NIST Computer Security Handbook Cryptography]

* * * * * * * * * * * * * NOTE * * * * * * * * * * * * * * * * *

This file is a DRAFT chapter intended to be part of the NIST Computer Security Handbook. The chapters were prepared by different parties and, in some cases, have not been reviewed by NIST. The next iteration of a chapter could be SUBSTANTIALLY different than the current version. If you wish to provide comments on the chapters, please email them to roback@ecf.ncsl.gov or mail them to Ed Roback/Room B154, Bldg 225/NIST/Gaithersburg, MD 20899.

* *

DRAFT -- DRAFT -- DRAFT -- DRAFT -- DRAFT

Introduction

Cryptography provides an important tool for the protection of information and is used in many aspects of computer security. For example, it can help provide data confidentiality and integrity, support sound user authentication and access controls, and increase the security provided by other technical controls. Many people realize that modern cryptography relies upon advanced mathematics. Not all understand, however, that users can obtain the benefits offered by cryptography without an understanding of its mathematical underpinnings.

Cryptography's uses are wide and varied. They include traditional uses such as eavesdropping protection and newer uses such as ensuring that computer files are unchanged or that computer programs are not infected with viruses.

This chapter describes the use of cryptography as a tool for satisfying a wide spectrum of IT security needs and requirements. It describes fundamental aspects of the basic cryptographic technologies, and some specific ways cryptography can be applied to improve security. This chapter also explores some of the important issues which should be considered when incorporating cryptography into IT systems.

BASIC CRYPTOGRAPHIC TECHNOLOGIES

Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a key. For instance, in a system where letters are substituted for other letters, the "key" is the chart of paired letters and the algorithm is substitution. In modern cryptographic systems, the algorithms are complex

mathematical formulae and keys are strings of bits. For two parties to communicate they must use the same algorithm. In some cases, they must also use the same key. Many cryptographic keys must be kept secret. Sometimes algorithms are also kept secret.

There are two basic types of cryptographic systems: secret key systems (also called symmetric systems) and public key systems (also called asymmetric systems). Table 1 summarizes and compares some of the distinct features of both secret and public key systems. Both types of systems offer advantages and disadvantages. Often, the two are combined to form a hybrid system in order exploit the strengths of each type. In order to determine which type of cryptography to utilize, an organization first has to identify its security requirements and operating environment. Then the organization can determine which type of cryptography best meets its needs.

#Secret Key Cryptography

Secret key cryptography is better known than public key cryptography. In secret key cryptography, two (or more) parties share the same key. In secret key cryptography, the same key is used to encrypt and decrypt data. As the name implies, secret key cryptography relies on keeping the key secret. If this key is compromised, the security offered by cryptography is severely reduced or entirely eliminated. Secret key cryptography assumes that the parties who share a key rely upon each other not to disclose the key and protect it against modification. Since both parties share the same key, secret key cryptography only protects information against third parties.

Secret key cryptography can be used to protect both confidentiality and integrity of information. It can also be used to support computer security technical controls, such as user authentication.

The best known secret key system is the Data Encryption Standard (DES), published by NIST as Federal Information Processing Standard (FIPS) 46-1. Although the adequacy of DES has at times been questioned, these claims remain unsubstantiated and DES remains strong. It is the most widely accepted, publicly available cryptographic system today. Besides being the only published secret key system approved for protection of Federal unclassified data, DES has been widely adopted by the commercial sector. The American National Standards Institute (ANSI) has adopted DES as the basis for encryption, integrity, access control, and key management standards.

Public Key Cryptography

Public key cryptography is a more modern invention than secret key cryptography. It is also very different and is not always easily understood. Whereas secret key cryptography employs a single key shared by two (or more)

parties, public key cryptography uses a pair of keys for each party. One of these is "public" and one "private." The public key can be made known to other parties, perhaps published in an on-line directory. The private key must be kept confidential and be known only to its owner. (All keys, however, must be protected against modification.)

