information and communication systems. Every organization that has a network, that uses e-mail, that uses dial-up modems, needs to consider conducting a risk analysis. The threats–everything from outside hackers to your own employees–are waiting to gain access to your sensitive data.

Most companies already have hot sites or cold sites, maybe even disaster recovery planning software. Disaster recovery planning, continuity of operations and contingency planning should never be done without first performing a rigorous quantitative risk analysis. Why create an organized recovery plan without first doing everything possible to actually eliminate the weaknesses that would allow threats to impact your operations?.

Now that software exists that can cut down the time of a corporate risk analysis from months to weeks, more companies will take advantage of this powerful tool and computer systems will reach a new level of security.

Caroline R. Hamilton is president of Expert Systems Consulting, a software development company specializing in risk analysis software. Expert Systems Consulting, Inc. works with private companies, state and federal agencies on risk analysis issues. Hamilton has been working with risk management software since 1986. Prior to that, she was a consultant with management information software companies and a forecasting/research consultant for political campaigns. She writes for a variety of magazines on issues related to risk analysis and vulnerability assessment and is currently writing a book on risk management. Hamilton lives near Annapolis, MD with three rabbits, two beagles and one horse.

Key Escrow Encryption: The Third Paradigm

By Dr. Dorothy E. Denning

First paradigm: single-key

Cryptography is an ancient art. During the Gallic Wars, Julius Caesar encrypted his messages by shifting the alphabet forward by three letters, so that an A was encoded as a D and so on. With modern-day encryption systems, communications are first digitized into a stream of 0s and 1s, and the encryption algorithm transforms the "plaintext" stream of bits into a "ciphertext" stream that appears random. The transformation is parameterized by a secret key, which is also a random string of 0s and 1s, and the receiver must know this key in order to decrypt and recover the original message. One of the most popular methods of encryption is the Data Encryption Standard (DES), which encrypts 64-bit blocks using a 56-bit key. DES was adopted as a federal standard in 1977 and is used extensively by the banking industry. It is called a single-key cryptosystem since the same key is used both for encryption and decryption. Until the late 1970s, all cryptosystems were single-key systems.

Second paradigm: public-key

A new paradigm of cryptography emerged in 1976 when Whitfield Diffie and Martin Hellman of Stanford University published a paper introducing the concept of public-key cryptography. Public-key cryptosystems use matched pairs of keys, one public and the other private (secret). A sender can encrypt a message with the public key of the intended recipient, but then the message can be decrypted only with the receiver's private key. Or, the sender can "sign" the message with the sender's private key, which the receiver then validates with the sender's public key. Diffie and Hellman's landmark paper was followed quickly by one from MIT by Ron Rivest, Adi Shamir, and Len Adleman, which presented a method for achieving public-key cryptography. Now known as the RSA system, encryption and decryption involve exponentiations over large message blocks (e.g., 1024-bit) in modular arithmetic using keys of like size. Other public-key systems, for example, the Digital Signature Standard, which was adopted as a federal standard in 1994, use similar size blocks and keys. The keys are much longer than for DES because the mathematical structure of public-key systems would otherwise enable a private key to be readily computed from its corresponding public one.

Public-key cryptography was a major breakthrough since it enabled two people to communicate securely without first exchanging a secret key and it enabled digital signatures. However, public-key algorithms are several orders of magnitude slower than single-key algorithms. RSA chips, for example, run about 6,000 times slower than DES chips. For this reason, public-key systems are generally combined with single-key systems, with the single-key system being used for data encryption, and the public-key system to distribute the data encryption key and for digital signatures. For example, Internet Privacy Enhanced Mail (PEM) uses DES for message encryption and RSA for key distribution and digital signatures.

Third paradigm: key escrow

Although encryption has obvious benefits for information security, it is a dual edged sword in that it can be used by criminals and terrorists to conceal their communications from lawful surveillance by the government. Communications intercepts, loosely referred to as "wiretaps," have helped prevent and solve many crimes, often involving potentially substantial economic damage or loss of life. Even in the area of corporate

espionage where encryption is a valuable preventative measure, wiretaps have been useful in obtaining evidence against insiders who were leaking company secrets. Although encryption has so far not affected many wiretaps, this is expected to change with continuing advances in technology and increased availability of encryption products both for telephone and for computer communications. Encryption also can interfere with lawful searches and seizures of computer documents. Already, investigations of child pornography cases have been hindered because seized computer files were encrypted.

