

Encryption: Practices, Techniques and Guidelines

**A Student Term Paper for Dr. Detmar W. Straub's Information
Security Course**

Winter, 1996

Overview

Cryptography is the discipline of secret communications or messages. This includes authentication of the identity of the sender, as well as disguising the message itself to ensure its secrecy. Maintaining a message's secrecy is often accomplished by some form of encryption. Encryption involves the alteration of information so as to make it unreadable and therefore unusable to the person who improperly receives it. It is the transformation of 'plaintext' into 'ciphertext' through *transposition* or *substitution*. With transposition, the contents of a block of information is rearranged according to an algorithm. Substitution approaches transform a message into one of an enormous number of possible representations through the use of mathematical or logical functions. A reversal of these processes is performed to decrypt the message. A unique key is required to encrypt/decrypt messages, making decryption by an illegitimate interceptor a formidable task. The length of the key is the primary determinant of the strength of the encryption technique. A sophisticated algorithm strengthens the effectiveness of the encryption technique, but an assumption is made that all algorithms can be identified with varying degrees of effort. Cryptanalysis involves the strength analysis of the encryption/decryption technique and/or its implementation process, as well as the penetration or breaking of this system.

Cryptography's history can be traced from ancient Egypt to India, Mesopotamia, Babylon, Greece, Western Civilization and finally into the current computer age (Forcht, p112). Examples of the use of ciphers or encryption are in Egypt, around 2000 B.C., in the form of hieroglyphics and to writings in the Bible. Julius Caesar reportedly used a substitution encryption technique to send couriered messages. Benedict Arnold used a code book to send and receive messages from the British during the Revolutionary War. The Allied Force's interception and decrypting of Germany's encrypted messages resulted in invaluable intelligence information. Prior to the computer age, the primary use of encryption fell in the military, diplomatic and political arenas, but now the applications are numerous.

The capabilities of encryption technology have enabled corporations to secure their data, information, and programs in a more reliable means than ever before. With the advances in encryption technology and its application to today's business comes an increased need for IS managers to increase their awareness of the strengths, weaknesses and uses of various encryption methods. From securing data transmission to attaching

electronic/digital signatures to documents, IS managers need to be aware of the capabilities of the myriad of encryption methods available.

This paper examines some of the more common encryption techniques/methods, such as RSA, DES (Data Encryption Standard), Kerberos, and PGP (Pretty Good Privacy). While examining these methods, the weaknesses, strengths and primary uses of each will be addressed. This paper will provide IS managers with a means of assessing the current methods and determining which to use and for what purpose.

Encryption Techniques

There are two facets of encryption that should be considered - one involves the algorithm used to transform the original plaintext message into ciphertext and the other involves the management of encryption keys. In addition, there is a relationship between the key(s) and the particular algorithm used. In general, in order to encrypt a message, the message is broken into equal size **blocks** and a mathematical algorithm that involves both the key and the ciphertext is applied. At the other end, the algorithm is reversed, using either the same key or a related one, to recover the plaintext of the message originally sent.

Cipher Approaches

As described above, most algorithms break the message up into blocks that are then fed into the algorithm along with a key. The simplest approach to this is called Electronic Code Book (ECB) - suggesting that if an attacker obtains the plaintext along with the corresponding ciphertext, he will most likely be able to analyze the relationships between the two and create a code book for deciphering future messages. Caesar's simple algorithm of transformation had this "tragic" flaw. A more secure method of implementing encryption makes use of a feedback mechanism whereby the latter ciphertext is influenced by the earlier context of the message. This alternative approach, including Cipher Block Chaining (CBC) and other feedback modes, uses the Exclusive-Or (XOR) operation to link the current block with previous blocks, thus thwarting the hacker's attack.

Single-Key vs. Public-Key

In the past, encryption has used what is known as a **single-key** or **secret-key** method. In a single-key system, when two parties exchange communications, the sender encrypts the information with a key that they both share. At the other end, the receiver uses the *same* key to decrypt the message into its original, readable form. Some very serious problems are inherent in this kind of system -- mainly, in order to hold secure communications with a number of people you would require a separate key to share with each person. When applied to a whole network of people, this quickly adds up to a nightmare of a problem. In addition, if the secret key becomes compromised, which it might if it is shared between multiple parties, all communications become insecure.

Therefore, in order to address this issue of key management, the **public-key** or two-key system was devised. As is implied by the name, this technique uses two related keys in the encryption process. Basically, the process in a public key system follows the following path:

- 1) The receiver has two keys, a *private key*, that she keeps to herself, and a *public key* that she advertises to the “world.”
- 2) When anyone wants to send an encrypted message to her, he looks up her *public key* (that is in the public domain) and uses that key, with a related encryption algorithm, to encode the message.
- 3) Now when the receiver gets the message, she uses her *private-key* to decode it into plaintext.

