SECURE MANAGEMENT OF KEYS IN CRYPTOGRAPHIC APPLICATIONS: GUIDANCE FOR ORGANIZATIONS

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

Organizations that depend upon information technology (IT) systems to carry out essential and mission-critical functions must protect their sensitive information from unauthorized access and modification. Cryptographic methods are powerful IT tools that organizations can use to maintain the confidentiality and integrity of their information, to verify that information was not changed after it was sent or stored, to authenticate the originator of information, and to authenticate the entity accessing the information. To use cryptography effectively, organizations must integrate security activities into the IT system development life cycle, and rigorously select the products, algorithms, and protocols that meet their security requirements.

A cryptographic algorithm and a key are used to provide a number of cryptographic services, including encrypting data, generating a digital signature, decrypting encrypted data, and verifying a digital signature. Other cryptographic services include generating challenges, random numbers, and Message Authentication Codes (MACs). Secure management of the cryptographic keys is critically important, since 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 given to the keys. Cryptographic keys can be compared to the combination of a safe. If an attacker learns the combination of a safe, it is no longer protected from a break-in. Similarly, poor key management can compromise the security provided by strong cryptographic algorithms.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued Part 3 of its Special Publication (SP) 800-57, *Recommendation for Key Management*. Part 3, *Application-Specific Key Management Guidance*, supplements Parts 1 and 2 of NIST SP 800-57, by providing guidance on the management of keys and the selection of cryptographic features of currently available applications and systems.

NIST Special Publication 800-57, *Recommendation for Key Management,* Part 3, *Application-Specific Key Management Guidance*

NIST SP 800-57, *Recommendation for Key Management,* offers comprehensive guidance on the secure generation, storage, distribution, and destruction of keys for cryptographic systems. Part l of NIST SP 800-57 contains basic information for users, cryptographic system developers, and system managers. The publication discusses the rules and protocols for generating, establishing, and protecting keys, and recommends best practices that organizations can use to protect keys.

Part 2 of NIST SP 800-57, *General Organization and Management Requirements*, identifies the structural and functional elements that are common to effective key management systems, and helps system owners and managers to implement and manage these systems. Part 2 covers federal laws and directives concerning security planning and management, and recommends ways that organizations can incorporate their key management practices into their security planning activities.

Parts 1 and 2 establish a sound basis for selecting appropriate cryptographic algorithms and for managing the cryptographic keys.

Part 3, *Application-Specific Key Management Guidance*, was written by Elaine Barker, William Burr, Alicia Jones, Timothy Polk, Scott Rose, and Quynh Dang of NIST, and by Miles Smid of Orion Security Solutions, and was issued by NIST in December 2009. Part 3 focuses on helping system installers and system administrators select and use currently available key management infrastructures, protocols, and applications. It recommends secure combinations of algorithm suites, key sizes, and other related options, and discusses the implementation issues that impact the security effectiveness of an organization's key management processes.

Part 3 discusses the compliance issues that affect federal organizations and their ability to protect government information. It also advises staff members who make purchasing decisions for new systems for an organization, and end users who make their own installation, administration, and purchasing decisions.

The appendices to Part 3 include a glossary, an explanation of acronyms used, basic advice to new end users on obtaining and using cryptographic keys, and an extensive list of references for the documents cited in the publication.

Parts 1, 2, and 3 of NIST SP 800-57 are available from the NIST Web page http://csrc.nist.gov/publications/PubsSPs.html.

Key Management Infrastructures, Protocols, and Applications

The currently available key management infrastructures, protocols, and applications that are discussed in Part 3 include:

• **Public Key Infrastructures (PKIs)** are used for the distribution of public keys for information services that include confidentiality of information, authentication, digital signatures, and integrity of information. Public key systems use public key algorithms and a key pair, consisting of two related keys, to perform their functions: a public key that can be publicly known and a private key that is kept secret by its owner. With a strong binding between the owner and the owner's public key, the identity of the originator of a message can be traced to the owner of the private key. Public key algorithms are used to establish secure services between communicating entities, to provide assurance that data has not been modified, and to authenticate the originator of

the data. PKI-enabled applications and protocols include the Internet Protocol Security (IPsec) protocol, the Transport Layer Security (TLS) protocol, the Secure/Multipurpose Internet Mail Extensions (S/MIME) protocol, and some versions of Kerberos.

