February 2000

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

GUIDELINE FOR IMPLEMENTING CRYPTOGRAPHY IN THE FEDERAL GOVERNMENT

By Annabelle Lee, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

This bulletin summarizes a new ITL document, NIST Special Publication (SP) 800-21, *Guideline for Implementing Cryptography in the Federal Government.*

In today's world, both private and public sectors depend upon information technology systems to perform essential and mission-critical functions. In the current environment of increasingly open and interconnected systems and networks, network and data security are essential for the optimum use of information technology. For example, systems that carry out electronic financial transactions and electronic commerce must be protected against unauthorized access to confidential records and unauthorized modification of data.

Cryptography should be considered for data that is sensitive or has a high value if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage. Cryptographic methods provide important functionality to protect against intentional and accidental compromise and alteration of data. These methods support communications security by encrypting the communication prior to transmission and decrypting it at receipt. These methods also provide file and data security by encrypting the data prior to placement on a storage medium and decrypting it after retrieval from the storage medium.

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. The guideline focuses on federal standards documented in Federal Information Processing Standards (FIPS) and the cryptographic modules and algorithms that are validated against these standards. However, to provide additional information, other standards organizations (e.g., American National Standards Institute [ANSI] and International Organization for Standardization [ISO]) are briefly discussed.

Audience

The guideline is intended for federal employees who are responsible for designing systems and procuring, installing, and operating security products to meet identified security requirements. The document may be used by:

- A manager responsible for evaluating an existing system and determining whether cryptographic methods are necessary,
- A technical specialist requested to select one or more cryptographic methods to meet a specified requirement, or
- A procurement specialist developing a solicitation for a system or network that will require cryptographic methods to perform security functionality.

The goal is to provide these individuals with sufficient information to allow them to make informed decisions about the cryptographic methods that will meet their specific needs to protect the confidentiality, authentication, and integrity of data

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 address to this office.

Bulletins issued since September 1998

that is transmitted and/or stored in a system or network.

The guideline is **not** intended to provide information on the federal procurement process or provide a technical discussion on the mathematics of cryptography and cryptographic algorithms.

Scope

The guideline limits its discussion of cryptographic methods to those that meet federal standards. The majority of the information in the document may be useful to both federal and commercial personnel and applicable to all computer networks and environments. Both the federal government and industry use products that meet federal standards, and standards bodies such as ANSI have also adopted federal standards.

The guideline provides information on selecting cryptographic services and methods and implementing the methods in new or existing systems. Specifically, the document discusses the cryptographic products selection process, which may include one or more of the following:

1. Performing a *risk assessment* (or other process) to identify:
   - ❒ assets that must be protected,
   - ❒ vulnerabilities of the system, and
   - ❒ threats that might exploit the vulnerabilities.
2. Identifying the *security regulations and policies* that are applicable to the system.
3. Specifying the *cryptographic security requirements.*
4. Specifying the *security services* that will address the needs identified in items 1-3.

Content

The guideline is organized into three parts. Part one provides an overview of selecting cryptographic services and products:

- Chapter 1 includes background information (purpose, audience, and scope) and the advantages of using cryptography.
- Chapter 2 defines the role and use of standards, describes standards organizations that are outside the federal government, and discusses the new international security standard, ISO 15408, the Common Criteria (CC).
- Chapter 3 describes some implementation issues (e.g., key management, authentication, and recommendations).

Part two focuses on specific methods:

- Chapter 4 describes the methods that are available for symmetric and asymmetric key cryptography.
- Chapter 5 discusses the Public Key Infrastructure (PKI).
- Chapter 6 discusses testing, including the Cryptographic Module Validation Program (CMVP).

Part three ties together all of the information:

- Chapter 7 describes the process of choosing types of cryptography and selecting a cryptographic method(s) to fulfill a specific requirement.
- Chapter 8 includes some examples of federal projects that use cryptography.
- Chapter 9 describes future activities.

Three appendices supplement the guideline:

- Appendix A contains an acronym list.
- Appendix B presents terms and definitions.
- Appendix C includes a bibliography of cryptographic standards and guidelines and cryptography texts.

Uses Of Cryptography

Cryptography is a branch of mathematics based on the transformation of data. Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and the transformation of ciphertext into plaintext by decryption. Cryptography relies upon two basic components: an *algorithm* (or cryptographic methodology) and a *key*. The algorithm is the mathematical function used for encryption or decryption, and the key is the parameter used in the transformation.

There are two basic types of cryptography: *secret-key* systems (also called symmetric systems) and *public-key* systems (also called asymmetric systems). In secret-key systems, the same key is used for both encryption and decryption. That is, all parties participating in the communication share a single key. In public-key systems, there are two keys: a *public* key and a *private* key. The public key used for encryption is different from the private key used for decryption. The two keys are mathematically related, but the private key cannot be determined from the public key.

