Global Information Assurance Certification Paper

Cryptographic Services – A Brief Overview

Larry D Bennett

October 10, 2001

Version 1.2e

Abstract

This paper examines the use of cryptography in implementing the services of authentication, integrity, non-repudiation, and confidentiality. The various methods of cryptography are reviewed. Finally some of the pros and cons for the use of cryptography are discussed.

Cryptography

According to Bark94, cryptography is the science of mapping readable text, called plaintext, into an unreadable format, called ciphertext, and vice versa. The mapping process is done through the use of algorithms, i.e. a solution to a problem, and ciphers, i.e. keys via some mathematical computations. The appearance of the data is changed only, not it's meaning.

Therefore, cryptography is the use of various mathematical functions to render a plaintext, i.e. readable, unencrypted, intelligible document into an unreadable, encrypted, and unintelligible ciphertext document.

According to Bark94, cryptography is used to provide the following services: authenticity, integrity, non-repudiation, and secrecy.

Cryptography contains two bodies of implement, they are, conventional encryption, also known as symmetrical encryption and public key encryption also known as asymmetrical encryption.

Conventional encryption

Conventional encryption can be further divided into the categories of classical techniques, and modern techniques and algorithms. The hallmark of conventional encryption is that the cipher or key to the algorithm is shared, i.e. known by the parties involved in the secure communication. This arrangement however makes null and void the issue of non-repudiation. According to Tabo98, non-repudiation is an attribute of a communication which protects against a party to [it] denying that it occurred. By sharing the key, either party could create a message and claim that the other party created it. For example, Tom advocates that Jim authorized the purchase of stock via an email doc, however the email system used only allows for conventional encryption, therefore both individuals share the key. Tom forges a message and implicates Jim. However, Bark94 points out that if kept secret, both the secrecy and authentication services are provided. Secrecy is provided, because if the message is intercepted, the intruder cannot transform the ciphertext into its plaintext format. Assuming that only two users know the key, authentication is provided because only a user with the key can generate ciphertext that a recipient can transform into meaningful plaintext. The integrity of the message may also have been comprised if the key

is known to unauthorized others. Therefore, a method of assuring the recipient that the message was not modified en route is needed. In conventional encryption the use of a cryptographic checksum of the message and key is computed. This checksum is called a Message Authentication Code (MAC). According to Stal99; a MAC function is similar to encryption, however a MAC need not be reversible as is the case for decryption, i.e. the computed value is not readily recoverable to a readable format.

Bark94 explains it this way; the MAC is computed by the message originator as a function of the message being transmitted and the secret key. Upon receipt, the MAC is computed in a similar fashion by the message recipient. If the MAC computed by the recipient matches the MAC appended to the message, the recipient is assured that the message was not modified. A MAC therefore is a hashed, i.e. encrypted, representation of a message, and has the following characteristics: A MAC is much smaller (typically) than the message generating it. A MAC is also called a fingerprint of the message. Given a MAC, it is impractical to compute the message that generated it. Given a MAC and the message that generated it, it is impractical to find another message generating the same MAC.

Therefore, according to Stal99, the receiver is assured of the message's integrity because if the attacker alters the message but does not alter the MAC, then the receiver's calculation of the MAC will differ from the received MAC. It is assumed that the attacker does not know the secret key and therefore cannot alter the MAC to correspond to the altered message.

Be aware that the MAC only provides for authentication and integrity only if the key remains secret between two parties. The MAC does not provide for message confidentiality. The plaintext document must still be encrypted to ciphertext. The MAC can be encrypted along with the message. The MAC and conventional encryption in this implementation does not provide for non-repudiation.

A Conventional Encryption Model

A conventional encryption model can be illustrated by assigning Xp to represent the plaintext message to be transmitted by the originator. Xp can also contain the MAC. The parties involved select an encryption algorithm represented by E. The parties agree upon the secret key represented by K. The secret key is distributed in a secure manner represented by SC. Conventional encryption's effectiveness rests on keeping the key secret. Keeping the key secret rest in a large part on key distribution methods. When E processes Xp and K, Xc is derived. Xc represents the ciphertext output, which will be decrypted by the recipient. Upon receipt of Xc, the recipient uses a decryption algorithm represented by D to process Xc and K back into Xp. In conventional encryption, secrecy of the encryption or decryption algorithm is not need. In fact, the use of an established, well-known and tested algorithm is desirable over an obscure implementation. This brings us to the subject of key distribution.

