Codes, Keys and Conflicts: Issues in U.S. Crypto Policy

Report of a Special Panel of the *ACM U.S. Public Policy Committee (USACM) June 1994*

by Susan Landau
Stephen Kent, chair
Clint Brooks
Scott Charney
Dorothy Denning
Whitfield Diffie
Anthony Lauck
Doug Miller
Peter Neumann
David Sobel

Association for Computing Machinery, Inc.

The Association for Computing Machinery, Inc.
1515 Broadway
New York, NY 10036

ACM ISBN: 0-89791-677-8

Additional print copies of this report can be ordered prepaid from the ACM Order Department, P.O. Box 12114, Church Street Station, New York, NY 10257; Tel: 1-800-342-6626 (U.S.A. and Canada), 1-212-626-0500 (all other countries); Fax: 1-212-944-1318; E-mail: acmhelp@acm.org; Price: $10.00 per copy; reference ACM Order Number 207940.

The report can also be obtained in various electronic formats from ACM's Internet host. Internet users can access the report through any of the following URLs:

`http://Info.acm.org/reports/acm_crypto_study.html`
`ftp://Info.acm.org/reports/acm_crypto_study/`
`gopher://gopher.acm.org/11[the_files.reports.acm_crypto_study]`

Contents

Executive Summary

On April 16, 1993, the White House announced the Escrowed Encryption Initiative, "a voluntary program to improve security and privacy of telephone communications while meeting the legitimate needs of law enforcement." The initiative included a chip for encryption (Clipper), to be incorporated into telecommunications equipment, and a scheme under which secret encryption keys are to be escrowed with the government; keys will be available to law enforcement officers with legal authorization. The National Security Agency (NSA) designed the system and the underlying cryptographic algorithm SKIPJACK, which is classified. Despite substantial negative comment, ten months later the National Institute of Standards and Technology approved the Escrowed Encryption Standard (EES) as a voluntary Federal standard for encryption of voice, fax, and computer information transmitted over circuit-switched telephone systems.

Underlying the debate on EES are significant issues of conflicting public needs. Every day, millions of people use telephones, fax machines, and computer networks for interactions that were once the province of written exchanges or face-to-face meetings. Private citizens may want to protect their communications from electronic eavesdroppers. Law enforcement seeks continuation of its legally authorized access to communications of suspected criminals. In order to compete in the global marketplace, U.S. manufacturers want to include strong cryptography in their products. Yet national security interests dictate continued access to foreign intelligence. Both the EES and the controversy surrounding it are but the latest and most visible developments of a conflict inherent in the Information Age.

The issues EES raises are fundamental. When the Constitutional protections of the Bill of Rights became law in 1791, speech took place in the streets, the market, the fields, the office, the bar room, the bedroom, etc. It could be used to express intimacy, conduct business, or discuss politics. Privacy was an indispensable component of the character of many of these conversations. In the two hundred years since then, electronic communications have taken the place of many of those face-to-face meetings of two centuries ago. The world has undergone a fundamental change in the way it conducts its business, both personal and professional.

The EES is primarily for use with telephones and fax machines. The broad public debate it has sparked is primarily, though not exclusively, con-

cerned with the expected extension of escrowed encryption to other forms of electronic communications. This debate has provided many press clippings – but fewer facts. Proponents of EES argue that escrowed encryption using a secret algorithm is a reasonable and logical way to provide security for electronic communications without unleashing cryptography that will thwart law enforcement and national security. Critics of EES see the Federal program as nothing less than a large step in the direction of Big Brother.

The fact is that the issue of cryptography is complex. All who have thought seriously about the issues of communications security – from civil libertarians to law enforcement officials to the computer industry and national security experts – agree that strong cryptography is necessary for protecting the confidentiality, integrity, and authenticity of the information infrastructure and that this protection is extremely important for economic stability and national security. The disagreements are partially disputes over potential costs: What would be the cost to society if criminals concealed their communications using codes the government cannot decipher? How will U.S. economic competitiveness be affected by export controls on cryptographic systems? It is even more a disagreement on values: How important is protecting society from abuses by criminals and terrorists versus protecting personal privacy from all threats – including potential eavesdropping by the government?

In this report, we attempt to remove the rhetoric, lay bare the facts, and frame the issues. We examine the issues of communications security from a variety of viewpoints: (i) we explain the technical considerations of communications security; (ii) we consider the dual-edged sword cryptography presents to both law enforcement and national security; (iii) we present the history of wiretap law in the United States; and (iv) we put the current policy on cryptography in the context of decisions over the last twenty years. We explain the anticipated impact of EES on the computer and cryptography industries, on privacy, and on law enforcement and national security, and we raise a number of questions that deserve examination in this discussion.

We hope to have laid a foundation on which an informed public debate can begin. The discussion on solutions to the problems of communications security encompasses broad issues and values, and the choices that will be made should be made in full consideration of the facts. President Franklin Delano Roosevelt eloquently stated the balance that should underlie fundamental policy decisions:

> The only sure bulwark of continuing liberty is a government strong enough to protect the interests of the people, and a people strong enough and well enough informed to maintain its sovereign control over the government.[1]

In order to determine policy for the protection of communications, the public deserves full information on the issues.[2] That is what this report seeks to provide.

Notes

1. Fireside Chat, April 14, 1938.
2. Note, however, that the information provided in this report is derived from unclassified sources only.

Preface

Cryptography is being debated in public – again. One wag claims that every few years there is a study on cryptography and public policy, whether it is needed or not.[1] With the increasing use of distributed networks for computing, the emerging National Information Infrastructure and its need for communications security, the international availability of two strong cryptographic algorithms, DES and RSA, the Federal "Clipper" Initiative, many unresolved issues have come to the fore. It is clear that a public debate on these issues is necessary. This report, by a panel convened by the Association for Computing Machinery's U.S. Public Policy Committee (USACM), is an attempt to clarify the technical and policy issues surrounding cryptography, so that a careful and clear public debate may result.

This panel, which includes members of the U.S. government, attorneys, and members of the computer industry and academia, has not come to conclusions about the direction of cryptography in the public domain, or about the appropriateness of the government-proferred Escrowed Encryption Standard. While not always reaching consensus, we have attempted to present the issues carefully and correctly, removing rhetoric and replacing it with facts. This report represents the work of the panel members as individuals, and does not necessarily represent the opinions of their organizations, nor of the ACM, which sponsored this study. Funding was provided in part by the National Science Foundation, under grant number CDA-9400157.

ACM, the first society in computing (founded in 1947), is a 85,000-member nonprofit educational and scientific society dedicated to the development and use of information technology, and to addressing the impact information technology has on the world's major social challenges. The Association's major programs and services include its scholarly journals (currently 18), which are world-class repositories of the finest computing literature, and Special Interest Groups (34) that specialize in providing educational resources and help to establish the standard of excellence in specific computing disciplines through technical conferences and newsletters.

USACM was created by ACM to provide a means for presenting and discussing technological issues to and with U.S. policy makers and the general public. Presentation of this information includes white papers, news releases, journal articles, and expert testimony for Congressional hearings. This report is the first major undertaking of USACM.

A brief road map is in order. Chapter 1 provides background on information protection in the Information Age, including an explanation of the different functions cryptography provides, and the algorithms currently being used. Chapter 2 describes the way cryptography secures electronic communications, both for computers and for telephones. The description provided in this chapter is somewhat more technical than the remaining ones, and can be skipped by those who are less concerned with detail on the technological issues. Chapter 3 explains the problems of cryptography from a law-enforcement perspective; it includes a brief history of wiretapping in the United States. Chapter 4 explains the dual nature of cryptography in the context of national security. Chapter 5 discusses the value and importance of privacy in the United States.

Cryptography is not a new issue for the public forum, and Chapter 6 presents the policy issues, resolved and unresolved, that have been debated over the last twenty years. Chapter 7 presents the Escrowed Encryption Standard (EES), a cryptographic scheme in which government agencies hold the keys. This controversial standard, approved by the National Institute of Standards and Technology earlier this year, is part of the reason for the current report. Chapter 8 discusses the issues highlighted by the EES, including privacy concerns, export policy, interoperability issues, and the impact of EES on the U.S. computer industry. Chapter 9 concludes the report, by placing the issues in a broader context. Notes appear on the last page of the chapter.

Acknowledgements

This report is the idea of Dr. Barbara Simons, chair of USACM. Within days of the White House announcement of the Escrowed Encryption Initiative, Dr. Simons conceived of this panel, and it was she who arranged a chair and initial funding from ACM. This report would not have occurred without her efforts.

This report benefitted from the review by members of USACM and the ACM Committee on Computers and Public Policy. We greatly appreciate their help.

The panel would like to thank those individuals who provided guidance and information. These include: David Banisar, James Bidzos, Dennis Branstad, Lewis Branscomb, James Burrows, John Cherniavsky, Geoffrey

Greiveldinger, Doris Lidtke, Alan McDonald, Douglas McIlroy, Marc Rotenberg, Herman Schwartz, James Simons, and Barry Smith.

Notes

1. Panel studies include American Council on Education, "Report of the Public Cryptography Study Group," February 7, 1981; U.S. Department of Commerce, National Telecommunications and Information Administration, "White Paper: Analysis of National Policy Options for Cryptography," October 29, 1980; Office of Technology Assessment, "Defending Secrets, Sharing Data, New Locks and Keys for Electronic Information," 1987; Final Report of the Industry Information Security Task Force Industry Information Protection, June 13, 1988. There have also been numerous studies by individuals, including several done at the Harvard University Program on Information Resources Policy.

About the Authors

Susan Landau is Research Associate Professor at the University of Massachusetts. She works in algebraic algorithms.

Stephen Kent is Chief Scientist-Security Technology for Bolt Beranek and Newman Inc. For over 18 years, he has been an architect of computer network security protocols and technology for use in the government and commercial sectors.

Clinton C. Brooks is an Assistant to the Director of the National Security Agency. He is responsible for orchestrating the Agency's technical support for the government's key-escrow initiative.

Scott Charney is Chief of the Computer Crime Unit in the Criminal Division in the Department of Justice. He supervises five federal prosecutors who are responsible for implementing the Justice Department's Computer Crime Initiative.

Dorothy E. Denning is Professor of Computer Science at Georgetown University. She is author of "Cryptography and Data Security" and one of the outside reviewers of the Clipper system.

Whitfield Diffie is Distinguished Engineer at Sun Microsystems. He is the co-inventor of public-key cryptography, and has worked extensively in cryptography and secure systems.

Anthony Lauck is a Corporate Consulting Engineer at Digital Equipment and its lead network architect since 1978. His contributions span a wide range of networking and distributed-processing technologies.

Douglas Miller is Government Affairs Manager for the Software Publishers Association.

Peter G. Neumann has been a computer professional since 1953, and involved in computer-communication security since 1965. He chairs the ACM Committee on Computers and Public Policy and moderates the Risks Forum.

David L. Sobel is Legal Counsel to the Electronic Privacy Information Center (EPIC). He specializes in civil liberties, information, and privacy law and frequently writes about these issues.

Chapter 1

Information Protection in the Information Age

If this is the Information Age, how do we protect information? Many times a day people transmit sensitive data over insecure channels: reciting credit card numbers over cellular phones (scanners are ubiquitous), having private exchanges over electronic mail (Internet systems are frequently penetrated), charging calls from airports and hotel lobbies (our Personal Identification Numbers (PINs) easily captured). The problem is magnified at the corporate level. For several years in the 1970s, IBM executives conducted thousands of phone conversations about business on the company's private microwave network – and those conversations were systematically eavesdropped upon by Soviet intelligence agents [Broa].[1]

IBM is not unique in having suffered from electronic eavesdroppers. Weak links exist throughout electronic communications, in networks and in distributed computer systems. An Alaskan oil company kept losing leasing bids by small amounts to competitors. The line between a computer in the Alaska office and one at the home base in Texas was being tapped, and a competitor was intercepting pricing advice transmitted from the Texas office [Park, pg. 322].

Computer systems themselves can be a weak link. Employees at British Airways read Virgin Atlantic Airlines' passenger records. From that information the employees carried on systematic efforts to induce Virgin's travelers to switch their flights to British Air [Stev].

Deceptive communications can easily undermine users' confidence in a system. For example, a group of students at the University of Wisconsin forged an E-mail letter of resignation from the Director of Housing to the Chancellor of the University [Neu]. There can be denials of service because of altered or jammed communications; "video pirates" have disrupted satellite television programs a number of times [Neu].

Electronic communications are now an unavoidable component of modern life. Every day, millions of people use telephones, fax machines, and computer networks for interactions that were once the province of written exchanges or face-to-face meetings. Private citizens may want to protect their communications from electronic eavesdroppers. Privacy is a fundamental value of this society, reflected in the Fourth Amendment – which provides safeguards for the security of our "persons, houses, papers and effects" against intrusion by the government.

Over the past five years, thousands of mainframe computers have been replaced by networked computing systems. This process is accelerating, and that change will increase the importance of secure electronic communications. The National Information Infrastructure (NII), the "information superhighway," will have an even greater effect. Businesses will teleconnect with customers to sell and bill. Manufacturers will electronically query suppliers to check product availability. Insurance companies, doctors, and medical centers will carry on electronic exchanges about patient treatment. Much of the information being sent on the NII will be sensitive. At the same time, most of its users will be quite unsophisticated in the complexities of the networks they access, or in the problems that can arise from intercepted communications. Protecting the confidentiality, integrity, and authenticity of the information infrastructure is extremely important to economic stability and national security.

Cryptography as a Solution

How can communications security be achieved? A very important part of the solution is cryptography. It has long been the military solution to the problem of transmitting sensitive information over insecure channels. Cryptography can help prevent penetration from the outside. It can protect the privacy of users of the system so that only authorized participants can comprehend communications. It can ensure integrity of communications. It can increase assurance that received messages are genuine.

Confidentiality, the service most often associated with cryptography, consists of transforming (encrypting) information so it is unintelligible to anyone except the intended recipient. Because cryptography for confidentiality purposes has the potential to interfere with foreign intelligence gathering, it is often subject to stringent export controls. In the U.S., export control of cryptography used for confidentiality is managed by the State Department, and products incorporating "strong"[2] cryptographic algorithms for confidentiality are generally not exportable.

Integrity is a security service that permits a user to detect whether information has been tampered with during transmission or while in storage. Closely related to integrity is authenticity, which provides a user with a means of verifying the identity of the sender of a message. Authentication frequently involves associating a unique cryptographic key with a user.

Integrity and authenticity services are often implemented in tandem. In part, the motivation is that it generally is not useful to be able to establish the authenticity of a message unless one can also establish the integrity of the message (and vice versa). However, information that is authenticated and integrity-checked is not necessarily confidential; that is, confidentiality can be separated from integrity and authenticity.

Cryptography that provides integrity and authenticity only does not interfere with many types of intelligence gathering. In the U.S., export control of products offering only these services is generally managed by the Commerce Department; export licenses are usually granted.

