the various tasks in the processes (available in final draft at http://csrc.nist.gov/publications/drafts.html).

NIST SP 800-42, *Guidelines on Network Security Testing*, describes available security testing techniques, their strengths and weaknesses, and the recommended frequencies for testing as well as strategies for deploying network security testing.

NIST SP 800-44, *Guidelines on Securing Public Web Servers*, assists organizations in installing, configuring, and maintaining secure public web servers.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides information about selecting security controls to meet the security requirements for the system (available in draft at http://csrc.nist.gov/publications/drafts.html).

NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*, provides guidance in assigning security categories and analyzing the impact of risks, based on security categorization definitions in FIPS 199 (available in draft at http://csrc.nist.gov/publications/drafts.html).

NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*, discusses the analysis of system security requirements and methods for incorporating security into IT procurements.

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