In addition to posing a threat to law enforcement and public safety, encryption threatens national security by interfering with foreign intelligence operations. For this reason, encryption technology is treated as munitions and subject to export controls. Except under limited conditions, products that use the DES and other strong encryption methods cannot be exported. Because DES-based products can be obtained overseas, industry has argued that the controls have succeeded only in putting U.S. industry at a competitive disadvantage. However, even though export controls have not prevented implementation of DES and other methods of encryption elsewhere, they have been effective in protecting valuable and fragile intelligence capabilities.

Finally, encryption poses a threat to organizations and individuals. If valuable data is stored in encrypted files, that data could become inaccessible if the file encryption key is accidentally lost or corrupted, intentionally destroyed or held for ransom by a disgruntled

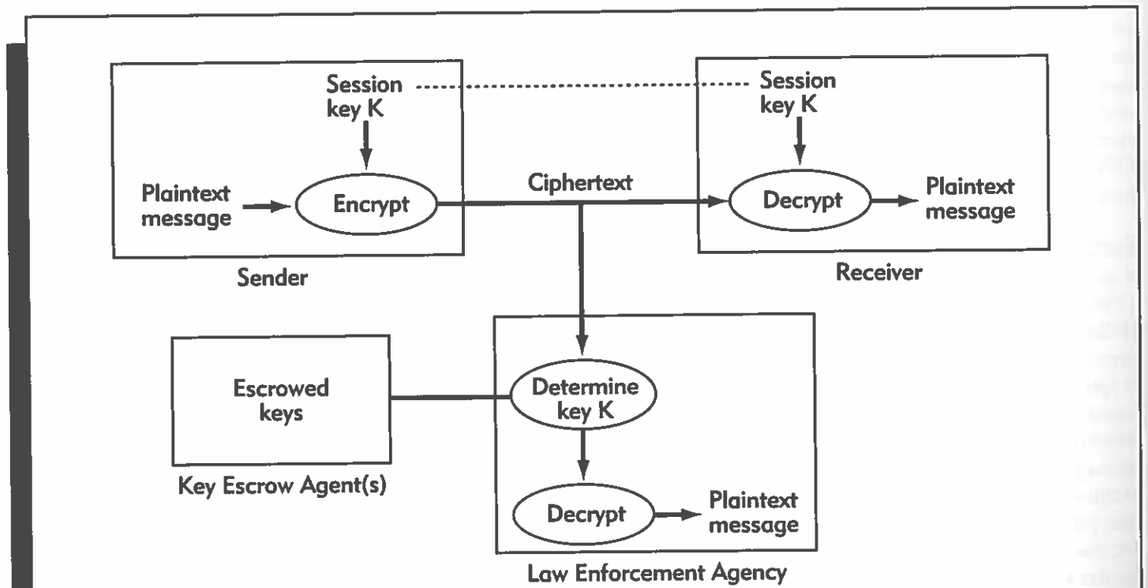

Figure 1. Key escrow encryption used in communications

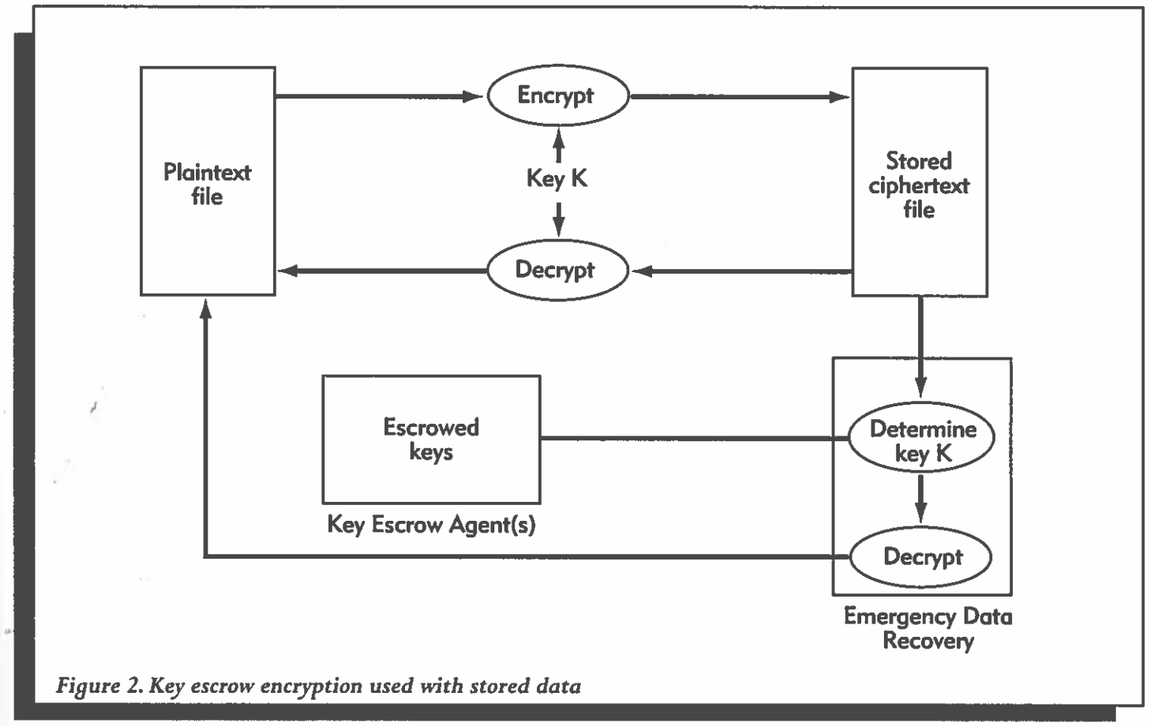

Figure 2. Key escrow encryption used with stored data

employee or former employee. In addition, encryption could be used by an employee to cover up fraud, embezzlement, espionage and other illegal activity.

Key escrow encryption emerged as a third paradigm in cryptography in order to minimize the potential harm of encryption while allowing its benefits to be realized. It does not replace single-key or public-key cryptography, but rather is an additional feature that is added to a cryptographic system. Its goal is to provide strong security while enabling authorized government decryption of intercepted communications, export of products with strong encryption, and emergency data recovery for organizations and individuals.

Key escrow encryption

Key escrow encryption (or escrowed encryption) is a form of encryption whereby authorized entities under prescribed conditions can decrypt ciphertext with the help of information supplied by trusted parties, called "key escrow agents," who manage one or more escrowed keys. These keys need not be the ones used for data encryption, but they must enable access to the data encryption keys. In this context, the term "key escrow" denotes the holding of secret keys by trusted third parties and not "escrow" in the legalistic sense.

The primary objective of escrowed encryption is to provide strong confidentiality protection with an emergency decryption capability that enables access to the plaintext of encrypted data through some mechanism other than the normal decryption process used by the intended