Weak Links

Electronic communication networks are complex systems built out of many components. An intruder wishing to access the communications in a network will look for unprotected points or segments. The weakest link is where one might be able to bypass or avoid the security mechanisms altogether. Cryptography or other security measures in one part of a system, or in one aspect of the transaction, could provide no protection at all if weak links are not protected. Because we want products to ship the day before the last line of code is written, proper cryptography is often never implemented.

However, even the most carefully designed system can have flaws (see Chapter 2 for a more detailed discussion). The following are among the most common weak links:

* Modifications to software or hardware: An adversary modifies code or some aspect of a product that controls the cryptography or access. Such an intruder could even make modifications to collect information, such as cryptographic keys.

* Access control: Someone masquerades as the user and thus has the user's privileges and can alter or read information. This may include control of the cryptography.

* Cryptographic vulnerabilities: One can have sound cryptographic algorithms properly implemented, but the associated initialization, randomization, or key management may be sources of weakness.

* Cryptographic algorithms: The fundamental mathematics of the cryptography may have a subtle vulnerability that can be discovered through clever analysis.

* Cryptographic administration: Even the best cryptographic algorithms can be subverted if their use is not properly administered. Sloppy key management can lead to exposures of the keys. Operating system vulnerabilities may lead to compromises of unencrypted text or of the cryptography itself.

Cryptographic Algorithms

In the last two decades the civilian sector has adopted certain crytographic schemes for protecting electronic communications. In 1975, the United States proposed the Data Encryption Standard (DES) for the protection of "sensitive but unclassified information" by government agencies. DES, designed by IBM, was vetted by the National Security Agency (NSA), the U.S. agency responsible for secure codes for military and diplomatic communications. It was adopted as a Federal Information Processing Standard (FIPS) in 1977 (in the same series that now includes the EES). It is a classic private- or single-key system; the key used to protect communications between two parties must be known to both parties and kept secret from everyone else. DES requires a secure method to establish the key.

At the time DES was proposed, it enjoyed a period of controversy in which its keys were characterized as too small and other weaknesses were suspected. Despite this, the algorithm has proven remarkably resistant to public attacks.

DES was designed for use by Federal agencies for the protection of sensitive but unclassified data. Software versions of DES are quite common outside the Federal government. Although export of the algorithm for confidentiality purposes is restricted, DES is believed to be the most widely used cryptosystem in the world, except perhaps for scramblers used for pay television. In the United States, the American Bankers Association recommends DES whenever encryption is needed to protect financial data [ABA].[3] DES is the cryptographic scheme most often used in commercially available secure telephones [Bran]. A DES variant is used for password encryption in almost all versions of Unix, a very popular operating system for multitasking environments.

At about the same time as DES was introduced, academic researchers developed a family of cryptographic techniques that became known as public-key or two-key cryptography. One approach, proposed by Ralph Merkle at Berkeley and refined by Whitfield Diffie and Martin Hellman at Stanford, allowed two parties to negotiate a common secret piece of information over an insecure channel. Another, proposed by Diffie and Hellman and realized by Ronald Rivest, Adi Shamir, and Leonard Adleman of MIT, made it possible to use a key that was not secret (a public key) to encrypt a message that could be decrypted only by a particular secret key. Conversely, a message transformed by a secret key could be verified as coming from the sender by applying the sender's public key. This second use of public-key technology came to be called a digital signature.

Products containing RSA (as the Rivest-Shamir-Adleman algorithm came to be known) are available commercially. It is used as the basis for Privacy Enhanced Mail (PEM) and Pretty Good Privacy (PGP), widely available systems for protecting electronic mail. It is also used in some commercial secure telephones.

There are many applications for which DES and RSA are combined, including PEM [Kent], and telecommunications equipment by Motorola and Northern Telecom [DOW]. For comparable levels of security, the fastest implementations of DES are about a thousand times faster than the fastest RSA implementions;[4] RSA is used for key exchange when two parties wish to establish private communications, and their only link is over an insecure channel. Having established a private key, DES is used to encrypt the information.

These algorithms provide the U.S. commercial sector with techniques for achieving confidentiality, integrity, and authenticity. However, with the exception of exporting DES for use by financial institutions or foreign offices of U.S.-controlled companies, the State Department typically refuses export license for confidentiality systems employing strong cryptography. This presents a serious problem to U.S. industry, all the more so because DES is widely available outside the United States. A March 1994 study by the Software Publishers Association lists 152 products being developed and distributed in 33 countries, all using DES [SPA-94].

The Emerging Problem – and a Possible Solution

DES is coming to the end of its useful life with its key size and complexity being overtaken by improvements in speed and cost of computers [Wie]. Yet the U.S. private sector, from bankers to the future users of the NII, need strong cryptography. Strong cryptography can impede law enforcement and the collection of foreign intelligence by national security organizations. A repeat of a publicly disclosed, government-certified, strong cryptosystem for confidentiality purposes seems unlikely.

On April 16, 1993, the White House proposed the Escrowed Encryption Standard (EES) as a solution that attempts to balance the privacy and security needs of American citizens and business with the needs of U.S. law enforcement and national security. It has been controversial from the day it was proposed. There are various competing viewpoints. Civil libertarians view privacy protection as fundamental while law enforcement officers are concerned over criminal use of encryption. National security needs are for continued excellence in communications intelligence, and for effective protection of the civilian information infrastructure. U.S. undustry wants to be allowed to energetically compete in the world marketplace. In the next chapters of this report, we present these views.

Notes

1. Private communication with Lewis Branscomb on March 22, 1994. Branscomb was IBM's liason with U.S. government intelligence agencies from 1972 -1986.

2. Strong cryptographic algorithms are ones that are exceedingly difficult to break by all attacks, including exhaustive search over the entire key space.

3. The Treasury Directive on Electronic Funds and Securities Transfer Policy – Message Authentication (TD81-80) makes it Department of Treasury policy that all Federal EFT transactions be "properly authenticated." The authentication measures adopted in TD81-80 are those recommended by the American National Standards Institute (ANSI) in Standard X9.9. In addition, authentication equipment must comply with FIPS 140-1 regarding minimum general security requirements for implementing the Data Encryption Standard (DES) algorithm. Key management standards are based on ANSI X9.17 [USDoT, pg II-1].

4. A typical commercial RSA chip, the Cylink CY1024, can encrypt a thousand-bit number in about one tenth of a second — a throughput rate of ten kilobits. By comparison, the AMD9518 DES chip can encrypt data at approximately fifteen megabits.

Diffie-Hellman Key Exchange

Diffie-Hellman key exchange is a public-key technique that takes advantage of the fact that it is easy to compute powers in modular arithmetic, but very difficult to extract logarithms. If y is the xth power of b, modulo p:

$$y = b^x \pmod p$$

where b is a suitable base number, then, as in ordinary arithmetic, x is the logarithm of y to the base b, modulo p:

$$x = \log_b y \pmod p$$

Calculation of y from x is easy, but computing x from y is difficult. In the following illustration using exponential key exchange to establish session keys, the equipment being used to carry out the key distribution is personified as Alice and Bob, just as if the users were doing the computing in their heads.

The base b is known to both users. To initiate communication, Alice chooses a random number: A. She keeps A secret, but sends:

$$b^A \pmod p$$

to Bob. Bob in turn chooses a random number, B, and sends the corresponding b^B to Alice. Both Alice and Bob can now compute

$$b^{AB} \pmod p$$

and use this as their key. Bob computes b^{AB} by raising the b^A he obtained from Alice to his secret power B:

$$(b^A)^B \pmod p = b^{AB} \pmod p.$$

Similarly, Alice obtains $(b^B)^A = b^{AB}$. Only Alice and Bob know the secret value b^{AB}. There is no known way for anyone who does not know either A or B to compute b^{AB} without first attacking the difficult problem of taking the logarithm of b^A or b^B.

If p is a prime about 1,000 bits in length, only about 2,000 multiplications of 1000-bit numbers are required to compute the exponentiations. By contrast, the fastest techniques for taking logarithms in arithmetic modulo p currently demand more than 2^{100} (or approximately 10^{30}) operations. Even with today's supercomputers, it would take a billion billion years to perform this many operations.

Chapter 2

Integrating Cryptography

<table><tr><td>Vocabulary words:

Distributed system: A system in which there may be multiple processors, possibly geographically dispersed. Control is typically decentralized, and is coordinated among the various processors.
STU-III: Third generation of U.S. government secure telephones.</td></tr></table>

Why is cryptography important? The unique virtue of cryptography is that it provides security that does not depend on the characteristics of the channel through which the text passes. This makes it the only way of protecting communications over channels that are not under the user's control. Often it is the most economical way of protecting communications over channels that are.

Secure Telephony

Secure telephony gives an excellent example of cryptography's utility. No telephone user, even the government, can afford to secure the entire telephone system. The only way to provide a secure voice path between two telephones at arbitrary locations is to encrypt the words spoken into one and decrypt them as they come out of the other. Public key cryptography makes it possible for the two phones to agree on a common key known only to them without consulting any other party. The users simply establish the call, push a button, and wait a few seconds for the phones to make the arrangements.

Encryption assures the confidentiality of the phone call, but what assures its authenticity? In the simplest systems, the users must rely on voice recognition, just as with unsecured phone calls.[1] If the system must provide authentication to users who do not know one another, some central administration is required to issue cryptographic credentials by which each phone can recognize the other. Although such systems have been designed and built, lack of standards has limited purchasers of commercial systems to the products of a single manufacturer. Only the government's STU-III secure telephone system, which is inaccessible to the general public, offers such services on a large scale.[2]

The shortcoming of secure telephones is that they are expensive. In addition to the cryptographic devices, a secure phone must include a voice digitizer to convert speech to a form in which it can be encrypted and a modem to encode the digitized signal for transmission over the phone line. Currently, the least expensive secure phones cost over a thousand dollars apiece.

Secure Computer Communications: the Problems

Securing communications in a distributed computer system presents somewhat different problems. In data communication, there is no analogue of the voice recognition that plays such a valuable role in the telephone case. If authentication is to be available at all, it must be done by formal cryptographic procedures. This requires the computers to identify people or machines through long-term keys. The relationship between telephones, even secure telephones, is conceptually simple: they set up calls and transmit sound. The relationship between computers in a distributed system is considerably more complex: they permit their users to login remotely, and to share files. The networked machines routinely execute programs for each other. These wedded interactions complicate the process of protection and make computer break-ins difficult to prevent.

Systems owners are typically unwilling to make substantial investments in hardware or software for security purposes, although they may be willing to pay some premium for products that contain integrated security features.[3] Many vendors see software as the least expensive means of adding cryptographic security features to their products.

A secure mail system like Privacy Enhanced Mail (PEM) is the workstation analogue of a secure telephone; it encrypts and decrypts mail so the user can correspond privately. Unfortunately, a software implementation of PEM is vulnerable to penetration of the program including the compromise of its long-term keys. One of the ways in which penetrations occur is through the implanting of modified programs or other data into the user's working environment.[4]

An essential element in many distributed systems is the Remote Procedure Call, wherein one computer asks another to perform a task on its behalf. This primitive underlies the Network File System,[5] which permits computers to access files on remote disks as though they were locally available. One computer, the client, asks another, the server, to send it information, print a file, or perform a computation. Without authentication of the request, the server has no way of knowing that the client is entitled to the service requested. Without authentication of the response, the client has no way of knowing that the information returned is genuine.

Cryptography as Part of a Solution

Continuing our example, let us reexamine the secure mail program. The user at his workstation requests the PEM program from a server. If the network file system is not secure, an intruder can send a program that has all the functionality of PEM, and an additional dangerous one: when the user types in the password that decrypts his private key, the bogus PEM sends this key to the intruder.

If the communications between the workstation and the file server provide authentication, the copy of PEM received by the workstation is verified as being valid. This serves to protect the user against the broad class of attacks that involve substituting one file for another.

To provide this broad basis for protection, cryptography must be incorporated in the basic interactions of workstations and servers so that its capabilities are available when establishing communications between machines. It must be done in such a way that the cryptography cannot be easily compromised. Without trustworthiness in the operating system, cryptography embedded in an application is no panacea.

In a large company system, security facilitates moving sensitive applications from mainframes to more economical networked machines. Adding such sensitive applications as personnel, purchasing, or travel agency services to the system involves ensuring that the applications interoperate correctly with the system standards. If the underlying distributed system is not sufficiently secure, each of the sensitive applications must provide its own security, a more cumbersome and risky way to solve the problem. Nonetheless, some applications, such as E-mail, will require specific security measures in addition to underlying system security facilities.

The Cryptography Market

The cryptographic market is paradoxical. It is easy to build a case for buying cryptography futures. The number of tasks that can be done by computer is growing by leaps and bounds. Many of these either involve substantial sums of money or confidential information about individuals, business plans, etc. Cryptography's supporters have been predicting an explosion in the market for more than twenty years.[6] Nonetheless, cryptography remains a niche market in which (with the exception of several hundred million dollars a year in government sales by a few major corporations) a handful of companies gross only a few tens of millions of dollars annually.

The arguments for the importance of cryptography and the brightness of its future remain as strong as ever: the cost of cryptography is declining, information products have become a major industry, and the popularity of (vulnerable) wireless communications is increasing. Attempts to explain the apparent discrepancy point to the government's failure to carry through on the standards thrust begun in the mid-seventies and the effect of the export-control regulations. Selling cryptography, however, is selling insurance against a loss (being spied on) that is hard to detect. It may be that users find the inconvenience of add-on products, complexities of key management, and complications of competing standards unacceptable, and are waiting for seamlessly integrated cryptographic capabilities. It may simply be that although the price is dropping, it has not yet dropped far enough. Or it might be that the need for such insurance has not yet become manifest.

Notes

1. A technical trick is used to guarantee that an intruder has not snuck in by participating in the key setup process. The phones display a checksum of the key, and the users verify that their phones are in agreement. The only way for the intruder to fool them is to intercept the part of the call in which the first caller says, "My display reads: '3C6E' " and change it to "My display reads: '5A00' " so that the second caller, whose display reads 5A00, will assume that the two displays agree. That would require the interceptor to alter the conversation in real time, a challenge that is probably insurmountable at present. For example, see the explanation of the Diffie-Hellman Key Exchange at the beginning of this chapter. This is a public-key encryption method used for secure telephones.

2. In fact, STU-III users are encouraged, if not expected, to rely on voice authentication too, since many organizations do issue keys which are not unique to the individual.

3. NSA's Mosaic system, employing the CAPSTONE cryptographic chip in a 'Tessera' PCMCIA card is an attempt to make this approach economical. See Chapter 7.

4. This was a technique used by the Morris Worm of November 2, 1988, which attacked at least two thousand of the six thousand BSD UNIX computer systems on the Internet. It caused administrators to disable some Internet network connection sites for two or three days [SSSC, pg. 64].

5. The widely used NFS was developed at Sun Microsystems in the early 1980s.

6. An early false prophet in this respect is a panel member, Whitfield Diffie, inventor of the concept of public key cryptography. In reports in 1978 [Diff-78] and 1979 [Diff-82] he predicted that it would become ubiquitous by the mid-1980s.