Key Distribution – Conventional Cryptography

According to Stal99, the strength of any cryptographic system rest with the key distribution technique. Conceivably for two parties, A could select a key and hand delivers it to B, or A and B

could rely on a trusted courier. If A and B have an established secure connection, they could exchange a new key via encrypted messaging, or if both A and B have an established secure connection with a trusted third party C, C could provide this trusted courier service. The first two options can present a logistical nightmare as the number of communicating pairs increase; the number of discrete keys needed also increase exponentially. Option three weaknesses are reveal in that if an attacker ever succeeds in compromising one key all of the keys are compromised, i.e. the attacker can masquerade as a trusted party. The fourth option demonstrates a key distribution center (KDC), which have been largely adopted. A KDC is responsible for securely delivering unique key pair to its clients. It is also responsible key management. A key distribution center uses a hierarchy of keys to provide authentication, integrity, non-repudiation, and confidentiality to its users. This hierarchy of keys consists of session keys, which are used for logical connections between end users. The session keys are encrypted by a master key, which is shared by the KDC and an end user. Stal99 presents the following key distribution scenario: A uses its secret key to request a session key from the KDC to establish a logical connection to B. The request includes the identity of both A and B and a unique identifier, i.e. a nonce, for the transaction. A nonce is a contrivance invented or used for this particular, singular occasion. The KDC replies to A with an encrypted message which contains the requested one-time session key and the original requesting message with the nonce. The original message is used to verify the reply's integrity. The nonce is used by the requestor to verify that the returned message is not a replay of an older request. The reply also contain two item relating to B. They are the one time session key, to be used for the session and an identifier for A. Both of these items are encrypted with the master key that is shared by the KDC and B. These item are used to authenticate A to B. Party A forwards to B the information that originated at the KDC which was encrypted with B's master key. This gives the process its integrity. For B to be authenticated to A the following steps should also occur: Party B now uses the logical connection created by the shared session key to send a self defined nonce to party A. Upon receipt of the B defined nonce, A perform a mathematical function on the nonce and returns the results to B through the logical connection. The keys have to be managed across KDC domains. Keys issued to an entity by one KDC have to be validated by the issuer before they can be accepted by an entity serviced by a difference issuer. The issuers have to collaborate on an acceptable method of authenticating inter-domain transactions. Currently, KDCs use a hierarchy for key sharing. Each local KDC negotiates keys for its subscribers through a global KDC. Session key generated must have a finite lifetime. Keys are exchanged frequently to prevent an opponent from having a large amount of data encoded with the same key. If the key is secured then how else can the system be comprised? This brings us to the subject of cryptanalysis.

Cryptanalysis

According to Demm99, code making involves the creation of encryption products that provide protection of confidentiality. Code breaking involves defeating this protection by some means other than the normal decryption process used by the intended recipient. Demm99 also explores five scenarios for which code breaking, i.e. cryptanalysis is used. They are to ensure accessibility, spying on opponents, selling cracking products and services, pursing the intellectual aspects of code breaking, and testing whether one's own codes are strong.
According to Stal99, cryptanalysis is the process of attempting to discover either the plaintext

message i.e. Xp or the cipher key i.e. K. Discover of the encryption key is most desired as with its discover all subsequent message can be deciphered. Therefore the length of the encryption key, and the volume of the computational work necessary, provides for its strength i.e. its resistance to breakage. The longer the key, the stronger the protection, the more brute-force is needed. Neither conventional encryption nor public key encryption is more resistant to cryptanalysis than the other. As noted by Stal99, all that the user of an encryption algorithm can strive for is an algorithm that meets one or both of the following criteria: the cost of breaking the cipher exceeds the value of the encrypted information, the time required to break the cipher exceeds the useful lifetime of the information.