The Clipper Chip

Each Clipper Chip has a unique identifier (ID) and 80-bit key, which are 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 the exclusive-or (XOR) of two 80-bit key components, which are encrypted and given to the two key escrow agents for safekeeping. Although the device unique key is not used for data encryption, a government official must acquire both of its escrowed key components in order to decrypt communications encrypted by the chip.

For phone communications encrypted with the Clipper Chip, the two parties must first agree to use compatible security devices with Clipper Chips. These devices could be part of the phones or they could be separate units that plug into standard phones. After the call is made in the usual way, the two devices enter into a protocol to establish a common 80-bit secret session key. Each device then passes the session key to its Clipper Chip, which uses the key with the Skipjack algorithm to encrypt outgoing communications and decrypt incoming communications.

Skipjack is similar to DES in that both transform 64-bit input blocks into 64-bit output blocks. However, Skipjack's 80-bit keys are 24 bits longer than DES's 56-bit keys. The extra 24 bits provides about 16 million times better security against trial and error guesses at keys.

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 chip ID and the session key for the conversation. The session key is encrypted under the device 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 the device unique key plus a special key escrow decrypt processor that contains the Skipjack algorithm, a LEAF decryptor, and the family key.

If a law enforcement official encounters what appears as noise on an installed intercept, then the communications must be passed through a special decrypt processor to determine if they are Clipper communications. If they are, then the decrypt processor locates the LEAF transmitted in each direction and extracts the ID of each.

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 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. 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.

In the current key escrow system, keys must be carried manually from the programming facility to the escrow agents and from the escrow agents to the law enforcement facility. A target key escrow system is under development to support electronic transmission of data and automatic deletion of device unique keys.

recipient of the data. The data recovery capability can serve users of the encryption facilities, their organizations or authorized government officials.