Chapter 3

A Law Enforcement View of Encryption: The Problems

> Vocabulary words:
>
> Electronic bug: A minature electronic device that overhears, broadcasts, or records a speaker's conversation.
>
> Electronic communication: Any transfer of signs, signals, writing, image, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photoelectric or photooptical system.
>
> Electronic surveillance: The interception of oral, wire, or electronic communication.
>
> Wiretap: The interception of wire or electronic communication.

Technology causes a constant rearrangement in the relationship between the criminal and the law. The advent of telecommunications enabled criminals to execute their plans more covertly. Once law enforcement learned how to listen in, officials could obtain information without placing themselves in danger. Wiretapping is a tool that diminishes the value of communications to criminals; cryptography is its potential counter.

Wiretaps and the Law (pre-1968)

The Civil War demonstrated the value of eavesdropping on an opponent's telegraph communications; afterwards, law enforcement adopted wiretapping as a tool against crime. Its legality was unclear: some states passed legislation permitting wiretapping; others ignored it. The first Federal statute appeared in 1918, and permitted wiretapping during the First World War. Its use was restricted to counterespionage purposes. After the war, Federal agents used wiretaps to enforce Prohibition. This was challenged, and in 1928, a closely divided Supreme Court ruled in Olmstead v. United States [Olm] that the Fourth Amendment protected tangibles only, that conversation was an intangible, and that evidence from wiretaps did not constitute an unconstitutional search. Because a majority of the Justices believed no violation of the Fourth Amendment had occurred, they further posited that there was no compelled self-incrimination and consequently no violation of the Fifth Amendment.

Justice Brandeis dissented. He eloquently argued that the right "to be let alone" by the government included such intangibles as conversation; in his view, the Fourth Amendment required a search warrant if a wiretap was to be used. In 1934 the Federal Communications Act (FCA), containing provisions prohibiting the interception and divulgence of wire or radio communications, was enacted. Through a series of cases, the Supreme Court ruled that information gained from wiretapping was not admissable as evidence in court.

The Second World War changed the stakes, and President Roosevelt authorized wiretapping of foreign agents to protect the nation. Meanwhile, the Court treated searches using electronic bugs differently from those using wiretaps.

In 1942, in Goldman v. United States [Gold], law enforcement officers placed a bugging device against a wall of an office adjacent to the suspect. The Supreme Court held that the FCA did not apply, as there were no "communications" or "interceptions" as defined by the statute. The Court ruled that absent physical trespass, searches employing electronic bugs were allowed under the Fourth Amendment. Later cases maintained this distinction. In 1954, in Irvine v. California [Irvi], the Court upheld a state court conviction based on evidence obtained by microphones concealed in walls of the defendants' homes. But in 1961, in Silverman v. United States [Silv], the Court ruled inadmissable evidence that had been obtained via a spike mike that had been driven through the wall of an apartment adjacent to that of the defendant. It was the beginning of a change.

In 1967, the court dropped the distinction between searches conducted through wiretaps and those conducted through electronic bugs. That year, in Katz v. United States, the Court held that there was reasonable expectation of privacy in using a public phone booth, the public nature of the booth notwithstanding. The Fourth Amendment applied, and a search warrant was needed. The Court abandoned a protection of places in favor of a protection of people; specifically, what was to be protected was the privacy of the person and his or her communications.

The Katz decision led to the current Federal wiretapping statutes. In 1968, organized crime was considered a serious national problem, and several Congressional and Executive Branch studies had concluded that the impenetrability of these criminal groups made electronic surveillance – both wiretapping and bugs – a necessary tool for law enforcement.[1]

Wiretaps and the Law (1968 and after)

In 1968, the Omnibus Crime Control and Safe Streets Act[2] was passed; Title III of the Act established the basic law for interceptions performed for criminal investigations. Wiretaps are limited to the crimes specified in Title III; this list includes murder, kidnapping, extortion, gambling, counterfeiting, and sale of marijuana.

Electronic surveillance does not come cheap: in 1993, the average cost of installing a wiretap and subsequently monitoring it was $57,256 [AO-93]. A court order is required for the installation of a tap. The investigator draws up an affidavit showing there is probable cause to believe that the targeted communications device – whether phone, fax, computer – is being used to facilitate a crime. The crime must be serious and indictable. A government attorney must prepare an application for a court order, and approval must be by a member of the Justice Department no lower in rank than Deputy Assistant Attorney General. The application must be decided upon by a Federal District Court Judge.

In order for a judge to approve a wiretap order, he must determine that (i) there is probable cause to believe that an individual is committing, or is about to commit, an indictable offense; (ii) there is probable cause to believe that communications about the offense will be obtained through the interception;

(iii) normal investigative procedures have been tried and have either failed, or appear unlikely to succeed, or are too dangerous; and (iv) there is probable cause to believe that the facilities subject to surveillance are being used, or will be used, in the commission of the crime. Such requirements may be waived in an emergency, if an application for a court order is made within forty-eight hours. Any oral or wire communication intercepted in violation of Title III cannot be divulged.[3]

When a court order for a wiretap is approved, it is taken to the communications service provider for execution. Under Title III, the provider is required to assist in discharging the wiretap, and the provider is compensated for all expenses. Taps are approved for at most thirty days, with any extension needing a new court order.

Based on Title III, thirty-seven states have passed statutes permitting wiretaps by state and local law enforcement officers for criminal investigations. By law, state acts must be at least as restrictive in their requirements as the Federal code; many are more so. Applications for wiretap orders at the state level are handled similarly to Federal ones.

Much data is kept on electronic surveillance – duration, number of persons intercepted, type of surveillance used, etc. – for a variety of reasons, including the importance of having a careful record for legislators conducting oversight.

Since 1968, when Title III was passed, there have been an average of approximately nine hundred Federal and state wiretaps annually. The number of conversations intercepted has increased, the number of nonincriminating conversations intercepted has increased; the number of incriminating conversations intercepted has remained the same. The arrest level has remained unchanged. More specifically, in data released by the Administrative Office of the U.S. Courts, the average annual number of incriminating conversations intercepted between 1968 and 1993 has remained between two and four hundred thousand, while the number of intercepted conversations has shown a steady increase from roughly four hundred thousand in 1968 to over 1.7 million in 1993. In 1993, for example, there were 976 court-ordered electronic surveillance orders, which resulted in the interception of 1.72 million conversations. By the end of 1993, there were over two thousand arrests as a result of this surveillance [AO-93].[4]

The Foreign Intelligence Surveillance Act, Title 50 USC,[5] authorizes electronic surveillance for foreign intelligence. This act governs wire and electronic communications sent by or intended to be received by United States persons who are within the United States. (A U.S. person is defined to be a U.S. citizen, a permanent resident alien, or groups of such people.) FISA does not cover intercepts of U.S. persons who are overseas (unless the communications are with a U.S. person resident in the U.S.). Under FISA provisions, U.S. citizens could be subject to surveillance if they are aiding and abetting international terrorism.

A court order is normally required for a FISA wiretap, but there are two exceptions. Following a declaration of war, the President, through the Attorney General, can authorize a wiretap for foreign intelligence purposes for up to fifteen days without a court order. The other exception can occur if the communications are exclusively between foreign powers or involve intelligence other than spoken communications from a location under the exclusive control of a foreign power.

FISA wiretap orders are granted by a special court, consisting of seven judges appointed by the Chief Justice of the United States. Applications for a court order are made by a federal officer, and require approval by the Attorney General. Semiannually the Attorney General must inform the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence of all wiretap activity. Although information on FISA wiretaps is classified, the Attorney General is required to give the Administrative Office of the United States Courts an annual report on the number of FISA applications and orders. Since 1979, there have been an average of slightly over five hundred FISA wiretap orders annually [AG-FISA].[6] As of 1988, over four thousand requests had been made by the government for surveillance under FISA; none had been turned down [Cinq].

Wiretaps as a Tool of Law Enforcement

The law enforcement community views wiretaps as essential. Such surveillance not only provides information unobtainable by other means; it also yields evidence that is considered more reliable and probative than any that can be secured by other methods of investigation. Members of the law enforcement community argue that wiretapping is indispensable in certain cases [Freeh, pg.7].

According to the FBI, the hierarchy of the Cosa Nostra has had severe setbacks due to the use of electronic surveillance [Freeh, pg.8].[7] Almost two-thirds of all court orders for wiretaps are for drug cases; the FBI believes the tool is essential in those situations [Denn]. With the help of wiretaps, an FBI investigation into the importation and distribution of $1.6 billion of heroin by the Sicilian Mafia and the Cosa Nostra resulted in the indictment of 57 high-level drug traffickers in the United States, and five in Italy [Denn]. FBI Director Louis Freeh recently testified to Congress about an organized crime scheme to skim gasoline excise taxes, foiled by evidence obtained through wiretaps. Fourteen individuals have been charged with defrauding the governments of the United States and New Jersey of $60 million in tax revenues; four convictions have occurred to date [Freeh, pg. 16].

Wiretapping is an important investigative technique in cases where the crime is partially hidden. In cases of governmental corruption, such taps are often the only way to uncover aspects of the crime as well as the participants in it. The recent procurement scandal, "ILL-WIND," involving members of the Department of Defense and military contractors, has led to sixty-four convictions and $271 million in fines, restitutions, and recoveries ordered; according to law enforcement critical evidence was uncovered through wiretaps [Denn]. The detection of other forms of governmental corruption may also rely on wiretaps: John Kaye, Prosecutor for Monmouth County, New Jersey, reported that wiretap evidence accounted for almost every police officer who has been indicted in the county [Kaye]. In a recent case of Medicare/Medicaid fraud seventy-nine individuals were convicted or pleaded guilty; much of the evidence came from wiretaps [Freeh, pg. 15].

Nonetheless, it is difficult to prove the efficacy of wiretapping. There is no way to know in every case what ultimately led to a conviction. Although hearing a defendant participate in criminal conduct undoubtedly influences a jury, it may be impossible to know what would have occurred without that particular evidence.

In the period 1985-1991, the FBI reported that court-ordered taps conducted by the Bureau formed part of the evidence that led to 7,324 convictions, almost $300 million in fines levied, and over $750 million in recoveries, restitutions, and court-ordered forteitures [Denn]. Since the FBI conducts fewer than one-third of the non-FISA wiretap cases, it can be assumed that the numbers above would be substantially higher if all such surveillance were taken into account.

While the number of taps is small, many people in the law enforcement community view wiretaps as essential to effective law enforcement. The FBI argues that such surveillance attacks the captains of the crime industry, goes after government corruption, and performs important antiterrorist functions. Not surprisingly, the law enforcement community views with great trepidation the introduction of nonescrowed strong cryptography into public electronic communications systems.

Technology and the Ability to Tap

Off-the-shelf encryption technology may provide an easy way for lawbreakers to foil criminal investigative work. Even with a court order, law enforcement investigators might find it impossible to "listen in" to criminals' communications. The law enforcement community has already expressed concern that technological developments will impede its ability to intercept communications. In March 1992, the FBI prepared a Digital Telephony proposal for Congress; the proposal would have required providers of electronic communications services to ensure that advanced switching technology would not hinder the government in conducting legally authorized wiretap searches. A new proposal was submitted in March 1994; the Digital Telephony proposals are discussed in more detail in Chapter 6.

Cryptographic protection of communications presents a difficult problem for the law enforcement community. Neither they nor computer security experts in academia and private industry advocate easy-to-break cryptography as a solution. So much economic activity occurs through electronic networks that weak cryptographic schemes – whether for banks, airlines, hospitals, or corporations – would seriously endanger the United States. The Willie Sutton model suggests that today's malicious hackers will be followed by professional criminals. Considered from a law enforcement perspective, what is needed is strong cryptography that protects the nation's communications infrastructure but that does not simultaneously imperil the government's ability to comprehend intercepted communications – when law enforcement comes armed with a court order.

Notes

1. The history of wiretap is based on information from [NWCCS].

2. This is 18 USC §2510-21.

3. However, electronic communications intercepted in violation of Title III may be received in evidence (18 USC §2515).

4. Under Title III requirements, all electronic-surveillance court orders must be reported upon – even if the surveillance was ultimately not undertaken. However not all reports are filed. In order to determine the number of intercepted calls for 1993, we used 959 as the number of electronic-surveillance orders. This was derived from 976 (= number of court authorizations for electronic surveillance) - 17 (= number of surveillances that were never installed).

5. This is the Foreign Intelligence Surveillance Act, Title 50 USC §1801-1811.

6. The discussion of current wiretap law is based on information from [DDKM].

7. Although not all electronic surveillance takes the form of wiretaps, the vast majority of electronic-surveillance court orders are for telephone wiretaps. For example, in 1993, there were 976 authorizations for electronic surveillance. Prosecutors did not submit reports on 21 of those cases, and there were also 17 court-authorized orders which did not result in electronic surveillance. Of the remaining 938 court authorizations, there were: 679 telephone taps, 55 electronic bugs, 141 electronic taps, and 63 combination taps [AO-93, pg. 21]. However, many important cases that used electronic surveillance rested on evidence obtained through electronic bugs and not through wiretaps; the John Gotti [Blum] and John Stanfa [Caba] cases are two such examples.

Chapter 4

A National Security View of Encryption: The Complexities

Vocabulary words:
Dual-use technology: Technology which has both military and commercial applications.
Real-time system: A real-time system is a system in which operations are expected to complete by specified deadlines.

In the context of national security, public availability of strong cryptography is a double-edged sword. Strong cryptography protects U.S. commerce and enhances U.S. products; economic strength is critical for national security. But foreign accessability to strong cryptography compromises communications intelligence. Any decision about dual-use technology is a judgment about balancing risks.

Telecommunications Transformed Government

The development of telecommunications in the 19th century, first via cable and later by radio, presented a challenge to national security so severe as to challenge the very notion of national sovereignty. Nations could still regulate the flow of people and products across their borders, but in a process that continues unabated, news, ideas, and information began to travel in channels far harder to control.

National states survived, of course. They acquired a degree of control over the new media and found that decreased control over the flow of information was more than made up for by increased control over far-flung possessions. Telegraph cables bound the British Empire together as the famous roads had bound the Roman Empire.

Telecommunications transformed government, giving administrators immediate access to their employees and representatives in remote parts of the world. It transformed commerce, facilitating worldwide enterprises and beginning the internationalization of business that has become the byword of the present decade. It transformed warfare, giving generals the ability to control large theaters of battle and admirals the ability to control fleets scattered across oceans.

So great was this impact that the interception and analysis of enemy communications had become an indispensable component of intelligence by the time of World War I. The organizations that resulted have grown steadily throughout the century, providing governments with information about the political, commercial, and military activities of friends and foes alike.

Communications Intelligence

Communications intelligence is a complex art, and the sheer volume of modern communications makes intelligence a constant struggle against limited resources. Networks must be mapped. Intercept facilities must be established. The most important channels must be targeted. And just the right messages must be selected from the flood of traffic that passes through the channels. It is only at this point that the familiar part of the process begins: messages must frequently be stripped of their protective encryption before intelligence evaluation can begin.