Using this type of cryptography, any party can use any other party's public key to send an encrypted message; however, only the party with the corresponding private key can decrypt, and thus read, the message. For example, it can be used to send an encrypted confidential message between Person A and Person B. Each person has two keys, one public and one private. Person A can encrypt a message to Person B. To do this, he uses Person B's Public key. Only Person B can decrypt the message, which requires use of his private key. This ensures that only Person B can read the message, thus providing data confidentiality.

Public key cryptography can also be used for other purposes. For example, consider again Person A sending a message to Person B.

In this case, however, Person A not only wants to keep the message confidential but also for Person B to know that the message really came from Person A. In this case, Person A can encrypt the data with both Person A's private key and Person B's public key. When the message is received, Person B decrypts the message using both Person A's public key and Person B's private key. Like the other example, Person B is the only one who can decrypt the message, thus providing data confidentiality. However, in this case only Person A could have sent it, since it was encrypted with Person A's private key. There are many variations of these basic examples, which are explained in the Services section below.

Public key cryptography is particularly useful in those situations when the parties wishing to communicate can not rely upon each other or do not share a common key. Public key cryptography is typically used to protect cryptographic keys used by secret key cryptography and in digital signatures, but also for other purposes as discussed later in this chapter.

There are several public key cryptographic systems. One of the first public key systems, named RSA after its three MIT creators, Ronald Rivest, Adi Shamir, and Len Adleman, is in wide use and can provide many different security services. The Digital Signature Standard (DSS), which is described later in the chapter, is another example of a public key system.

Hybrid Cryptographic Systems

Public and secret key cryptography have relative advantages and disadvantages, although it may initially seem that public key cryptography is preferable because of its versatility. However, speed is typically a significant advantage for secret key

systems. Equivalent implementations of secret key cryptography can run 1,000 to 10,000 times faster than public key cryptography.

To exploit the advantages of both secret and public key cryptography, an IT system can use both types in a complementary manner, with each performing different functions. Typically, the speed advantage of secret key cryptography means that it is used for encrypting bulk data. Public key cryptography is used for smaller transmissions, which are less demanding to the IT system's resources. A practical use of the public key side of a hybrid system, for example, is to automate the distribution of the keys used by secret key cryptography. This is known as an example of automated key distribution. This type of hybrid system provides many of the advantages of both public and secret key cryptography while minimizing the disadvantages.

USES OF CRYPTOGRAPHY

As discussed in the Introduction, cryptography can be used to provide for data confidentiality and integrity. It can also be used to determine the originator of a message (also known as non- repudiation, see sidebar) and as a basis for other security controls, such as identification and authentication and logical access controls. (See chapters ***** and ***** respectively.) These benefits, called security services by computer security specialists, are obtained through specific implementations of cryptography (frequently referred to as security mechanisms).

Once it is determined what security services are required, the mechanisms that provide that service can be reviewed. Then the most cost-effective ones can be selected. The following subsections describe some of the common cryptographic implementations mechanisms, and the benefits that each can provide.

Data Encryption]

One of the best ways to obtain cost-effective data confidentiality if through the use of encryption. Encryption transforms intelligible data (understandable to either a human [e.g., a novel] or machine [e.g., executable code]), called "plaintext," into an unintelligible form, called "ciphertext." This process is reversed through the process known as decryption. Once data is encrypted, the ciphertext does not have to be protected against disclosure, since it reveals little (except perhaps length) about the plaintext. It does, however, have to be protected against modification. If it is not, it will not decrypt correctly.

Both secret key and public key cryptography can be used for data encryption. Secret key encryption, as noted above, is typically much faster, but has attendant key distribution difficulties. With secret key cryptography, the same key is used to both encrypt and decrypt data. With public key cryptography, selecting which key or keys to use for encryption can be more complicated as it is based upon the type of security objectives desired. Both encryption methods are designed so that

only an authorized party has the key necessary to decrypt the ciphertext, thus assuring that only intended parties have access to the data.

