February 2003

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURE INTERCONNECTIONS FOR INFORMATION TECHNOLOGY SYSTEMS

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

Organizations may decide to interconnect their information technology (IT) systems so they can share their data and information resources with each other. Benefits that participating organizations may realize include reduced operating costs, greater functionality, improved efficiency, and centralized access to data. Organizations choose to interconnect their IT systems for a variety of reasons, depending on their organizational needs or the requirements of Congressional mandates or Executive department agreements.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, *Security Guide for Interconnecting Information Technology Systems*, provides guidance for planning, establishing, maintaining, and terminating secure yet cost-effective interconnections between IT systems that are owned and operated by different organizations. This ITL Bulletin summarizes the document, which also discusses the benefits of interconnecting IT systems, the basic components of an interconnection, the methods and levels of interconnectivity, and the potential security risks associated with interconnections. Written by Tim Grance, Joan Hash, Steven Peck, Jonathan Smith, and Karen Korow-Diks, NIST SP 800-47 is available at http://csrc.nist.gov/publications/nistpubs/index.html.

The appendices contain sample documents to help organizations interconnect their IT systems, including an Interconnection Security Agreement (ISA), which specifies the technical and security requirements of the interconnection; a Memorandum of Understanding/Agreement (MOU/A), which defines the responsibilities of the participating organizations; and a System Interconnection Implementation Plan, which defines the process for establishing the interconnection. Also included are a glossary, references, and an index.

Interconnection Issues

Organizations deciding to interconnect their systems should determine the method of interconnection. IT systems can be interconnected by a dedicated line that either is owned by one of the organizations or is leased from a third party, such as an Integrated Services Digital Network (ISDN), a T1, or a T3 line. Dedicated physical lines provide a higher level of security for the interconnected systems, because they can be breached only through direct physical access to the line. However, dedicated lines can be expensive.

A less expensive alternative to the dedicated line is interconnection over a public network, using a virtual private network (VPN). A VPN is a data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them. This alternative can be less secure than the dedicated line, however, because unauthorized parties could intercept unprotected data that is transmitted over the public network.

Interconnected IT systems can expose the participating organizations to risks. In planning for interconnected systems, organizations should apply risk management procedures. Federal agencies are required to protect government information commensurate with the risk and magnitude of harm

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 8901, Gaithersburg, MD 20899-8901, 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 September 2001

- *Security Self-assessment Guide for Information Technology Systems*, September 2001
- *Computer Forensics Guidance*, November 2001
- *Guidelines on Firewalls and Firewall Policy*, January 2002
- *Risk Management Guidance for Information Technology Systems,* February 2002
- *Techniques for System and Data Recovery,* April 2002
- *Contingency Planning Guide for Information Technology Systems*, June 2002
- *Overview: The Government Smart Card Interoperability Specification,* July 2002
- *Cryptographic Standards and Guidelines: A Status Report*, September 2002
- *Security Patches and the CVE Vulnerability Naming Scheme: Tools to Address Computer System Vulnerabilities*, October 2002
- *Security for Telecommuting and Broadband Communications*, November 2002
- *Security of Public Web Servers*, December 2002
- *Security of Electronic Mail*, January 2003

that could result from the loss, misuse, unauthorized access, or modification of such information.

If the interconnection is not properly designed, security failures could compromise the connected systems and the data they store, process, or transmit. In addition, if one of the connected systems is compromised, the interconnection could be used to compromise the other system and its data. In most cases, the participating organizations have little or no control over the operation and management of the other party's system.

Therefore, both parties should learn as much as possible about the risks associated with the planned or current interconnection and the security controls that they can implement to mitigate those risks. A written agreement is needed to establish and describe the management, operation, and use of the interconnection. The agreement should be reviewed and approved by appropriate senior staff from each organization.

OMB Circular A-130, Appendix III, requires agencies to obtain written management authorization before connecting agency IT systems to other systems, based on an acceptable level of risk. The written authorization should define the rules of behavior and controls that must be maintained for the system interconnection, and it should be included in the agencies' system security plans.

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.

Four Phases of the System Interconnection Life Cycle

The NIST SP 800-47 guide recommends a "life-cycle management" approach for interconnecting IT systems:

- planning for the interconnection;
- establishing the interconnection;
- maintaining the interconnection; and
- disconnecting an interconnection.

Planning for the Interconnection.

The planning phase is the first step in establishing an efficient and secure interconnection. The participating organizations should examine all relevant technical, security, and administrative issues; and form an agreement governing the management, operation, and use of the interconnection.

A joint planning team should be established by the participating organizations, composed of management and technical staff, including program managers, security officers, system administrators, network administrators, and system architects. The joint planning team should coordinate the planning process with the support of senior managers and system and data owners. The team would be responsible for coordinating all aspects of the planning process and ensuring that it had clear direction and sufficient resources. After the initial planning phase, the team may remain active to discuss future issues involving the interconnection.