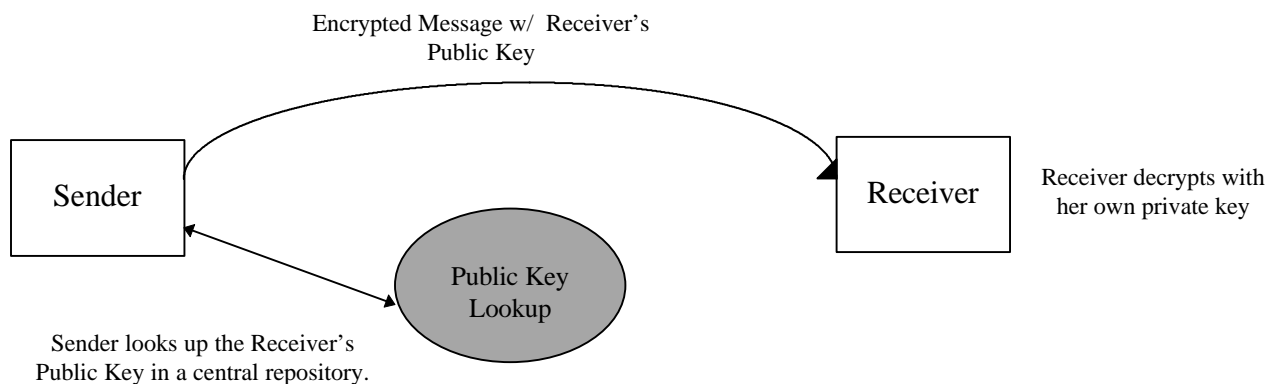


Figure 1

The secrecy of the message relies on the fact that once a message is encoded with one of the keys in the pair (the public key in this example), then **only** the **other** key in the pair (the private key, here) can unlock the message. A potential weakness of public-key systems is the very relationship between the keys. One might argue that since they are related, it is possible to obtain the private key from the widely available public key. Some algorithms, like the knapsack problem, have not stood the test of time.

Understanding this relationship between the two keys also brings out the point that a Public Key System can be used in the reverse manner as well. A sender can use their **own** private key to encrypt a message -- therefore, the key that unlocks the message is the **sender's** public key, which is known to everyone. This may not seem secure, and indeed it is not meant to be. The application of this second scenario is specifically for digital signatures. With digital signatures, the message that is sent should be readable by anyone, but the success of decryption with the sender's public key indicates that the sender, and only the sender, could have originated the message. This added feature of public key systems has great promise for electronic commerce.

Single-Key Implementations

Despite the problems with single-key systems, they have a great advantage over Public-Key -- single-key algorithms are significantly faster than their Public-Key counterparts. The most widely used single-key cipher **DES (Data Encryption Standard)**, was developed at IBM and has been the encryption method of choice for the US government since 1977. DES makes use of a 56 bit key. This key is shorter than those used by most alternative secret-key systems, which makes DES more vulnerable to brute-force attacks. However, over the years DES has remained secure despite the intense scrutiny of the scientific community. In fact, it is this very fact that has made DES attractive as a security mechanism.

A particular security package implementation that makes use of DES encryption for authentication purposes is **Kerberos**. Kerberos (whose name comes from the Latin Cerberus -- the three-headed dog that guarded the entrance to the underworld) originated at MIT in the 1980s as part of their Athena Project (Jaspan). Kerberos is a very narrow product and is only meant to authenticate communications over a network between a client and a server by making use of encryption rather than conventional

passwords (which have proven to be suspect to numerous types of attacks, especially tapping the network.) A central key server, sometimes known as the Kerberos Server, holds the secret keys and supplies session keys for secure communications. The strength of Kerberos is directly related to the secrecy of the Kerberos key server; therefore, any successful attack against the server renders the whole system useless (RSA Laboratories).

In competition with DES are the single-key algorithms invented by Ron Rivest of RSA fame (see Public-Key implementations for RSA.) These include RSA's **RC2**, **RC4** and the newest, **RC5**, ciphers. The distinguishing feature of RC2 and RC4 is their use of variable size keys - making it possible to vary the level of security according to one's needs. In addition, the ability to use shorter keys makes RC2 and RC4 ciphers ideal for export (There are limitations on exportation of encryption that relates to the key sizes. DES cannot be exported outside the US.) The newest advancement in this area from RSA is the RC5 algorithm that adds the ability to use "data-dependent rotations" (Rivest) in addition to the variable size key resulting in a greater level of security.

