April 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

PROTECTING SENSITIVE INFORMATION TRANSMITTED IN PUBLIC NETWORKS

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 critical to the overall security of an organization's information and information systems. The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently issued guidance to assist organizations in strengthening their network security and in lessening the risks associated with the transmission of sensitive information across networks. The publication offers practical guidance on implementing security services based on Internet Protocol Security (IPsec).

IPsec is a framework of open standards for ensuring private communications over public networks. IPsec is frequently used to achieve security controls in the layered protocols of network communications, and to create a virtual private network (VPN). An organization can build a VPN on top of existing physical networks to create a secure communications mechanism for the data and control information that is transmitted between networks. VPNs are used most often to protect communications carried over public networks, such as the Internet, which utilize Transmission Control Protocol/Internet Protocol (TCP/IP) network communications. When properly implemented, VPNs can protect the confidentiality and integrity of data, authenticate the origin of data, and provide data replay protection and access control. However, VPNs cannot eliminate all risks since flaws in algorithms or software, or insecure configuration settings and values may still be exploited by hackers.

NIST Special Publication (SP) 800-77, *Guide to IPsec VPNs*

Written by Sheila Frankel of NIST, and Karen Kent, Ryan Lewkowski, Angela D. Orebaugh, Ronald W. Ritchey, and Steven R. Sharma of Booz Allen Hamilton, NIST SP 800-77 helps network architects, network administrators, security staff, technical support staff, and computer security program managers who are responsible for the technical aspects of preparing, operating, and securing their organization's networks. The information discussed is general in nature and can be applied to many different hardware platforms, operating systems, and applications. Topics covered include the need for network layer security services, the services that are available at the network layer, and how IPsec can be implemented to provide these services. A case-based approach illustrates how IPsec can be used to solve common network security concerns. The guide explains IPsec planning and implementation issues; it also discusses alternatives to IPsec and the appropriate circumstances in which to deploy each alternative.

The appendices discuss the need for organizations to develop their IPsec-related policies and present examples of common IPsec policy issues that should be considered. Also included in the appendices are configuration files that are referenced by the case studies, a glossary, an acronym list, and a compilation of print and online resources that may be useful for IPsec planning and implementation.

The publication is available on NIST's web pages at: http://csrc.nist.gov/publications/nistpubs/index.html.

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 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
- *Implementation of FIPS 201, Personal Identify Verification (PIV) of Federal Employees and Contractors, August 2005*
- *Biometric Technologies: Helping to Protect Information and Automated Transactions in Information Technology Systems, September 2005*
- *National Vulnerability Database: Helping Information Technology System Users and Developers Find current Information About Cyber Security Vulnerabilities, October 2005*
- *Securing Microsoft Windows XP Systems: NIST Recommendations for Using a Security Configuration Checklist, November 2005*
- *Preventing and Handling Malware Incidents: How to Protect Information Technology Systems from Malicious Code and Software, December 2005*
- *Testing and Validation of Personal Identity Verification (PIV) Components and Subsystems for Conformance to Federal Information Processing Standard 201, January 2006*
- *Creating a Program to Manage Security Patches and Vulnerabilities: NIST Recommendations for Improving System Security, February 2006*
- *Minimum Security Requirements for Federal Information and Information Systems: Federal Information Processing Standard (FIPS) 200 Approved by the Secretary of Commerce, March 2006*

The Need for Network Security

Widely used throughout the world, Transmission Control Protocol/Internet Protocol (TCP/IP) network communications are composed of four layers of protocols that work together: application, transport, network, and data link. Security controls are available for network communications at each of the four layers:

The **application layer** sends and receives data for an application. Separate controls must be established for each application. While this arrangement provides a high degree of control and flexibility for the security of the application, it may cause the organization to devote considerable resources to implement. The development of new application layer security controls can also create new vulnerabilities, and it may not be possible to develop the controls for some applications.

The **transport layer** provides connection-oriented or connectionless services to transport application layer services across networks. Controls at this layer can protect data in a single communications session between two hosts, and must be supported by both clients and servers.

The **network layer** routes packets across networks. Controls at this layer apply to all applications, rather than to specific applications. Applications do not have to be modified to use the controls, but this arrangement provides less control and flexibility for protecting specific applications than the transport and application layer controls.

The **data link layer** handles communications on the physical network components. Controls at this level protect a specific physical link. Since each physical link must be secured separately, controls at this level are not feasible for protecting connections that involve several links, including most connections across the Internet.

As data is prepared for transport through the network, it is passed from the highest to the lowest layer, with each layer adding more information. Security controls at a higher layer cannot provide full protection for the lower layers, because the lower layers add information to the communications after the higher-layer security controls have been applied. The lower-layer security controls are less flexible and granular than higher-layer controls. As a result, controls at the network layer are widely used to secure communications and to provide a more balanced solution than can be achieved through the application of the higher-layer and lower-layer security controls.