Message Authentication Codes

In IT systems, it is not always possible for humans to scan information to determine if data has been erased, added or modified. Even if scanning were possible, the individual may have no way of knowing what the correct data should be. For example, "do" may be changed to "do not"; or $1,000 may be changed to $10,000. It is therefore desirable to have an automated means of detecting both intentional and unintentional modifications of data. While error detecting codes have long been used in communications protocols (e.g., parity bits), these are easily defeated to allow modifications to go undetected. Fortunately, cryptography can be used in a very secure technique for performing error detection.

A Message Authentication Code (MAC) is a means for performing error detection using secret key cryptography in order to detect unauthorized modifications to data. NIST FIPS 113, Computer Data Authentication, specifies a standard technique for calculating a MAC. Using a secret key, a MAC is calculated from and appended to the data. To verify that the data has not been modified at a later time, any party with access to the correct secret key can recalculate the MAC. The new MAC is compared with the original MAC, and if they are identical, the verifier has confidence that the data has not been modified by an unauthorized party. If the two MACs are different, then an unauthorized modification must be assumed. The calculation and verification of a MAC from data provides for its integrity, since any modification to the data by an unauthorized party can be detected.

Electronic Signatures

Today's IT systems are storing and processing more and more paper-based documents in electronic form. Having documents in electronic form permits rapid processing and transmission and thereby improves overall efficiency. However, approval of a written document has traditionally been indicated by a written signature. Thus, there is a need for the electronic equivalent of a written signature which can be recognized as having the same legal status as a written signature.

Why not just take a digital picture of a written signature? Unfortunately, a digital image of a written signature (also known as a digitized written signature) does not provide adequate security. Such a digitized written signature could easily be copied from document to document with no way to determine whether or not it is legitimate. Use of cryptography, however, provides a solution.

Cryptography can be used to protect electronic documents from modification and forgery by enabling the generation of an electronic signature that is intrinsically tied to each component in the electronic document. This means that the change to a single character in the document results in an unpredictable change in the signature. Therefore, when the electronic digital signature created via cryptography is verified, any alteration is highly likely to be detected.

While there are many uses for electronic signatures, they have particularly important implications for Electronic Data Interchange (EDI). For these important business technologies to succeed, adequate security services are necessary. The use of cryptography in general and the use of electronic signatures in particular is growing and is likely to become even more widespread as the use of EDI continues to grow. Discussed below are the two types of electronic signatures.

Message Authentication Codes

An electronic signature can be implemented using secret key cryptography. If a secret key is used to protect data, and the key used is shared only by the originator and recipient of the data, then the recipient can authenticate the originator of the data, provided that the key has not been released to an unauthorized party or otherwise compromised. For example, if two parties share a secret key and one party receives data with a MAC that is correctly verified using the shared key, that party may assume that the data was sent by the other party. This does assume, however, that the two parties trust each other. Thus, through the use of a MAC, in addition to data integrity, authentication of origin to the receiver of the data is also obtained. Such systems have been approved for use by the Federal government as a replacement for written signatures on certain electronic documents.

Digital Signatures

Another type of electronic signature called a "digital signature" can be implemented using public key cryptography. Data is electronically signed by applying the originator's private key to the data. (The exact mathematical process for doing this is not important for this discussion.) Often, the private key is applied to a shorter form of the data, called a "hash," rather than to the entire set of data. The resulting digital signature can be stored or transmitted along with the data. The signature can be verified by any party using the public key of the signer. This feature is very useful, for example, when distributing signed copies of virus-free software. Any recipient can verify that the program remains virus-free. If the signature verifies properly, then the verifier has confidence that the data was not modified after it was signed and that it was signed by the owner of the public key.

Now, recall that with secret key cryptography, both the signer and verifier can calculate the MAC, since they must share the same key. With public key

cryptography, however, the private key used to generate the signature is known only to its owner, and the signature can be verified by a third party by applying the signer's public key. A digital signature, therefore, not only provides for the integrity and the authentication of the source of data, but also inherently provides for non-repudiation of origin, whereby the signer cannot falsely deny having signed the data.

NIST has proposed a Digital Signature Standard (DSS) which uses public key cryptography and is appropriate for applications requiring a public key-based digital signature. When approved by the Secretary of Commerce, the DSS will become the Federal government's public key digital signature technique for all unclassified data. In addition, NIST has proposed a Secure Hash Standard (SHS) to be used in conjunction with DSS for generating signatures.