Key escrow encryption can be used with both communications and stored data. Figures 1 (page 44) and 2 (page 45) illustrate.

Types of key escrow systems

There are three types of key escrow: government, commercial and private.

Government key escrow: Government agencies or organizations under contract to the government hold the keys. Their services are available only to authorized government officials.

Commercial key escrow: Commercial entities hold the keys and offer services to client organizations and individual customers. In addition, they make their data recovery services available to the government in accordance with the law.

Private key escrow: An organization or individual holds the keys for internal or personal use. The data recovery services may be available to the government in accordance with the law. A private key escrow system would be used primarily to protect stored data.

A private key escrow system operated by an organization could be useless to the government if the organization as a whole is under investigation, since a request for keys in conjunction with a wiretap, for example, would expose the wiretap. On the other hand, both commercial and private key escrow systems serve the needs of users for data recovery, whereas a government key escrow system does not. Thus, neither a government nor private key escrow systems is sufficient for all needs, although they could be used in combination. A commercial key escrow system has the potential of meeting all needs with a single system.

Government key escrow systems

On April 16, 1993, the Clinton Administration announced a new microelectronic encryption chip called the Clipper Chip that was to be used with a government key escrow system. The Clipper Chip was introduced as part of government encryption initiative for providing secure communications while meeting the needs of law enforcement.

Clipper and ESS

The Clipper chip is a hardware approach to encryption and key escrow. The chip implements an encryption algorithm called Skipjack and a Law Enforcement Access Field (LEAF) creation method, both of which were designed by the National Security Agency (NSA) and are classified.

A LEAF is transmitted with all encrypted communications and contains the data encryption key called a session key. The session key is encrypted under a

device key that is unique to the particular chip so that it is not exposed in the LEAF. The device unique key is the combination of two key components held by separate key escrow agents (the National Institute of Standards and Technology (NIST) and the Department of Treasury Automated Systems Division). Under certain conditions (normally requiring a court order), an authorized government official can acquire the components of a chip's key in order to decrypt communications encrypted with that chip. The key components are entered into a special decrypt processor, where they are combined and used to decrypt the session key in each LEAF (see sidebar, page 46 for more details).

The general specifications for Clipper were adopted in February, 1994, as the Escrowed Encryption Standard (EES), a Federal Information Processing Standard (FIPS 185) for encrypting sensitive but unclassified telephone communications, including voice, fax and data. The EES is a voluntary standard, meaning that non-government agencies have no obligation to use it and government agencies can choose between it and any other government encryption standard, in particular, DES. Devices that implement the EES are exportable. The AT&T 3600 Telephone Security Device (TSD), which plugs into an ordinary phone and enables encrypted communications with other TSDs, is available with the Clipper Chip.

In addition to Clipper, the EES is implemented in a more advanced chip, called Capstone, which also includes algorithms for the Digital Signature Standard and a public key algorithm whereby the sending and receiving parties can agree on a session key for use with Skipjack. Capstone is embedded in the Fortezza PCMCIA Crypto Card and used for secure electronic mail in the Defense Messaging System.

Safeguards

Even if an encryption algorithm is unbreakable, the coupling of that algorithm with a key escrow system potentially introduces some risk to data encrypted with that algorithm. Without proper safeguards, an intruder might break into a computer containing escrowed keys, download the keys, and use the keys to decrypt communications intercepted illegally. Alternatively, a corrupt employee of the escrow center might use the keys to engage in illegal wiretapping or sell the keys to a foreign government or to the mafia.

Clipper's key escrow system is being developed with extensive security controls to protect against both insider and outsider threats to the keys. I will describe some of the safeguards that are currently implemented as well as those that are planned for the target system, which will automate the transmission of key components between the escrow agents and the chip programming site and the decryption site.

One safeguard that is fundamental to the entire design is key secrecy. No individual ever sees the value of any key or key component. Keys and key components are generated in computers and are never displayed or output in human readable form.

The principle of separation of duties is used to limit the power of a single person or agency. Escrow officers are not allowed to program the Clipper Chips, operate a decrypt processor, or even have a decrypt processor in their possession. Law enforcement officers have access to a decrypt processor, but never to keys. In the target system, the escrow officers will specify a "self destruct" date, corresponding to the end of the period of authorized surveillance, for keys that are released and transmitted to a decrypt processor.