Some Implementations - Conventional

Conventional encryption includes both classical and modern techniques. Conventional encryption is built on two basic methodologies, substitution and transposition. Substitution involves replacing a given letter or element in the communiqué with some other element. Caesar Cipher uses this method. Transposition involves changing the position of the letter or element. The rotor machine cipher uses this method. Data Encryption Standard (DES) adopted by the National Institute of Standards and Technology (NIST) in 1977 is an example of a modern encryption technique. All of these and other conventional techniques are breakable, however a variation on the Vernam cipher called a one-time pad is unbreakable. This method uses a non-repetitive, random key, which is the same length as the message.

Public Key Encryption

Public key encryption also known as asymmetrical encryption involves the use of two separate keys per individual. An individual has bound to their identity both a private, secret key known only self and a public, published key known to the masses. Public key cryptography differs from conventional cryptography by this binding of keys, public and private, to an individual rather than negotiating a secret key between parties. This non-sharing of private key enhances the non-repudiation services provided, over conventional cryptography. Public key cryptography also differs from conventional cryptography in that its algorithms rely on mathematical functions rather than on substitutions and transpositions. According to Bark94, each key generates a function used to transform text. The private key generates a private transformation function, and the public key generates a public transformation function. The functions are inversely related, i.e., if one function is used to encrypt a message, the other is used to decrypt the message. The originator encrypts the message using the recipient's public key. Only the recipient's private key can be used to decrypt the message. This is due to the computational infeasibility of inverting the public key transformation function. In other words, without the recipient's private key, it is computationally infeasible for an interceptor to transform the ciphertext into its original plaintext. Public key encryption has the following disadvantages: it is inefficient compared to conventional encryption due to the mathematical computations used to encrypt data more time is required, and depending on the algorithm, the ciphertext produced may be much larger than the plaintext which increases traffic volume. Public-key cryptography is therefore impractical for use in encrypting large messages. Also a public-key system can only send an encrypted message to a

single recipient. Since a recipient's public key must be used to encrypt the message, sending to a list of recipient's is not possible using public-key cryptography. Public-key cryptography, by itself, is inefficient for providing message confidentiality to large messages, it is however well suited for providing authentication, integrity, and non-repudiation services. Through the use of digital signatures these services are realized.

Digital signatures

According to Bark94, a digital signature is a cryptographic checksum computed as a function of a message and a user's private key (see Related Links #2). While similar to a MAC a digital signature offers authentication, integrity, and non-repudiation services in that it is produced via the user's private key i.e. the key known only to the key holder therefore it is not a shared key. A digital signature is different from a hand-written signature, in that hand-written signatures are constant i.e. your signature always express your name, your personage, regardless of the document being signed. A user's digital signature varies with the data, as it is a computation of the message and the user's private key. For example, if a user signs five different messages, five different signatures are generated. Each signature, however, can be authenticated for the signing user. A user often signs a hashed version of the message, called a message digest (MD), rather than the message itself. For communications to be established users have to agree upon a hashing function for transforming the message to test its authenticity and integrity and a signature algorithm for the signature verification process. Prior to 2 October 2000, there were three Federal Information Processing Standards (FIPS) approved algorithms for generating and verifying digital signatures: Digital Signature Algorithm (DSA), Rivest, Shamir, and Adleman Algorithm (RSA), and the Elliptic Curve Digital Signature Algorithm (ECDSA). These three algorithms were used in conjunction with the Secure Hash Algorithm (SHA-1), a hashing function that produced a160 bit message digest (see Related Links #3).