User Authentication

Cryptography can be used to increase security in user authentication techniques. Most password techniques store passwords on a host system in encrypted form to protect them from disclosure to unauthorized parties. When authenticating to a remote computer system via a network, passwords typically travel over the network in plaintext form where they are vulnerable to eavesdropping; again, cryptography could be used to protect the passwords from disclosure as they travel over the network. Cryptography can also allow the use of passwords to be reduced by replacement with a "cryptographic handshake," particularly for multiple logins across a network. For example, the host can challenge the user with an encrypted random number. The user can authenticate himself by responding with the correct decrypted number, thereby demonstrating that he shares a common key with the host. Thus, cryptography can play various useful roles either as a tool or as the actual basis for user authentication techniques.

CONSIDERATIONS WHEN IMPLEMENTING CRYPTOGRAPHY

This section explores several of the important issues which should be considered when integrating cryptography into an IT system.

Security of Cryptographic Modules

Cryptography is typically implemented in a "module" comprised of software, firmware, hardware, or some combination thereof. This module contains the cryptographic algorithm and the key(s). In order for the module to properly function, it must be protected from tampering. Protection may also have to be provided to protect the key(s) and possibly the algorithm against disclosure. Additionally, users and computer systems must be able to rely upon the proper functioning of the cryptography. For these reasons, the module requires some

protection. This is usually obtained through the secure design, implementation and use of a cryptographic module.

NIST Proposed FIPS 140-1, Security Requirements for Cryptographic Modules, specifies the physical and logical security requirements for a cryptographic module.

The proposed standard defines four security levels for cryptographic modules, with each level providing a significant increase in security over the preceding level. The four increasing levels of security allow for cost-effective solutions that are appropriate for different degrees of data sensitivity and different applications environments. The user is afforded the flexibility to select the best module for any given type of IT system, thus avoiding the cost of unnecessarily elaborate security features where they are not needed.

Key Management

The proper management of cryptographic keys is essential to the effective use of cryptography for security. Ultimately, the security of information protected by cryptography is directly dependent upon the protection afforded to the keys. Key management involves the procedures, both manual and automated, to be used throughout the entire life cycle of the keys, which includes the generation, distribution, storage, entry and use, and destruction and archiving of the cryptographic keys. Protection must be provided to protect all keys from modification. Some keys must also be kept secret. Unique key management issues must also be addressed by users of both public key and secret key cryptography.

With secret key cryptography, the secret key(s) must be securely distributed to the parties wishing to communicate. Depending upon the number and location of users, this may not be a trivial task. Automated techniques for distributing and generating cryptographic keys can ease the overhead of key management, but some resources will still have to be devoted to this task. FIPS 171, Key Management Using ANSI X9.17, provides key management solutions for a variety of operational environments.

Public key cryptography users also must confront key management issues. For example, since private keys are ties to specific users (or positions or organizations), it is necessary to "bind" a key pair to a specific user. This is done by a "certificate issuing authority," which determines the identity of an individual before "certifying" the public key.

Standards

NIST and other standards organizations have developed numerous standards for the design, implementation, and use of cryptography and for its integration into IT

systems. The use of cryptographic modules that conform to cryptographic standards can provide significant benefits to an organization. Standards provide solutions that have been accepted by a wide community and that have withstood the scrutiny of experts. Standards help ensure interoperability among different vendors' equipment, thus allowing an organization to select from among multiple alternatives in order to find cost-effective equipment. By using voluntary standards, Federal government organizations can reduce costs and protect their investments in technology by buying off-the-shelf products.

Configurations of Cryptographic Modules

Another area that needs to be considered is how the cryptographic module will interact with the IT system. Cryptographic modules can either be configured: off-line or in-line. In an off-line configuration, a cryptographic module accepts information from the IT system, performs the required the cryptographic operations, and then passes the processed information back to the IT system. In an in-line configuration, a cryptographic module accepts information to be processed from one part of the IT system, performs the required cryptographic operations, and then passes the processed information directly to other parts of the IT system.

