July 2005

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

PROTECTING SENSITIVE INFORMATION THAT IS TRANSMITTED ACROSS NETWORKS: NIST GUIDANCE FOR SELECTING AND USING TRANSPORT LAYER SECURITY IMPLEMENTATIONS

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

The protection of sensitive information that is transmitted across interconnected networks is an essential part of an organization's integrated program for the security of information and information systems. Management, operational, and technical controls are needed throughout the organization to protect information and information systems from threats of all kinds. New guidance recently issued by the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) helps federal and private sector organizations select and use technical controls at the transport layer of a layered communications protocol stack. Transport layer security (TLS) can be implemented and used effectively to authenticate network servers and clients, and to protect the confidentiality and integrity of data that is exchanged between two communicating information technology (IT) applications.

Background on Transport Layer Security (TLS)

Technical controls implemented at the transport layer of a communications protocol stack can protect sensitive information during electronic dissemination across the Internet. The TLS protocol (TSL 1.0) is a voluntary industry standard (RFC 2246) that was developed by the Internet Engineering Task Force. TSL 1.0 is based on the Secure Sockets Layer Version 3.0 (SSL 3.0), which had been developed originally by Netscape Corporation. These protocols are part of the seven-layer model (also known as the seven-layer stack) that provides for communications operations between applications running on disparate computing systems on the Internet. The seven-layer model defines the layers of computer communications services, which are provided by a protocol stack. The transport layer is frequently used to provide connection-oriented services between applications running on hosts that are on interconnected networks.

The layering of communications protocols enables systems developers to design new communication systems using already defined services, protocols, and specific communication requirements within each layer of the stack. Each protocol layer of the system that is transmitting information through the network communicates with the corresponding layer of the stack on the system that receives the information. Within the communications stack, the internal

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 May 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 of Selecting Cost-Effective Controls Using a Risk-Based Process, May 2005*
- *NIST's Security Configuration Checklists Program for IT Products,* June 2005

mechanisms of each layer generally are independent of each other layer. Placement of security services and the implementation of the security mechanisms within the stack are specific to each individual layer of the stack.

The seven-layer model does not explicitly define where security services are to be placed, and there has been considerable discussion about the correct placement of security services and other implementation mechanisms. These discussions will continue as new standards are developed to meet the communications needs of users, local and wide area networking vendors, Internet service providers (ISPs), and World Wide Web (Web) application designers.

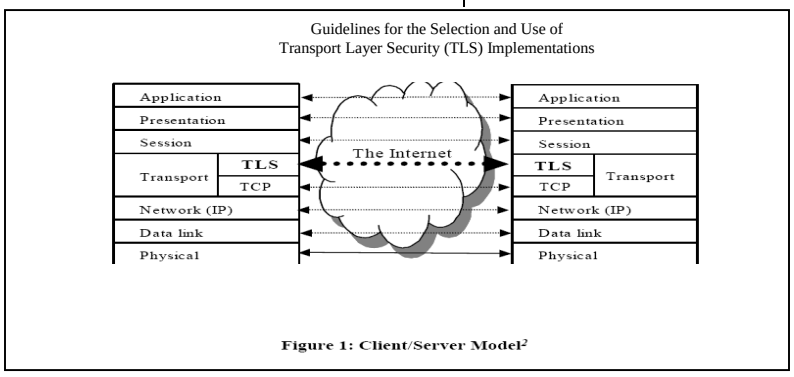

Figure 1: Client/Server Model[2]

In this model, the telephone lines, network routers, firewalls, and other network components that comprise the underlying structure of the network are usually not under the control of the end user's client software or of the server's application software. In the typical Internet architecture, the Transmission Control Protocol / Internet Protocol (TCP/IP) stack provides for the transmission of packets through complex arrangements of local, wide, or metropolitan area or globally connected sets of inter-networking or intra-networking technology. Protocols below IP include, for example, local area network (LAN) protocols or other link protocols such as dial up, or directly connected modems, fiber optic links, or satellite links.

Security services are needed to protect data privacy and data integrity, and to assure the authentication of the server and the end user. The TSL 1.0 specifications use cryptographic mechanisms, including encryption of data, message authentication codes, and public key cryptography-based digital signatures, to implement the security services and to establish and maintain a secure TCP/IP connection. Secure connections prevent eavesdropping, tampering, or message forgery.