To send a signed message the originator needs to: generate a message digest of the message using the shared hashing function. The originator then generates a digital signature as a function of the message or message digest and the originator's private key. The message and the signature are then sent to the recipient. The recipient performs the following procedures: generate a message digest of the received message using the shared hashing function. The digest, the originator's public key, and the received signature are inputted into a signature verification algorithm. The message is inputted into a decryption algorithm, if it was sent encrypted. This brings up the use of a hybrid symmetrical - asymmetrical encryption system. This system uses asymmetrical encryption to provide authentication, integrity, and non-repudiation services while symmetrical encryption is used to provide message confidentiality. Therefore through the use of digital signatures, the recipient is assured that the message was not modified for if even one bit of the original message was changed, the digest generated using the received message would cause the signature verification process to fail. The recipient is assured that the message was not forged because of the inverse relationship of encoding and decoding the keys. Public key transformation functions are 1-way hashes i.e., not forgeable; therefore, only a signature generated by the originator's private key can be validated using the originator's public key. To provide authentication and non-repudiation with proof of origin using a digital signature, a message originator signs a message (or digest) using the private key bound to the originator. Since only the originator can access the private key, the signature is unforgeable evidence that the originator

generated the message. In contrast, non-repudiation with proof of origin cannot inherently be provided in a conventional cryptosystem. Since both parties involved in a communication share a secret key, both parties can deny sending a message, claiming that the other party is the message originator as discussed above. In addition to providing integrity and authenticity, digital signatures, according to Tabo98, can also provide for non-repudiation with regards to proof of origin, proof of deliver and proof of submission. According to Tabo98, these services can be obtained by using a Trust Third Party (TTP). A TTP is tasked with providing mechanisms for gathering evidence in regard to transactions conducted by the parties involved. The TTP must provide unbiased, credible methods of non-repudiation for either party. The TTP, therefore, serves as a witnessing agency. Non-repudiation, however as set forth by Mccu00, should not negate a parties right to repudiate a claim of signatory.

A Public Key Encryption Model

A public key encryption model can be illustrated by assigning a published, public key, i.e. Kpu and a private key, i.e. Kpr to each entity. Party A uses B's public key Kpu to encrypt a plaintext message, i.e. Xp with an encryption algorithm, i.e. E, which produces Xc, i.e. the encrypted message. When B receives the encrypted message, Xc, it is decrypted by a decryption algorithm, i.e. D which takes Xc and B's private key, Kpr to produce Xp, the plaintext message.

Some Implementations – Public Key

Public key cryptography has been implemented through the RSA algorithm, the Advanced Encryption Standard i.e. the Rijndael algorithm, and Elliptic Curve cryptography.

Cryptographic Uses

In General

Information systems by their nature are prone to specific threats and attacks on their ability to deliver the information contain within. Threats are specific vulnerabilities that can be exploited against an information system infrastructures i.e. its operating system, its file system, its communications system, etc. Attacks are specific methods of exploitation against these vulnerabilities. These attack falls into four general categories: interruption, interception, modification and fabrication, according to Stal99. Interruption of the normal flow of information can be considered an availability attack. Interruption can occur because of power failure, down communication lines, or a denial of service attack for instance. Interception of the information is akin to eavesdropping. Interception can be considered an attack on the information's confidentiality. Modification is akin to tampering with the information. Modification can be considered an attack on the information's integrity. Fabrication is the ability to place false information in the system. Fabrication is an attack on the authenticity of the information in the system. These attack are not to be considered discrete functions against specific services but are commingled against the various services. For example, if fabrication is successful against an information system both the authenticity and integrity of the information is suspect. These attack fall into two categories: active and passive.

Cryptography is used to protect informational resources, i.e. data or messages, in information systems from both active and passive attacks. Active attacks involve unauthorized modifications to the data. According to Stal99, active attacks are divided into four categories: masquerade, replay, modification of messages, and denial of service. A masquerade attack gives an impostor access to secure resources by deception. The man in the middle attack is a masquerade attack. The replay attack involves capturing data packets and retransmitting them. The data may or may not have been modified. The modification of messages attack means the attacker has in deed modified the data by altering, delaying or reordering. The denial of service attack is launch against a specific target in an attempt to prevent or hinder communications to and from the target. Passive attacks involve unauthorized disclosure of information or unauthorized monitoring of resources. Both types of attack, active and passive, brings on a lowering of confident in the information systems used. **C**ryptography can be used to secure the authenticity, integrity, non-repudiation, and confidentiality of the information whether it is in transit on an LAN or WAN or residing on its storage media. **C**ryptography does little in preventing availability attacks.