Networking Issues

The use of a cryptographic module within an IT system that is used in networking applications may require special considerations. In these applications, the suitability of a cryptographic module may depend on its capability to handle any special requirements imposed by locally attached communications equipment or by the network protocols and software.

Another concern arises if encrypted information, MACs, or digital signatures, which may appear as random data, inadvertently contain data that may be misinterpreted by the communications equipment or software as being control information. In this case, it may be necessary to filter the encrypted information, MAC, or digital signature to ensure that it does not contain any control information that might confuse the communications equipment or software. It essential to ensure that the cryptography satisfies any requirements imposed by the communications equipment and does not interfere with the proper and efficient operation of the network.

@###Cost Considerations@[management]

The cost of employing cryptography to protect IT systems can be characterized in terms of both direct and indirect costs, as will be discussed below. Cost is in part determined by product availability; a wide variety of products exists for implementing cryptography in integrated circuit (IC) chips, add-on boards or adaptors, and stand-alone units, and many of these products implement

accepted cryptographic systems (e.g., DES) and conform to other security standards.

@####Direct Costs@[]

The direct costs of employing cryptography include:

_acquiring or implementing the cryptographic module and integrating it into the IT system; the medium (i.e., hardware, software, firmware or combination thereof) and various other issues such as level of security, logical and physical configuration, and special processing requirements will have an impact on cost;

_managing the cryptography, and, in particular, managing the cryptographic keys, which includes key generation, distribution, archiving and disposition as well as the security measures to protect the keys, as appropriate.

@####Indirect Costs@[]

The indirect costs of employing cryptography can include:

_a limited decrease in system or network performance, resulting from the additional overhead of applying cryptographic protection to stored or communicated data;

_changes in the way users interact with the system, resulting

from more stringent security enforcement. It should, however, be noted that cryptography can be made relatively transparent to the users such that the impact is minimal.

@##INTERDEPENDENCIES@[]

There are many interdependencies between cryptography and other security controls highlighted in this Handbook. Cryptography both depends on other aspects of IT security and also assists in providing many other security safeguards.

@###Physical and Environmental Security@[]

The physical protection of a cryptographic module is important for protecting the cryptographic system and keys within from scrutiny and tampering. In many environments, the cryptographic module itself must provide high levels of physical security. In other environments, a cryptographic module may be employed within IT systems residing in a secured facility with adequate physical security for the cryptographic module.

@###Identification and Authentication@[]

Cryptography can be used both to protect passwords that are stored on computer systems, and to protect passwords that are communicated between computers. Furthermore, cryptographic-based authentication techniques may be used in conjunction with password-based techniques to provide stronger authentication of users.

@###Logical Access Control@[]

In many cases, cryptographic software may be embedded within a host system, and it may not be feasible to provide extensive physical protection to the host system. In these cases, logical access control may provide a means to isolate the cryptographic software from other parts of the host system, and hence, protect the cryptographic software and keys from scrutiny and tampering. The use of such controls essentially provides the logical equivalent of physical protection.

@###Audit@[]

Cryptography may play a useful role in performing auditing. For example, audit records may need to be communicated from computers being audited to another computer that collects the audit information. In this case, cryptography may be needed to protect the communicated audit records from disclosure or modification, or to authenticate the source of the audit record. Cryptography may also be needed to protect audit records stored on IT systems from disclosure or modification.

@###Assurances@[]

Assurance that a cryptographic module is properly and securely implemented is essential to the effective use of cryptography to protect IT systems. NIST maintains validation programs for several of its standards for cryptography. Vendors can have their products validated for conformance to the standard through a rigorous series of tests. Such testing provides increased assurance that a module meets stated standards, and system designers, integrators, and users generally have greater confidence that validated products conform to accepted standards.

@##CONCLUSION@[]

Cryptography provides an important means for improving the security of IT systems. It can be used to provide both data confidentiality and integrity. User authentication procedures can also be strengthened through cryptographic techniques. Use of digital signatures, an important cryptographic application, will

speed the use of EDI. Cryptography, however, can not be implemented without costs. Careful study is required to determine the types of systems and applications best suited to an organizations's environment.