Those who think about the vulnerabilities of communications from the viewpoint of security frequently regard cryptography as the only substantial barrier to communications intelligence. In fact, the process of communications intelligence is fragile; anything that complicates the targeting of messages can diminish its effectiveness dramatically. An opponent who becomes aware of the degree to which his or her communications are being exploited (or worse, learns how the exploitation is being done) may make changes that render the process far more difficult and destroy years of intelligence effort. As a result, the field is characterized by secrecy even greater than that surrounding nuclear weapons.[1]

The growth of communications intelligence has been accompanied by a similar growth in techniques for protecting communications, particularly cryptography. What is not widely appreciated, however, is that despite the remarkable developments of cryptography, the communications intelligence products are now better than ever. In the recent past, there has been a migration of communications from more secure media such as wirelines or physical shipment to microwave and satellite channels; this migration has far outstripped the application of any protective measures. Consequently, communications intelligence is so valuable that protecting its flow by keeping secret both the intelligence technology itself and techniques for protecting communications is an important objective of U.S. national security policy.

Communications Security

The United States may be the greatest beneficiary of communications intelligence in the world today, but it is also its greatest potential prey. Perhaps no country is more dependent on electronic communications or has more to lose from the subversion of its commerce, its money, or its civic functions by electronic intruders. The protection of American communications against both spying and disruption is therefore vital to the security of the country. It is a major objective of U.S. national security policy.

The two objectives are hardly in harmony. Protecting American communications as a whole, rather than just the most sensitive government communications, requires wide deployment of cryptographic technology, whose availability to opponents could damage American intelligence capabilities. On the other hand, making such technology generally available in the United States, without making it available abroad as well, appears difficult if not impossible.

The first attempts to improve overall security in American voice and data communications were undertaken in the 1970s. Encryption devices were developed for protecting telephone switching information [Myer] and both analog [Ladn] and digital [Link] telephone trunks. Microwave links in areas such as Washington, New York, and San Francisco (where Soviet diplomatic facilities had easy access to U.S. communications) were either protected by encryption or replaced by underground cables.

In the most far-reaching component of this plan, a cryptographic algorithm developed at IBM and endorsed by the National Security Agency (NSA) was adopted as Federal Information Processing Standard 46 [FIPS46], the U.S. Data Encryption Standard. Several major electronics manufacturers and numerous minor ones began making DES-based equipment. For the first time, cryptographic protection of substantial quality became available in both hardware and software packages.

With hindsight, the intelligence community might consider the public disclosure of the DES algorithm to have been a serious error and one that should not be repeated. DES-based equipment became available throughout the world; crytographic principles revealed by studying the algorithm inspired new cryptographic designs; and DES provided a training ground for a generation of public cryptanalysts. The result was to make the task of America's intelligence agencies more difficult. This experience raised the issue that while strong cryptography is important for U.S. private interests, it should not come at the expense of American intelligence capabilities. Striking a balance between these two competing national security objectives is a daunting task that poses a serious challenge to those charged with protecting U.S. national security.

Export Control

National security experts argue that export control is essential if the U.S. is to protect its communications without affording protection to the rest of the world. The goals of U.S. export control policy in the area of cryptography are (i) to limit foreign availability of crytographic systems of strategic capability, namely, those capable of resisting concerted cryptanalytic attack; (ii) to limit foreign availability of cryptographic systems of sufficient strength to present a serious barrier to traffic selection or the development of standards that interfere with traffic selection by making the messages in broad classes of traffic (fax, for example) difficult to distinguish; and (iii) to use the export-control process as a mechanism for keeping track of commercially produced cryptosystems, whether U.S. or foreign, that NSA may at some time be called upon to break.

The second goal is perhaps less obvious than the first and third and presents an intrinsic conflict between the needs of intelligence and the needs of private users of cryptography. At present, the vast majority of the world's communications are unencrypted. This makes it feasible to sort traffic in real time and determine which messages are of interest and which are not. Even a weak cryptosystem can be a serious obstacle to traffic selection, and the rise of international encryption standards (of even moderate quality) would make the task of traffic selection immeasurably more difficult.

Export control presents a conflict between the requirements of the government and the needs of users and developers of cryptography. Commercial enterprises argue that export control weakens American business and thus is not in the nation's strategic interest. The situation is not so simple. Some foreign markets of interest would not accept U.S. cryptographic exports were export controls to be lifted. For example, France does not permit the use of cryptographic products unless the algorithm has been registered with the French government. Private use of encryption technology is illegal in South Korea, Taiwan, and the People's Republic of China.[2] For a number of markets, the fact that the U.S. government restricts export of products containing cryptography has not had any real effect on U.S. manufacturers of secure systems.

Digital Signatures

Many commercial applications of cryptography, both domestic and international, depend not on cryptography's ability to conceal the content of communications, but on cryptography's ability to assure authenticity and integrity of the message. Digital-signature technology can therefore be applied to authenticate such transactions as electronic funds transfers without presenting a barrier to intelligence.

A second element of the U.S. cryptographic program is the Digital Signature Standard [DSS] (discussed further in Chapter 6) that does not lend itself to encryption and decryption of messages. Export of equipment using DSS can be permitted without posing a threat to traditional communications intelligence, and such equipment may eventually replace DES-based equipment technology for authentication.[3]

Key Escrow

With cognizance of the conflict between national security needs and civilian requirements, Congress in 1987 placed the responsibility for civilian encryption standards with the National Institute for Standards and Technology. (See Chapter 6 for a discussion of the Computer Security Act.) As is discussed in Chapter 3, there are governmental concerns about the impact encryption may have on law enforcement. At present, the centerpiece of government plans for securing the bulk of American communications is the key-escrow initiative, a plan for a cryptographic system that can be widely deployed without providing opponents, either at home or abroad, with systems that impede American law enforcement or intelligence capabilities.

The plan has two essential components. Rather than publishing a standard cryptographic algorithm, as was done with DES, the new technology will be made available only in tamper-resistant hardware. This will permit the U.S. to control distribution and hinder public study or imitation. Equally important, an alternative means of decryption in the form of an escrowed key will be available to guarantee that encrypted traffic can always be read when American interests require it.

Export of key-escrow equipment will be permitted, but both the secrecy of the algorithm and the U.S. government's possession of keys are expected to dampen the enthusiasm of those who might otherwise be tempted to employ it in a manner contrary to U.S. interests. This will minimize the likelihood as well as the danger of uncontrolled foreign distribution. Authorized accessibility of the traffic will also serve the interests of such vital national security functions as domestic counterintelligence.

There have been concerns that use of key-escrow technology will result in isolation of U.S. commercial interests. However, other nations are also pursuing key-escrow technology. Nations in the European Community are considering a more complex version of key escrow using multiple keys. If implemented, this would allow government interception capabilities only for communications which originate or terminate within that nation, while simultaneously protecting the communicators against interception by all other intruders.[4]

Prospects for the Future

A proper understanding of U.S. national security policy in the area of cryptography requires recognition that it is a dynamic policy formulated to deal with a dynamic problem.

The growing importance of information as a commodity (entertainment, computer software, customer databases, etc.) and the worldwide expansion of radio-based mobile systems (cellular telephones and direct satellite communications) promise an enhanced flow of communications intelligence. If the most advanced cryptographic techniques are applied indiscriminately, however, the promise of improved or expanded communications intelligence will go unfulfilled.

Ultimately, cryptography capable of defeating today's cryptanalysis may become widely deployed, but for national security it is a critical matter whether this happens sooner or later. Improved analytic methods, together with such technologies as field-deployable cryptanalytic equipment, improved emitter identification, and computer penetration (if legally permissible) might provide continued access. National security experts emphasize the importance of continuity in communications intelligence. Making the opening break into a protected communication system is usually far more difficult than tracking technological changes in an already penetrated one. If the fruits of communications intelligence are sacrificed to an excessive zeal for security in the private sector, it may be a long and costly task to regain them.

Notes

1. That the security of communications intelligence exceeds that of nuclear weapons is apparent from the difference in both the clearances and the public literature. Access to most classified nuclear information requires a Department of Energy Q clearance, which lies roughly between the Department of Defense (DoD) Secret and Top Secret clearances. Access to communications intelligence requires a DoD Top Secret clearance with "Special Intelligence" indoctrination, a process that includes a "lifestyle polygraph."

   Despite its secrecy, nuclear strategy and technology are the subject of an extensive academic literature. The public-policy literature on communications intelligence and its technology is by comparison nonexistent.

2. Private communication with James Burrows on March 11, 1994. Burrows is Director of the National Computer and Telecommunications Laboratory at NIST.

3. The International Traffic in Arms Regulations (ITAR) has jurisdiction of all software with data encryption capability EXCEPT commercial software with encryption limited to these functions: (i) decryption-only, (ii) access control and Message Authentication Code (MAC), (iii) functions restricted to protecting passwords and personal identification numbers (PIN), (iv) specifically designed and limited to the issuance of cash or traveler's checks, deposits, etc., and (v) software for personalized smart cards.

   Commercial software with encryption capability limited to the above functions has been transferred to Commerce's jurisdiction. Software that performs encryption functions other than those listed above is presumed to be under the jurisdiction of ITAR and the State Department.

4. Burrows, telephone conversation.

Chapter 5

The Privacy View : The Importance of Encryption

Of all the differences between democracies and totalitarian states, one of the most fundamental is the right to privacy. The "right to be left alone" is at the core of American life. Cryptography enables people to protect their communications. Civil libertarians view availability of strong cryptography as necessary to the ability to communicate privately in an electronic world.

Attacks on Privacy

Protecting our privacy rights is a constant struggle. Businesses (including credit bureaus, insurance companies, and direct marketers) collect and maintain a vast amount of information about individuals. In order to "protect individuals from the adverse effects of unfair information practices in the consumer-reporting industry," Congress in 1970 enacted the Fair Credit Reporting Act.[1] But the proliferation of electronic databases has only exacerbated these problems.

There are now over five hundred companies that buy and sell data about Americans. The public is concerned with its privacy. For example, Lotus and the Equifax credit bureau were developing a CD-ROM that would contain the names, estimated incomes, purchasing habits, and other data of 120 million Americans. Public response was thirty thousand letters against the product – and the project was killed before it reached the marketplace [Pill, pg. 11].

Despite abuses by the private sector, civil-liberties groups view government abuse of privacy with even greater concern. The government is more powerful than the credit bureaus, insurance companies and direct marketers. In its attempt to ensure the safety of its citizens, the government can overstep boundaries of the rights of the individual.

The privacy of Japanese-Americans was not respected during World War II. Although the charter of the Census Bureau states that "in no case shall information furnished under the authority of this act be used to the detriment of the person or persons to whom such information relates," under Executive Order 9066, 112,000 people of Japanese ancestry were taken from their homes on the West Coast and placed in internment camps, with census data providing the information to locate them. The privacy of Martin Luther King was not respected during the 1960s; the FBI regularly taped King's conversations. The privacy of Americans was not always respected by the National Security Agency. In the report of the Church Committee, the Senate Select Committee to Study Governmental Operations with respect to Intelligence Activities, the NSA was cited for conducting surveillance of U.S. people: (i) "From 1947 until May 1975, NSA received from international cable companies millions of cables which had been sent by American citizens in the reasonable expectation that [the contents of the cables] would be kept private," [USS. pg. 12]; (ii) " ... in the 1960s NSA began adding to its watch lists ... the names of Americans suspected of involvement in civil liberties " (pg. 104); (iii) "Communications such as ... discussion of a peace concert; the interest of a Senator's wife in peace causes; a correspondent's report from Southeast Asia to his magazine in New York [were stored in Government files]" (pg. 108). As a result of these illegal activities, legislation, executive orders, and regulations were instituted to eliminate future such occurrences.[2] Civil libertarians note, however, the Church committee's finding that the "surveillance which we investigated was not only vastly excessive in breadth ... but was also conducted by illegal or improper means ... [there was] frequent testimony that the law, and the Constitution were simply ignored" [USS, pp. 12-13].

Privacy and the Government

The underlying principle behind the Bill of Rights was that the government is powerful while the individual is weak. The signers sought to protect the individual against intrusions by the state, as exemplified by the Fourth Amendment ("The right of the people to be secure in their persons, house, papers and effects against unreasonable searches and seizures shall not be violated; and no warrants shall issue but upon probable cause ...") and the Fifth ("No person shall ... be compelled in any criminal case to be a witness against himself ...").

For the first seventy-five years of the American experiment, changing technologies had little impact on individuals' privacy. Records were in longhand. Distances were great. Government surveillance was accomplished no more easily in 1850 than it had been in 1776. By 1928, the situation had changed.

Olmstead and other defendants were arrested and charged with violating the National Prohibition Act [Olm]. Evidence had been obtained through a phone tap placed by Federal agents who lacked a court order. The defendants pleaded they had been subjected to an "unreasonable search and seizure." The Supreme Court disagreed. Justice Louis Brandeis, in a famous dissent, agreed with the defendants:

> When the Fourth and Fifth Amendments were adopted, 'the form that evil had heretofore taken' had been necessarily simple. Force and violence were then the only means known to man by which a government could directly impel self-incrimination ... Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendment by specific language ... But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> Moreover, "in the application of a Constitution, our contemplation cannot be only of what has been, but what may be." The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home ...

> Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping [Olm, pp. 570-571].

Almost forty years later, Brandeis's dissent underlay the Supreme Court opinion overruling Olmstead. In 1967, in Katz v. United States, the Supreme Court recognized that there was a "reasonable expectation of privacy" in making a phone call – even if the call were at a public phone booth. The court held that a search warrant was required for wiretapping [Katz].

Privacy rights are one of the individual's most potent defenses against the state. Privacy rights of the individual are embedded in the Fourth and Fifth Amendments. They are embedded in the Katz decision. Brandeis observed that privacy lies at the heart of Constitutional freedom:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and his intellect ... They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized man ... [Olm, pg. 752].

Privacy is also of the heart. Citizens of the former East Bloc countries testify to the corruption of society that resulted from a loss of privacy. In East Germany, the pervasive collection of information about individuals led to an inability to trust human relationships on even the most intimate levels [Kinz]. The United States is a very different nation, with a very different history. Nonetheless, loss of privacy occurs here, sometimes in small ways, sometimes unnoticed, but together these losses change the fabric of society [Abra].

Sometimes privacy is traded for convenience. We are captured on video recordings as we shop; we leave behind electronic chronicles as we charge phone calls. We pay for milk and bread via an ATM withdrawal at the supermarket, and we leave a record of our actions where five years ago we would have left a five-dollar bill. Sometimes it is traded for safety. Each day hundreds of thousands of people pass through metal detectors to get on airplanes. Most people consider those intrusions of privacy well worth the assurance of greater public safety.

The emerging technologies of the Information Age are revolutionizing the ways in which people exchange information and transact business. Much constitutionally protected activity – political, social, cultural, financial – will soon occur electronically. Regardless of the ease and availability of encryption, many electronic communications will not be encrypted. But many people would prefer to keep other interactions, from social to financial, private. Government and citizenry agree that as the nation faces such technological challenges as the National Information Infrastructure, electronic communications require privacy protection. A split arises in how much protection is needed, and what kind.

