S E N S ' 2 0 0 6
Second Scientific Conference with International Participation
SPACE, ECOLOGY, NANOTECHNOLOGY, SAFETY
14 – 16 June 2006, Varna, Bulgaria

CRYPTOGRAPHY: ROLES, MARKET, AND INFRASTRUCTURE

Radoslav Kardjhiev, Kremen Hristov

ICON Ltd.
Shoumen, 43, Maritsa St., e-mail: kremen.hristov@gmail.com

Keywords: cryptography, security

Abstract. *Cryptography is a technology that can play important roles in addressing certain types of information vulnerability, although it is not sufficient to deal with all threats to information security. As a technology, cryptography is embedded into products that are purchased by a large number of users; thus, it is important to examine various aspects of the market for cryptography*.

In an age of explosive worldwide growth of electronic data storage and communications, many vital national interests require the effective protection of information.When used in conjunction with other approaches to information security, cryptography is a very powerful tool for protecting information. Consequently, current U.S. policy should be changed to promote and encourage the widespread use of cryptography for the protection of the information interests of individuals, businesses, government agencies, and the nation as a whole, while respecting legitimate national needs of law enforcement andintelligence for national security and foreign policy purposes to the extent consistent with good information protection.

Computer system security, and its extension networksecurity, are intended to achieve many purposes. Among them are safeguarding physical assets from damage or destruction and ensuring that resources such as computer time, networkconnections, and access to databases are available only to individuals--or to other systems or even software processes--authorized to have them. Overall information security is dependent on many factors, including various technical safeguards, trustworthy and capable personnel, high degrees of physical security, competent administrative oversight, and good operational procedures. Of the available technical safeguards, cryptography has been one of the least utilized to date.

In general, the many security safeguards in a system or network not only fulfill their principal task but also act collectively to mutually protect one another. In particular, the protection or operational functionality that can be afforded by the various cryptographic safeguards treated in this report will inevitably require that the hardware or software in question be embedded in a secure environment. To do otherwise is to risk that the cryptography might be circumvented, subverted, or misused-- hence leading to a weakening or collapse of its intended protection.

In the classical use of cryptography to protect communications, it is necessary that both the originator and the recipient(s) have common knowledge of the cryptographic process (the algorithm or cryptographic algorithm) and that both share a secret common element--typically, the key or cryptographic key, which is a piece of information, not a

material object. In the encryption process, the algorithm transforms the plaintext into the ciphertext, using a particular key; the use of a different key results in a different ciphertext. In the decryption process, the algorithm transforms the ciphertext into the plaintext, using the key that was used to encrypt4 the original plaintext. Such a scheme, in which both communicating parties must have a common key, is now called symmetric cryptography or secret-key cryptography; it is the kind that has been used for centuries and written about widely.5 It has the property, usually an operational disadvantage, of requiring a safe method of distributing keys to relevant parties (key distribution or key management).

It can be awkward to arrange for symmetric and secret keys to be available to all parties with whom one might wish to communicate, especially when the list of parties is large. However, a scheme called asymmetric cryptography (or, equivalently, public-key cryptography), developed in the mid-1970s, helps to mitigate many of these difficulties through the use of different keys for encryption and decryption.6 Each participant actually has two keys. The public key is published, is freely available to anyone, and is used for encryption; the private key is held in secrecy by the user and is used for decryption.7 Because the two keys are inverses, knowledge of the public key enables the derivation of the private key in theory. However, in a well-designed public-key system, it is computationally infeasible in any reasonable length of time to derive the private key from knowledge of the public key.

A significant operational difference between symmetric and asymmetric cryptography is that with asymmetric cryptography anyone who knows a given person's public key can send a secure message to that person. With symmetric cryptography, only a selected set of people (those who know the private key) can communicate. While it is not mathematically provable, all known asymmetric cryptographic systems are slower than their symmetric cryptographic counterparts, and the more public nature of asymmetric systems lends credence to the belief that this will always be true. Generally, symmetric cryptography is used when a large amount of data needs to be encrypted or when the encryption must be done within a given time period; asymmetric cryptography is used for short messages, for example, to protect key distribution for a symmetric cryptographic system. Regardless of the particular approach taken, the applications of cryptography have gone beyond its historical roots as secret writing; today, cryptography serves as a powerful tool in support of system security.