Protocol options must be selected and used by both clients and servers in order to achieve communication security at the transport layer. The transport layer is not the only place in this architectural model where these security services can be provided. In overall security design, the transport layer is only a small portion of the network, and it alone cannot provide complete network security. Security involves an integrated and complex set of related properties that work together to protect information and systems.

NIST Special Publication (SP) 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations: Recommendations of the National Institute of Standards and Technology*

NIST has issued new guidelines to help organizations select and implement transport level security, making effective use of Federal Information Processing Standards (FIPS)-approved cryptographic algorithms and open source technology. Written by C. Michael Chernick (NIST), Charles Edington III (Booz Allen Hamilton), Matthew J. Fanto (NIST), and Rob Rosenthal (Booz Allen Hamilton), the guide advises organizations how to use authentication, confidentiality, and integrity mechanisms to protect information at the transport layer. Authentication mechanisms provide assurance of the identity of the sender or receiver of information. The confidentiality mechanisms provide assurance that data is kept secret and prevent eavesdropping. The message integrity mechanisms detect any attempts to modify data and prevent deletions, additions, or modifications of data.

NIST SP 800-52 explains the concepts of security in the layered communications architecture in general, and in the transport layer in particular. The security options in selecting an encryption method, or cipher, and communications protocols are explained, and recommended selections are discussed. Tables are provided for mapping the security parts of TLS to FIPS, and for recommended client and server cipher suites. The reference section includes documents, publications, and organizations that provide extensive

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 and 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

information on many aspects of transport layer security.

While primarily designed to help federal agencies achieve more secure information systems, other activities including state, local and tribal governments, and private sector organizations should find the guide useful in selecting transport layer security implementations. NIST SP 800-52 and other publications dealing with controls and procedures needed for secure systems are available from the NIST Computer Security Resource Center at: http://csrc.nist.gov/publications/nistpubs/index.html.

NIST SP 800-52 and FISMA Requirements

NIST SP 800-52 is one of the guidelines developed by NIST to help federal agencies implement their responsibilities under the Federal Information Security Management Act (FISMA). FISMA requires that all federal agencies develop, document, and implement agency-wide information security programs to protect the information and information systems that support the operations and assets of the agency, including those systems provided or managed by another agency, contractor, or other source.

Under Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, federal managers of publicly accessible information repositories, or of dissemination systems that contain sensitive but unclassified data, are required to ensure that sensitive data is protected. The protection mechanisms used should be in accordance with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such data. Security requirements are usually derived from an assessment of the threats or potential attacks that an adversary could mount against a system. Threats to systems take advantage of implementation vulnerabilities found in many system components including computer operating systems, application software systems, and the computer networks that interconnect them.

Security within the network is just one consideration in establishing an effective information security program. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, describes the management process to analyze and balance the operational and economic costs of protective measures and to protect the IT systems and data that support the organization's mission. Special Publications and Federal Information Processing Standards (FIPS) mentioned in this bulletin are available in electronic format at: http://csrc.nist.gov/publications/nistpubs/index.html.

Guidance in Implementing Transport Layer Security

NIST recommends that organizations consider the following issues when implementing transport layer security mechanisms, such as web servers and browsers:

- Implementation of standards. The interaction between components in transport layer security mechanisms should be through a well-defined communication protocol with no deviations. FIPS-approved algorithms for authentication, encryption, and the generation of message digests should be used in all implementations.
- Interoperability. An implementation should promote interoperability among components. The selection of a particular server solution should not prevent the use of any standards-based client or vice versa.
- Use of evaluated products. Key components of the implementation should be independently evaluated for conformance to standards, such as FIPS 140-1 and 140-2, *Security Requirements for Cryptographic Modules*.
- Selection of important features. The implementation should include those features that users consider most important to their operating environments.
- Open source solutions. The implementation should be an open source solution that allows users to choose future implementations that will support interoperability or standards.

NIST recommends the use of the TLS 1.0 protocol specifications, which call for cryptographic mechanisms to implement the security services that establish and maintain a secure TCP/IP connection. The secure connection prevents eavesdropping, tampering, or message forgery. Implementing data confidentiality with cryptography prevents eavesdropping; generating a message authentication code with a secure hash function prevents undetected tampering; and authenticating clients and servers with public key cryptography-based digital signatures prevents message forgery.

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.

In all of these processes, a key or shared secret is required by the cryptographic mechanism. A pseudorandom number generator and a key establishment algorithm are used to provide for the generation and sharing of these secrets.