The latest single-key encryption method to reach the press is the infamous Clipper-Chip. The Clipper-Chip is but one part of a larger security standard that has been devised by the US Government to address their concerns about the possibility of encryption preventing valid investigation of illegal activities. The Clipper Chip (a hardware solution) combined a single-key encryption algorithm, called **Skipjack** (developed by the NSA), with a *key-escrow scheme*. Since Skipjack has not been available for public review, it is hard to know whether it is truly safe from all kinds of cryptanalytic attacks.

The idea of a key-escrow scheme controlled by the government sent visions of "Big Brother" through the minds of the public, creating quite a stir in the press, and forcing the administration to retreat and rethink the whole standard. Despite the controversy, it is likely that we may see some form of key-escrow in the future. In addition to the government's interest, key escrow can protect the owner of information from key loss. At present, without some way to recover the key, data would be, in essence, gone. If a central authority, or combination of agents, held the key in trust, this scenario could be avoided.

Public-Key Implementations

The public-key idea was first introduced in 1976 by Diffie and Hellman in a paper on exponential key exchange. At that time, the authors gave no specifics about how to implement this new kind of encryption. Shortly thereafter, Ron Rivest, Adi Shamir and Leonard Adleman at MIT invented the RSA public key cryptosystem. The RSA algorithm as well as the public-key algorithms are patented, limiting the competition in this area. A mathematical sieve takes information about the private key to derive the public key. However, in order to reverse the formula, arriving at the private key from the public key, requires factoring a very large number - which mathematically is a very difficult task. Hence, the private key remains virtually secure and there is no need to share a secret key.

Best of Both Worlds

Because the public key system's major drawback is its slower speed, a combination of a public key method to exchange privately shared session keys is a strong marriage of the two techniques. In essence it gives the user the best of both worlds -- a session key is encrypted using the public key method as described above, and then the secret key is used in conjunction with either DES or some other secret key algorithm to encrypt the communications at a faster speed. At present, Kerberos is working to add public key features to its traditionally secret key authentication system (Neuman and Ts'o).

Hash Functions

Thus far the discussion has centered around encryption techniques. Hash functions serve as a companion to encryption in the authentication and digital signature area. A hash function takes a message and creates what is called a **message digest**. The purpose of a hash function is to create a short, fixed length, but unique value out of the message to be sent. The message digest is encrypted and sent along with the original message. At the other end the receiver verifies the authenticity of the message by re-calculating the hash value from the message received and comparing it to the unencrypted message digest. If they do not match, the original message has been altered.

PGP (Pretty Good Privacy), is a security program that combines the secrecy of encryption with the authentication of a hash function value. PGP has had its share of controversy because first it is based upon RSA's public-key encryption, and second it was placed on the Internet and therefore effectively exported. Thus far, the program has survived and is a well known product in the protection of e-mails.

Vulnerabilities and Threats

Many of the weaknesses and vulnerabilities of the various techniques have been mentioned. For the most part, threats to the various systems come from either brute-force attacks -- trying all of the keys, or a strategically selected subset; analysis of ciphertext for patterns (cryptanalysis); eavesdropping; man-in-the middle attacks or spoofing; and replaying intercepted ciphertext.

The defense against a brute force attack and other forms of cryptanalysis in a secret key system includes changing the keys frequently. In some cases the use of a time-stamp as part of the key is used to prevent replay attacks. In a public-key system, the private key is more secure, since it does not have to be shared with anyone. The main area of vulnerability is the potentiality of solving the reverse mathematical problem to discover the private key, given the public key. Before any encryption scheme should be trusted, it needs to stand the test of time and scrutiny.

Uses of Encryption or Who Needs it Anyway?

To answer the question, "Who needs encryption?", one can examine the various reasons why banks, businesses, professionals, military, everyday people, and even criminals require some sort of protection. Encryption can play a critical role in contributing to communications and data security. As discussed above, there is an array of encryption methods, techniques, algorithms, and products available. Why are these products so important? Any transaction, transmission of data, storage of data, voice conversation, or computer system (particularly networks) are vulnerable to attack.

From the FBI's high-profile arrest of hacker Kevin Mitnick to Citibank's admission that \$400,000 had been cyber-swiped from its electronic vaults, many individuals and businesses are starting to recognize the need for communications and data security. There are instances of cyber-thieves and wiretapping in almost every business publication today.