Two person control, which requires that at least two people be present when a critical function is performed or when sensitive data might be exposed, is used throughout the key escrow system to further limit the power of a single individual to abuse the system. It is combined with split knowledge so that it is not even possible for one person to act independently. Not only are Clipper keys split between two independent escrow agents, but at each agent, it takes two escrow officers to unlock the safes that contain the key components, and in the target system, it will take two persons to release keys electronically to a remote decrypt processor. Two person control has worked successfully in the banking world and in the military to control the nuclear launch control codes.

All operations that involve the generation, release or use of escrowed keys are logged and periodically audited by the Department of Justice. In the target system, logging will be done automatically by the computers that perform the operations. From the logs, it should be possible to determine that keys are used only as authorized and only to decrypt communications intercepted during a period of authorized surveillance.

Physical security is used extensively to protect sensitive material. Programming is performed in a Sensitive Compartmented Information Facility (SCIF). Key components are always stored in a place that is approved for classified information and requiring two persons to gain access. When key escrow data are transported on floppy disks, they are wrapped in tamper-detecting packages.

The key escrow system uses encryption and cryptographic authentication techniques to protect all keys and key components, and to control access to the system by authenticating users and computers. Keys and key components are always stored and transmitted in encrypted form. In the target system, when the escrow agent workstations are set up to communicate electronically with a decrypt processor and with the programming facility, encryption and authentication techniques, including digital signatures, will ensure that unauthorized persons and devices cannot even connect to any component of the key escrow system.

Computer security practices are employed to protect against unauthorized access and against malicious software. The workstations used for key escrow operations are dedicated to key escrow functions and kept in secured facilities. When the target system is fully operational, trusted operating systems will be used to enforce access control and need-to-know protection.

All designers, implementors and escrow officers are cleared to at least the Secret level. The key escrow system does not, however, rely solely on clearances. All components use additional safeguards to protect against attacks that could be made by cleared personnel.

Configuration management is used to protect against unauthorized modifications of software. Key components will not be released for other than testing purposes until the software has been placed under configuration control (no components have thus far been released). In addition, the key escrow system must be accredited by the Department of Justice.

The key escrow system is undergoing independent validation and verification. In addition to paid contractors, four individuals, including myself, are voluntarily reviewing the system as an extension of our earlier review of the Skipjack algorithm. From what I have seen so far, my assessment is that the risk of an insider or outsider acquiring unauthorized access to keys will be negligible.

Although the key escrow system should provide sufficient security that Clipper keys are not vulnerable to theft or compromise, some people are concerned that a future Administration could order the release of keys to conduct questionable if

not outright illegal wiretaps. I believe that the possibility of such activity occurring will be remote, and that if any abuses do occur, they will be stopped. Neither the public nor Congress has tolerated wiretap abuses in the past, and federal wiretap laws, government regulations and procedures, and Congressional oversight committees have been established to protect against their occurrence in the future. I know of no recent evidence of widespread abuse of wiretaps by law enforcement or intelligence agencies. Wiretaps today are conducted under tight controls and subject to considerable oversight.

TIS software Clipper

Clipper is implemented in special tamper-resistant hardware in order to protect the classified Skipjack algorithm from disclosure and to minimize the risk of its being used without the law enforcement access feature. Some vendors have stated that they would prefer a software approach, mainly because it would be cheaper, but also because it could be integrated readily into software applications. Although a software solution would preclude the use of Skipjack (there is no known way of hiding classified information in software), replacing Skipjack with a public algorithm such as DES could increase the market for key escrow products since some potential users may not trust an NSA-designed algorithm. Software provides less security and integrity than hardware, but for some customers, this may not be a deciding factor.

Trusted Information Systems (TIS) has proposed a software key escrow system that is similar to Clipper, but uses software rather than hardware. Like Clipper, it uses a LEAF to make the data encryption key available, and it assigns a unique identifier and key to each product (in this case, program instance). However, in order to avoid putting either secret algorithms or secret keys in software, it uses unclassified algorithms and public-key cryptography to compute the LEAF and for key escrow functions. Only the public keys of public-private pairs are actually stored in the products. One disadvantage of a public-key LEAF is that it is longer and has more overhead than a single-key LEAF, which could be a factor in certain applications. TIS has built a prototype of their design that runs on a Sun workstation and handles interactive computer communications.

Commercial and private systems

There have been several proposals for commercial and private key escrow systems. The following are brief descriptions of four of these.