Internet Protocol Security (IPsec)

IPsec is the most commonly used network layer security control for protecting communications. It was developed by the IPsec Working Group of the Internet Engineering Task Force (IETF) as a framework of open standards. Depending upon the implementation and configuration, IPsec can provide the following types of protection:

- Ensuring the **confidentiality** of data through the application of a cryptographic algorithm and a secret key, known only to the two parties exchanging data. The data that is transmitted can be decrypted only by someone who has the secret key.

- Assuring the **integrity** of data through the application of a message authentication code (MAC), which is a cryptographic hash of the data. The checksum is sent with the data. The recipient can detect when the data has been changed, either intentionally or unintentionally during transit, if a new MAC is calculated on the received data and it does not match the original MAC.

- Providing **peer authentication** to ensure that network traffic and data are sent from the expected host. The receiving IPsec endpoint can confirm the identity of the sending IPsec endpoint.

- Providing **replay protection** to assure that the same data is not delivered multiple times and that the data is delivered in an acceptable order. IPsec cannot, however, ensure that the data has been received in the exact order that it was sent.

- Providing **traffic analysis protection** by obscuring the identities of the endpoints and the size of the data. Those who are monitoring network traffic may not know which parties are communicating, how often communications occur, or how much data is being exchanged.

- Providing **access control** by assuring that only authorized users can access particular network resources. IPsec endpoints can also allow or block certain types of network traffic, such as allowing web server access but denying file sharing.

Components of IPsec

The IPsec network layer security protocol provides protection through the following components, which are used in various combinations:

Authentication Header (AH) and Encapsulating Security Payload (ESP) security protocols. ESP provides encryption and integrity protection for packets, but it cannot directly protect the outermost IP header. (It can protect it indirectly, if Internet Key Exchange (IKE) is used to negotiate the IPsec protections.) AH provides integrity protection for packet headers and data but without encryption. AH can also protect some header information that ESP cannot protect. ESP is used more frequently than AH because of its encryption capabilities and other operational advantages.

Internet Key Exchange (IKE) protocol. IKE negotiates the cryptographic algorithms and related security parameters and controls that comprise the security associations (SAs) that are applied to IPsec-protected connections. Other protections provided by this protocol include mutual authentication of endpoints; negotiation of secret keys; and management, update, and deletion of IPsec-protected communication channels. An updated, streamlined IKE (version 2) has been standardized, but most current implementations adhere to the original IKE, version 1.

IP Payload Compression Protocol (IPComp). IPsec uses this protocol to compress packet payloads before encrypting them.

For the IPsec-applied encryption and integrity-protection processes, federal agencies are required to use cryptographic algorithms that are specified in Federal

Information Processing Standards (FIPS) or in NIST Recommendations that are issued in NIST Special Publication 800 series. The FIPS-approved algorithms must be contained in cryptographic modules that have been validated for conformance to FIPS 140-2, *Security Requirements for Cryptographic Modules*, through the Cryptographic Module Validation Program (CMVP). Algorithms that are FIPS-approved include FIPS 197, *Advanced Encryption Algorithm (AES),* the strongest approved algorithm and the preferred algorithm for federal agency use. Also approved is the Triple Data Encryption Algorithm (TDEA), which is specified in American National Standard (ANSI) X9.52-1998 and validated using the tests that are contained in NIST SP 800-20, *Modes of Operation Validation System for the Triple Data Encryption Algorithm*. In addition, the FIPS-approved algorithm for message authentication is FIPS 198, *Keyed-Hash Message Authentication Code*. This algorithm is used to construct a Keyed-Hash Message Authentication Code (HMAC) using secure hash algorithms that are specified in FIPS 180-2, *Secure Hash Standard*.

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.

Virtual Private Networks (VPNs)

The VPN is a virtual network, which is built on top of existing physical networks, and which provides a secure communications mechanism for data and IP information exchanged between public networks. This method of networking can be less expensive for an organization than utilizing dedicated private telecommunications lines to provide communications between the organization's home and branch offices, and between remote telecommuters and the main servers. There are three models for VPNs:

The **gateway-to-gateway model** protects communications between two specific networks, such as an organization's main office network and a branch office network, or between two business partners' networks.

The **host-to-gateway model** protects communications between one or more individual hosts and an organization's specific network, allowing hosts on unsecured networks, such as traveling employees and telecommuters, to have access to the organization's internal services.

The **host-to-host model** protects communications between two specific computers and is most often used when a small number of users need access to a remote system.

IPsec implementations can be used to support VPN services. SP 800-77 establishes the following requirements for the configuration of IPsec VPNs:

● The VPN must provide confidentiality protection through encryption for any information that will traverse a VPN and that should not be seen by non-VPN users.

● A VPN must use a FIPS-approved encryption algorithm. The Advanced Encryption Algorithm in Cipher Block Chaining mode (AES-CBC) is highly recommended. Triple DES in Cipher Block Chaining mode (3DES-CBC) is acceptable as well.

● A VPN must always provide integrity protection.