The business case for the interconnection should be defined, including its purpose and expected benefits, costs for staff and equipment, and potential technical, legal, and financial risks. Privacy issues and access rules also should be discussed.

Systems to be interconnected should be certified and accredited in accordance with federal certification and accreditation (C&A) guidelines. Certification involves testing and evaluating the technical and nontechnical security features of the system to determine the extent to which it meets a set of specified security requirements. Accreditation is the official approval by a Designated Approving Authority (DAA) or other authorizing management official that the system may operate for a specific purpose using a defined set of safeguards at an acceptable level of risk.

The planning team should consider the interconnection requirements, including all relevant technical, security, administrative, and personnel issues. This information will be used to develop an Interconnection Security Agreement (ISA) and a Memorandum of Understanding or Agreement (MOU/A). Further, the collected information may be used to develop an implementation plan for establishing the interconnection. Issues that should be considered include the level and method of the interconnection, impact on existing operations, hardware and software requirements, data sensitivity, user community, security controls, and rules of behavior, among others.

The joint planning team should document an agreement governing the interconnection and the terms under which the organizations will abide by the agreement, based on the team's review of all relevant technical, security, administrative, and personnel issues. An ISA should be developed to specify the technical and security requirements for establishing, operating, and maintaining the interconnection. The MOU/A documents the terms and conditions for sharing data and information resources in a secure manner.

The ISA and MOU/A should be reviewed by management officials of participating organizations and approved or rejected. Approval of the ISA and MOU/A constitutes approval of the interconnection. Approval may also be granted on an interim basis. The ISA and MOU/A that are developed should be kept in a secure location to protect against theft, damage, or destruction. Copies stored electronically should be protected from unauthorized disclosure or modification.

Establishing an Interconnection.

The following steps are recommended for establishing a system interconnection after it has been planned and approved. The participating organizations develop and execute a plan for the interconnection, including security controls.

The joint planning team should develop an implementation plan. The plan should document all aspects of the interconnection effort and clarify how technical requirements specified in the ISA will be implemented. The plan should include a description of the IT systems to be interconnected, the sensitivity of the data to be exchanged, the staff members who will be responsible for the interconnected systems, and the security controls, tests, and procedures that will be in place.

The implementation plan should be reviewed and approved by the planning team. Once approved, the plan may be implemented. Recommended steps for establishing the interconnection are described below.

Security controls should be implemented or configured. These controls may include firewalls and intrusion detection systems. Audit logs should be installed to record the activities that take place across the interconnection and should be appropriately reviewed, protected, and maintained. Identification and authentication procedures should be established to prevent unauthorized access to the interconnected systems. Passwords, biometrics, and smart cards are additional measures that may be used.

Logical access controls should be used to designate users who have access to system resources and the type of transactions and functions that they are permitted to perform. Data passing from one system to another should be scanned with antivirus software to detect and eliminate malicious code. Antivirus software should be installed on all servers and computer workstations linked to the interconnection. The software should be automatically updated and maintained with current virus definitions.

Encryption can be used to protect the confidentiality and integrity of data during transmission and storage, to authenticate users to the interconnection and to shared applications, and to provide for nonrepudiation of data.

Hardware and software supporting the interconnection should be located in a secure location that is protected from unauthorized access, interference, or damage. Interconnections should be protected from hazards such as fire, water, and excessive heat and humidity. Computer workstations should be in secure areas to protect them from damage, loss, theft, or unauthorized physical access.

Hardware and software to establish the interconnection should be installed or configured. The hardware and software should be installed with proper communications lines, VPN software, routers, and switches. Database, web, and application servers should support services provided across the interconnection, and needed hubs should be installed to join multiple computers into a single network segment. Computer workstations should be configured to provide authorized users with a link to the interconnection.

Applications or protocols for services that are provided across the interconnection should be integrated. These includes word processing, database applications, e-mail, web browsers, application servers, authentication servers, domain servers, development tools, editing programs, and communications programs.

Conduct operational and security testing to ensure equipment operates properly and to mitigate or counter the ways for unauthorized users to circumvent or defeat security controls. The interface between applications should be tested across the interconnection, and security controls should be tested under realistic conditions. Testing should be done in an isolated, non-operational environment to avoid disturbing the systems. Weaknesses or problems should be corrected, and the interconnection retested. Operational and security testing may be performed as part of the recertification and reaccreditation processes.

Conduct security training and awareness for all authorized personnel who will be involved in managing, using, and/or operating the interconnection. Ensure that staff members understand the rules and that they know how to report suspicious or prohibited activities.

Both organizations should update their system security plans and related documents to reflect the changed security environment in which their respective systems operate. The MOU/A should address the details of conducting a mutual review of the interconnection.