Should persons be concerned about surveillance by governmental or non-governmental actors? Yes. For instance, political campaigns are notorious for dirty tricks, including the bugging of opponents; the yellow pages in any major city contain numerous advertisements for detective agencies and investigators; and eavesdropping and bugging devices are readily available in stores. A. Michael Froomkin discusses a vast history of governmental and non-governmental intrusion into personal and business communications in his article (Froomkin). In light of this history of public and private intrusion into personal privacy, and the growing interconnection of computers and communications envisioned by the National Information Infrastructure, it is even more evident that there is truly a need for personal communications and records security.

Banks, ATM-Users, Electronic Transactions

Citibank recently admitted to a security breach in their system. Even though banks are required by law to report any loss of funds or security breaches, there is doubt that many of them have. Banks, ATM's, and Electronic Transfers primarily use the Public Switched Telephone Network (PSTN), leased lines, and internal LANs and WANs to conduct business. This makes them susceptible to wiretapping, eavesdropping and a variety of other techniques to listen or take information off wire media.

Currently, banking institutions rely heavily on encryption, both in the United States and abroad. Fedwire and the Clearing House Interbank Payment System process a daily total of more than 350,000 messages with an estimated value of between \$1 and \$2 trillion. These transactions rely on US government-approved encryption to protect against unauthorized modification and forgery. The US Department of the Treasury requires encryption of all US electronic funds transfer messages (Froomkin).

More and more, the economy continues to move away from cash transactions and towards “digital cash”. The Internet is playing a key role in this move. With this change come new problems. Forgery is a perennial problem with electronic mail: copying is easy, there are no tangible permanent media involved in the communication, and programmers or system managers can alter e-mail headers to fake the source of a message. Cryptography can provide an authenticating function for these electronic transactions. This requires both merchants and consumers to look for ways to encrypt and authenticate transactions by way of digital signatures in order to prevent forgery and insure transactions are completed with confidence. As previously discussed, public key encryption techniques are an excellent method for providing digital signatures.

Recently, a press release from MasterCard International stated that they have embarked on a new standard for securing electronic fund transfers, SET (Secure Electronic Funds). This one standard is meant to allow consumers and merchants to conduct bank card transactions on the Internet as securely as they do in stores and ATM machines today. In addition, Intuit and RSA are teaming up to offer Internet banking through several services and insure security of transactions.

Businesses with Commercial and Trade Secrets

A northeast manufacturing company narrowly lost a \$1 billion project after a rival broke into its network of Unix workstations and learned what it planned to bid. (Groenfeldt, pg 64). Stealing a secret is often much cheaper than discovering, or even rediscovering it oneself. The United States annually invests more than \$130 billion in non-governmental research and development. The fruits of this investment present a tempting target for industrial espionage, from both foreign and domestic competitors. (Froomkin)

Business information need not be scientific or technical to be of enormous value. Sensitive marketing information, strategic plans, acquisition activity, and even intellectual property can be intercepted from faxes, cellular and microwave telephones, and unprotected computer network systems.

Professionals

Lawyers, doctors, therapists, and accountants are some of today's professionals that receive client confidences. Legally and ethically they are required to maintain these confidences. Professionals have long relied on ordinary telephones to communicate with clients and are increasingly using cellular telephones and electronic mail. Every lawyer knows that client confidences should not be discussed in a crowded restaurant. If such a confidence is overheard by a third party, even unintentionally, waiver of the attorney-client privilege may be imputed.

Anyone with the right sort of receiver can overhear cellular telephone conversations. Unfortunately, the ease with which electronic mail messages can be intercepted by third parties means that communicating by public electronic mail systems, like the Internet, is becoming almost as insecure as talking in a crowded restaurant. Similarly, the ease with which intruders can gain access to unprotected computers via the Internet means that unencrypted data on such machines is also at risk.

Credit Card Users

Most of us do not realize that the anonymity we are accustomed to in our commercial life is steadily shrinking with the use of credit cards, frequent shopper cards and many other means businesses use to collect information on our activities. Purchasing a drink from a vending machine for a few coins leaves no audit trail, but transactions with credit cards do. Encryption will not only allow individuals to keep their communications and records secret, it also allows them to keep their identities secret. It seems reasonable to suppose that some transactions, while even legal, might not occur if the only payment option leaves an audit trail.

Undoubtedly, criminals and conspirators will find a use for encryption, but so too will many others. Not every diarist records crimes in his daybook, but for many people there will be a certain satisfaction in knowing that their most private thoughts are safe from anyone's prying eyes, be they major governments or personal realtions.

