May 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

AN UPDATE ON CRYPTOGRAPHIC STANDARDS, GUIDELINES, AND TESTING REQUIREMENTS

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

For the past thirty years, cryptography has been an important technical tool for protecting the federal government's information and information systems. Cryptographic methods have been used to maintain the confidentiality and integrity of information, to verify that information was not changed after it was sent, and to authenticate the originator of the information. During these years, NIST's Information Technology Laboratory has worked actively with other government and industry organizations to develop standards and guidelines for the cost-effective uses of cryptography. As information technology has changed and as new federal requirements have been established to strengthen information technology security, NIST has updated older methods and developed new methods for the application of cryptography. This bulletin discusses current federal requirements and the techniques that are available to help federal agencies use cryptography to protect their information and information systems.

Revised NIST Special Publication (SP) 800-21, *Guideline for Implementing Cryptography in the Federal Government*

A revised version of NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, was issued in December 2005 to replace an earlier version of the guide that had been released in 1999. The revised guide, written by Elaine B. Barker, William C. Barker, and Annabelle Lee, explains new requirements for federal agencies to protect their information systems, and points to current cryptographic standards and techniques that can provide the needed protection.

NIST SP 800-21-1 focuses on cryptographic standards and guidelines that had been adopted or amended since 1999. It discusses the development of standards for cryptography, current cryptographic methods, and issues that agencies deal with in implementing cryptography in information systems. The guide covers the process for selecting and implementing cryptographic controls as part of federal agency responsibilities under the Federal Information Security Management Act of 2002. NIST's Cryptographic Module Validation Program is also discussed. The appendices contain a list of acronyms, cryptographic terms and definitions, references to standards and guidelines, and information about laws and regulations related to information security. NIST SP 800-21-1, as well as the other guidelines and standards that are referenced in this

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 June 2005:

bulletin, is available at http://csrc.nist.gov/publications/index.html.

Federal Information Security Management Act Requirements

The Federal Information Security Management Act (FISMA) established requirements for all federal agencies to develop, document, and implement agency-wide information security programs and to provide appropriate levels of security for the information and information systems that support the operations and assets of the agency. FISMA tasked NIST to develop federal standards for the security categorization of federal information and information systems according to risk levels, and to develop minimum security requirements for information and information systems in each security category.

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, issued in February 2004, addresses the first task specified by FISMA. FIPS 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. A loss of confidentiality is the unauthorized disclosure of information. A loss of integrity is the unauthorized modification or destruction of information. A loss of availability is the disruption of access to or use of information or an information system. Agencies must assign a security category for both information and information systems.

FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, issued in March 2006, addresses the second task identified by FISMA. FIPS 200 specifies minimum security requirements for information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements through the use of the security controls in accordance with NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

In applying the provisions of FIPS 200, agencies categorize their systems as required by FIPS 199 and then select an appropriate set of security controls from NIST SP 800-53. Security controls are the management, operational, and technical safeguards or countermeasures that are prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Controls based on the application of cryptographic functions are fundamental to the overall security of systems and their information. All security controls, including cryptography, should be selected as part of an organization's overall information security program.

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.

Cryptographic Functions

Cryptography is used to protect data that is sensitive, has a high value, or is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. NIST has developed standards, guidelines, and techniques for the application of cryptographic methods to protect the confidentiality and integrity of data, to authenticate data and users, to authorize users, and to verify the source of messages and data. For information about encryption, digital signatures, secure hashing, message (data) authentication codes, key management, entity authentication, and random number generation, see http://csrc.nist.gov/CryptoToolkit/.

Encryption transforms data into ciphertext before transmission or storage, and decryption transforms the data back into plaintext. Symmetric encryption algorithms operate on blocks of data of fixed size, and the same cryptographic key that is used to encrypt the information to be protected is also used to decrypt the information. The following symmetric encryption algorithms are available for federal agency use:

- The Advanced Encryption Algorithm (AEA) is a symmetric block cipher that is specified in FIPS 197, *Advanced Encryption Standard (AES)*. The AEA encrypts and decrypts data in 128-bit blocks, with three possible key sizes: 128, 192, or 256 bits.

