Data Encryption and Electronic Surveillance

By Dorothy E. Denning, Chair
Computer Science Department
Georgetown University

Phone calls and computer communications are often vulnerable to unauthorized interception. This is especially true for wireless communications, which can be picked up through cheap scanners. Similarly, information stored on computers can be susceptible to unauthorized retrieval.

Encryption protects sensitive information by concealing it from those who are not authorized to access it. It works by scrambling (encrypting) the information in such a way that it cannot be descrambled (decrypted) without knowing a secret key. For communications, this key must be shared by the sender and receiver for the duration of the session (for example, a phone call) and is usually referred to as the “session key.” If the method of encryption is sufficiently strong, an eavesdropper intercepting the encrypted communications will be unable to determine the secret session key and decrypt the information.

Encryption products have been on the market for years, but their primary use has been to protect classified information, and the main customers have been the government and government contractors. Until recently, the products have been expensive, bulky and difficult to use, and voice quality has been poor.

All this is changing as more and more encryption products are becoming available. AT&T is selling a telephone security device that is small, portable, easy-to-use, affordable and has high-quality audio. Strong encryption is being packaged into inexpensive software products and is being integrated into computer systems, networks and software applications. Free encryption software, such as Phil Zimmerman’s Pretty Good Privacy (PGP), is available on the Internet and local bulletin board systems, and its availability and use for file and e-mail encryption has been spreading throughout the world. In a continuing study originally commissioned by the Software Publishers Association, as of May 1994, Trusted Information Systems had identified...
Encryption and law enforcement

Encryption is an essential tool for organizations and individuals with sensitive information to protect. But it also presents an enormous challenge to the law enforcement and criminal justice community. The technology can be used not only by honest persons to protect against espionage and other forms of illegal activity, but also by criminals who use the technology to conceal their illegal activities from law enforcement. Already, investigations of child pornography cases have been hindered because seized computer files were encrypted with PGP, which could not be broken.

By rendering communications immune from lawful interception, encryption poses a particular threat to investigations that depend on wiretaps. Court-authorized interception of communications has been essential for preventing and solving many serious and often violent crimes, including organized crime, drug trafficking, government fraud, public corruption and terrorism. If the ability to conduct wiretaps is seriously diminished or precluded altogether, this could have major consequences for public safety and law enforcement.

Although encryption has not presented a serious problem to law enforcement so far, unless steps are taken now to avert it, it will become a major problem as the technology proliferates. The government’s Key Escrow Encryption Initiative is a first step toward providing such intervention, and is aimed at the area of greatest immediate concern: voice, facsimile, and other data transmitted over the telephone system.

The Key Escrow Encryption Initiative

On April 16, 1993, the U.S. government announced a new encryption initiative aimed at providing a high level of communications security and privacy without jeopardizing effective law enforcement, public safety and national security. The initiative is based on a special tamper-resistant hardware encryption device (Clipper Chip) and a key escrow system which allows an authorized government official to decrypt communications encrypted by a particular chip.

The Clipper Chip and its application

The Clipper Chip implements a strong encryption algorithm, called SKIPJACK, which uses 80-bit secret keys to control the encryption and decryption functions. The algorithm was designed by the National Security Administration and is classified secret.

Each chip has a unique identifier and key that is generated and programmed onto the chip after the chip is manufactured, but before it is placed in a security product. The device unique key is also split into two key components, which are encrypted and given to separate key escrow agents for safekeeping. The initial escrow agents are the National Institute of Standards and Technology and the U.S. Department of Treasury Automated Systems Division. Although the device unique key is not used for data encryption, a government official, pursuant to a lawful authorization, must acquire both of its escrow key components in order to decrypt communications encrypted by the chip.

On February 4, 1994, the government announced adoption of the technology as the Escrowed Encryption Standard (EES). The EES is a voluntary government standard for sensitive but
unclassified phone communications, including voice, facsimile, and data transmitted on circuit-switched systems at rates of standard commercial modems or which use basic rate Integrated Systems Digital Network or a similar grade wireless service.

The first product to use the Clipper Chip is the AT&T 3600 Telephone Security Device. The government purchased 9,000 of these devices for use by law enforcement and other Federal agencies.

The AT&T device plugs into an ordinary telephone between the handset and base-set. Although both parties to a conversation must have a device, the party at either end can initiate a secure conversation by pushing a button. Once this is done, the security devices enter into a protocol to establish a one-time secret session key for the conversation. This key is established using public key cryptography techniques that allow both devices to agree on a common secret key without exchanging any secret information, including the key. The same session key is used to encrypt and decrypt the communications transmitted in both directions.

Since the SKIPJACK algorithm operates on digital data, the device must convert the outgoing voice signals to digital before they can be encrypted. After encryption, a built-in modem converts them back to analog for transmission through the phone system. For incoming communications, the device converts the signals to digital, decrypts them, and converts them back to voice.

To allow for authorized government access, each Clipper Chip computes a Law Enforcement Access Field (LEAF) which is transmitted over the line before the encrypted communications. The LEAF contains the device ID and the session key for the conversation. The session key is encrypted under the unique key so that an eavesdropper cannot learn the key. In addition, the entire LEAF is encrypted under a family key that is common to all chips. To obtain the session key from an intercepted LEAF, one needs access to the escrowed device unique key plus a special key escrow decrypt processor that contains the SKIPJACK algorithm, a LEAF decryptor and the family key.

**Law enforcement decryption**

If a law enforcement official encounters what appears as noise on an installed intercept, then the communications must be passed through the key escrow decrypt processor — a PC with a specially designed board — to determine if they are Clipper communications. If they are, then the decrypt processor locates the LEAF transmitted in each direction and extracts the device ID of each (see illustration).