Public key certificates are a basic component of PKIs. These certificates are issued by a Certification Authority (CA) to bind the user's name to the user's public key, using a digital signature generated by the CA. The digital signature process consists of the computation of a message digest value on the information using a cryptographic hash algorithm, and the signing of the message digest using the CA's private key. The user is authorized to use the private key associated with the public key in the certificate. The CA that issues the certificate is a trusted third party that generates and signs the certificate after verifying the identity of the user; the validity of the public key; associated algorithms and any relevant parameters; and the user's possession of the corresponding private key.

The CA often delegates responsibility for the verification of the subject's identity to a Registration Authority (RA). The certificate is used to distribute the user's public key to other interested parties, known as relying parties, since they rely on the assurances provided by the PKI and the certificate creation process.

Part 3 provides detailed recommendations for many security and compliance issues associated with the use of PKI systems, including key sizes, the selection of digital signature and hash algorithms, and the software and hardware used by the CA and RA.

• **Internet Protocol Security (IPsec),** a suite of protocols for securing Internet communications at the network layer, operates within the Internet Protocol (IP). It is frequently used to establish Virtual Private Networks (VPNs), requiring both parties to share keying material, and enabling telecommuters or travelers to gain secure access to their business networks. VPNs are used to protect communications carried over public networks. A VPN can provide several types of data protection, including confidentiality, integrity, data origin authentication, replay protection, and access control. IPsec provides the cryptographic security functions for versions 4 and 6 of the Internet Protocol.

IPsec operates by inserting headers that provide integrity protection, confidentiality, data origin authentication, and replay protection. Some of the implementation issues for IPsec that are discussed in Part 3 include use of the proper version of the IPsec protocols, the selection of a key exchange protocol, and the selection of cryptographic algorithms.

• **Transport Layer Security (TLS)** and **Secure Socket Layer (SSL)** protocols, developed by the Internet Engineering Task Force (IETF), are the primary end-to-end security protocols used to protect information on the Internet. TLS is an enhanced version of SSL; the protocols are similar, but are not identical.

TLS is a robust protocol that is used to protect links, such as the authentication server to a wireless access point, or the email link between client and server. Part 3 focuses on the situation when a browser is acting as a client for a human user, and is interfacing with a

Web site. In a TLS session, there is a cryptographic negotiation between the end user's Web browser and the Web server of the party that the end user is contacting to conduct business or exchange information. The negotiation involves establishing a set of symmetric cryptographic keys to be used for functions that are carried out during subsequent interactions, using a public key algorithm and a key establishment method. The newly established keys are used with symmetric key algorithms - algorithms that use a single cryptographic key for each operation and its inverse, such as for encryption and decryption. A cipher suite bundles the choice of key-establishment method, symmetric key algorithm, and data-integrity hash function to be used into a single value.

A large number of cipher suites have been defined for TLS. NIST SP 800-57, Part 3, recommends the cipher suites that are best for the protection of federal government information.

• **Secure/Multipurpose Internet Mail Extensions (S/MIME)** provide a consistent way to send and receive secure Internet mail. S/MIME is defined by IETF specifications. S/MIME provides cryptographic security services for electronic messaging applications, including the authentication of a sending party using digital signatures; message integrity and non-repudiation of origin using digital signatures; and confidentiality using encryption.

S/MIME requires a suite of algorithms for creating digital signatures, generating hash values, establishing keys, and encrypting the content of the email, as well as some means of establishing and sharing digital identities. Federal implementations rely on a public key infrastructure to establish S/MIME user identities, to bind those identities to the user's public key through public key certificates, to provide digital signatures and to provide keys to be used for content encryption or to establish symmetric keys for use on a per-message basis.

Part 3 includes recommendations for the use of the components of S/MIME products, which can be implemented with different combinations of security features and with different cryptographic algorithms. Key management features that are appropriate for the protection of federal government information are discussed.

• **Kerberos** is an authentication mechanism that was developed by a team at the Massachusetts Institute of Technology to enable the secure authentication of users to Target Servers (TSs) over an unprotected network, where client software acts on behalf of a user. Kerberos is used for local logins, remote (over the network) authentication, and for client-to-TS requests. It can also be extended to provide for the establishment of cryptographic keys between a client and a TS. Kerberos has been designed so that a user and a TS rely on a trusted third party to provide assurance of each party's identity.

The trusted third party is a Key Distribution Center (KDC), which consists of an Authentication Server (AS) and a Ticket Granting Service (TGS). The AS and TGS may or may not reside on the same machine. The KDC has a database of user, TS, and TGS

symmetric keys. All KDC symmetric keys are accessible by the TGS. The user's key is normally created using a hash algorithm, the user's password, and other information.

SP 800-57, Part 3, advises on the selection of encryption algorithms and protection of the symmetric keys used by Kerberos authentication mechanisms.