Perform recertification and reaccreditation if significant changes have been made to the connected systems.

Activate the interconnection for use by both organizations. One or both organizations should monitor the interconnection for at least three months to ensure that it operates properly and securely.

Maintaining the Interconnection.

After it is established, the interconnection must be actively maintained for secure operation. The maintenance steps are:

***Maintain clear lines of communicatio*n** to ensure that the interconnection is properly maintained and that both sides are notified of changes or security incidents. Communications should be conducted between designated personnel using approved procedures.

Authorized personnel should maintain the equipment in accordance with the manufacturer's specifications. Appropriate documentation and notification procedures should be used.

User profiles should be managed to assure access to authorized users only. Active management of user profiles helps to prevent intruders from using inactive accounts.

Security reviews should be conducted to ensure security controls are working properly and providing appropriate levels of protection.

Audit logs should be analyzed at predetermined intervals to detect and track unusual or suspicious activities across the interconnection that might indicate intrusions or internal misuse.

Security incidents should be reported to participating organizations. Both organizations should respond to security incidents by isolating systems if necessary and by coordinating their incident response activities.

Coordinate contingency planning, training, testing, and exercises to minimize the impact of disasters and other contingencies that could damage the connected systems or jeopardize the confidentiality and integrity of shared data.

Perform change management procedures to ensure that the interconnection is properly maintained and secured. A change control board should review and approve planned changes for each organization. Changes should be based on the security requirements specified in the ISA and a determination that the change will not adversely affect the interconnection. A joint change control board should review and approve changes that affect the interconnection.

Update system security plans and other relevant documentation at least annually or whenever there is a significant change to the IT systems or to the interconnection.

Disconnecting an Interconnection.

If an interconnection must be terminated, the process should be conducted in a methodical manner to avoid disrupting the IT system of either organization. The decision to terminate the interconnection should be made by the system owner with the advice of appropriate managerial and technical staff. Before terminating the interconnection, the initiating party should notify the other party in writing, and it should receive an acknowledgment in return.

If an organization detects an attack, intrusion attempt, or other contingency that exploits or jeopardizes the connected systems or data, it may be necessary to abruptly terminate the interconnection without written notice to the other party. This is an extraordinary measure taken only in extreme circumstances and only after consultation with appropriate technical staff and senior management.

Both organizations may choose to restore the system interconnection after it has been terminated. The decision to restore the interconnection should be based on the cause and duration of the disconnection. Both organizations should modify the ISA and MOU/A to address issues requiring attention. If the interconnection has been terminated for more than 90 days, each party should perform a risk assessment on its respective system and reexamine all relevant planning and implementation issues, including developing a new ISA and MOU/A.

Summary

Interconnecting IT systems can provide significant benefits to participating organizations, but can expose both to risks. Interconnections must be properly designed, and appropriate security controls must be in place to avoid compromise of systems and data. Both parties must understand the risks associated with the interconnection and the security controls they can implement to mitigate those risks. The organizations should establish a formal agreement concerning the management, operation, and use of the interconnection. The agreement should be reviewed and approved by appropriate senior staff from each organization.

Reference List

NIST's Information Technology Laboratory issues publications covering research, guidance, standards, and the results of collaborative outreach efforts with industry, government, and academic organizations. NIST publications dealing with information security topics, including archived copies of bulletins, are available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications/ .

The following NIST Special Publications provide guidance to help organizations plan, establish, maintain, and terminate secure IT system interconnections:

NIST Special Publication 800-3, *Establishing a Computer Security Incidence Response Capability (CSIRC*), provides information on detecting and reporting security incidents.

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handboo*k, provides guidance on certification and accreditation (C&A), and other security procedures.

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology System*s, provides details on access control issues, and developing and updating security plans.

NIST Special Publication 800-30, *Risk Management Guide for Information Technology System*s, provides guidance on conducting risk assessments.

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 800-31, *Intrusion Detection Systems (IDS*), and NIST Special Publication 800-41, *Guidelines on Firewalls and Firewall Policy*, provide information on selection of security controls.

NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology System*s, gives information on coordinating contingency planning activities.

Guidance on physical security techniques is included in NIST Special Publications 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*; and NIST Special Publication 800-30, *Risk Management Guide for Information Technology System*s.

Details on integrating applications and protocols can be found in NIST Special Publication 800-27, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security*); NIST Special Publication 800-28, *Guidelines on Active Content and Mobile Code*; and NIST Special Publication 800-33, *Underlying Technical Models for Information Technology Security*.

NIST Special Publication 800-42 (draft), *Guidelines on Network Security Testing*, includes a methodology for using network-based tools to test IT systems for vulnerabilities.

Information about Federal Information Processing Standards (FIPS)-approved algorithms and cryptographic modules that must be used by federal agencies is available at http://csrc.nist.gov/publications/fips/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.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900