NIST SP 800-52 provides tables that guide an organization in implementing services to prevent eavesdropping, tampering, or message forgery. The guide identifies the key establishment, confidentiality, digital signature, and hash mechanisms that are Federal Information Processing Standards (FIPS). Recommendations are made for the selection of FIPS-approved ciphers.

Some specific implementation details include:

- In selecting and procuring transport layer security implementations, officials should ensure that products meet a minimum set of universally accepted tests. Products should provide quality random numbers for key generation, protect the keying material and its storage, and properly implement and test key establishment, encryption, and signature algorithms and hash functions. NIST has published information to help agencies in buying security products in NIST SP 800-23, *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, and in NIST SP 800-36, *Guide to Selecting Information Technology Security Products*.
- Organizations should follow the vendor's general guidelines, as well as local practices, when installing TLS implementations. For example, a client's local policy might state that server authentication is required. The system administrator should follow the vendor's prescribed methods for enabling client/server authentication.

  Security services for confidentiality, data integrity, and peer entity authentication for clients and servers should be configured and provided by the TLS implementation. Appropriate cipher suites must also be selected.
- In the maintenance phase, administrators should follow local policies and operating procedures. For example, the site system administrator may be required to check for product updates and security patches and to install them as needed. Within the local operating procedures, provisions should be made for checking for and obtaining updated information concerning the issuance and validation of authentication certificates, which are issued by public key infrastructure services.

Some Operational Considerations

After administrators select cipher suites to support transport layer security within the TLS protocol, applications should be configured only for those selected cipher suites. In addition, the key lengths used in the cipher suites for both clients and servers must be specified. TSL 1.0 and SSL 3.0 use the Hypertext Transfer Protocol (HTTPS), which is an extremely flexible protocol that allows for many uses and implementations and that introduces vulnerabilities. The client should be configured to check all data received and to verify the pathway of the message and the message's integrity. This includes verifying the server's identity at the time the connection is established.

Both the server and the client should not base authentication decisions solely upon the Transport Layer Security's mechanism for determining possession of the private key corresponding to the authentication certificate. Rather, the decision should also consider whether or not the authentication certificate is valid or has been revoked. Information on public key infrastructure services is available in NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure.*

Organizations should consult NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*, for complete details concerning selection of protocols, cipher suites, client-server issues, generation of random numbers, and other implementation issues.

COMPUTER SECURITY DIVISION CHIEF SOUGHT

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) is seeking a highly qualified individual for the position of Division Chief for the Computer Security Division (CSD). The Division Chief provides executive direction for the scientific and technical activities of CSD and is responsible for administrative, financial and personnel management. The Division consists of approximately 62 FTEs and 18 NIST Associates and has a 2005 budget of $27M.

The Computer Security Division of ITL has a long-standing role in leading the non-military establishments in cyber security by working effectively with industry, academia, and federal agencies on IT system security and vulnerabilities, and promoting effective computer security practices. Congressional passage of the Cyber Security Research and Development Act (CSRDA) of 2002 and the Federal Information Security Management Act (FISMA) of 2002 reinforced NIST's long-standing statutory responsibilities for developing cyber security standards and guidelines and researching associated methods and techniques.

The new Division Chief will be responsible for developing an Operational Plan in alignment with the strategic and operational goals of the Laboratory and NIST. He/she will review and ensure the quality and productivity of the Division

and the relevance of its programs to ITL and NIST missions and national goals. The Division Chief also has administrative responsibilities for the mandated Information System Security and Privacy Advisory Board, which has the mission of identifying emerging technical issues related to computer security, privacy, and cryptography. The Division Chief serves as a consultant and advisor on important issues and problems in computer security technology for federal agencies, academia, and industry. The Division Chief is also responsible for developing and periodically presenting Congressional testimony on computer security-related topics. The Chief may be called upon to represent the Laboratory and the Institute at technical meetings; on government policy-level committees and boards of scientific, technical, and standards organizations; and in developing policy for interagency/international memoranda of understanding.

The computer security program requires a particular competency to lead change that impacts the entire federal infrastructure and strongly influences U.S. industry, as well. Strong technical credentials with extensive expertise in working with the federal government are preferred. A Masters degree or Ph.D. in a relevant field is preferred.

Further information on NIST is available on the Web at http://www.nist.gov, on ITL at http://www.itl.nist.gov/ and on CSD at http://www.itl.nist.gov/div893/. Please contact Shashi.Phoha@nist.gov for further information on this position. Interested parties should submit a complete resume through the USAJOBS website at http://www.usajobs.opm.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