• **Over-the-Air Rekeying of Digital Radios (OTAR)** includes a protocol that has been designed to handle several types of cryptographic security, including the protection of unclassified, sensitive communications. Different security requirements require the implementation of different cryptographic algorithms.

For key management, a secure mobile system consists of Key Management Facilities (KMFs) and mobile radios that are subordinate to each KMF. Key Management Messages (KMMs) are exchanged between each KMF and its subordinate mobile radios. Cryptographic keys are transferred from a KMF to a mobile radio, protected using a key-wrapping algorithm and key-wrapping key; key wrapping involves encrypting keys to provide confidentiality and integrity using a symmetric key. Many of the KMMs are protected by encrypting the data in the messages; the integrity of the messages is protected using a Message Authentication Code (MAC).

SP 800-57, Part 3, recommends the selection of cryptographic algorithms, message authentication methods, and key sizes for OTAR installations.

• **Domain Name System Security Extensions (DNSSEC)** are part of the Domain Name System (DNS), the international hierarchical distributed database system for mapping Internet addresses, Simple Mail Transfer Protocol (SMTP) servers, and other information to a human-readable name. DNS handles mappings between host domain names and Internet addresses, as well as other forms of data, such as host system information, the geographic location of servers, and encoded digital certificates. DNS data is stored as individual Resource Records (RRs) that associate data, such as an IP address and mail server name, with a domain name and an identifying Resource Record type code (RR type).

All of the RRs for a particular organization are stored in an administrative unit called a zone. Zones are hierarchical with a small group of servers, or a single server, that holds a local zone database. Multiple secondary servers obtain their copies of the zone database from the primary server. Other servers query the primary and secondary servers, and cache the replies. The end user's client system makes DNS queries to the cache servers or to the primary and secondary servers.

The basic DNS does not have many security features. Proposals have been developed to provide security enhancements contained in three IETF documents, collectively called the DNS security extensions (DNSSEC), which provide a layer of authentication and integrity protection for any kind of data stored in the DNS, including data used by other protocols. For example, there are RR types allocated for storing Secure Shell (SSH) keys in the DNS, which then rely on DNSSEC to protect the integrity of that information.

NIST SP 800-57, Part 3, includes recommendations for the selection of cryptographic algorithms, message authentication methods, and key sizes for DNS applications.

• **Encrypted File Systems (EFSs)** present somewhat different key management issues than the encryption of network-communicated data. Network communications security focuses on the privacy and integrity of information in transit. Storage or file issues are concerned with the privacy and integrity of persistent data and the secure sharing of this data.

While the other protocols and standards discussed above have been thoroughly studied by the network security community, the commercial solutions for file encryption employ a wide variety of security schemes and methods for storing keys. A range of methods are available for file encryption. Designers of file encryption systems must determine how the keys are used in the system; how they are protected; where the keys are stored on the system; and whether the method accommodates many user communities without requiring the storage of an extremely large number of keys.

Future Activities

NIST plans to revise the key management recommendations with updates to the topics covered, and to add topics such as Secure Shell (SSH), IEEE 802.1x Port-Based Network Access Control, Physical Access Control Systems (PACS), and other areas as new techniques are widely implemented.

Conformance testing for implementations of key management mechanisms will be conducted under the provisions of the Cryptographic Module Validation Program (CMVP), a joint effort of NIST and the Communications Security Establishment of Canada. Cryptographic implementations must adhere to the requirements for cryptographic algorithms as specified in Federal Information Processing Standards (FIPS) and NIST Special Publications (SPs) in order to be validated under the CMVP. Information on the CMVP is available on the NIST Web page http://csrc.nist.gov/groups/STM/cmvp/index.html.

For More Information

NIST publications that provide information and guidance on cryptographic key management issues include:

FIPS 140-2, *Security Requirements for Cryptographic Modules*
FIPS 180-3, *Secure Hash Standard (SHS)*
FIPS 186-3, *Digital Signature Standard (DSS)*
FIPS 197, *Advanced Encryption Standard (AES)*
FIPS 198-1, *The Keyed-Hash Message Authentication Code (HMAC)*
NIST SP 800-21, *Guideline for Implementing Cryptography in the Federal Government*

NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*
NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*
NIST SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*
NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*
NIST SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications*
NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
NIST SP 800-102, *Recommendation for Digital Signature Timeliness*

For information about these NIST standards and guidelines, as well as other security-related publications, see NIST's Web page http://csrc.nist.gov/publications/index.html.

Information about NIST's information security programs is available from the Computer Security Resource Center at http://csrc.nist.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.