One of the concerns raised by the American Civil Liberties Union and Computer Professionals for Social Responsibility is that governmental attempts to limit the use of cryptography, whether through force of law, or through more subtle efforts such as market domination, can result in a serious erosion of the rights to privacy. It has been pointed out that the Fifth Amendment's protection against compelled self-incrimination creates a substantial obstacle in the prosecution of criminal activity, yet the Amendment remains a valued part of American jurisprudence. No law can guarantee that a subpoena or search warrant will result in the revelation of the contents of a private message.

Civil-liberties groups believe that constitutional protections need to keep pace with new technology. They argue that government action should not weaken the privacy protection a citizen can use, and that Americans should enjoy the ability to protect communications by the strongest means possible, including the best commercially available encryption.

In any society, laws build on what came before. In the next chapter, we present an overview of cryptography policy during the last two decades.

Notes

1. HEW Advisory Committee on Automated Personnel Data Systems, Records, Computers and the Rights of Citizens, 1973, pg. 69.

2. These include the Foreign Intelligence Surveillance Act, and Executive Order 12333, which restrict NSA's activities targetting U.S. persons. In addition, oversight processes were established: President's Intelligence Oversight Board, DoD Intelligence Oversight, Attorney General's Office of Intelligence Policy and Review, Senate Select Committee on Intelligence, and House Permanent Select Committee on Intelligence.

Chapter 6

Cryptography in Public: A Brief History

Cryptography is being debated in public – again. The particular confluence of events – the worldwide availability of strong cryptosystems (including DES and RSA), the accessability of computer networks, and the Escrowed Encryption Standard – is new, but as cryptography has evolved from a military tool to a corporate product, many policy issues have been discussed and resolved. Reinventing the wheel is poor engineering; it is even worse in public policy. The current discussion of cryptography needs to be placed in context.

The overriding conflict is the same as it has been for two decades: Who should make the policy decisions for civilian cryptography? Before commercial and academic groups became active in developing cryptography, the area "belonged" to the National Security Agency. Twenty years ago, conflicts over control of cryptography arose. In 1987, Congress passed the Computer Security Act, legislating that decisions about civilian computer security (including cryptography) would be made by a civilian agency. Seven years later Computer Professionals for Social Responsibility (CPSR) and various industrial organizations believe the NSA dominates civilian cryptography policy, a charge members of the defense agency dispute. This chapter presents a brief review of the last twenty years of cryptography in the public domain. The story has several strands, which we have separated into sections: (i) The Government's Standard: DES; (ii) Cryptography Research in the late 1970s : The Emerging Conflict; (iii) The Mid-Eighties: the Computer Security Act; (iv) the Digital Signature Standard; and (v) Securing the Communications

Infrastructure: Digital Telephony and EES.

The Government's Standard: DES

Our history begins in the mid-seventies. The Federal government sparked the encryption controversy when in 1975, the National Bureau of Standards (NBS) proposed a Data Encryption Standard (DES). What the Bureau published in the Federal Register was an IBM design with changes recommended by the NSA, including a shorter key length (56 bits).

A public comment period followed. Concern centered on whether the key length left the algorithm vulnerable to attack and whether the algorithm contained a trapdoor. Finally in 1977, DES (with a 56-bit key) was issued as a Federal Information Processing Standard (FIPS); the standard has been subject to a review every five years. It was recertified in December 1993.

Only recently – nineteen years after DES was introduced – have any attacks short of exhaustive search threatened the security of the algorithm [Mats, BiSh]. As discussed in Chapter 1, DES is used in a broad array of applications.

Cryptography Research in the late 1970s : The Emerging Conflict

In the mid-seventies Whitfield Diffie and Martin Hellman at Stanford were wrestling with two problems:

* Key distribution: In the absence of a secure method to exchange information, how do two distant parties exchange keys?

* Digital signatures: Could a method be devised so as to provide the recipient of an electronic message a way of demonstrating that the communication had come from a particular person?

This led to public-key cryptography and the RSA algorithm (described in Chapter 1).

The RSA algorithm attracted interest from a number of circles. Ronald Rivest planned to present the work at an IEEE conference in Ithaca, New York. Before the conference, the authors received a letter from one "J.A.Meyer," who warned that since foreign nationals would be present at the scientific meeting, publication of the result was a potential violation of the International Traffic in Arms Regulations.

On lawyers' advice, the MIT scientists halted distribution of their paper so that the matter could be reviewed. Meyer was identified as an employee of

NSA; the Agency promptly disavowed his letter. Rivest presented the paper. The scientists resumed distribution, and the furor died down for the moment.

The following year brought a new incident and greater apprehensions. This time NSA involvement was official. The Agency requested a secrecy order on a patent application submitted by George Davida, a professor at the University of Wisconsin; this meant that Davida could not publish or discuss his research. After Davida and the University of Wisconsin chancellor publicly protested, the secrecy order was lifted.

In 1979, the director of the NSA went public with the Agency's concerns. In a speech at the Armed Forces Communications and Electronics Association Admiral Bobby Inman warned that open publication of cryptography research was harmful to national security. NSA would seek statutory authority limiting publication of crytographic research unless a satisfactory solution could be found.

The American Council on Education formed a study group that recommended a two-year experiment in prepublication review by NSA of all cryptography research [PCSG]. Review would be voluntary and prompt. Despite the voluntary nature of the review, there was anxiety in the academic cryptography community that this process would have a chilling effect on the emerging field.

Meanwhile there was action on a third front: funding. Two agencies were responsible for funding cryptography research: NSA and the National Science Foundation (NSF), the organization responsible for support of "basic" research. When Adleman submitted a research proposal to the NSF in the spring of 1980, the situation came to a head. NSA offered to fund the cryptographic portions of the grant; NSF declined. (NSF policy is to refuse to support work with alternative funding sources.) Adleman feared that NSA's requirement of prior review of research could lead to classification of his work. An agreement was reached at the White House: both agencies would fund work in cryptography.

Fourteen years later, the two-year experiment in prepublication review continues. However, researchers' fears about prior restraint and impounded research have eased. There have been times when an author, on NSA request, did not publish; there have been NSA suggestions for "minor" changes in some papers [Land, pg. 11]. But the requests have been few; the academic community has not felt imposed upon by the prepublication reviews. On one occasion, NSA apparently aided the academic community in lifting a secrecy order placed on a patent application. Shamir was one of the researchers involved, and he thanked "the NSA ... who were extremely helpful behind the scenes ..."[Land, pt. 12]. As far as the research community has been concerned, it is fair to say that there have been no long-term chilling effects.

The Mid-Eighties: The Computer Security Act

The concerns of the 1970s – government interference in the development of publicly available cryptography – seemed to have been laid to rest. Then in September 1984, President Reagan issued National Security Decision Directive (NSDD-145), establishing the safeguarding of sensitive but unclassified information in communications and computer systems as Federal policy. NSDD-145 stipulated a Defense Department management structure to implement the policy: the NSA, the National Security Council, and the Department of Defense. There were many objections to this plan, from a variety of constituencies. Congress protested the expansion of Presidential authority to policy-making without legislative participation. From the ACLU to Mead Data Central, a broad array of industrial and civil liberty organizations objected to Department of Defense control of unclassified information in the civilian sector [USHR-87].

Congress responded. In 1987 it passed the Computer Security Act (CSA), which:

> ... assign[s] to the National Bureau of Standards responsibility for developing standards and guidelines to assure cost-effective security and privacy of sensitive information in Federal computer systems, drawing on the technical advice and assistance (including work products) of the National Security Agency, where appropriate.

Civilian computing standards were to be set by a civilian agency. NSA was placed in an advisory role. The legislative history of the Act makes that desire clear:

> The key question during the hearings was: Should a military intelligence agency, NSA, or a civilian agency, NBS, be in charge of the government's computer standards program? The activities of NSA ... reinforced the view of the Committee and many

> others that NSA is the wrong agency to be put in charge of this important program [USHR-87, pg.19].
>
> Since work on technical security standards represents virtually all of the research effort being done today, NSA would take over virtually the entire computer standards from the Bureau of Standards. By putting NSA in charge of developing technical security guidelines (software, hardware, communications), NBS would be left with the responsibility for only adminstrative and physical security measures – which have generally been done years ago. NBS, in effect, would on the surface be given the responsibility for the computer standards program with little to say about the most important part of the program – the technical guidelines developed by NSA [USHR-87, pg.95].

The House was specifically concerned that cryptography be allowed to develop in the public sector:

> ... NSA's secretiveness resulted in an inappropriate approach when it attempted to deal with national policy issues such as the issue of public cryptography. Historically, this science has been the exclusive domain of government, and in this country it is one of NSA's primary missions. However, with the advent of modern computers and communications, there has been in recent years considerable interest in cryptography, particularly by the business community, which is interested in keeping its proprietary information from competitors. As a result of the emerging need to protect information, the academic community has done research work in the field. NSA has made numerous attempts to either stop such work or to make sure it has control over the work by funding it, pre-publication reviews or other methods [USHR-87, pg.21].

During the debate on the Act, Director of the Office of Management and Budget, Jim Miller, had told the Government Operations Committee how the legislation would be implemented:

> Computer security standards, like other computer standards, will be developed in accordance with established NBS procedures. In

> this regard the technical security guidelines provided by NSA to NBS will be treated as advisory and subject to appropriate NBS review [USHR-87, pg. 37].

The implementation of the Act has been controversial. The National Institute of Standards and Technology (NIST, formerly NBS) and NSA signed a Memorandum of Understanding (MOU) to implement the Act, outlining areas of necessary agency interaction. As part of this, they established a Technical Working Group "to review and analyze issues of mutual interest pertinent to protection of systems that process sensitive or other unclassified information." The MOU also states:

> The NIST and the NSA shall ensure the Technical Working Group reviews prior to public disclosure all matters regarding technical systems security techniques to be developed for use in protecting sensitive information in federal computer systems to ensure they are consistent with the national security of the United States.

In this document, NIST and NSA were acknowledging that the public development or promulgation of technical security standards regarding cryptography could present a serious possibility of harm to national security. Critics of the MOU, including CPSR, contended that Congress, cognizant of the national security considerations, had nonetheless sought to restrict NSA's ability to dictate the selection of security standards for unclassified information standards. These critics contend that this and other aspects of the MOU violate the intent of Congress. In the next two sections of this chapter, we examine several Federal initiatives in cryptography, two of which had a large NSA role.

Digital Signature Standard

As noted in Chapter 1, cryptography performs a variety of functions: "[It] can help prevent penetration from the outside. It can protect the privacy of users of the system so that only authorized participants can comprehend communications. It can ensure integrity of the communications. It can increase assurance that the received messages are genuine."

Digital signatures facilitate electronic funds transfer, commitment of computer resources, and signing of documents. Without that electronic establishment of authenticity, how can you establish the validity of a signature on an electronic contract? It was no surprise that NIST should decide to establish a digital-signature standard; the one the agency chose was.

RSA Data Security was established in 1981; by 1991 the list of purchasers of its digital-signature technology included Apple, AT&T, DEC, IBM, Lotus, Microsoft, Northern Telecom, Novell, Sun, and WordPerfect. RSA had been accepted as a standard by several standards organizations;[1] it was fast on its way to becoming the defacto digital-signature standard.

In establishing a standard for digital signatures, NIST's criteria were somewhat different from that of the computer industry. In particular, the government wanted to avoid the possibility that the digital-signature standard could be used for confidentiality. It was also important that the standard be nonproprietary. NIST proposed the Digital Signature Standard (DSS) [NIST-XX] as a FIPS. There was great consternation – and not only at RSA Data Security. It was immediately apparent that DSS could not interoperate with digital signatures already in use.

Although NIST announced that DSS would be patented by the government and would be available free of charge, patent problems arose immediately. The government agency had chosen an algorithm that was based on unpatented work of an independent researcher, Tahir ElGamal. David Kravitz, an employee of NSA, filed a patent application for the Digital Signature Algorithm; this was subsequently awarded [Krav].

To its chagrin, NIST discovered that Claus Schnorr, a German mathematician, had already received U.S. and German patents for a similar algorithm [Schn-89, Schn-90b]. Public Key Partners (PKP) acquired Schnorr's patent rights. PKP offered the government free use of the algorithm in exchange for exclusive rights to Kravitz's algorithm. Under the PKP proposal, DSS users outside the Federal government would have to pay for use of the DSS algorithm. Following public opposition, the government declined the offer.

There were other objections to DSS, most notably that NIST was promulgating a weak standard. NIST proposed a key size of 512 bits. Earlier work on the algorithm had suggested that 512 bits "appear[ed] to offer only marginal security "[LaOd, BFS]. Scientists complained that restricting the key size unnecesarily constrained flexibility, and that improvements in algorithms could quickly render the NIST standard obsolete. A flexible key size would not have that difficulty. These issues were similar to ones raised when DES was proposed.

There were also differences from the DES situation, and these raised concern. For DSS, there had been no public request for proposals, and NSA had designed the algorithm. CPSR and members of industry and academia asserted that NIST's reliance on NSA was directly contrary to the Computer Security Act. These concerns were noted by Representative Jack Brooks, who had served as Chairman of the House Government Operations Committee during the passage of the Computer Security Act:

> [u]nder the Computer Security Act of 1987, the Department of Commerce [through NIST] has primary responsibility for establishing computer security standards including those dealing with cryptography. However, many in industry are concerned that in spite of the Act, the NSA continues to control the Commerce Department's work in this area. For example, Commerce (at the urging of the National Security Agency) has proposed a "digital signature standard" (DSS) that has been severely criticized by the computer and telecommunications industry [USHR-92, pg.2].

DSS was proposed in 1991. Public concerns resulted in modifications, including a flexible key size (key sizes from 512 to 1024 bits are permitted, in jumps of 64 bits). Problems with the patent have slowed the process, but on May 19, 1994, the government adopted DSS as a Federal Standard [FIPS-186], announcing that the "Department of Commerce is not aware of patents that would be infringed by this standard" [NIST-186]. James Bidzos, President of both PKP and RSA Data Security Inc., believes otherwise, "We disagree. There are a number of patents that we believe cover DSS."

Securing the Communications Infrastructure: Digital Telephony and EES

As the phone system has moved to a digital system, another issue arises. Encryption affects the government's ability to comprehend an intercepted signal, but the government is also concerned about its ability to intercept the signal. For this reason we include a discussion of the FBI's "Digital Telephony" proposal in this chapter.

As a result of increasing standardization of telephone switching practices, modern communication systems can provide much more information about each call, revealing in real time where the call came from even when it originates a long way away. But advanced communications systems, including such improvements as cellular telephones and call forwarding, can also present problems to law enforcement. The FBI was concerned about the ability of service providers to locate a call and, at law enforcement's behest, install a tap. In 1992, the Bureau prepared a legislative proposal.

At the time, the FBI was responding more to a problem the Bureau saw coming than to one that had hit full force. A Washington Post story of April 30, 1992 reported that "FBI officials said they have not yet fumbled a criminal probe due to the inability to tap a phone ..." [Mint]. The FBI contended that there were numerous cases where court orders had not been sought, executed, or fully carried out by law-enforcement agencies because of technological problems [DGBBBRGM, pg. 26]. However, Freedom of Information Act litigation initiated by CPSR in April 1992 produced no evidence of technical difficulties preventing the FBI from executing wiretaps as of December 1992.