- The Triple Data Encryption Algorithm (TDEA) is specified in NIST SP 800-67, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*. The TDEA is based on the Data Encryption Algorithm (DEA), which was specified in FIPS 46-3, *Data Encryption Standard*. FIPS 46-3 has been withdrawn since it was no longer considered strong enough to protect sensitive, unclassified information. The DEA is still used as the primary cryptographic component of the TDEA. This latter application uses three DEA keys for encryption and decryption and is more robust than the DEA alone.

Modes of operation describe how encryption algorithms can be used to provide services such as confidentiality protection or

authentication of users and information. Currently, there are seven modes of operation that may be used with the approved encryption algorithms. The five modes for confidentiality, one for authentication, and one combined mode for confidentiality and authentication are described in the following publications:

- NIST SP 800-38 A, *Recommendation for Block Cipher Modes of Operation - Methods and Techniques*;

- NIST SP 800-38 B, *Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication*;

- NIST SP 800-38C, *Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality*; and

- A fourth publication (to be designated NIST SP 800-38D) dealing with the Galois/Counter Mode (GCM) for Confidentiality and Authentication has been released for public review and comments.

Information on current modes of operation is available at http://csrc.nist.gov/CryptoToolkit/modes/.

Message authentication codes (MACs) (also known as data authentication codes) and digital signatures are cryptographic functions that provide assurance to the receiver of data that the sender of the data is truly the sender and that the data has not been modified since it was authenticated. A MAC is a cryptographic checksum that is computed on data using a MAC algorithm and a secret key. After the MAC is computed, it is sent with the data. The authenticity of the received data can be verified by the receiver who computes a MAC on the data using the same key as the sender. FIPS 198, *The Keyed-Hash Message Authentication Code (HMAC)*, specifies the computation of a MAC using an approved hash function and a key. NIST SP 800-38B provides for the computation of a MAC, using AES or TDEA. NIST SP 800-38C provides for the use of a mode that both authenticates and encrypts data using AES.

A **hash function** is a one-way function that produces a short representation of a longer message. It is easy to compute the hash value from the input, but it is difficult to reverse the process from the hash value back to the input. Hash functions are used to determine whether or not data has been changed after it was transmitted. Applications of hash functions are used by MACs, digital signature algorithms, key derivation functions, and random number generators. Five hash functions are specified in FIPS 180-2, *Secure Hash Standard*: SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. Since new attacks have indicated that SHA-1 may provide less security than originally thought, SHA-1 is not recommended for the generation of digital signatures in new systems.

Digital signatures are used to prove to the recipient of data or to a third party that a message or data was signed by the originator and that the data was not changed. Digital signatures are generated and verified using asymmetric key algorithms, commonly known as public key algorithms. These algorithms use a pair of keys: a public key that may be known by anyone and a private key that must be known only by the owner of the key pair. The private key is used to generate a digital signature on the information. The signed information and the digital signature are transmitted to the receiver, who uses the public key, which corresponds to but is not the same as the private key, to verify the digital signature. If the digital signature is verified as correct, the receiver can be assured of the identity of the signer and that the signed information was received correctly. The identity of the message signer and the integrity of the data can also be proved to an independent third party, if necessary.

FIPS 186-2, *Digital Signature Standard (DSS)*, specifies three algorithms: Digital Signature Algorithm (DSA); RSA signature algorithm (American National Standard ANSI X9-31); and Elliptic Curve Digital Signature Algorithm (ECDSA) (ANSI X9-62). The security of digital signature systems is dependent upon maintaining the secrecy of users' private keys. The data to which signatures are applied are hash functions that have been implemented as specified in FIPS 180-2.