In general, cryptography is used to meet the following security objectives:

- *Confidentiality* services restrict access to sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the *unauthorized* disclosure of information to unauthorized individuals or processes.
- *Data integrity* services address the unauthorized or accidental modi-

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.

fication of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect *unauthorized* data modification. The goal is for the receiver of the data to verify that the data has not been altered.

- *Authentication* services establish the validity of a transmission, message, or an originator. (Authentication services also verify an individual's authorization to receive specific categories of information. These services are not specific to cryptography.) Therefore, this service applies to both individuals and the information itself. The goal is for the receiver of the data to determine its origin.
- *Non-repudiation* services prevent an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

Standards And Criteria

Standards contain consistent technical specifications or other criteria to be used as rules or guidelines to ensure that products, processes, and services are appropriate for their stated purpose. Under the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987 (Public Law 100-235), the National Institute of Standards and Technology (NIST) is responsible for developing technical standards and guidelines for the security and privacy of federal information resources. Some of the standards and guidelines used to protect sensitive information are issued by NIST as Federal Information Processing Standards (FIPS). Federal agencies must comply with all standards made mandatory and binding by the Secretary of Commerce.

Technically, the Secretary of Commerce has authority to establish standards only for the federal government. However, since FIPS are established through a public process, the public is aware of their existence, and industry often uses conformance to applicable NIST standards as a factor when purchasing products. Also, NIST has a long history of participation in industry standards groups, including ANSI, ISO, the Institute of Electrical and Electronics Engineers (IEEE), the Internet Engineering Task Force (IETF), and others. In some cases, the federal government adopts industry standards (ANSI X9.17, *Key Management*, was adopted with restrictions as FIPS 171), and industry has adopted FIPS (e.g., Data Encryption Standard (DES) and DES Modes were adopted by ANSI).

Benefits of Standards

Standards are important because they define common practices, methods, and measures/metrics. Therefore, standards increase the reliability and effectiveness of products and ensure that the products are produced with a degree of quality. Standards provide solutions that have been accepted by a wide community and evaluated by experts in relevant areas. By using standards, organizations can reduce costs and protect their investments in technology.

Standards provide for information technology (IT) interoperability, security, and integrity, and other benefits:

- **Interoperability.** Products developed to a specific standard may be used to help support interoperability with other products that conform to the same standard. By using the same cryptographic algorithm, data that was encrypted using vendor A's product may be decrypted using vendor B's product. The use of a common standards-based cryptographic algorithm is necessary, but may not be sufficient to ensure product interoperability. Other common standards, such as communications protocol standards, may also be necessary. By ensuring interoperability among different vendors' equipment, standards permit an organization to select from various available products to find the most cost-effective solution.
- **Security.** Standards may be used to establish a common approved level of security. Most agency managers are not cryptographic security experts. By using a FIPS-approved cryptographic algorithm, a manager knows that a standard has been developed, the algorithm has been tested against this standard, and the results validated by NIST. NIST validation means the algorithm has been found to be adequate for the protection of sensitive government data. In addition, most FIPS-approved algorithms have gone through a significant period of public analysis and comment.
- **Integrity.** Standards may be used to assure the integrity of a product. Standards may:
  - Specify how a feature is to be implemented, e.g., the feature must be implemented in hardware.
  - Require a test or alarm to detect a malfunction.
  - Require specific documentation to assure proper implementation and product change management.

  Many FIPS contain associated conformance tests and specify the conformance requirements. The conformance tests may be administered by NIST-accredited laboratories and provide validation that the standard was correctly implemented in the product.
- **Common Form of Reference.** A standard may become a common form of reference to be used in evaluating vendors' products. FIPS 140-1, *Security Requirements for Cryptographic Modules*, contains security and integrity requirements for *any* cryptographic module implementing cryptographic operations. FIPS 140-1 establishes a common form of reference by defining four levels of security for each of eleven security attributes.
- **Cost Savings.** A standard can save a great deal of money by providing a single commonly accepted specification. Without standards, users may be required to become *experts* in every IT

product that is being considered for purchase. Also, without standards, products may not interoperate with products purchased by other users. This results in a significant waste of money or the delayed implementation of IT.

Common Criteria

The *Common Criteria* (CC) is referenced throughout the guideline. The CC represents the outcome of efforts to develop criteria for evaluation of IT security. These criteria will be used throughout the international community. The CC defines a set of IT requirements of known validity that can be used in establishing security requirements for prospective products and systems. The CC also defines the Protection Profile (PP) construct that allows prospective consumers or developers to create standardized sets of security requirements that will meet their needs. The CC presents requirements for the IT security of a product under the distinct categories of functional requirements and assurance requirements.