Major members of the computer and communications industries, including AT&T, Digital Equipment, Lotus, Microsoft, and Sun, strongly opposed the 1992 proposal. The Electronic Frontier Foundation helped coordinate this opposition. Industry was particularly concerned that the proposal was too broad, covering operators of private branch exchanges and computer networks. Industry feared that it would have to foot the bill. The General Accounting Office briefed Congress, and expressed concern that alternatives to the Digital Telephony proposal had not been fully explored [GAO-92]. The U.S. General Services Administration characterized the proposed legislation as unnecessary and potentially harmful to the nation's competitiveness [GSA-92]. There were no Congressional sponsors for the proposal.

In 1994, the FBI has prepared a revised proposal that limits the scope to common carriers and allocates $500 million to cover their costs. Carriers would have three years to comply; after that, failure to fulfill a wiretap order could result in a fine of up to ten thousand dollars a day. The revised proposal, the "Digital Telephony and Communications Privacy Improvements Act of 1994," was submitted to Congress in March 1994.

On February 17, 1994, FBI Director Louis Freeh reiterated the agency's concerns in a speech to the Executives' Club of Chicago: "Development of technology is moving so rapidly that several hundred court-authorized surveillances already have been prevented by new technological impediments with advanced communications equipment." In testimony to Congress on

March 18, 1994, Freeh reported that a 1993 informal survey of federal, state and local law-enforcement agencies revealed 91 instances of recent court orders for electronic surveillance that could not be fully implemented [Freeh, pg 33]. The problems were due to a variety of causes, including 29 cases of special calling features (such as call forwarding), and 30 cases involving difficulties with cellular phones (including the inability of the carriers to provide dialed number information). Under questioning by Senator Leahy, Freeh answered that the FBI had not encountered court-authorized wiretap orders the Bureau could not execute due to digital telephony. However, in his prepared testimony Freeh cited two examples where wiretaps could not be executed due to digital telephony [Freeh, pg. 34].

While wiretapping can procure signals, secure telephones can render those signals useless to the wiretapper. Secure telephones using advanced key management are widespread in the national security community. Although voice-encryption systems for the commercial market have been a staple of companies such as Gretag and Crypto AG in Switzerland and Datotek and TCC in the U.S., only in 1992 was the first mass market device for secure voice encryption brought forth by a major corporation. AT&T announced the Model 3600 Telephone Security Device, which employed a DES chip for encryption.

The Department of Justice had been concerned about just such a development, and a federal initiative had been underway to preempt it. In April 1993 the President announced the key-escrow initiative: the "Clipper" chip and its associated key escrow scheme, while AT&T announced a telephone privacy device that uses the device. This proposed standard raises a number of questions about cryptography within telecommunications. In the next chapter we discuss the Escrowed Encryption Standard.

Notes

1. RSA is listed by International Standards Organization standard 9796 as a compatible cryptographic algorithm. RSA is part of the Society for Worldwide Interbank Financial Transactions (SWIFT) standard, and the ANSI X9.31 standard for the U.S. banking industry. It forms part of the Internet Privacy Enhanced Mail (PEM) standard.

Using Clipper

1. Two participants establish a communication channel and set up a "session key" (KS).

2. Once the session key is established, each device passes the session key, KS, to its Clipper chip, which encrypts it using the chip's unique key (KU). From this and other information, including the chip's identifier (UID), the encrypted session key forms a Law Enforcement Access Field (LEAF), that is transmitted to the other device.

3. Encrypted communications can begin.

4. Government officials with legal authorization "listen in" to encrypted conversation, and tape it. Tape is sent to FBI for analysis.

5. The decrypt processor determines that Clipper was used for encryption and decodes LEAF. The UID is determined from the LEAF.

6. The FBI uses the UID to identify the chip to the escrow agents (presently the National Institute of Standards and Technology, and the Department of Treasury's Automated Systems Division). The FBI gets the two halves of the chip's key, KU1 and KU2. (KU is determined by taking the XOR of KU1 and KU2.) The shared session key can be recovered from the LEAF produced by either chip.

7. The decrypt processor uses the chip's unique key (KU) to decode the session key (KS) in the LEAF. Once the chip's unique key has been obtained, the process can be abbreviated, since all encrypted calls made using this chip can be similarly decoded.

Chapter 7

The Government Solution: The Escrowed Encryption Standard

Vocabulary words:

Capstone: Name of the chip with Clipper plus Digital Signature Algorithm, key exchange, and associated mathematical functions.

Clipper: Name of the chip with the SKIPJACK algorithm and the key-escrow feature.

Key-escrow: A system by which the device private keys are kept in a repository.

PCMCIA card: The Personal Computer Memory Card Industry Association (PCMCIA) card is an industry standard format and electrical interface for various computer components, including memory, very small disks, etc.

Session key: A key established by the participants and used for a single communication.

SKIPJACK: The encryption algorithm that underlies the Escrowed Encryption Standard.

On April 16, 1993, the White House announced the Escrowed Encryption Initiative, "a voluntary program to improve security and privacy of telephone communications while meeting the legitimate needs of law enforcement" [OPS]. The initiative included a chip for encryption, Clipper,[1] to be incorporated into telecommunications equipment, and a key-escrow scheme. The National Security Agency (NSA) designed the system, and the underlying cryptographic algorithm, SKIPJACK, is classified.

Public response, both in the form of testimony presented at hearings held by National Institute of Standards and Technology (NIST) at the Computer Systems Security and Privacy Advisory Board, and in written comments to NIST, was overwhelmingly negative. Despite that, on February 4, 1994, after months of governmental review, the Department of Commerce announced the approval of the Escrowed Encryption Standard (EES) as a voluntary Federal Information Processing Standard (FIPS); "voluntary" means that if a Federal agency determines that telecommunications equipment transmitting sensitive but unclassified information should encrypt the data, it can choose EES – or any other FIPS (e.g., DES). In this chapter, we present EES and the policies surrounding its use.

We begin with a brief description of the workings of the standard; a more complete description is found in the appendix.

EES Encryption

If two participants want to communicate using EES, both must have telecommunications security devices with a Clipper chip. The devices establish an 80-bit "Session Key," and pass this to their chips, which encrypt it with information specific to the chip (the chip-unique key). This creates a Law Enforcement Access Field (LEAF), which is transmitted to the other party. Encrypted communication can begin.

As in other cryptosystems, the encryption algorithm, SKIPJACK, and the session key protect confidentiality. But this is a cryptosystem with a difference: if there is a legal authorization for a wiretap, the secrecy provided by EES will not be a barrier to law enforcement. It's an adroit twist: communications are secure unless there is probable cause of an indictable offense (and all other requirements of Title III, FISA, or the state statutes, also apply).

Every Clipper chip will have its chip-unique key registered with the Federal government. To protect the confidentiality of the key, it will be "split," and the components will be held by two Federal escrow agents – NIST and the Treasury Department's Automated Systems Division – one at each. Both components are needed to reconstruct the key. The standard authorizes keeping each chip's private key secret – unless there is legal authorization to do otherwise. Key registration will occur during manufacturing at a secure commercial facility, and escrow officers from the two agencies will be present during the chip-programming process.

EES Decryption by Law Enforcement

The Federal government knows the SKIPJACK algorithm, and it can build devices to decrypt it. If a law enforcement officer is listening to a legally tapped conversation, and the communications becomes incomprehensible, the law enforcement officer will tape it, and send the tape to the FBI for analysis. Bureau officers will analyze the communication to see if it is EES encrypted. If so, a special decrypt processor will decrypt the LEAF (recall that transmission of the LEAF precedes the encrypted conversation) transmitted from the target phone. The processor will extract the chip ID.

With that identification, the two escrow agents will be able to supply the two halves of the escrowed chip-unique key. These are entered along with the expiration date for the court order into the decrypt processor. The processor performs the decryption, using the chip-unique key to decrypt the session key.

Presently the key will have to be manually erased from the decrypt processor. It is currently envisioned that when the key is erased, an audit trail record will be generated and transmitted to the escrow agents.[2] Under procedures issued by the Department of Justice [DoJB], the investigating agency may not retain the key past the expiration of the surveillance authorization. The Department of Justice procedures explicitly state that they "do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance, and noncompliance with these procedures shall not provide the basis for any motion to suppress or other objection to the introduction of electronic surveillance evidence lawfully acquired" [DoJB].

For interceptions conducted under Title III, FISA, or the state statutes, procedures for receiving the escrowed keys will require legal authorization, and an inability to comprehend a tapped conversation. Rules for decrypting communications intercepted outside the nation's borders are somewhat less clear. NSA has legal authorization to intercept communcations outside the

United States so long as those being tapped are not U.S. persons. (Such surveillance, however, may not be legal under the laws of a foreign country.) But interception is a different matter from obtaining escrowed keys. The Department of Justice has announced that decryption of EES-encoded messages "[would be] carried out within the law," but "Procedures might not be released" [DoCB]. Thus, at this point, Federal policy on interception and decryption of foreign EES-encrypted messages is not known.

Security of the System

Some cryptography experts and others in industry and academia are skeptical of using a publicly untested classified algorithm for encryption. NSA has attested to the strength of the algorithm. A panel of cryptography and security experts (including two members of this panel) invited by NIST to study the quality of the SKIPJACK algorithm concluded that SKIPJACK appeared to be both strong and resistant to attack [BDKMT]. The effort was limited in scope. Working within a tight time frame, they could not attempt a complete investigation of the algorithm's security. However, they examined the structure of the algorithm, and the procedures followed by NSA in developing and evaluating the algorithm, and they were satisfied. Nonetheless, public skepticism of classified design has been fueled by the recent discovery that under certain circumstances the function of the LEAF can be subverted.[3]

As discussed in Chapter 4, three aspects of EES make it attractive to law enforcement and national security. Key-escrow ensures law enforcement access to encrypted conversations whenever there is legal authorization. The classification of the algorithm means that advanced encryption design is not made available even while strong cryptography is.

Use of Escrowed Encryption

EES is a standard for encryption of voice, fax, and computer information transmitted over a circuit-switched telephone system. It is fully anticipated that escrowed encryption will be extended to other forms of electronic communications. In mid-April NSA awarded Group Technology Corporation a contract for 22000 to 75000 Tessera cards. Tessera is a PCMCIA card, an electronic device roughly the size of a credit card, for which many computers now include an interface. Tessera can be used with computer software to support encrypted and/or digitally signed communication applciations such as electronic mail. By retaining the user's keys on the card, the card protects the keys from compromise should the computer in use be penetrated.

FIPS 185, the Federal publication defining EES, does not contain enough information to design or implement EES devices. Specifications must be obtained from the NSA, and the agency's approval is required for the manufacture of Clipper chips. At present, Clipper chips are being manufactured only by Mykotronx; they are being used in AT&T secure telephone devices. Government approval, however, is also required for the use of the key-escrow chips in commercial products [NIST-94, pg. 6004].

Export of devices containing escrowed keys will be permitted, except to those countries that face a Congressional embargo on military technology (e.g., Libya). It is anticipated that the Federal government will shortly announce a Distribution Agreement for EES technology; this will streamline the export license procedure for escrowed encryption products.

The February 1994 announcement went some distance to answering questions regarding EES. Many concerns remain. In the next chapter, we examine the remaining issues.

Notes

1. The name "Clipper" had been previously trademarked by Intergraph Corp. for their microprocessor chip, and for a time, the government stopped using Clipper referring to the escrowed encryption chip. However, Intergraph graciously ceded to the government the right to use the name "Clipper" for the escrowed encryption chip.

2. Private communication with Miles Smid, June 3, 1994. Smid is Manager, Security Technology Group, Computer Security Division, of the Computer Systems Laboratory at NIST.

3. Working with publicly available material, Matthew Blaze of AT&T Bell Laboratories has developed a technique for replacing the LEAF containing the current session key by one containing an unrelated key [Blaz]. The practical implications of Blaze's findings are subject to debate. Perhaps his most significant finding was a technique that allows one participant in a communication to construct unilaterally a LEAF (with considerable pre-computation) that denies law enforcement access, but which will be accepted as "valid" by a communicant using EES-compliant technology. This technique is readily applied to computer-based communication such as E-mail, but it probably is not applicable to current secure telephone system designs.

Chapter 8

Issues Highlighted by the Escrowed Encryption Standard

Vocabulary words:

Capstone: Name of the chip with Clipper plus Digital Signature Algorithm, key exchange, and associated mathematical functions.

Dual-use technology: Technology which has both military and commercial applications.

Ethernet: A 10-megabit per second local area network developed by Digital Equipment, Intel, and Xerox, and standardized by the IEEE.

Modem: An interface between telephone transmission and computer storage.

Tessara: The government name for a PCMCIA card that contains the Capstone chip. (A PCMCIA (Personal Computer Memory Card Industry Association) card is an industry standard format and electrical interface for various computer components, including memory, very small disks, etc.)

Trojan horse: A program, a component of which is capable of unexpected effects.

The problem is how to secure electronic communications in the Information Age. Law enforcement believes the Escrowed Encryption Standard (EES) will provide strong communications security without making the communications of criminals and terrorists immune from lawful interception. National security officials believes EES will not interfere with its access to foreign intelligence, and thus is a secure solution to the complexities presented by the need for strong encryption. If public comments are any guide, the computer industry is persuaded that EES is a poor design that will add complexity and expense to American computer products; they see escrowed encryption as an inappropriate and expensive solution to the cryptographic problem that law enforcement and national security allege exists. Civil-liberties groups including the American Civil Liberties Union (ACLU) and the Computer Professionals for Social Responsibility (CPSR) argue that escrowed encryption technology is a major intrusion on the privacy rights of the public, and that EES is a change in policy masquerading as a government procurement standard.

The EES is a voluntary standard for encryption of voice, fax, and computer information transmitted over a circuit-switched telephone system. Many of the commercial objections to it concern its expected extension to computer communications. In this chapter we examine the issues EES raises. This chapter is split into five sections: (i) Privacy Concerns Raised by EES; (ii) Impact of EES on Export; (iii) Interoperability Issues Raised by EES; (iv) EES: Hardware versus Software; and (v) Impact of EES on the U.S. Computer Industry.

Privacy Concerns Raised by EES

Some facts are clear:

1. EES makes the users' secret keys available to the government.
2. EES was designed by the National Security Agency (NSA).
3. The underlying algorithm, SKIPJACK, is classified.

There agreement ends.

Advocates of EES claim the availability of strong cryptography (designed by NSA) will provide Americans with better and more readily available privacy protection than they presently enjoy. Privacy advocates believe that any cryptographic system where the government holds the keys endangers each individual's right to confidential communications. Proponents of EES observe that no one will be forced to use the system, and that EES does not prohibit other forms of encryption. Opponents respond that the National Institute of Standards and Technology (NIST) standard states "use is encouraged when [EES] provides the desired security." They maintain that if a large Federal agency such as the IRS adopts EES, electronic filers who chose to secure their transmissions may have to use the algorithm. Such a choice by IRS, would have the impact of making the voluntary standard the de facto national one.[1]

Notwithstanding the voluntary nature of the current EES initiative, opponents fear that the government might eventually outlaw other forms of encryption. These critics of the government's plans doubt that a voluntary program will be effective in preventing the use of alternative forms of cryptography by criminals, and they contend that with EES technology widely deployed and readily available in the future, a prohibition against other methods of encryption might be seen as more politically palatable than it would be today. As such, they view the government's adoption of a voluntary standard as the first step toward such a program.