Bankers Trust International

Bankers Trust has proposed an international commercial key escrow system for secure communications. Their proposal uses a combination of hardware, unclassified algorithms, and public-key cryptography for key establishment and key escrow functions. Each user has a trusted encryption device, which has a permanent unique identifier and a public-private signature key pair. In addition, each user has a public-private signature key pair and a public-private encryption key pair that is used for establishing session keys. The encryption keys are stored in escrow and may be split among several escrow agents. The keys are escrowed through a device registration process. Upon completion of registration, the user's device is given an escrow certificate identifying an escrow center and providing other information needed for data recovery. Each escrowed certificate has a unique number.

To send an encrypted message, the sender's device creates a Message Control Header (MCH), which contains a randomly generated session K encrypted under the public encryption key of the sender plus a copy of K encrypted under the public encryption key of the receiver. In addition, it identifies the sender and receiver and their escrow centers, and it contains encrypted escrow certificate numbers for both the sender and receiver. The MCH serves the dual role of distributing K to the intended recipient and enabling data recovery. The MCH is signed by the sending device.

For emergency data recovery, the private encryption key of either the sender or receiver is obtained from the key escrow agents and used to decrypt K in the MCH.

TIS commercial key escrow

TIS has proposed a commercial software key escrow system that could be used with either stored data or communications. With this system, a commercial entity serves as a key escrow agent and operates a Data Recovery Center. To use the services of a particular center, a user must register with the center and obtain a user identifier and the center's public key. Whenever data are encrypted, a Data Recovery Field (DRF) is created and attached to the encrypted data. The DRF, which is analogous to Clipper's LEAF, contains the data encryption key K (or any other data) encrypted under the center's public key. It also identifies the user, the center, and the particular public key of the center that was used (these keys can be regularly updated).

If the user later loses the key to an encrypted file, say, then the user presents the DRF to the center along with data that authenticates the user. After authenticating the user, the center decrypts K using the center's matching private key and returns K to the user. An authorized government official similarly use the center's services to obtain the key needed to decrypt data that had been legally intercepted or seized.

The data recovery services could be performed by licensed (and possibly bonded) organizations. They may also be performed within an organization as a private key escrow service.

AT&T CryptoBackup

CryptoBackup is an AT&T proprietary design for a commercial or private key escrow encryption system. The data encryption key for a document is derived from a public key of a Backup Agent (which is like an escrow agent) and a random number. The random number is inserted into a Backup Recover Vector (BRV) in such manner that the Backup Agent can recover the data encryption key using its corresponding private key. The BRV is stored in the document header and serves a role similar to that of the DRF in the TIS design.

TECSEC VEIL

VEIL is a cryptographic product of TECSEC, Inc., which provides file encryption with a private key escrow capability. All file encryption keys are derived from a set of "sub-key splits" that are managed by the organization. Each user has a subset of these splits. When a file is encrypted, a 1024-byte file header is attached to the file. The header contains pointers to the particular sub-key splits used to derive the file key and serves both as a mechanism for distributing the key to persons authorized to access the file and as a data recovery field. The key can be recovered only if one has all of the sub-key splits used to create the key.

VEIL is a stand-alone Windows application that can be interfaced into Windows applications. It works with both hardware and software implementations of encryption algorithms. Up to ten different encryption algorithms can be used at a given time.

Conclusions

The introduction of key escrow encryption shifted the paradigm of cryptography from one that recognized only encryption's benefits for secrecy and authentication to one that rec-

ognized encryption's potential harm to individuals, organizations and society if keys are lost or law enforcement is undermined. It attempts to maximize encryption's benefits, while minimizing its potential harm. In addition, because it allows for authorized government decryption, key escrow encryption may allow industry to develop a single product line that contains strong encryption and is exportable.

The Clipper Chip is an initial approach to key escrow that combines a hardware encryption chip with a government key escrow system. It provides excellent security–indeed the best security on the market–and is exportable. The Fortezza card with Capstone is particularly attractive since it implements the cryptographic functionality needed for secure applications such as electronic commerce and electronic mail. However, the market potential for Clipper/Capstone is limited by its use of a classified algorithm and government key escrow system, and by its special hardware requirements. Other approaches to key escrow that allow for unclassified algorithms, commercial key escrow, or software implementation may increase the market for key escrow products, especially if such products can be implemented with DES or better-strength encryption algorithms and still be exportable.