The CC is a *voluntary* standard used to describe the security properties (functional and assurance) of IT products (or classes of products) and systems. In essence, the CC is a standard security specification "language." Products whose security properties have been specified using the CC may then be validated (tested) for conformance to their CC specifications. Such a validation, when performed by an accredited testing laboratory, confirms that the product meets its security specification(s).

In general, FIPS referenced in the guideline are standards made mandatory and binding by the Secretary of Commerce. For example, FIPS 46-3, *Data Encryption Standard*, is a specific set of technical security requirements for the Triple Data Encryption Standard algorithm.

When developing a specification or criteria for selection of a cryptographic module/product, both the CC and FIPS may be used. The CC may be used to specify the *functions* the algorithm will perform. The FIPS designate the specific type of algorithm (3DES, DSA) and the level of independent testing required (FIPS 140-1).

Some Implementation Issues

There are many issues that are applicable to the implementation of security methods/products. These are extensively discussed in other documents such as NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook*; NIST SP 800-14, *Generally Accepted Principles and Practices for Security Information Technology System*; and OMB Circular A-130, *Security of Federal Automated Information Resources*, Appendix III. Of particular relevance are the sections on training, contingency planning, assignment of roles and responsibilities, and security violation reporting and response.

Hardware vs. Software Solutions

The tradeoffs among security, cost, simplicity, efficiency, and ease of implementation need to be evaluated. Cryptography can be implemented in hardware, software, and/or firmware; each has its related costs and benefits.

Historically, software has been less expensive and slower than hardware, although for large applications, hardware may be less expensive. In addition, software is easier to modify or bypass than equivalent hardware products. The advantages of software solutions are flexibility and portability, ease of use, and ease of upgrade.

In many cases, cryptography is implemented in a hardware device but is controlled by software; therefore, a hybrid solution is provided. Again, the user must evaluate the solutions against requirements to determine the best solution.

Public- vs. Secret-Key Cryptography

The primary advantage of public-key cryptography is increased security and convenience; private keys never need to be transmitted or revealed to anyone. In a secret-key system, the secret keys must be transmitted, either manually or through a communication channel. There may be a chance that an unauthorized individual can access the secret keys during their transmission.

The primary advantage of secret-key cryptography is speed. There are popular secret-key encryption methods that are significantly faster than any currently available public-key encryption method. Alternatively, public-key cryptography can be used with secret-key cryptography to get the best of both worlds, the security advantages of public-key systems and the speed advantages of secret-key systems. The public-key system can be used to encrypt a secret key that is used to encrypt the bulk of a file or message.

In some situations, public-key cryptography is not necessary and secret-key cryptography alone is sufficient. This includes environments where secure secret-key agreement can take place, environments where a single authority knows and manages all the keys, and a single-user environment. In general, public-key cryptography is best suited for an open multi-user environment.

Key Management

The proper management of cryptographic keys is essential to the effective use of cryptography for security. Ultimately, the security of informa-

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 to listproc@nist.gov with the message **subscribe itl-bulletin**, and your proper 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.

tion protected by cryptography depends directly on the protection afforded the keys. All keys need to be protected against modification, and secret and private keys need to be protected against unauthorized disclosure. Listed below are recommendations for effective key management.

❑ *Ensure that users are aware of their liabilities and responsibilities, and that they understand the importance of keeping their keys secure.*

The security of cryptographic keys in an electronic or digital signature system is the foundation of a secure system; therefore, users must maintain control of their keys! Users must be provided with a list of responsibilities and liabilities, and each user should sign a statement acknowledging these concerns before receiving a key (if it is a long-term, user-controlled key). If different user roles (e.g., security officer, regular user) are implemented in a system, users should be aware of their unique responsibilities, especially regarding the significance of a key compromise or loss.

❑ *Prepare for the possibility of compromise.*

It is imperative to have a plan for handling the compromise or suspected compromise of central/root keys or key components at a central site; this should be established before the system goes "live." The contingency plan should address what actions should be taken with system software and hardware, central/root keys, user keys, previously generated signatures, encrypted data, etc.

If someone's private key is lost or compromised, others must be made aware of this, so that they will no longer encrypt messages using the invalid public key nor accept messages signed with the invalid private key. Users must be able to store their private keys securely, so that no intruder can find them, yet the keys must be readily accessible for legitimate use. Keys need to be valid only until a specified expiration date.