There is no question that the market impact of the Federal government can be huge, although recent experience illustrates that the government's ability to influence the computer communication market is not always successful.[2] Adoption of EES as a standard, voluntary or otherwise, decreases the chance there will be competing systems available. Indeed the true success of EES, as measured by law enforcement's continued ability to decrypt tapped conversations, can come only at the expense of competing systems for secure telecommunications. There is already one example. In 1992 AT&T announced a DES-based secure telephone for the mass market. After being approached by the government, the phone company changed its plans and withdrew the DES version. It now produces an EES version and also versions with proprietary algorithms. If EES is a success in its own terms, there will be no other secure telecommunications equipment contending for the civilian market – at least in the United States.

Proponents of escrowed encryption argue that privacy protection will be better than ever. There will be a proliferation of secure telephones. It is anticipated that the escrowed system will leave an electronic audit trail.[3] In the event that the government illegally taps a communication, the illegal interception will be much easier to uncover than it is under the present system. Opponents of escrowed encryption believe that a privacy system in which the government holds the key to every lock is no privacy system. Escrowed encryption may have been designed with the best of intentions, but Brandeis, in his famous dissent in the Olmstead wiretapping case, warns to be cautious in such situations,

> Experience should teach us to be most on our guard when the government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest danger to liberty lurks in insidious encroachment by men of zeal, well-meaning but without understanding [Olm, pg. 752 - 753].

Civil-liberties groups strongly argue against a civilian standard being developed by a military organization. For example, CPSR points to the Computer Security Act, which the organization says decided the issue seven years ago. CPSR asserts that in a democratic society the public should play a significant role in deciding how the communications infrastructure will be designed. But the underlying algorithm for EES is classified, and the strength of the algorithm cannot be assessed by the (public) cryptography community. Reminding us of the abuses of Watergate and the revelations of the Church Committee, CPSR contends that the NSA should not be building government trapdoors into the civilian communications infrastructure.

Impact of EES on Export

The U.S. State Department controls the export of cryptography, under the authority of the International Traffic in Arms Regulations. Despite a 1991 decision by the Coordinating Committee on Multilateral Export Controls (COCOM)[4] declaring cryptography a dual-use technology, the United States has kept cryptography on its munitions list. A vendor, seeking an export license for a product containing cryptography, first determines whether export of the product falls under Commerce Department or State Department rules. If jurisdiction is within the Commerce Department, approval is swift. If not, the procedure becomes more complex, and NSA may become involved.

With the exception of use by financial institutions and by foreign offices of U.S.-controlled companies, NSA generally will not approve export of products containing DES used for confidentiality. Approval is granted for the export of cryptography for authenticity and integrity purposes. If a product such as DES is dual-purpose, then export approval will be granted only if the vendor can demonstrate the product cannot be easily modified to protect confidentiality.

Striking a balance between economic strength (by opening markets for U.S. companies) and protecting national security (by restricting the sale of military technology) requires making complex choices. Cryptography is not the only American product subject to export control. What differentiates this conflict from, say, the exportability of supercomputers is that comparable cryptographic products are available for sale internationally. A year ago, the Software Publishers Association (SPA), quantifying what had been anecdotal, searched for foreign cryptography products. By March 1994, the organization had located 152 foreign products with DES cryptography, from such countries as Australia, Belgium, Finland, Israel, Russia, Sweden, and Switzerland [SPA-94]. RSA is also routinely available in foreign cryptographic software. Neither of these facts should come as a surprise, since the specifications for both algorithms are publicly available.

Supporters of export controls argue that the most serious threat to foreign-intelligence gathering comes not from stand-alone products that constitute most of the market, but from well-integrated, user-friendly systems in which cryptography is but one of many features. From this perspective, it is essential to control export of the commodity, namely desktop hardware and software with integrated cryptography. The U.S. is the preemininent supplier of such products.

National security experts believe that the export-control policy is working. DES on the Internet has little impact on U.S. communications intelligence. Foreign organizations that are concerned about protecting their information from sophisticated intercept are not likely to download an encryption software program from the Internet. Instead they will buy products they trust from reputable vendors.

Testifying to the Subcommittee on Economic Policy, Trade and Environment last fall, Stephen Walker, President of Trusted Information Systems, explained that his company had attempted to implement Privacy Enhanced Mail (PEM) for the British Ministry of Defence. Since PEM uses both RSA and DES, Trusted Information Systems was unable to export the algorithm directly. Instead the British subsidiary of the company, Trusted Information Systems Limited, arranged to implement a British version of PEM, using DES and RSA algorithms available in the U.K. The Ministry of Defence got their program. DES and RSA were not exported, and several British computer scientists got the work [Walk, pg. 68].

Quantifying lost sales is difficult. One can count the number of export-license applications denied or withdrawn, but that misses the mark. Foreign customers who know that the products they want will not receive U.S. export approval are unlikely to waste time approaching American companies. At the same time, export controls are sometimes cited as the reason for a lost sale when the facts are otherwise. The Department of State export-license statistics give only a partial picture of the situation.

Features, even ones not purchased, increase sales. If U.S. companies cannot include cryptography used for confidentiality in their products, that fact turns away sales even if cryptographic security is not presently required. Buyers are reluctant to commit to a company for fear that sometime later they will want to upgrade their system, perhaps including cryptographic security, and the American company will not be able to supply them, because of U.S. export controls.

Multinational companies are particularly interested in protecting their electronic communications. The U.S. policy on export control of encryption makes adaption of U.S. encryption products a poor choice, since compatibility is a prime consideration to purchasers. In seven different instances between April 1993 and April 1994, the Semaphore Communications Corporation was advised by the State Department or the NSA that it would be unable to export secure communications equipment with strong cryptography for confidentiality. One such example occurred when Semaphore Communications Corporation lost out to a German competitor. The competitor offered a German-built DES-based system that could be exported to the buyer's U.S. office. Semaphore was unable to export a DES-based product to the buyer's home office in Germany [Walk, pg. 70]. The seven contracts for which Semaphore could not compete represented one million dollars in sales, a large amount for a small firm. Furthermore, this also resulted in Semaphore losing a multiyear agreement with an estimated value of several million dollars in that period.

The government's response has been to ease export restrictions on some cryptographic products. For example, Ronald Rivest of MIT has designed two variable-key-length cipher functions, RC2 and RC4, that can be used instead of DES in export versions of products. Under an agreement with the Software Publishers Association, the Department of State has a streamlined export-license process for versions of RC2 and RC4 that are limited to a 40-bit key size. (56-bit keys are allowed if the export is to foreign subsidiaries or overseas offices of U.S. companies.) But the 40-bit key size is smaller than a 56-bit DES key, and thus these algorithms are perceived by users as being less secure than the DES. Moreover, RC2 and RC4 are not compatible with DES, creating potential interoperability problems for users.

Export-control policy on cryptography has complicated development of secure systems. Digital Equipment Computer's DESNC, a DES encryptor placed between a workstation (or several workstations) and an Ethernet cable to encrypt traffic to and from the workstation, is an example of a useful product that died an untimely death in part because of export control.

Because of the product's use of DES for confidentiality, government policy did not permit the general export of DESNC. There was still a domestic market. But Digital Equipment marketing managers feared that publicizing DESNC, without the availability of a comparable product for export would alienate Digital Equipment's foreign customers by suggesting that unencrypted Ethernet technology is vulnerable (it is), but without providing a solution for non-U.S. customers. A high-cost item, DESNC was unlikely to be a big seller in either foreign or domestic markets, but an inability to offer this product on a global basis posed a critical customer relations problem. These concerns, in combination with the negative publicity it would bring to Ethernet technology, were deemed unacceptable trade-offs.[5]

National security experts have argued that removal of U.S. export controls on cryptography could be replaced by the imposition of foreign import controls; they point to France, which requires registration of cryptographic algorithms, as an example. However, at present no Western European governments other than France restrict the import of cryptographic products, and only a few Asian governments do so.

The impact of FIPS185 on the export of American cryptography is unclear. From the government's perspective, if strong cryptography is widely used, then EES will be deemed successful if it dominates the market for cryptographic products in the telecommunications arena. Presently there are but a handful of U.S. companies offering secure telephones, including Datotek (now owned by AT&T) and Technical Communication Corporation; these businesses are small, with each representing about $10 million in sales annually.

Interoperability Issues Raised by EES

Interoperability – the ability of users to communicate between different systems – is essential for any telecommunications system. For example, problems arose during the Gulf War because the coalition forces that were assembled did not share a common, secure communications system.

Civilian needs during peacetime are quite different from military needs during wartime. It remains true, however, that interoperability is crucial in the communications arena. Assuming that the United States government has no plans to change the classified status of the SKIPJACK algorithm, it is unlikely that the European Community will adopt EES as a standard for secure telecommunications.

EES: Hardware versus Software

The government's attempt to create strong cryptography that would not hinder law enforcement's abilities to comprehend legally intercepted conversations resulted in several controversial aspects of the EES design: escrowed encryption, classification of the SKIPJACK algorithm, and availability of the algorithm only in hardware.

As far as law enforcement access is concerned, an implementation of the SKIPJACK algorithm without the Law Enforcement Access Field would completely miss the point. Law enforcement agents would be unable to decrypt. To make such implementations more difficult, EES is available only in tamper-resistant hardware.

This is more expensive than a software solution – and not only the government will be paying. In lots of ten thousand, Clipper chips will cost approximately \$15; industry experts contends that this translates to a finished product with escrowed encryption capabilities costing about \$60 more than one without. In lots of one hundred thousand, the price drops to \$10 each, with a corresponding drop to \$40 for the finished product.

Software implementations also offer a flexibility that hardware does not. A family of compatible products is an excellent way to sell new technology. Vendors will often offer the capability of beginning with low-cost software, with the option of upgrading to higher-performance hardware when needed. But hardware-only implementations of encryption do not allow that kind of versatility.

NIST is investigating the possibility of a software version of key-escrow encryption. Several proposals are currently under investigation.

Impact of EES on the U.S. Computer Industry

For nearly two decades, industry and academic experts have argued that protecting computer communications is vitally important. Many have posited that the civilian market for cryptography is about to take off. The EES initiative would encourage the adoption of cryptography. From the day it was proposed, the computer industry has protested. Why? It will need to be used only by those who wish to encrypt voice, fax, or computer information sent to a Federal agency that has adopted the standard.

The computer industry sees the standard as significantly less than voluntary. Should EES be adopted by a Federal agency with a large constituency, such as the Social Security Administration, industry will have to make EES standardly available in domestic equipment. In such circumstances, consumers will demand products with EES. The computer industry has made an investment in DES and RSA solutions for secure systems. From a vendor viewpoint, escrowed encryption will be an expensive add-on that will add little new functionality. Furthermore, multiple methods of encryption increase complexity, thus discouraging demand.

Computer vendors believe that the combination of a classified algorithm and key registration with the U.S. government will make EES unattractive internationally. If this is true, U.S. computer companies will have to implement other forms of cryptography to make American products competitive in the world marketplace. At the same time, domestic demand may mean that EES will need to be in products for the U.S. market. Manufacturers support dual product lines when they must, but from a vendor viewpoint, this is an unnecessary distraction and added expense.

Semiconductor manufacturers are concerned about government control of the manufacture of Clipper chips. (NSA licenses the manufacturers of the chip.) Vendors avoid sole-source supplies when possible, but the government has committed to establishing multiple sources for the chips. Vendors also do not like to adopt technology whose manufacture they cannot control.

Finally, some in the industry are disturbed about the possibility of the government controlling more than just the manufacture of Clipper chips. Suppose a company wants to integrate EES into its central processing unit. The government controls that right. Does that mean that the National Security Agency will be making design decisions for a U.S. civilian product? Some vendors have raised the concern that the government might want to exert close oversight over vendor integration of escrowed encryption. The fact that the government is promoting the use of Capstone/Tessera would strongly suggest not, since this peripheral provides workstation software with substantial opportunities to manipulate the interface to escrowed encryption.

Perhaps somewhat surprisingly, some of the largest suppliers of cryptographic equipment do not feel that their businesses are imperilled by the government's adoption of EES. Cylink, with $30 million in annual sales of link encryption equipment, says that for those customers who choose escrowed encryption, replacing current cryptographic algorithms with EES is simple; for overseas sales, they already substitute their own propriety software for domestic DES encryption. James Bidzos, President of RSA Data Security Inc., agrees that a "voluntary" government standard could lead to the inclusion of key escrow in computing equipment being the norm, but he says that that situation would not hurt his company. Corporations will want to transmit their communications in ways that are truly private – and Bidzos says that means using a cryptographic system in which the keys are not registered with the government.

As with any other new technology, escrowed encryption creates complications for the computer industry. It does so for the larger society as well. The Escrowed Encryption Standard brings to the fore issues of policy and issues of technology, issues of the public good and issues of private freedom. Some aspects of the problem – the cost of Clipper chip – are easily quantifiable. Others, from the potential dangers to society of encrypted conversations to the loss of privacy (perceived and actual) are not. In the final chapter of this report, we raise further questions about codes, keys, and the conflicts.

Notes

1. In recent years the IRS has experimented with electronic filing, and this year the agency accepted electronic filing by individuals. Compuserve Information Service offered the service, via the Internet. Presently, transmissions travel unencrypted, in plaintext form [Lewi].

2. The failure of the GOSIP initiative, an attempt to mandate procurement of computer communication protocols that conform to the ISO OSI standards, is one such example.

3. Private communication with Miles Smid, June 3, 1994. Smid is Manager, Security Technology Group, Computer Security Division, of the Computer Systems Laboratory at NIST.

4. COCOM was comprised of NATO countries (except Iceland), Australia, and Japan. It has recently been disbanded.

5. Private communication with Steven Lipner, May 17, 1994. Lipner was Engineering Group Manager, Secure Systems Group, at Digital Equipment Company.

Chapter 9

Codes, Keys, and Conflicts: The Questions

In this report, we have discussed the various policy and technical concerns surrounding cryptography. The problems of communications security and its cryptographic solutions are technical ones, but the issues faced are much broader.

They deserve careful and thoughtful public debate. It took the Supreme Court nearly forty years to expound on the privacy of telephone communications. In the Olmstead case in 1928, the Supreme Court held that wiretapping evidence did not need court authorization. Over the next four decades, the Court slowly created a penumbra of privacy for telecommunications. Finally, in 1967, in Katz versus the United States, the Court held that a phone call in even so public a place as a phone booth was deserving of privacy – it could not be tapped without prior court authorization. Computer communications differ from the telephone, but it is likely that the public's embrace of the medium of computer communications will be considerably more rapid than the acceptance of the earlier technology.