Cryptography can provide many useful capabilities:

- Confidentiality - the characteristic that information is protected from being viewed in transit during communications and/or when stored in an information system. With cryptographically provided confidentiality, encrypted information can fall into the hands of someone not authorized to view it without being compromised. It is almost entirely the confidentiality aspect of cryptography that has posed public policy dilemmas. The other capabilities, described below, can be considered collectively as nonconfidentiality or collateral uses of cryptography:
- Authentication - cryptographically based assurance that an asserted identity is valid for a given person (or computer system). With such assurance, it is difficult for an unauthorized party to impersonate an authorized one.
- Integrity check - cryptographically based assurance that a message or computer file has not been tampered with or altered.8 With such assurance, it is difficult for an unauthorized party to alter data.
- Digital signature - cryptographically based assurance that a message or file was sent or created by a given person. A digital signature cryptographically binds the identity of a person with the contents of the message or file, thus providing nonrepudiation--the inability to deny the authenticity of the message or file. The capability for nonrepudiation results from encrypting the digest (or the message or

file itself) with the private key of the signer. Anyone can verify the signature of the message or file by decrypting the signature using the public key of the sender. Since only the sender should know his or her own private key, assurance is provided that the signature is valid and the sender cannot later repudiate the message. If a person divulges his or her private key to any other party, that party can impersonate the person in all electronic transactions.

- Digital date/time stamp - cryptographically based assurance that a message or file was sent or created at a given date and time. Generally, such assurance is provided by an authoritative organization that appends a date/timestamp and digitally signs the message or file.

Cryptographic strength depends on two factors: the size of the key and the mathematical structure of the algorithm itself. For well-designed symmetric cryptographic systems, "brute-force" exhaustive searchÑtrying all possible keys with a given decryption algorithm until the (meaningful) plaintext appearsÑis the best publicly known cryptanalytic method. For such systems the work factor (i.e., the time to cryptanalyze) grows exponentially with key size. Hence, with a sufficiently long key, even an eavesdropper with very extensive computing resources would have to take a very long time (longer than the age of the universe) to test all possible combinations. Adding one binary digit (bit) to the length of a key doubles the length of time it takes to undertake a brute-force attack while adding only a very small increment (or sometimes none at all) to the time it takes to encrypt the plaintext.

As for the exploitation of alternatives to brute-force search, all known asymmetric (i.e., public-key) cryptographic systems allow shortcuts to exhaustive search.Because more information is public in such systems, it is also likely that shortcut attacks will exist for any new systems invented. Shortcut attacks also exist for poorly designed symmetric systems. Newly developed shortcut attacks constitute unforeseen breakthroughs, and so by their very nature introduce an unpredictable "wild card" into the effort to set a reasonable key size. Because such attacks are applicable primarily to public-key systems, larger key sizes and larger safety margins are needed for such systems than for symmetric cryptographic systems. For example, factoring a 512-bit number by exhaustive search would take 2256 tests (since at least one factor must be less than 2256); known shortcut attacks would allow such numbers to be factored in approximately 265 operations, a number on the order of that required to undertake a brute-force exhaustive search of a message encrypted with a 64-bit symmetric cryptographic system. While symmetric 64-bit systems are considered relatively safe, fear of future breakthroughs in cryptanalyzing public-key systems has led many cryptographers to suggest a minimum key size of 1,024 bits for public-key systems, thereby providing in key length a factor-of-two safety margin over the safety afforded by 512- bit keys.

Cryptography is a product as well as a technology. Products offering cryptographic capabilities can be divided into two general classes:

- Security-specific or stand-alone products that are generally add-on items (often hardware, but sometimes software) and often require that users perform an operationally separate action to invoke the encryptioncapabilities. Examples include an add-on hardware board that encrypts messages or a program that accepts a plaintext file as input and generates a ciphertext file as output.
- Integrated (often "general-purpose") products in which cryptographic functions have been incorporated into some software or hardware application package as part of its overall functionality. An integrated product is designed to provide a capability that is useful in its own right, as well as encryption capabilities that a user may or may not use. Examples include a modem with on-board encryption or a word processor with an option for protecting (encrypting) files with passwords.