● A VPN must use a FIPS-approved algorithm to provide for integrity protection. HMAC-SHA-1 is highly recommended and is based on FIPS 198, *Keyed-Hash Message Authentication Code (HMAC)*, and FIPS 180-2, *Secure Hash Signature Standard*.

● A VPN should provide replay protection.

● IKE security associations (SAs) for applications of IKE version 1 should have a lifetime no greater than 24 hours, and IPsec SAs should have a lifetime no greater than 8 hours. For IKE version 2, IKE SAs for the original packets should be re-keyed at least every 24 hours, and SAs for encapsulated packets associated with the original packets should be re-keyed after 8 hours at most.

● The Diffie-Hellman (DH) group of values is used to specify the encryption generator type and key length to be used for generating shared secrets. The value used to establish the secret keying material for IKE and IPsec should be consistent with current security requirements. Specific DH groups are defined for use with IKE. DH group 2 should be used for Triple DES and for AES with a 128-bit key. For greater security, DH group 5 or DH group 14 may be used for AES. IPsec implementations include DH group 2; most include DH group 5; very few include DH group 14. Use of the larger DH groups results in increased processing time.

IPsec Planning and Implementation

NIST advises that agencies apply the principles of the System Development Life Cycle and carry out a risk-based and phased approach in planning for and implementing IPsec in their networked systems. This approach enables agencies to determine appropriate priorities for protecting their systems, to apply appropriate technologies, including the use of IPsec and VPNs, and to incorporate new technology when needed to meet changing requirements.

Organizations should **identify their needs** to protect their networked communications and determine which computers, networks, and data are part of the networked communications. They should determine how their needs can best be met, and where and how security technology should be implemented.

The next phase of the risk-based approach is to **design the solution** that meets the needs, taking into account four major issues: The architectural design includes consideration of host and gateway placement, IPsec client software selection,

and host address space management. An authentication method, such as pre-shared key or digital signature, should be selected. The algorithms for encryption and integrity protection, and the key strength for algorithms that support multiple key lengths, should be selected. The packet filter should be determined to control the types of traffic to be permitted and denied, and to apply appropriate protection and compression measures to each type of permitted traffic, and packet filters. The decisions made regarding authentication, cryptography, and packet filters should be documented in the organization's IPsec policy.

Organizations should then **implement and test a prototype** of the designed solution in a laboratory or test environment. The primary goals of the testing are to evaluate the functionality, performance, scalability, and security of the solution, and to identify any issues, such as compatibility and interoperability of the IPsec components. The security of the implementation is a special concern, since no protocol can be totally secure. Special attention should be paid to the security of stored keys, the traffic that passes through the packet filters, and the use of patches that are developed as new vulnerabilities are found.

When the testing has been completed and all issues have been resolved, organizations should **deploy the solution** by migrating gradually to the use of IPsec throughout the enterprise. The gradual approach enables managers to replace the existing network infrastructure and applications, to train users, to evaluate the impact of the IPsec solution, and to resolve issues. Most of the issues that can occur during IPsec deployment are the same types of issues that occur during any large IT deployment. Service to users, the performance of the network, and client software may be affected.

The last phase of the planning and implementation cycle is to **manage the solution** throughout its life cycle. In this phase, the IPsec architecture, policies, software, and other components of the deployed solution are maintained. Patches to IPsec software should be tested and applied as appropriate. The management phase also involves providing support for new sites and users, monitoring performance, testing the system periodically, and adapting new policies as requirements change. The life cycle process is repeated when enhancements or significant changes need to be incorporated into the solution.

More Information

The IPsec protocols were developed within the IPsec Working Group of the Internet Engineering Task Force (IETF). They are defined in two types of documents: Request for Comment (RFC), which are accepted standards, and Internet-Drafts, which are working documents that may become RFCs. A list of IPsec documents can be found at http://www.ietf.org/html.charters/OLD/ipsec-charter.html.

Federal agencies must use FIPS-approved encryption algorithms contained in validated cryptographic modules. The Cryptographic Module Validation Program (CMVP) is a joint effort of NIST and the Communications Security Establishment (CSE) of the Government of Canada. The CMVP coordinates FIPS 140-2 testing and has issued validation certificates for more than 600 cryptographic modules. The CMVP website is located at http://csrc.nist.gov/cryptval/.

FIPS 140-2, *Security Requirements for Cryptographic Modules*, is available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. See http://csrc.nist.gov/cryptval/des.htm for information on FIPS-approved symmetric key algorithms. FIPS-approved algorithms must also be used for digital signatures. See http://csrc.nist.gov/cryptval/dss.htm.

The National Vulnerability Database (NVD) is a comprehensive database of cyber security vulnerabilities in information technology (IT) products. It was developed by NIST with the support of the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security. The NVD integrates all publicly available U.S. government vulnerability resources and includes references to industry resources. See http://nvd.nist.gov.

NIST publications can help you in planning and implementing a comprehensive approach to IT security. For information about NIST publications and standards that are referenced in the IPsec guide, as well as other security-related publications, see http://csrc.nist.gov/publications/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.

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.