Businesses with Distributed Networks

The day has long since gone when businesses could secure their mainframe in a single room and locate their workstations in one building, where physical access control as well as software access control using tools like IBM's RACF was sufficient. Today businesses have desktops, mini-computers, and mainframes distributed not only through a single building, but in some cases, throughout the world. These machines are all interconnected with media ranging from the PSTN to satellite microwave as LANs, WANs, and Enterprise networks. Businesses can spend a fortune on installing inter-network firewalls to reduce the vulnerabilities that distributed environments face. However, as soon as the data leaves the firewall and is transmitted onto shared media, it is vulnerable to eavesdropping, wiretapping, etc.

Remote users present another key vulnerability to distributed networks. When a remote user accesses the PSTN to connect to the business's WAN, the logon id and password are vulnerable to hackers using wiretapping or eavesdropping. The hackers can copy the data packets going across the media and then use the intercepted logon and password to break into the system. Once into the system, the business' IS assets and databases are vulnerable to the hacker. Encrypting passwords and sensitive information stored on corporate IS systems will provide some protection against this threat.

Users of Telephones, Electronic Mail, Faxes, or Computers

There are at least twelve million cellular telephone subscribers in the United States. Few of these telephones use encryption. Most of the cellular telephones that use some form of encryption use a very simple masking algorithm which is easy to defeat with parts available in any Radio Shack for less than \$200. (DePompa, pg 54)

Currently, only the US government has a large network of secure telephones, and they are expensive. AT&T has developed secure telephones based on the Clipper Chip that will provide encrypted communications, so long as both parties have a Clipper Chip-equipped telephone. Despite this, their use is not widespread, and most telephone conversations remain vulnerable to both legal and illegal wiretapping. The telephone signal often travels

by microwave, radio, or satellite, it is vulnerable to other forms of interception as well.

Faxes are as susceptible to interception as any other telephone call, yet few fax transmissions are encrypted. Fax interception equipment is relatively inexpensive and in some countries, is routinely used by telephone companies or the government to monitor fax traffic. Consequently, software vendors are now adding encryption options to common operating systems, such as Microsoft's Windows.

Encryption also protects against the consequences of misdialing a telephone number and reaching the wrong fax machine—an increasingly common problem as the number of dedicated fax lines grows.

Electronic mail is vulnerable on LANs, WANs and the Internet. The exponential growth in the Internet's popularity has fueled the private demand for encryption.

Many people have things they want to hide from their colleagues or family members. These records may be on paper or stored on a computer disk. Some people derive a sense of security from the knowledge that their communications and data are safe from unauthorized snooping by their friends, family, or anonymous computer hackers. Others seek an even greater sense of security by attempting to encrypt their communications and records in a manner that cannot be decrypted even by authorized law enforcement.

Law and Privacy

There is a currently a serious clash between the individual's and business' view on their rights to privacy and the safeguarding of their personal and corporate secrets, versus the government's view on its needs to adequately carry out law enforcement and national security procedures. Personal freedoms and privacy have come to be expected in this country, and are the basis for the writing of the Constitution and Bill of Rights.

Businesses have increasingly felt the need for this same protection, particularly following the mass proliferation of the use of computers. With intense competition in the marketplace comes great concern over the inappropriate eavesdropping or interception of business conversations and exchanges of data. Individuals and businesses have no control over the security of public channels used for transmission, whether they be wirebased or wireless. Private lines provide more protection, but provide no guarantees that messages

will not be intercepted. The need for encrypted communications is quite evident, particularly for business. The difficulty arises when the exchange of conversation or data is used for criminal activity. The use of strong encryption techniques prohibits certain types of law enforcement activities, and some argue infringes on their ability to fight certain crimes, as well as preserve national security. The views are greatly polarized.

Law Enforcement

Although not used in the majority of cases, law enforcement has employed communication interception in the prosecution of criminals and the exposure of government corruption. The most common methods are wiretapping and electronic bugs. This type of surveillance can result in strong evidence through the direct exposure of plans, instruction and execution of the crime, as well as the revealing of additional individuals that may have been involved in the crime. It can expose the most covert activities. Several high profile drug trafficking, organized crime, and government corruption cases have attributed their successful convictions to the use of wiretaps. It is not hard to understand why jurors would be strongly influenced by hearing defendants discussing the details of criminal activity, as opposed to trying to piece together physical evidence. Although the conviction rate in cases containing evidence from wiretaps and bugs is extremely high, it is impossible to say whether the conviction would have occurred in the absence of this evidence (Landau et al.).

