87-20-20 Key Escrow Encryption Policies and Technologies

Dorothy E. Denning
William E. Baugh, Jr.

Payoff

In today's information age, encryption is considered essential to ensure the security of electronic data and transactions. At the same time, there is growing recognition that the spread of powerful encryption is not entirely beneficial. Terrorists, drug dealers, and others can use it to facilitate their crimes and operate with impunity. As encryption proliferates worldwide, it could seriously imperil the ability of law enforcement agencies to counter domestic and international organized crime and terrorism. It could also cut off valuable sources of foreign intelligence, which have been vital to national security. Even within an organization, encryption has potential drawbacks. If keys are lost or damaged, valuable data may become inaccessible. Employees can use encryption to cover up fraud, espionage, and other crimes. This article discusses joint US government and industry initiatives to develop key escrow encryption standards and products that will greatly minimize security risks to electronic data.

Introduction

In April 1993, the Clinton Administration announced an initiative to promote encryption in a way that would simultaneously satisfy the objectives of security and privacy, public safety, and national security. This initiative was to be accomplished through the adoption of key escrow encryption standards and products. Key escrow encryption makes use of special data recovery keys, which are held by a trusted fiduciary for the purpose of enabling backup decryption. Use of the backup decryption capability is restricted to users and government officials who have been authorized to access the information that has been encrypted.

By providing a mechanism for authorized government access, key escrow products were to have another advantage: They would be exportable. US law defines encryption products as munitions, which cannot be exported without a license. Businesses have objected that export regulations have made it more difficult for them to obtain strong encryption to protect international communications. US manufacturers of computer products say it puts them at a competitive disadvantage in the global marketplace.

As part of the government's encryption initiative, the National Security Agency (NSA) developed an initial implementation of escrowed encryption in a microelectronic chip called the Clipper Chip. AT&T integrated the chip into a telephone security device to provide secure voice communications. Although the Clipper Chip offered strong, exportable encryption, it met with criticism from industry for four reasons:

- Its encryption algorithm was classified.
- It required special hardware.
- The government held the keys.
- It did not accommodate user data recovery.

Subsequently, the government began working with industry to develop a more flexible approach to key escrow that would address the objections raised and meet the needs of both

Previous screen

users and the government. In August 1995, the government announced a proposal to allow the general export of software encryption products with unclassified algorithms and up to 64-bit keys, provided the products were combined with an acceptable key escrow mechanism. Keys would be held by government-approved trusted parties within the private sector, where they would support both user data recovery and legitimate government decryption. The proposal, which is still undergoing refinement as of December 1995, is expected to be implemented in early 1996.

The Administration also announced plans to develop a Federal Information Processing Standard (FIPS) for key escrow encryption implemented in software. The Federal Information Processing Standard promulgated by the National Institute of Standards and Technology would be used by federal agencies and other interested organizations in conjunction with Federal Information Processing Standard promulgated by the National Institute of Standards and Technology-approved encryption techniques.

Key Length

Under current export policy, software encryption products with keys longer than 40 bits are exportable only by obtaining a license from the Department of State. The vendor must apply for a separate license for each customer. In comparison, products with key lengths not exceeding 40 bits are readily exported under general licenses administered by the Department of Commerce. Consequently, many products developed by US companies for the international market use 40-bit keys.

40-Bit Keys

The longer the key, the harder it is to break the code. For many applications, 40-bit keys provide adequate protection. However, they are not foolproof. In the summer of 1995, a French student cracked a 40-bit key in eight days using 120 workstations and a few supercomputers. The key gave him access to a dummy purchase order that had been encrypted with the overseas version of a popular program used for browsing the World Wide Web. Even though a substantial investment of resources was required to crack a single message, many potential users regard the incident as indication that 40-bit keys are unacceptable.

As a result, some US companies complain they have lost sales to foreign competitors that were able to provide stronger encryption, including the Data Encryption Standard (DES), which uses 56-bit keys. They cite the widespread availability of products using DES and other encryption algorithm worldwide as evidence that export controls limit US companies' competitiveness in the global market. As of June 1995, Trusted Information Systems (TIS) of Glenwood, Maryland had identified 455 encryption products from 27 countries, 179 of which use DES. In some cases, software vendors have built separate product lines for domestic and foreign sales in order to meet the demands of US customers for DES or better encryption.

64-Bit Keys

Some critics contend that the increase from 40 to 64 bits is minimal, despite the fact that each bit doubles the number of possible keys and thus the effort required to crack a key. Therefore, the additional 24 bits gives about 17million times better security. It would have taken the French student 136million days—or about 2 billion computers in 8 days—to crack a single 64-bit key. At the current rate of technology advancement, it would be several decades before the French student could break a 64-bit key in 8days with updated computers. 64 bits is likely to provide a high level of security for at least the next 20 years. Furthermore, if a company sends out numerous messages per day, each encrypted with a

Previous screen

different key, the effort required of an adversary to break all keys in the hopes of finding a message worth reading becomes all the more impractical.