The device ID of the chip belonging to the subject of the intercept is then presented to the key escrow agents with a request for the device’s key components (since the same session key is used to encrypt both ends of the conversation, it is not necessary to obtain the device unique key for both parties). The request must provide certification of the legal authority to conduct the wiretap. Upon receipt of the certification, the escrow agents bring their respective key components to the law enforcement monitoring facility and enter them into the decrypt processor along with the termination date of the wiretap. Inside the decrypt processor, the key components are decrypted and combined to form the device unique key. The request for and release of escrowed key components must be done in accordance with procedures established by the U.S. Attorney General.

Once the decrypt processor has the device unique key, it can decrypt the session key in the LEAF, and then use the session key to decrypt the communications in both directions. For voice communications, additional equipment is needed to convert the decrypted digital streams to voice.

If subsequent conversations involving the target are encrypted, the decrypt processor can decrypt the session key directly, without the need to go through the escrow agents. This allows for real-time decryption. However, at the end of the authorized period of surveillance, the device unique key must be destroyed inside the decrypt processor so that it cannot be used beyond the period of authorization.

Currently, there is a single prototype decrypt processor. The target devices will support electronic transmission of data to and from the escrow agent workstations and automatic deletion of...
THE CLIPPER CHIP — HOW IT WORKS

A Law enforcement agency receives permission to conduct a wiretap.

B The conversation. A protocol establishes a one-time secret “session key” for the conversation. The same session key is used to encrypt and decrypt the communications transmitted in both directions.

C To allow for authorized government access, each Clipper Chip computes a Law Enforcement Access Field (LEAF) which is transmitted over the line before the encrypted communications. The LEAF contains the device ID and the session key for the conversation.

D The escrow agents. The device ID of the chip belonging to the subject of the intercept is presented to the key escrow agents with a request for the device’s key components. The request must provide certification of the legal authority to conduct the wiretap.

E Upon receipt of the certification, the escrow agents bring their respective key components to the law enforcement monitoring facility and enter them into the decrypt processor along with the termination date of the wiretap.

F Inside the decrypt processor, the key components are decrypted and combined to form the device unique key. Once the decrypt processor has the device unique key, it can decrypt the session key in the LEAF, and then use the session key to decrypt the communications in both directions.
device unique keys.

The key escrow system has extensive technical and procedural safeguards to ensure that keys do not get in the wrong hands or are used for anything other than a lawfully authorized surveillance. The entire system will be subject to verification and audit, and the U.S. Department of Justice will conduct inquiries to ascertain that keys are used only as authorized.

The Clipper controversy

The announcement of Clipper Chip has sparked a lively and often heated debate. Clipper’s strongest opponents have portrayed it as an Orwellian tool of oppression that will cripple privacy in advance of due process. They believe that citizens have the right to use strong encryption that evades government surveillance, and that exercising this capability is one way to protect against a government that cannot be trusted. While acknowledging the value of wiretaps in certain cases, they argue that society needs to be protected from the government more than the government needs to wiretap its citizens.

Clipper also has been criticized for being developed in secrecy without prior public review. Critics argue that encryption standards should be developed by an open process, with input from industry, academia, privacy groups and other interested parties.

Some of the criticism has been aimed not at the principle of key escrow encryption, but its use through Clipper. Clipper uses a classified encryption algorithm, which precludes public scrutiny and limits its acceptability. Moreover, because it uses a classified algorithm, it must be implemented in special tamper-resistant hardware. For many applications, software is preferred. The selection of escrow agents has been criticized, with critics arguing that at least one should be outside the Executive branch, either from the judiciary or private sector.

Critics also argue that Clipper products will have a limited foreign market as long as the algorithms are classified and the U.S. holds the keys, and that Clipper will not serve the needs for secure international communications. There is some interest in developing an international key escrow system.

Since Clipper is voluntary, many people argue criminals will not use it and it will be a waste of taxpayer money. In fact, cryptography without key escrow is spreading. Since key escrow is voluntary, the government could very well find itself locked out of many communications and stored files. The government, however, has a dilemma. If it promulgates encryption standards that preclude government access, such standards will be used by criminals to the detriment of society. The policy, therefore, is to adopt standards that permit only authorized government access.

While maintaining its commitment to key escrow, the Administration has responded to the criticisms by meeting with representatives from Congress, industry, academia, and privacy and public interest groups in order to better understand their concerns and explore alternative approaches to key escrow. Several alternatives have been proposed, including software-based approaches to key escrow that use unclassified algorithms, and private sector approaches that would give corporations and individuals a backup capability for protecting their own information assets, stored encrypted in files, from becoming inaccessible in case the keys are ever lost, destroyed or held for ransom.

While these proposals are promising, they do not appear to be replacements for Clipper, but rather alternative options that may be better suited for some applications. Clipper is a sound approach for phone communications. It offers excellent security, while serving the real-time needs of law enforcement. Most of the alternatives under discussion apply more to computer networks or file systems. However, even for computer networks, the Capstone Chip, which is a more advanced version of Clipper that includes algorithms for implementing the Digital Signature Standard and key exchange, is an attractive option for secure electronic mail and electronic commerce.

This report was written by Dorothy E. Denning of Georgetown University. Points of view or opinions are those of the author and do not necessarily represent those of SEARCH or the SEARCH Membership Group.
Capstone has been embedded in a Personal Computer Memory Card International Association crypto card for use in the Defense Messaging System.

Key escrow encryption offers the possibility of providing strong cryptographic protection while meeting the needs of society for law enforcement and national security, and the needs of organizations for a backup decryption capability. Eventually, international standards for escrowed encryption may emerge, and key escrow may become the dominant form of encryption.

Endnotes
1 Walker, S. T., testimony to the Committee on the Judiciary, Subcommittee on Technology and the Law, United States Senate, May 3, 1994.