Even when a user is aware that communications security is threatened and wishes to take action to forestall the threat, a number of practical considerations can affect the decision to use cryptographic protection. These considerations include the following:

- Lack of critical mass. A secure telephone is not of much use if only one person has it. Ensuring that communications are secure requires collective action--some critical mass of interoperable devices is necessary in order to stimulate demand for secure communications. To date, such a critical mass has not yet been achieved.
- Uncertainties over government policy. Policy often has an impact on demand. A number of government policy decisions on cryptography have introduced uncertainty, fear, and doubt into the marketplace and have made it difficult for potential users to plan for the future. Seeing the controversy surrounding policy in this area, potential vendors are reluctant to bring to market products that support security, and potential users are reluctant to consider products for security that may become obsolete in the future in an unstable legal and regulatory environment.
- Lack of a supporting infrastructure. The mere availability of devices is not necessarily sufficient. For some applications such as secure interpersonal communications, a national or international infrastructure for managing and exchanging keys could be necessary. Without such an infrastructure, encryption may remain a niche feature that is usable only through ad hoc methods replicating some of the functions that an infrastructure would provide and for which demand would thus be limited.
- High cost. To date, hardware-based cryptographic security has been relatively expensive, in part because of the high cost of stand-alone products made in relatively small numbers. A user that initially deploys a system without security features and subsequently wants to add them can be faced with a very high cost barrier, and consequently there is a limited market for add-on security products.

The widespread use of cryptography requires a support infrastructure that can service organizational or individual user needs with regard to cryptographic keys. In general, to enable use of cryptography across an enterprise, there must be a mechanism that:

- Periodically supplies all participating locations with keys (typically designated for use during a given calendar or time period--the crypto-period) for either stored materials or communications; or
- Permits any given location to generate keys for itself as needed (e.g., to protect stored files); or
- Can securely generate and transmit keys among communicating parties (e.g., for data transmissions,telephone conversations).

In the most general case, any given mechanism will have to perform all three functions. With symmetric systems, the movement of keys from place to place obviously must be done securely and with a level of protection adequate to counter the threats of concern to the using parties. Whatever the distribution system, it clearly must protect the keys with appropriate safeguards and must be prepared to identify and authenticate the source. The overall task of securely assuring the availability of keys for symmetric applications is often called key management.

If all secure communications take place within the same corporation or among locations under a common line of authority, key management is an internal or possibly a joint obligation. For parties that communicate occasionally or across organizational boundaries, mutual arrangements must be formulated for managing keys. One possibility might be a separate trusted entity whose line of business could be to supply keys of specified length and format, on demand and for a fee.

With asymmetric systems, the private keys are usually selfgenerated, but they may also be generated from a central source, such as a corporate security office. In all cases, however, the handling of private keys is the same for symmetric and asymmetric systems; they must be guarded with the highest levels of security. Although public keys need not be kept secret, their integrity and association with a given user are extremely important and should also be supported with extremely robust measures.

Cryptography provides important capabilities that can help deal with the vulnerabilities of electronic information. Cryptography can help to assure the integrity of data, to authenticate the identity of specific parties, to prevent individuals from plausibly denying that they have signed something, and to preserve the confidentiality of information that may have improperly come into the possession of unauthorized parties. At the same time, cryptography is not a silver bullet, and many technical and human factors other than cryptography can improve or detract from information security. In order to preserve information security, attention must be given to all of these factors. Moreover, people can use cryptography only to the extent that it is incorporated into real products and systems; unimplemented cryptographic algorithms cannot contribute to information security. Many factors other than raw mathematical knowledge contribute to the supply of and demand for products with cryptographic functionality. Most importantly, the following aspects influence the demand forcryptographic functions in products:

- Critical mass in the marketplace,
- Government policy,
- Supporting infrastructure,
- Cost,
- Performance,
- Overall security environment,
- Usability,
- Quality certification and evaluation, and
- Interoperability standards.

Finally, any large-scale use of cryptography, with or without key escrow, depends on the existence of a substantial supporting infrastructure, the deployment of which raises a different set of problems and issues.

REFERENCES

1. Niels Ferguson, Bruce Scneier, Practical Cryptography, 2003
2. Intranets.com, Security White Paper.
3. Internetworking Technologies Handbook.
4. Adam Young, Moti Yung, Malicious Cryptography, 2004.
5. A. Lukatsky. Protect Your Information with Intrusion Detection. A-LIST Publishing; (November 2002).
6. Network Associates, Inc., Cryptography - An Introduction To Cryptography.
7. Peter Gutmann, Cryptography and Data Security, 2004