While wiretapping and electronic bugs have focused on listening to verbal communications, written messages are also an area of concern to law enforcement officials. With the advances in technology, only a small investment is required to purchase the computer hardware and software needed to pass written messages to other computer users. These messages could prove invaluable in criminal cases. Persons not wanting their intercepted messages read can employ encryption techniques to secure their data transmissions or phone conversations. This is crippling to the value of intercepted information by law enforcement. In addition, modern techniques make it difficult to determine which data streams to intercept, and once intercepted, law enforcement may not be able to decrypt the message without the key.

National Security

Cryptography has long been the means used by the military to transmit sensitive information over insecure channels. Strong cryptography being a dual-use technology (a technology with military and civilian uses) presents a dilemma. It protects US commerce and enhances US products, thus increasing economic strength which is critical to national security. At the same time, foreign accessibility to cryptography compromises communications intelligence.

With the growth in communications intelligence has come a growth in techniques for protecting communications. The migration from wirebased communications and physical shipment to wireless media however, has far outstripped the application of any protective measures. Cryptography is seen as the only major barrier to communications intelligence. The challenge not only involves decrypting the messages, but identifying which data stream to capture in the first place. Communications intelligence is so valuable that keeping both the intelligence technology itself and the techniques for protecting communications are important objectives of US national security policy (Landau et al.).

The revealing of the DES algorithm may be considered a mistake by the intelligence community. Once revealed, DES-based equipment became available worldwide, the principles led to new cryptographic designs, and DES became a 'training ground' for a generation of public cryptanalysts. The task of American intelligence became more difficult. This has led to the view that the need to protect private interests should not come at the expense of intelligence capabilities.

Privacy

As individuals and businesses move along the technology learning curve, they recognize the vulnerability of their communications. This is even more apparent with the increased popularity, and risk, of using wireless technology. Many people, particularly in the United States, believe in the inherent right to privacy in all forms of communication. Recognizing the potential loss of this privacy while talking on telephones (especially cellular telephones) or transmitting data has resulted in an increased desire and demand for secure encryption solutions. Encryption techniques are well understood and very effective in securing both voice and data communications.

In addition to the desire for personal privacy, businesses are aware of the vulnerability of the information they store, process and transmit. Data ranging from personnel files to manufacturing processes, marketing information and trade secrets is found in today's corporate databases. Years ago, this information was centrally located in the corporate mainframe, where it could be reasonably protected. Today, the widespread transition to network computing has resulted in this same information no longer being isolated or easily protected. Business information is often transmitted across networks within the office, as well as between business locations and even to employee's homes. There has been an alarming increase in the number of 'industrial spy' cases which have resulted in the loss of millions of dollars for businesses whose secrets were lost to eavesdroppers or interception (Landau et al.).

Current Law and Its Impact

Strong encryption products have been classified by the government as munitions. Export controls on these products fall under the International Traffic in Arms Regulations (ITAR), governed by the National Security Agency (NSA). Exceptions to these controls are made for financial institutions and foreign offices of US-controlled companies. Products using encryption just to provide authentication and integrity (weak encryption) are not included under ITAR, making them exportable (and governed by the Department of Commerce). These controls limit US companies to the export of weak products, resulting in significant loss of market share. Foreign companies are unlikely to select products with weak encryption if they either currently need strong encryption, or feel they may in the future. A future need for strong encryption would require businesses to abandon their investment in the US product and reinvest in a stronger encryption product. Strong encryption is already available, legally, in foreign products. DES is also available on the Internet for those knowing what to do with it. DES is believed to be the most widely used cryptosystem in the world, except possibly the scramblers used for pay television (Landau, p 114).

The Government's Proposed Solution

On April 16, 1993, the Clinton Administration announced the proposal of the Escrowed Encryption Standard (EES) as a solution that would balance the privacy and security needs of individuals and businesses with the needs of law enforcement and national security. Instead of uniting the differing viewpoints, it has only stirred up more controversy. EES is a program involving the use of the Clipper Chip (which uses the Skipjack algorithm developed by the National Security Agency (NSA)) and a key-escrow system. There is also an additional feature known as a Law Enforcement Access Field (LEAF), which as implied, enables law enforcement access (and the ability to decode) the encrypted messages. The EES program is standard for non-classified government agencies and is voluntary for the private sector. The Administration felt this solution would allow for privacy without compromising law enforcement capability.