Insiders

By far, employees and others who have trusted access to an organizations informational resources can be regarded as a greater threat to the authenticity, integrity, and confidentiality of an information system than outsiders such as hackers. Alex95 presents these insiders as disgruntled employees, who are unhappy with their employer for whatever reason, dishonest employees, who are looking to exploit the organization's resources for personal gain, and snoopy employees, whose eavesdropping on fellow employees, lowers morale and productivity. According to Demm99, insiders can expose an organization's information infrastructures to intentional and unintentional exploitations. These exploitations can be achieved through the use of the following categories: traitors and moles, business relationships, visits and requests, fraud and embezzlement, acts of sabotage, and penetration from the outside. Traitors and moles can be present, past, future, and temporary employees. Many businesses can compromise their relationships by not have the same standards of security implemented. A more lax business partner may expose your confidential information. Visits and requests are social engineering tactics used to cajole information through intimidation. Fraud and embezzlement have been achieved through bogus transactions and data diddling. Insiders who have access to financial systems can make fraudulent transfers from one account to another. The can also use the data diddling, salami attack to trim off revenue from transactions. Sabotage of information systems can render them unavailable for use or make the information contained within suspect. The physical security of your facilities should be reviewed for potential penetration from the outside. Individual's motivations to compromise an organization are as varied as the individuals.

With motives aside, through the use of cryptography and proper access control policies for information, the threats of unauthorized disclosure can be mitigated. Access to information should be based on an individual's need to know. The information should be encrypted base on its value to the organization's success.

Defense in Depth

According to Paul01, defense in depth is a layered approach to providing protection for information resources. Defense in depth raises security by increasing the cost of attacking a system, i.e. it presents more barriers to overcome which calls for a greater outlay of an opponent's resources. Defense in depth can be implemented through the use of the following technologies: Firewalls (FW), Demilitarization Zones (DMZ), and Intrusion Detection Systems (IDS) these implementations can be further enhanced by the incorporation of Cryptographic Systems. Firewalls are routers used to establish a boundary between networks. The boundary prevents unauthorized access of private networks by egress and ingress filtering of the passage of Internet Protocol packets between networks. Encrypted packets are treated the same as unencrypted packets because the IP address header is not encrypted. IP Security is implementation in the fashion. Demilitarization Zones are network segments isolated by firewalls to provide services to untrusted connections. These untrusted connections can be from external sources such as web browsers to web servers or intradepartmental communications that you may wish to segregate. As with firewalls encryption of information on internal network segments can be beneficial, as it can deter eavesdropping. Intrusion Detection Systems are used to monitor either unauthorized access to a network segment or an individual host. These systems use logs to audit and generates reports on various activity found in the environment. Cryptography can be used to secure the authenticity, integrity, non-repudiation, and confidentiality of the information contained in these logs and reports.
The use of cryptography does impact performance in a negative way by increasing processing time, and packet volume through the various devices. These delays may be critical to specific applications.

Legal and Legislative Issues

Both good guys and bad guys use cryptography. Demm99 expounds on the issues of law enforcement's need for better cryptanalysis. The right to privacy is of course at the heart of these issues. One of the issues involves implementing mandatory key recovery. Mandatory key recovery would enable law enforcement agencies to have access to plaintext data by retrieving keys that have been escrowed with a key repository. However, as Demm99 notes, mandatory key recovery has several drawbacks. Cost, difficulties in developing the necessary infrastructure, and infringing on constitutional freedoms and rights are all cited, as well the ability of an individual to obtain encryption products abroad. Cryptanalysis will be further challenged by the proposed adoption of the Advanced Encryption Standard (AES). According to Pecs00 of the Gartner Group the NIST reports it could take over an estimated 149 trillion years of computerized code-cracking work to decipher a Rijndael based encryption key. Rijndael is the new encryption algorithm developed by, Joan Daemen, and Vincent Rijmen, two Belgian cryptologists. It was chosen to replace the Data Encryption Standard (DES), which uses a 56-bit key. Adopted in 1977, DES's 56 bit key has became susceptible to brute-force attacks by code-cracking computers, as illustrated by Fitz98, with the processing power of a Pentium CPU. Advanced Encryption Standard (AES) however, offers three key sizes: 128, 192 and 256 bits. On 6 September 2000, RSA Security Inc. released the RSA public key encryption algorithm into the public domain, foregoing patent renewal efforts therefore opening development opportunity

based on the algorithm (see Related Link #4).