Key escrow encryption might provide a basis for an international encryption standard. So far, there is no international standard providing end-to-end confidentiality protection. DES is used world-wide, especially by the financial industry, but its use is mainly for authentication and integrity protection of financial transaction rather than message secrecy. GSM (Global System for Mobile) has been adopted in countries around the world for mobile radio communications security, but GSM encrypts only the over-the-air link between a mobile phone and a base station.

Thus, governments can intercept communications elsewhere in the network. An encryption method providing end-to-end secrecy between two parties with no capability for government access is unlikely to be accepted by governments as an international standard given national cryptography policies. Key escrow, however, offers the possibility of providing both end-to-end security and government access. Each country could operate its own escrow agents, which might be private sector agents providing commercial key escrow services. Mutual assistance agreements might be established whereby a country holding keys that are needed for an investigation in another country could assist the latter with decryption under appropriate conditions.

In summary, key escrow encryption offers the possibility of meeting user needs for strong security, data recovery, and secure international communications; vendor needs for providing products that satisfy user requirements and are exportable; and law enforcement and national security needs.

Dr. Dorothy E. Denning is professor of computer science at Georgetown University, where she is currently working on policy and technical issues relating to encryption and its impact on law enforcement. She has been an outside reviewer of the government's Clipper Chip and key escrow system and is studying alternative approaches to key escrow while working towards an international solution. Prior to Georgetown, she was a researcher at Digital Equipment Corporation, a senior staff scientist at SRI, and an associate professor at Purdue University. She is author of Cryptography and Data Security *and numerous papers on information security. In 1990, she received the Distinguished Lecturer in Computer Security Award. She chaired the Forum on Rights and Responsibilities in Network Communities for the National Research Council and is chair of the International Cryptography Institute sponsored by the National Intellectual Property Law Institute. She is past president of the International Association for Cryptologic Research. She received her doctorate in computer science from Purdue.*

Point/Counterpoint: Phil Zimmerman and Dorothy Denning on Key Escrow and the Future of Crypto

By Richard Power

Encryption technology is a subject of growing importance in the development of comprehensive information security solutions for the 21st century. There is furious debate concerning which standards to adopt and how to resolve the various technical and human issues involved. To help elucidate some of the vital areas of contention, we've asked two of the major voices in this debate–Phil Zimmerman and Dorothy Denning–to engage in a brief point/counterpoint on the future of crypto.

Phil Zimmerman is the author of Pretty Good Privacy (PGP), a public-key encryption software package. PGP is freely available in the public domain. According to Zimmerman, the program has become a kind of de facto world-wide standard for public-key encryption for individuals. The global popularity of PGP has brought Zimmerman both acclaim and discord. The U.S. government has been investigating whether or not he has participated in the violation of its export restrictions on encryption. Whatever happens vis-a-vis this ongoing hassle, the widespread use of Zimmerman's product has raised our consciousness about some of the critical issues that must be resolved.

Dr. Dorothy Denning of Georgetown University is one of the leading authorities on cryptography and has made a significant contribution to information security in both the private and public sectors. She is also an articulate voice in the heated national controversy surrounding the Clinton administration's Clipper Initiative. She has done much to counteract misconceptions about this much-maligned proposal.

Phil, you've mentioned that Clipper could become de facto standard in spite of widespread disapproval, could you expand on that idea?

Zimmerman: The government has made it clear that they are still going to push Clipper for telephones and fax machines. If government spending power is used to pump it into the commercial channels Clipper could become a de facto standard. But there is this peculiar dynamic when you predict what's going to happen. If you're too pessimistic, people say "Oh, there's nothing I can do." If you're too optimistic, people sit back and say, "Oh, I don't have to do anything." What happens to Clipper depends on what we do, and we're going to have to work hard to stop it. And I really mean the whole problem, Capstone, Clipper, who cares what chip it is? Who cares if it's even a chip? It's all the same thing–it's key escrow.

Denning: The government has been working closely with industry to investigate alternatives to Clipper that would overcome many of the objections that have been raised. But I don't understand Phil's objection to the use of Clipper as long as it's voluntary. Right now, most of our phone conversations are in the clear and vulnerable to illegal interception. Widespread adoption of Clipper is not going to make those conversations more vulnerable than they already are. Rather, to the extent that Clipper is used, it will protect them! Phil is free to push PGP, but I find it ironic that he argues for the free and widespread use of encryption methods of his choice while attempting to stop those of us who want to use Clipper from using a