For the near term, DES combined with key escrow can provide strong security while being implementable in exportable software products. For the longer term, DES, which is now about 20 years old, can be replaced with a 64-bit algorithm. Despite its age, Data Encryption Standard still offers robust encryption. It may have a decade or more of useful life remaining.

Revised Export Criteria

To qualify for general export under the Administration's proposal, an encryption product must provide an acceptable key escrow mechanism. Draft criteria for export of software key escrow encryption were issued in early September 1995and then refined and reissued in November for comment. Meetings were held at the National Institute of Standards and Technology (NIST)in September and December for the purpose of discussing the criteria and soliciting comments from industry.

The export criteria are intended to ensure that the government can, when lawfully authorized, readily access keys and decrypt intercepted communications and stored information in a timely manner. Products must include information in the encrypted data that identifies the escrow agent(s) and the particular keys needed for decryption. Keys must be held by escrow agents certified by the US government or by foreign governments with which the US government has formal agreements. The conditions under which companies could hold their own keys have not yet been addressed.

Access

Compliant products must allow access to encrypted communications from both ends of the channel. This is so communications sent both to and from a subject of investigation can be decrypted using only the subject's keys. Compliant products must allow for the decryption of multiple messages during a period of authorized access without requiring repeated presentations of the access authorization to the escrow agent(s).

Resistance to Alteration

Products must be designed to resist alterations that would circumvent or disable the key escrow mechanism. The escrowed encryption functions must interoperate only with escrowed functions in other products. They must not interoperate with products whose key escrow features have been altered or disabled.

Multiple Encryption Modes

Exportable products will be allowed to use keys up to 64 bits long, but they must not provide multiple encryption modes that effectively increase the key length. For example, the criteria will allow the use of Data Encryption Standard, but not triple DES, which uses two keys (112 bits)or three keys (168 bits).

System Integrity and Security

The draft criteria for the selection of escrow agents, released at the December 1995 meeting of National Institute for Standards and Technology, address requirements for escrow system integrity and security and key access. Escrow agents will be required to ensure the confidentiality, integrity, and availability of key escrow information and the confidentiality of requests for that information. They will need to ensure due form of all

Previous screen

requests and respond to such requests in a timely fashion. They will also need to maintain audit records of all events relating to the management and release of keys.

To obtain a license under the Administration's new proposal, a vendor with a candidate product would submit the product to the Department of State for review. If the Department determines that the product meets the criteria for export, it would be granted a commodity jurisdiction transfer. It would then be exportable under a general license administered by the Department of Commerce.

Industry Reaction

Reaction to the government's proposal has been mixed. TIS and TECSEC, Inc. have submitted products for review and are likely to be joined by other companies. Some major corporations that are adopting corporate key escrow policies to protect their own interests have said that the government's proposal might mesh with their goals if they are permitted to hold their own keys. The Software Publisher's Association and the Business Software Alliance issued statements calling for the liberalization of export controls independent of whether key escrow is used. A coalition of nearly 40 public-interest groups, trade associations, and representatives from industry led by the Center for Democracy and Technology(CDT) sent a letter to Vice President Albert Gore in November saying that the proposal did not address the need for immediate liberalization of export restrictions and that it was no substitute for a comprehensive national cryptography policy. The CDT-led coalition pledged to develop an alternative proposal in six months.

However, the Administration's proposal is a major step forward. It would allow a vendor to develop a single product line for both domestic and international sales, using software or hardware implementations of Data Encryption Standard or stronger 64-bit algorithms. This step should facilitate the seamless integration of strong encryption into network and applications software, thereby making it cheaper and easier for businesses to encrypt their electronic transactions and proprietary data, and thus facilitating electronic commerce. If strong algorithms are implemented in both domestic and international products, businesses will be able to communicate securely with customers, suppliers, partners, investors, and subsidiaries throughout the world.

Some vendors and users may not accept the 64-bit limit on keys. One company, which uses 128-bit keys in its domestic products, said that such a limit would compel the company to continue manufacturing two product lines. Critics of the limit argue that because safe access is possible through the key escrow system, there is no reason to restrict key size. The government's stand is that the strength of 64-bit keys, given the limited experience with key escrow and the inherent risk, is adequate. After key escrow systems have been more widely deployed and proven effective, longer key lengths may be permitted. All in all, 64 bits is more than adequate for virtually all business transactions.

Key Escrow Approaches and Products

There is no single approach to escrowed encryption, but all methods follow a few general principles.