The Administration further stated that it would exempt EES products from the export ban in the International Traffic in Arms Regulations (ITAR) , making EES products the only US made, exportable products offering strong encryption. The day that the Administration announced its plans for Clipper, AT&T announced that its new secure telephone (the 3600) would not use a DES device as originally announced, but would use Clipper instead Landau et al.) This does not help resolve the disadvantage to US-based competitors in the world market, since there is great doubt that foreign companies will be interested in having their keys escrowed with the US government. There are further complications regarding how and when the ability to decrypt messages will be shared with foreign governments, and the impact of this sharing on the security promised to participating customers.

The ESS proposal has raised many issues which need resolution. Among these are:

1. Who should hold the keys? Both agencies proposed (the Department of Commerce NIST and the Department of Treasury Automated Systems Division) serve at the Administrations' pleasure. They have no legal support not to provide keys to such agencies as the FBI, and certainly don't have the authority to determine the legitimacy of such a request. A suggestion for allowing non-governmental escrow agents is now being considered by the Administration.

2. The 'components' of the keys held by the two agents must come together to provide law enforcement usable access. This combined information needs protection, and depends on an individual destroying this information at the expiration of the warrant or other legal document authorizing the 'search'. What about liabilities for unauthorized release of the key, or unauthorized access which results in a security compromise?
3. How should the government handle requests from foreign governments for the keys?
4. The exportability may be good for US companies with foreign subsidiaries, but would foreigners want to buy products that allow the US government listen access their data and messages, particularly when alternative strong encryption products are legally available in other foreign countries?
5. There is discomfort in the use of a classified algorithm. Businesses would have to trust that the strength of the algorithm and the length of the key are sufficiently strong. There has already been an instance of a scientist gaining access to the LEAF (Landau et al.) This raises further concern over the actual level of protection provided.
6. The EES program's algorithm would be available in hardware form, which is more costly and less flexible than software (albeit more secure). Vendor's want to be able to develop software solutions.
7. Many feel this proposal is a first step leading to prohibition of un-escrowed strong cryptography. Prohibition now would be too great a step, likely to result in strong opposition. However, going from a voluntary escrow to a mandatory escrow may not result in as strong of a confrontation.

Management Guidelines

The fear of corporate and MIS managers of someone breaching their security and stealing, muddling, or just looking at research plans, acquisition mergers, and company personnel

files is not without merit. Recently at a congregation of the Internet Society in Honolulu, Tsutomu Shimomura showed a video tape of a hacker he tracked breaking into the systems at the US Navy's Pacific Fleet Command. From start to finish, the assault took less than 6 minutes. Shimomura also showed an assault on the systems at the Kennedy Space Center which occurred in an equally brief time period (Schnaidt, pg 31).

The first step in determining the amount of encryption and what needs to be encrypted is to assess your business risk. Digital Equipment Corp. security consultant Dave Cullinane says, "You don't want to spend \$50,000 fixing a \$10,000 problem-and leave a \$1 million hole." (Robinson, pg 63) The major importance of doing a risk assessment is determining where in the business are the vulnerabilities and what information is important to the business. The risk assessment must review the potential threats to the business and identify the perceived and real vulnerabilities.

A good risk assessment will match possible solutions to the vulnerabilities. The risk assessment should determine what information will be encrypted and on which segment of the network the information will be encrypted. Selecting encryption approaches are based on the value of the information, the length of time the information has value, the cost of the product being used to protect the information, and how secure the information is against attack. (Wade, pg 15)

What to Encrypt and When

In your risk assessment you will identify assets such as e-mail, electronic commerce, trade secrets, personal private information and critical business information which need to be protected. An important step is to match the encryption technique to the resource that needs protection. The main options include public-key and single-key techniques such as RSA, DES, and PGP. Security managers must keep up with new technologies through regular environmental scanning.

Encryption can be expensive, time-consuming, and computer-intensive when generating keys, creating ciphertext, and decrypting into plaintext. Security managers must consider these factors before blindly encrypting all transmissions on a network or data stored in a system. Encrypting every file on a PC or every packet sent on a network is not a realistic security policy. The time required to decrypt every piece of information becomes cumbersome. A business should consider choosing a content-sensitive type of encryption

that encodes information that most deserves it. Financial data, confidential files, product formulas, and strategic plans are examples of data that probably need encryption.

Areas such as e-mail, office memos and letters may need some form of encryption. The length of time the message needs to stay encrypted is a factor of the type and level of data. For example, short-lived office communications may only require simple encryption techniques such as a shorter key or simple encryption algorithm. The variable length key encryption methods like those available from RSA are ideal for situations that require different of levels of protection.

If the speed of encryption and decryption processes is critical to the application, then alternatives include single-key techniques and hardware implementations.