@##REFERENCES@[]

- [1] Data Encryption Standard (DES), National Institute of
- Standards and Technology (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 46-1, National Technical Information Service, Springfield, VA, April, 1977.
- [2] New Directions in Cryptography, IEEE Transactions on Information Theory, W. Diffie and M. Hellman, Vol. IT-22, No. 6, November 1976, pp. 644-654.
- [3] Public-Key Cryptography, National Institute of Standards and Technology Special Publication 800-2, James Nechvatal, April 1991.
- [4] A Method For Obtaining Digital Signatures and Public-Key Cryptosystems, R. Rivest, A. Shamir, and L. Adleman, Communications of the ACM, Vol. 21, No. 2, 1978, pp. 120-126.
- [5] Computer Data Authentication, National Institute of Standards and Technology (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 113, National Technical Information Service, Springfield, VA, May 30, 1985.
- [6] CSL Bulletin on Advanced Authentication Technology, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, November 1991.
- [7] A Proposed Federal Information Processing Standard for Digital Signature Standard (DSS), Federal Register Vol. 56, No. 169, August 30, 1991.
- [8] Proposed Federal Information Processing Standard for Secure Hash Standard (SHS), Federal Register Vol. ??, No. ??, January 31, 1992.
- [9] Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (U.S.), Draft Federal Information Processing Standards Publication (FIPS PUB) 140-1.
- [10] American National Standard for Financial Institution Key Management (Wholesale), ANSI X9.17-1985, American Bankers Association, Washington, DC.
- [11] Key Management Using ANSI X9.17, National Institute of Standards and Technology (U.S.), Federal Information Processing Standards Publication (FIPS PUB) 171, National Technical Information Service, Springfield, VA, April 1992.
- [12] Information Processing Systems - Open Systems Interconnection Reference Model - Part 2: Security Architecture, International Organization for Standardization, ISO 7498/2:1988.
- [13] Security Mechanisms in High-Level Network Protocols, V.L. Voydock and S.T. Kent, ACM Computing Surveys Vol. 15, No. 2, June 1983.

@##SIDEBAR NOTES@[]

- _Cryptography can be used to protect data communicated among computers and to to protect data and programs stored within computers. (1.)
- _Cryptography can be used to control access to computers and networks. (1.)
- _There are two basic types of cryptography systems: "secret key" and "public key." (2.)
- _The best known secret key system is the Data Encryption Standard (DES). (2.1)
- _Secret key systems are often used for bulk data encryption and public key systems for automated key distribution. (2.3)
- _Cryptography can provide security services such as data confidentiality, data integrity, data origin authentication, non-repudiation, and access control. (3.)
- _A Message Authentication Code (MAC) can be used to verify the integrity and origin of data. (3.2.2)
- _Cryptography can provide the electronic equivalent of a written signature. (3.2.3)
- _NIST has proposed the Digital Signature Standard. (3.2.3.2)
- _The contents of a cryptographic module should be protected from scrutiny and tampering. (4.1)
- _NIST Draft FIPS 140-1 defines basic security requirements for cryptographic modules. (4.1)
- _Key management involves the secure generation, distribution, storage, entry and use, and destruction and archiving of cryptographic keys. (4.2)
- _Applicable security standards provide a common level of security and interoperability among users. (4.3)
- _NIST maintains validation programs for several of its cryptographic standards. (5.5) junk:

The effective use of cryptography within IT systems requires that an organization first identify which security services are needed, based on its security or protection objectives. Appropriate mechanisms to attain the objectives can then be selected.

@###Services@[]

The most common security services that can be achieved through the use of cryptography include the following:

- _Data confidentiality: ensures that data is not disclosed to unauthorized parties.
- _Data integrity: ensures that data is not modified in an unauthorized manner.
- _Non-repudiation of origin: provides evidence that the source of received data is as claimed, whereby that evidence can be verified by a third party. Or, in other words, that the originator of the data cannot falsely deny having originated the data.
- _Access control: provides protection against unauthorized use of IT resources.