Generating a Data Recovery Key

The data recovery key used with a particular encryption product is generated by or given to a trusted party sometime before the product is used. For example, it might be generated and escrowed during product manufacture or when the product is initialized and registered with an escrow agent. The key could be unique to an individual product or user or it could be shared by many users. It could be held by a single escrow agent or it could be split into several components, with each component held by a separate entity.

Previous screen

Allowing Backup Decryption

Whenever a document (or message stream) is encrypted by the product, the product attaches to the encrypted document sufficient information to allow backup decryption. For example, the data encryption key might be encrypted under the data recovery key and placed in a document header. If the encryption key is later lost, the user or an officer in the user's organization would give that information to the escrow agent and request assistance. After determining that the request is authentic, the escrow agent would either release the data recovery key (if it is unique to the user) or else use the key to determine and release the data encryption key. If an investigative or intelligence agency needs access to the key during the course of an authorized search or communications intercept, the agency would present certification of the legal authority to access that information (normally a court order) to the escrow agents. Legitimate privacy interests can be protected through access procedures, auditing, and other technical, legal, and operational safeguards.

Clipper Chip vs. Fortezza

The Clipper Chip implements the Escrowed Encryption Standard (EES), a voluntary government standard (FIPS 185) for encrypting sensitive but unclassified low-speed telephone communications, including voice, fax, and data. Each chip has a unique data recovery key, which is split between two government escrow agents: the National Institute for Standards and Technology and the Department of Treasury Automated Systems Division. Data is encrypted with the classified Skipjack algorithm, which uses 80-bit keys. Products that implement the EES must use tamper-resistant hardware in order to protect the classified algorithms. They are generally exportable.

The Clipper Chip is a scaled-back version of a more advanced chip, called Capstone, which the NSA developed for use in the Fortezza card (a Personal Computer Memory Card International Association card). The goal was a small, affordable, and extremely secure hardware token that would provide a full suite of cryptographic services for confidentiality protection, authentication, and digital signatures.

Capstone implements the EES plus public-key cryptographic algorithms for the Digital Signature Standard and for generating and establishing session keys. A Fortezza Personal Computer Memory Card International Association modem card also is available so that encryption and decryption can be performed either as part of the transmission protocols or as independent service calls, for example, to encrypt or decrypt files and electronic mail messages. The government plans to extend the scope of the EES to cover high-speed communications over computer networks so that Fortezza and other Capstone-based devices will meet approved standards for use by federal agencies.

Clipper's key escrow system supports backup decryption by authorized government agencies but does not help users with lost or damaged keys. Fortezza, on the other hand, was designed to also allow user data recovery. This is accomplished through the certificate authorities which grant certificates for the public keys used for key establishment and digital signatures. Those same authorities escrow the user's corresponding private keys, which are stored on the Fortezza card; the keys can be recovered from the certificate authority in case the card is lost or the keys become corrupted.

Although Fortezza was developed as part of NSA's Multilevel Information Systems Security Initiative (MISSI), the technology is available commercially. Support for Fortezza has already been added to AT&T SecureAgent, Netscape Navigator, Oracle's Secure Network Services, and other products.

Some type of key escrow is a feature or option of several commercial products including Fisher Watchdog, Nortel's Entrust, PC Security's Stoplock KE, Rivest_Shamir-Adleman Secure, and TECSEC Veil.With all these products, escrowing can be done within the user's organization. In some cases, it is integrated into the company's key management infrastructure. Bankers Trust is developing a commercial key escrow system that uses third

Previous screen

party escrow agents. Keys, which are stored on hardware cryptographic tokens, can be split between multiple agents. TIS is developing a commercial key escrow system which could be used with either hardware or software encryption products. National semiconductor has proposed to implement the TIS system using the PersonaCard (a PCMCIA cryptographic card) with the goal of producing an exportable product with strong security and a data recovery capability. Other proposals have come from researchers at AT&T, Bell Atlantic, Cylink, Fortress U&T, Karlsruhe University, Massachusetts Institute of Technology, Royal Holloway, and the University of Wisconsin.

The cost of key escrow is difficult to estimate, especially given the wide range of approaches. One approach, used by Fortezza and Entrust and adopted by several of the proposals, includes escrow with the services provided by public-key certificate authorities. Another, used by Stoplock and Veil, integrates escrow into the overall key management infrastructure. With both of these approaches, the incremental cost of escrow may be relatively low.

Although the government's export proposal explicitly addresses software encryption, hardware products may also be considered for export. The advantage of hardware is that it generally offers greater security than software. In addition, it can better protect against tampering, which would disable or circumvent the key escrow mechanism. For this reason, hardware products with key escrow might be approved for export with even longer keys. Clipper and Fortezza, for example, use 80-bit keys with Skipjack. While software has the advantage of being cheaper, with mass production the cost of hardware need not be prohibitive. One cost-effective strategy is if the encryption is combined with authentication mechanisms on a single token that can be used for access control and other security purposes (e.g., as with Fortezza).