By nature, common carrier services are more susceptible to eavesdropping than leased lines. However, leased-lines are more expensive and can even be cost prohibitive. Therefore to defray the cost, encryption can be used in addition to the public lines to effectively secure your information in transit.

Conclusion

Corporations today cannot afford to become isolationists and limit the information sent over telecommunication media. An effective means to provide security to prevent the potential loss of data is by instituting procedures for the routine encryption of information. Cryptography has proven to be highly effective against wiretapping and monitoring public and private networks.

The issues that a security manager must consider when addressing encryption are:

- ◆ Business risk assessment (determine assets requiring encryption)
- ◆ Identify feasible encryption solutions (hardware vs. software, single-key vs. public-key)
- ◆ Weigh speed, time-sensitivity, and computer intensity factors
- ◆ Cost of implementation versus cost of loss of the asset being protected
- ◆ Affect on applications

Information policies for encryption should be determined by the risk to your business if the information is compromised or destroyed. If management does not commit to these policies as a priority, all security efforts are meaningless. Encryption methods must be fully evaluated to determine the best solution to the areas of information vulnerability identified for the business.

References

Denning, Dorothy E. "Key Escrow Encryption: The Third Paradigm." Computer Security Journal. Vol. XI, No. 1, 1995, p 43-52.

Cheswick, William R. Firewalls and Internet Security: repelling the wily hacker. Massachusetts: Addison-Wesley, pg 211-234, 1994.

Conner, Louis. "Can you trust Web Transactions?" Communications Week. Issue 592, pg 41, Jan. 15, 1996.

Cox, John. "Oracle Takes Wraps Off Data-Encryption Software - Offering provides protection at the transport level." Communications Week. Issue 539, pg 15, January 16, 1995.

DePompa, Barbara. "Locking up Data." Communications Week. Issue 498, pg 54, March 28, 1994.

Forcht, Karen A.. Computer Security Management. Massachusetts, Boyd and Fraser Publishing Co., pg 109-127, 1994.

Froomkin, A. Michael. "The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution." <http://acr.law.miami.edu/~froomkin/welcome.html>, June 24, 1995.

Girishankar, Saroja. "When the Best Defense is a New E-Mail Network." Communications Week. Issue 569, pg 1, August 7, 1995.

Groenfeldt, Tom. "How Secure is Your System? Illegal access to sensitive data costs businesses billions_so many have tightened security policies." Information Week. Issue 498, pg 64, October 24, 1994.

Hoffman et al., "Cryptography: Policy and Technology Trends." US Department of Energy. January 30, 1994.

Jaspan, Barry. "Kerberos Users' Frequently Asked Questions." <http://www.ov.com/misc/krb-faq.html>, September 14, 1995.

Landau et al. "Codes, Keys and Conflicts: Issues in U.S. Crypto Policy." Association for Computing Machinery, Inc. http://Info.acm.org/reports/c_report.html, June 1994.

Liebmann, Lenny. "How to Protect Distributed Data." Communications Week. Issue 577, pg 53, September 28, 1995.

Neuman, B. Clifford and Theodore Ts'o. "Kerberos: An authentication Service for Computer Networks." IEEE Communications Magazine. Vol. 32, No. 9, pg 33-38, September 1994.

Peterson, Ivars. The Mathematical Tourist: snapshots of modern mathematics. New York: W.H. Freeman and Company, 1988, pg 34-43.

Robinson, Teri. "Encryption+Firewalls+Passwords+Token Authentication+User ID=Security Overkill?" Communications Week. Issue 584, pg 63, November 13, 1995.

Schnaidt, Patricia. "Less Convenience, More Security." Network Computing. Issue 610, pg 31, Sept. 1, 1995

Schneier, Bruce. "Untangling Public-Key Cryptography." Dr. Dobbs Journal. May 1992, pg 16-28.

Sobel, David. "Comments on Draft Export Criteria for Key Escrow Encryption." National Institute of Standards of Technology. December 5, 1995.

Stallings, William. "Pretty Good Privacy." Byte. July 1994, pg 193-196.

Stallings, William. "SHA: The Secure Hash Algorithm" Dr. Dobbs Journal. April 1994, pg 32-34.

Rivest, Ronald L. "The RC5 Encryption Algorithm." Cryptobytes Spring 1995.

RSA Laboratories. "RSA's Frequently Asked Questions About Today's Cryptography." <http://www.rsa.com/rsalabs/faq>

Wade, Bob. "Encryption: A primer." Security Management, Supplement. March 1993, pg 15A-20A.

Walker et al. "Commercial Key Escrow: Something for Everyone Now and for the Future." Trusted Information Systems, Inc. January 3, 1995.