The issues of non-repudiation and repudiation are again address by the American Bar Association in their publication "Digital Signature Guidelines" found at http://www.abanet.org/scitech/ec/isc/dsgfree.html.

Another issue is that of export controls placed by the U.S. government on commercial encryption products. Export controls on commercial encryption products was transferred from the State Department to the Commerce Department in 1996 (FedR96). The Bureau of Export Administration (BXA) is tasked with administrating Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774. Sections 740.13, 740.17 and 742.15 set forth the governing rules for the export of encryption products (see Related Links #1). Up until that time most encryption products were considered munitions products. Under the Clinton administration (FedR00), export controls were relaxed to assist US firms in establishing a global market share. The October ruling permits most encryption products to be exported to the 15 nations of the European Union and 8 other trading partners, including Australia, Japan, New Zealand, Norway, Switzerland, Czech Republic, Poland, and Hungary. You must apply for a license to export encryption items to the following-noted terrorist-supporting countries as well as other embargoed destinations, e.g., Serbia and the Taliban controlled areas of Afghanistan, Cuba, Iran, Iraq, Libya, North Korea, Sudan or Syria.
The European Union had relaxed its posture on encryption export. The October ruling makes our policy comparable to the EU's. The BXA 's FAQ page at http://www.bxa.gov/Encryption/Oct2KqandAs.html addresses and answers more of these issues e.g., does posting encryption source or object code on the Internet constitute an export under the EAR?

In Conclusion

Cryptography is not information security's silver bullet. It can provide, in varying degrees, the services needed by information security through various implementations. Cryptography should be approached with specific goals outlined, to enhance a defense in depth posture. In either form of cryptography keeping the key confidential is of the utmost importance.

References Cited:

Alex95 Alexander, Micheal. The Real Security Threat: The Enemy Within. Datamation, volume 41, number 13, 15 July 1995.

Bark94 Ed. Barkley, John. NIST Special Publication 800-7. July 1994. URL: http://csrc.ncsl.nist.gov/publications/nistpubs/800-7/main.html

Demm99 Demming, Dorothy E. Information Warfare and Security. Addison-Wesley, 1999.

FedR96 Federal Register, volume 61, number 251, 30 December 1996. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1996_register&docid=fr30de96-10.pdf

FedR00 Federal Register, volume 65, number 203, 19 October 2000. URL: http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2000_register&docid=fr19oc00-5.pdf

Fitz98 Fitzgerald, Michael. EFF quickly cracks Data Encryption Standard. Ziff-Davis Net News, 17 July 1998. URL: http://www.zdnet.com/eweek/news/0713/17acrypt.html

Mccu00 McCullagh, Adrian and Caelli, William
Non-Repudiation in the Digital Environment. First Monday, volume 5, number 8 (August 2000), URL: http://firstmonday.org/issues/issue5_8/mccullagh/index.html

Paul01 Paul, Brooke. Building an In-Depth Defense. Network Computing, volume 12, number 14, 9 July 2001.

Pesc00 Pescatore, John. Code Call: New IT Encryption Standard Selected. Gartner Group, 5 October 2000. URL: http://www3.gartner.com/UnrecognizedUserHomePage.jsp
Search on "encryption".

Stal99 Stallings, William. Cryptography and Network Security Principals and Practice, 2nd edition. Prentice-Hall, 1999.

Tabo98 Tabor, Sharon W. Non-Repudiation and Certification Practices. 15 October 1998. URL: http://telecomm.boisestate.edu/ecommerce/Fall98/ec14/sld001.htm

Related Links

http://www.bxa.doc.gov/encryption/

http://csrc.nist.gov/publications/fips/fips186-2/fips186-2.pdf

http://csrc.nist.gov/encryption/tkhash.html

http://www.encryption.com/news/pr/000906-1.html