Key management includes the rules and protocols for generating, establishing, and protecting keys. The security and reliability of cryptographic processes depend upon the strength of the keys, the effectiveness of the protocols associated with the keys, and the protection of the keys. NIST SP 800-57, *Recommendation on Key Management*, provides guidance on the generation, use, and disposal of cryptographic keys. Other topics covered include the selection of cryptographic algorithms and key sizes, and the development of policies for the uses of cryptography.

A **Public Key Infrastructure (PKI)** is the combination of software, encryption technologies, and services that creates and manages the use of public keys used in public key cryptography. Public key (or asymmetric) cryptography allows parties that do not know each other to exchange data securely. The PKI binds public keys to entities, enables other

entities to verify public key bindings, and provides the services needed for ongoing management of keys in networks. A PKI enables confidentiality, integrity, authentication, and digital signature services to be available on a broad scale to many organizations. FIPS 196, *Entity Authentication Using Public Key Cryptography*, specifies two protocols for entity authentication that use a public key cryptographic algorithm for generating and verifying digital signatures. One entity can prove its identity to another entity by using a private key to generate a digital signature on a random challenge. The use of public key cryptography provides strong authentication, without the requirement for authenticating entities to share secret information. Information about the federal PKI is available at http://csrc.nist.gov/pki/.

Random numbers are used within many cryptographic applications to generate keys, other cryptographic values, digital signatures, and challenge-response protocols. Deterministic Random Bit Generators (DRBGs), which use cryptographic algorithms to generate random numbers, have been specified in draft NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*. The DRBGs provide random numbers for cryptographic applications.

Use of Cryptography in Personal Identity Verification (PIV)

FIPS 201, *Personal Identification Verification (PIV) of Federal Employees and Contractors*, approved in February 2005 and recently updated as FIPS 201-1, applies to the identification cards that are issued by federal agencies to their employees and contractors who require access to federal facilities and information systems. PIV cards incorporate an individual's identity credentials on smart cards. PIV components and subsystems use the electronically stored data on the cards to carry out automated identity verification of the individual. FIPS 201 was developed in response to Homeland Security Presidential Directive (HSPD) 12, which called for a federal standard for secure and reliable forms of identification for employees and contractors.

Cryptographic methods support the PIV applications and the information that is stored on the smart cards. NIST SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, specifies the acceptable cryptographic algorithms and key sizes to be implemented in the PIV system to achieve secure and reliable means of identification. The publication discusses the infrastructure components for issuance and management of the PIV card, and the applications for security services that rely on the credentials supported by the PIV card. The cryptographic methods discussed include symmetric and asymmetric encryption algorithms, digital signature algorithms, message digest algorithms, and mechanisms to identify the algorithms associated with PIV keys or digital signatures. Algorithms and key sizes were selected to be consistent with federal standards and to ensure adequate cryptographic strength for PIV applications.

Validation and Testing Requirements

NIST and the Communications Security Establishment of the Government of Canada coordinate a validation program with independent accredited testing laboratories that validate modules for conformance to Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Modules*. The Cryptographic Module Validation Program (CMVP) provides for the validation of implementations of many cryptographic standards and guidelines developed by NIST, including encryption algorithms, digital signature algorithms, hashing algorithms, random number generators, and message authentication methods. Information about the CMVP is available at http://csrc.nist.gov/cryptval/.

NIST has established a program for testing and validating PIV components and subsystems for conformance to FIPS 201-1. This effort is managed by the NIST PIV Program (NPIVP). Testing organizations will be accredited by NIST's National Voluntary Laboratory Accreditation Program (NVLAP), which provides third-party accreditation to testing and calibration laboratories. NVLAP accredits public and private sector laboratories, including commercial, manufacturers' in-house, university, and federal, state, and local government laboratories, based on evaluation of their technical qualifications and their competence to carry out specific calibrations or tests. Information about this new validation program is available at http://csrc.nist.gov/npivp/.

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