❑ *Sign and verify the code that implements the cryptographic functions.*

Software at the central key management site should be electronically signed and periodically verified to check the integrity of the code. This provides a means of detecting the unauthorized modification of system software. Within a cryptomodule, this feature of generating and verifying a cryptographic checksum is required by FIPS 140-1.

❑ *Ensure that a system implemented for a federal government agency has its centrally stored keys and system software controlled by federal employees.*

Proper control of central/root keys and key management software and hardware is critical to the security of the system. In the situation where a federal agency operates a system that was developed by a contractor, federal employees should be in control of this material. This also applies to configuring the key management hardware and software. Once the system goes live, unlimited access to central data, code, and cryptomodules should not be given to nonfederal employees, including those who were contracted to develop and/or maintain the system.

❑ *Secure Key Management.*

Key management provides the foundation for the secure generation, storage, distribution, and translation of keys. Another role of key management is key maintenance, specifically the update/replacement of keys at the completion of a cryptoperiod. The cryptoperiod is determined based on the sensitivity of the information and the risk of key compromise.

Key Generation

The generation of keys is the most sensitive of all cryptographic functions. Any inadequacies in the implementation of the key-generation function or in the physical security safeguards of that function will seriously undermine the integrity of other cryptographic mechanisms. The physical security measures are necessary to prevent unauthorized disclosure, insertion, and deletion of the system or keys produced by the system. Specifically, all automated resources which generate keys and initialization vectors (IVs) should be physically protected to prevent:

- disclosure, modification, and replacement of the keys,
- modification or replacement of the IVs, or
- modification or replacement of the generation algorithm or device.

Depending on the desired management structure, there are some applications where the generation of keys is desirable and other applications where the distribution of keys from another source, such as a central authority, may be more desirable.

Key Use

❑ *Cryptographic keys may need special physical protection.*

If keys or key components are stored on a token (e.g., floppy disk, personal computer (PC) card, smartcard, etc.), this token may have to be stored in a special manner to prevent unauthorized individuals from accessing the key or key component. For example, if key components for starting a Certification Authority (CA) or Key Management Facility are stored on tokens which are secured in a safe, multiple people might have access to this token. Therefore, additional protection is needed for each token, possibly by using a tamper-evident envelope, to enable the token's owner to determine if another person used a token.

❑ *Authentication timeout features are important for protecting keys from compromise or misuse.*

An authentication timeout feature for a cryptographic module or token is important to minimize the possibility of an unauthorized individual accessing an "active" cryptomodule and using its cryptographic keys. This could happen if a cryptomodule is left unattended by a user who has authenticated to it and loaded their cryptographic keys. One alternative is to force a user to periodi-

cally reauthenticate oneself to a cryptomodule, rather than allow them to stay logged in for an indefinite amount of time. For sensitive applications, it may be necessary to restrict the hours during which this can take place.

❑ *Key recovery capabilities are important.*

IT systems must protect the confidentiality of information. There must be safeguards to ensure that sensitive records are neither irretrievably lost by the rightful owners nor accessed by unauthorized individuals. Key recovery capabilities provide these controls. All key components should be available to an organization regardless of whether the associated user is currently working in the organization. Employees leave organizations voluntarily and some are removed; in either situation, the organization may need to access the key components to recover encrypted data. Key recovery capabilities allow organizations to restore key components.

It is very important to have backup copies of central/root keys, since the compromise or loss of those components could prevent access to keys in the central database, and possibly deny system users the ability to decrypt data or perform signature verifications.

Key Archiving

❑ *Archive user keys for a sufficiently long cryptoperiod.*

A cryptoperiod is the time during which a key can be used for signature verification or decryption; it should extend well beyond the lifetime of a key (where the lifetime is the time during which a key can be used to generate a signature and/or perform encryption). Keys should be archived for a lengthy cryptoperiod (on the order of decades), so that they can be used to verify signatures and decrypt ciphertext during the cryptoperiod.

Key Destruction

❑ *Determine reasonable lifetimes for keys associated with different types of users.*

Users with different roles in the system should have keys with lifetimes that take into account the users' roles and responsibilities, the applications for which the keys are used, and the security services which are provided by the keys (user/data authentication, confidentiality, data integrity, etc.). Reissuing keys should not be done so often that it becomes burdensome; however, it should be performed often enough to minimize the loss caused by a possible key compromise.

❑ *Handle the deactivation/revocation of keys so that data signed prior to a compromise date (or date of loss) can be verified.*

It should be possible to designate a signing key as "lost" or "compromised," so signatures generated prior to a specified date can be verified. Otherwise, all data previously signed with a lost or compromised key would have to be reviewed and resigned.

For More Information

NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*, is available at http://csrc.nist.gov.

NOTE: Any mention of commercial products is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology 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