There is a strong market for escrowed encryption products. In recognition of the threats posed by uncontrolled cryptography, some companies have adopted internal security policies requiring key escrow. At the International Cryptography Institute in September 1995, Nick Mansfield of Shell International reported that key escrow is used in Shell Group enterprises. Keys are escrowed by a trusted Shell service company on behalf of the shareholders and businesses. This provides the shareholders with an independent ability to decrypt information should the need arise. Business continuity is supported by a fallback mechanism to recover encrypted data in the event of a disaster.

International Efforts

Several products and proposals for key escrow have come from outside the United States. In addition, other governments have been considering encryption policies based on key escrow. Although not speaking on behalf of their governments at the International Cryptography Institute in September 1995, Peter Ford, from the Australian Attorney General's Department, and David Gould, formerly with the UK Cabinet Office, both expressed interest in the use of key escrow to resolve the dilemma posed by encryption.

Setting Up a Network

Gould commended the idea of a European-wide network of trust services, under the control of member states, accredited to offer digital signatures, confidentiality, data integrity, and other services. Such a network should be interoperable with other international arrangements. The trusted parties, which could be commercial or private entities, would also serve as key escrow agents. The European Commission is proposing a project to establish such a network of trusted third parties.

Previous screen

Developing Policy Guidelines

At a meeting sponsored by the Organization for Economic Development (OECD) and the International Chamber of Commerce (ICC) in December 1995 in Paris, representatives from the international business community and member governments agreed to work together to develop encryption policy guidelines based on agreed-upon principles that accommodate their mutual interests. The INFOSEC Business Advisory Group (IBAG) issued a statement of 17 principles that they believe can form the basis of a detailed agreement. IBAG is a collection of associations representing the information security interests of users.

The IBAG principles acknowledge the right of businesses and individuals to protect their information and the right of law-abiding governments to intercept and lawfully seize information when there is no practical alternative. Businesses and individuals would be required to lodge keys with trusted third parties which would be liable for those keys. In the case of multinational businesses, that third party could be a unit within the enterprise. The keys would be available to businesses and individuals on proof of ownership and to governments and law enforcement agencies under due process of law and for a limited time frame. The process of obtaining and using keys would be auditable. Governments would be responsible for ensuring that international agreements would allow access to keys held outside national jurisdiction. The principles call for industry to develop international standards and for governments, businesses, and individuals to work together to define the requirements for those standards. The standards would allow choices about algorithm, mode of operation, key length, and implementation in hardware or software. Products conforming to the standards would not be subject to restrictions on import or use and would be generally exportable.

EUROBIT (European Association of Manufacturers of Business Machines and Information Technology Industry), ITAC (Information Technology Industry Association of Canada), ITI (Information Technology Industry Council, US), and Japan Electronic Industry Development Association (JEIDA) also issued a statement of principles for global cryptography policy at the European Organization for Economic Cooperation and Development meeting. This quadripartite group accounts for more than 90% of the worldwide revenue in information technology. Acknowledging the needs of both users and governments, their principles call for harmonization of national cryptography policies and industry-led international standards.

The US government's software key escrow export proposal appears consistent with the principles identified by the international business community. Thus, it seems likely that if international standards are adopted, US vendors will be able to develop products that simultaneously conform to those standards and to the export criteria.

Conclusion

Key escrow offers a valuable service to individuals, organizations, and society. While benefiting law enforcement, it protects businesses from a host of problems ranging from misplaced keys to espionage. Various initiatives on the part of governments and industry worldwide are leading toward policies and standards for key escrow.

Because the government's key escrow program is voluntary, there is no guarantee that criminals will choose it over unescrowed encryption. Nevertheless, the program satisfies an important objective: Terrorists and criminals will be unable to take government-sponsored codes and turn them against the government and society. Further, it is hoped that government purchasing power combined with export controls will have some positive influence on both domestic and international markets. Finally, responsible corporate participation will ensure that entirely inaccessible networks are not created, to the detriment of both government and industry.

Previous screen

Author Biographies

Dorothy E. Denning

Dorothy E. Denning is a professor of computer science at Georgetown University. Her current work is focused on policy and technical issues relating to encryption and law enforcement, including Internet encryption policy and key escrow techniques.

William E. Baugh, Jr.

William E. Baugh, Jr., is Vice President, Information and Technology Systems, at Science Applications International Corporation in McLean, Virginia. Previously, he has served for twenty-six years in the Federal Bureau of Investigation, where he was Assistant Director of Technical Operations and Information Technology.