As we face growing reliance on electronic communications systems for our transactions, personal and professional, how do we want to build our communications infrastructure? Do we want protection of privacy to be paramount? The confidentiality of "what is whispered in the closet" [Olm, pg 752] cannot be the same if the message traverses an electronic pathway filled with switches and gateways. But the privacy of the communication can be fully protected by cryptography. Is that the solution we want? Justice

Brandeis, in his famous dissent on the Olmstead case, fervently argued for the protection of privacy of communications – but his argument was constructed so that the protection lay within the purview of the Fourth Amendment. Brandeis did not argue that the privacy of speech was absolute – only that it had as full Constitutional protection as any property of a person.

Do we believe there is an absolute right to communications privacy?

Or do we believe that the freedom afforded to society by communications technology must be kept in check? Technology has given us unprecedented freedom to travel, not only by various modes of transportation, but by removing distance as a barrier to communications. The same technology which allows a home office in Hong Kong to be in instantaneous communication with its branch office in London also affords this freedom to enemies of society. Use of encryption by criminals and terrorists will make law enforcement's and national security's job more difficult.

Members of the law enforcement community believe that the widespread use of encrypted telecommunications (especially phone calls) could interfere with their ability to carry out authorized wiretaps. Is this a problem that needs a solution? Should cryptographic solutions for communications security include authorized government access for law enforcement and national security purposes?

What will happen if criminals use cryptography other than EES? The Digital Telephony proposal involves investment in the telephone infrastructure in order to ensure that court-authorized wiretaps can be carried out. These wiretap capabilities will be less useful if communications are encrypted in ways that thwart law enforcement. What is the relationship between EES and Digital Telephony? Will there be any future attempt to outlaw alternative forms of cryptography?

What constitutes success of escrowed encryption? Would it simply mean government use of EES-type products? Or would it mean a much more widespread use of EES products? Would it mean the availability of EES-type products to the exclusion of all else?

It is clear that communications technology has shrunk distances in a way unimagined a generation ago. This country's technical innovations have had enormous impact on the rest of the world. The United States can legislate policy only within its borders, but the global impact of our domestic political decisions should not be underestimated. The choices the United States makes about escrowed encryption, confidentiality of communications, and government access to encrypted communications will reverberate across the globe.

We are experiencing fundamental transformations in the way that people and organizations communicate. What cryptography policy best accommodates our national needs for secure communications and privacy, industry success, effective law enforcement, and national security?

Bibliography

[Abra] Abrams, F., 1993, Big Brother's Here and – Alas – We Embrace Him, *New York Times Magazine,* March 21, 1993, pp. 36-37.

[ABA] American Bankers Association, 1979, Management and Use of Personal Identification Numbers, ABA Bank Card Statement, *Aids from ABA,* Catalog No. 207213, 1979.

[AG-FISA] As reported to the Congress by the Attorney General pursuant to the Foreign Intelligence Surveillance Act.

[AO-93] Administrative Office of the United States Courts, 1993, *Report on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications (Wiretap Report),* 1993.

[Ban] Banisar, D., 1993, Statistical Analysis of Electronic Surveillance, presentation at the National Institute of Standards and Technology, Computer System Security and Privacy Advisory Board, June 3, 1993.

[BFS] Beth, T., Frisch, M. and Simmons, G. (Eds.), 1992, *Public Key Cryptography: State of the Art and Future Directions,* Lecture Notes in Computer Science, No. 578, Springer-Verlag, 1992.

[BiSh] Biham, E. and Shamir, A., 1993, *Differential Cryptanalysis of the Data Encryption Standard,* Springer-Verlag 1993.

[Blaz] Blaze, M., 1994, "Protocol Failure in the Escrowed Encryption Standard," May 31, 1994.

[Blum] Blum, H., 1993, *Gangland: How the FBI Broke the Mob,* Simon & Schuster, New York 1993.

[BDKMT] Brickell, E., Denning, D., Kent, S., Maher, D. and Tuchman, W., 1993,"SKIPJACK Review: Interim Report, The SKIPJACK Algorithm," July 28, 1993, available electronically from cpsr.org.

[Broa] Broad, W., 1992, "Evading the Soviet Ear at Glen Cove," *Science*, Vol. 217 (3), September, 1982, pp 910-911.

[Bupc] Burrows, J. (Director, National Computer and Telecommunications Laboratory, National Institute of Standards and Technology), 1994, private communication, March 11, 1994.

[Caba] Caba, S., 1994, "FBI Nets Stanfa in Mob Sweep," *Philadelphia Inquirer,* March 18, 1994, Sec. A.

[Cinq] Cinquegrana, A., 1989, "The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978," 137 *University of Pennsylvania Law Review* 793, 814-815 (1989).

[DDKM] Delaney, D., Denning, D., Kaye, J. and McDonald, A., 1993, "Wiretap Laws and Procedures: What Happens When the U.S. Government Taps A Line," Sept. 23, 1993, available electronically from cpsr.org.

[Denn] Denning, D., 1994, "Encryption and Law Enforcement," Feb. 21, 1994, available electronically from cpsr.org.

[DGBBBRBM] Denning, D., Godwin, M., Bayse, W., Rotenberg, M., Branscomb, L., Branscomb, A., Rivest, R., Grosso, A. and Marx, G., 1993, "To Tap or Not to Tap," *Communications of the ACM,* Vol. 36 (3), March 1993 , pp. 24-44.

[DoCB] Department of Commerce Briefing re Escrowed Encryption Standard, 1994, Department of Commerce, February, 4, 1994, Washington, DC.

[DoJB] Department of Justice Briefing re Escrowed Encryption Standard, 1994, Department of Commerce, February, 4, 1994, Washington, DC.

[Diff-78] Diffie, W., 1978, "Data Security for EFT and Automated Business," New Problems - New Solutions, San Jose, California, SBS Publishing, 1978.

[Diff-82] Diffie, W., 1982, "Cryptographic Technology: Fifteen Year Forecast," in Gustavus J. Simmons, *Secure Communications and Asymmetric Cryptosystems*, AAAS Selected Symposium No. 69, Westview Press, 1982.

[Diff-88] Diffie, W., 1988, "The First Ten Years of Public Key Cryptography," *Proceedings of the IEEE*, Vol. 76 (5), May 1988, pp. 560-577.

[DH] Diffie, W. and Hellman, M., 1976, "New Directions in Cryptography," *IEEE Trans. Informat. Theory,* Vol. IT-22, pp. 644-654, Nov. 1976.

[DOW] Diffie, W., van Oorschot, P. and Wiener, M., 1992, "Authentication and Authenticated Key Exchanges," in *Designs, Codes, and Cryptography*, Volume 2, Number 2, 1992, pp. 107–125.

[ElGa] ElGamal, T., 1985, "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Trans. Informat. Theory*, IT-31 (1985), pp. 469-472.

[FISA] Foreign Intelligence Surveillance Act, 50 U.S.C. Sec. 1801 *et seq.*

[Freeh] Freeh, L., 1994, Written Statement before the Subcommittee on Technology and the Law of the Committee of the Judiciary, United States Senate and the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, March 18, 1994, Washington, DC.

[GSA] General Services Administration, 1992, Offices of Congressional Affairs, Memo of May 5, 1992, in *The Third CPSR Cryptography and Privacy Conference Source Book,* June 7, 1993, Washington, DC.

[Gold] Goldman V. United States, 316 U.S. 129, 1942.

[HEW] HEW Advisory Committee on Automated Personnel Data Systems, Records, Computers and the Rights of Citizens, 1973, Washington, DC.

[Irvi] Irvine v. California, 347 U.S. 128, 1954.

[Katz] Katz v United States, 389 U.S. 347, 1967.

[Kent] Kent, S., 1993, "Internet Privacy Enhanced Mail," *Communications of the ACM,* Vol. 36 (8), pp. 48-59, August 1993.

[Kinz] Kinzer, S., 1992, "East Germans Face Their Accusers," *New York Times Magazine*, April 12, 1992.

[Krav] Kravitz, D., Digital Signature Algorithm, U.S. Patent Number 5231668, applied for July 26, 1991, received July 27, 1993.

[Ladn] LADNER System, 1984, *Operation and Maintenance Manual*, Part No. ON332500, Prepared for Maryland Procurement Office, Ft. George G. Meade, MD, December 1, 1984.

[Land] Landau, S., 1988, "Zero Knowledge and the Department of Defense," *Notices of the American Mathematical Society (Special Article Series)*, Vol. 35, No. 1 (1988), pp.5-12.

[LaOd] LaMacchia, B. and Odlyzko, A., 1991, Computation of Discrete Logarithms in Prime Fields, in *Design, Codes, and Cryptography,* Vol. 1, 1991, pp. 47-62.

[Lewi] Lewis, P., 1994, "IRS Tries On-Line Filing," *New York Times,* February 19, 1994, Sec. D.

[Link] M/A-COM LINKABIT Corporation, 1983, *LC76 DES Data Encryption/Decryption Unit: Product Brochure,* August, 1983.

[Mats] Matsui, M., 1993, "Linear Cryptanalysis of DES Cipher," in *Proceedings Eurocrypt* 1993.

[Mint] Mintz, J., 1992, "Intelligence Community in Breach with Business," *Washington Post,* April 30, 1992, Sec. A.

[Myer] Myers, F., 1979, "A Data Link Encryption System," *National Telecommunications Conference*, Washington, D.C. November 27-29, 1979, pp. 43.5.1-43.5.8.

[NBS] National Bureau of Standards, 1977, Data Encryption Standard, *Federal Information Processing Standard 46*, January 1977, Washington, DC.

[Neu] Neumann, P., 1994, *Computer-Related Risks,* ACM Press (Addison-Wesley), 1994.

[NIST-XX] National Institute of Standards and Technology, 1991, *Publication XX: Announcement and Specifications for a Digital Signature Standard (DSS)*, August 19, 1991, Washington, DC.

[NIST-185] National Institute of Standards and Technology, 1994, *Federal Information Processing Standards Publication 185, Escrowed Encryption Standard*, February 9, 1994, Washington, DC.

[NIST-186] National Institute of Standards and Technology, 1994, *Federal Information Processing Standards Publication 186: Digital Signature Standard (DSS)*, May 19, 1994, Washington, DC.

[NIST-94] National Institute of Standards and Technology, 1994, Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard, *Federal Register,* Vol. 59, No. 27, February 9, 1994, Washington, DC.

[NIST-NSA] National Institute of Standards and Technology and National Security Agency, 1989, Memorandum of Understanding between the Director of the National Institute of Standards and Technology and the Director of the National Security Agency concerning the Implementation of Public Law 100-235, March 24, 1989, Washington, DC.

[NWCCS] National Commission for the Review of Federal and State Laws relating to Wiretapping and Electronic Surveillance, 1976, *Commission Studies,* Washington, 1976, Washington, DC.

[Olm] Olmstead v. United States, 277 U.S. 438, 1928.

[OPS] Office of the Press Secretary, The White House, 1993, Statement on the Clipper Chip Initiative, April 16, 1993, Washington, DC.

[Park] Parker, D., 1983, *Fighting Computer Crime,* Charles Scribner's, New York, 1983.

[Pil] Piller, C., 1993, "Privacy in Peril," *MacWorld,* July 1993, pp. 8 - 14.

[PCSG] Public Cryptography Study Group, 1981, *Report of the Public Cryptography Study Group*, American Council on Education, February 1981.

[Rive] Rivest, R., 1992, "Responses to NIST's Proposal," *Communications of the ACM*, Vol. 35 (7), July 1992, pp. 41-47.

[RSA] Rivest, R. Shamir, A. and Adleman, L., 1978, "A Method for Obtaining Digital Signatures and Public Key Cryptosystems," *Communications of the ACM,* Vol. 21 (2), pp. 120-126, Feb. 1978.

[Rote-89] Rotenberg, M., 1989, Testimony on Military and Security Control of Computer Security, Before the Subcommittee on Legislation and National Security of the House Committee on Government Operations, 101st Congress, 1st Session 80, May 4, 1989, Washington, DC.

[Rote-93] Rotenberg, M., 1993, "Communications Privacy: Implications for Network Design," *Communications of the ACM,* Vol. 36 (8), August 1993, pp. 61- 68.

[Schn-89] Schnorr, C., Procedures for the Identification of Participants as well as the Generation and Verification of Electronic Signatures in a Digital Exchange System, German Patent Number 9010348.1, patent applied for February 24, 1989, patent received August 29, 1990.

[Schn-90a] Schnorr, C., 1989, "Efficient Identification and Signatures for Smart Cards," *Advances in Cryptology – Crypto '89*, Springer-Verlag, New York, 1990, pp. 239-251.

[Schn-90b] Schnorr, C., Method for Identifying Subscribers and for Generating and Verifying Electronic Signatures in a Data Exchange System, U.S. Patent Number 4995082, patent applied for February 23, 1990, patent received February 19, 1991.

[Silv] Silverman v. United States, 365 U.S. 505, 1961.

[SmBr] Smid, M. and Branstad, D., 1988, "The Data Encryption Standard: Past and Future," *Proceedings of the IEEE*, Vol. 76 (5), pp. 550-559, May, 1988.

[SPA-94] Software Publishers Association, Trusted Information Systems and Hoffman Business Associates, 1994, *Encryption Products Database Statistics,* March 1994.

[SPA-93] Software Publishers Association, 1993, *Foreign Text, File, Data Encryption Programs and Products Identified by the SPA,* October 9, 1993.

[SSSC] System Security Study Committee, 1991, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991.

[Stev] Stevenson, R., 1993, "British Airways Tells Virgin Atlantic It's Sorry and Pays $945,000," *New York Times*, January 12, 1993, Sec. D.

[Tuer] Tuerkheimer, F., 1993, "The Underpinnings of Privacy Protection," *Communications of the ACM,* Vol. 36 (8), August 1993, pp. 69-73.

[TIII] Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. Sec. 2510 *et seq.*

[USDoT] U.S. Department of Treasury, 1985, *Criteria and Procedures for Testing, Evaluating, and Certifying Message Authentication Devices for Electronic Funds Transfer Use,* May, 1, 1985, Washington, DC.

[USC] U.S. Congress, Office of Technology Assessment, 1987, *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information,* OTA-CIT-310, Washington, D.C: Government Printing Office, October, 1987, Washington, DC.

[USGAO-92] United States General Accounting Office, 1992, "Advanced Communications Technologies Pose Wiretapping Challenges," *Briefing Report to the Chairman, Subcommittee on Telecommunications and Finance, Committee on Energy and Commerce,* House of Representatives, July 1992, Washington, DC.

[USS] United States Senate, 1974, *Final Report of the Select Committee to Study Governmental Operations with respect to Intelligence Activities,* April, 26, 1974, Washington, DC.

[USHR-87] House Report 100-153, 1987, Part 2, the Committee on Government Operations' Report on the Computer Security Act of 1987, Washington, DC.

[USHR-92] Hearing before the House Judiciary Subcommittee on Economic and Commercial Law, May 7, 1992, Washington, DC.

[Walk] Walker, S., 1993, Testimony for Subcommitte on Economic Policy, Trade and Environment, Committee on Foreign Affairs, U.S. House of Representatives, October 12, 1993, Washington, DC.

[Wie] Wiener, M., 1993, "Efficient DES Key Search," presentation at Rump Session of Crypto (August, 1993), Santa Barbara, CA. Available as TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994.