Encryption Policy Issues

Jon M. Peha[1]

October 1998

Section 1: Introduction

Controlling the flow of information in the information age is as important as controlling the flow of water in the desert. Encryption is a critical tool for managing and protecting information. In recent years, encryption has shifted from the obscure obsession of generals and mathematicians to an important policy issue for all citizens, with impact on crime, civil rights, national defense, and economic competitiveness.

A great deal of important and sensitive information is stored in computers, or transmitted across communications networks. Ironically, more and more of this information is carried on inherently unsecure media such as the Internet and cellular phones. Encryption makes it easier to prevent information from being observed, corrupted, or falsified.

This paper will briefly summarize current encryption controversies. Section 2 provides background on encryption technology and its common uses. Section 3 summarizes the typical objectives of encryption policy, which are often in conflict. Section 4 describes the extent to which strong encryption is currently available. Sections 5, 6, and 7 address the three areas where legislation is most likely in the next two years: key recovery, restrictions on domestic use of encryption, and export control. This paper is summarized in Section 8.

Section 2: Encryption Technology Fundamentals

Encryption transforms information from a form that is readable to a form that is not. *Decryption* reverses this process. Ideally, it should not be possible to perform one or both of these operations without knowing some secret *key*, which generally takes the form of a string of 1's and 0's.

Encryption makes information systems trustworthy in a variety of ways. First, encryption can protect information *confidentiality*. If information is encrypted before it is transmitted across a telephone network or stored in a database, eavesdroppers and hackers may capture the encrypted information, but they won't understand it. Second, encryption can be used for *authentication*, i.e. to verify the identity of other parties. For example, if only Ann holds the key to encrypt a message, then by performing this operation on an encrypted message, Ann can prove her identity. This is the basis of a *digital signature*, which can be used to authorize payments or sign contracts. Third, encryption can be used to protect the *integrity* of information. Consider a case where only Bob can encrypt a message, but anyone can decrypt it. Bob records the message and an encrypted version of the message. If decrypting the latter still produces the former, then the message could not have been altered by any one except Bob.

Using an encryption system that has been compromised is worse than using none at all, so much of the policy debate is about the availability of *strong* encryption. Given enough

[1] Associate Professor of Electrical Engineering and Public Policy. Carnegie Mellon University, Dept. of ECE, Pittsburgh, PA 15213-3890. (412) 268-7126, peha@ece.cmu.edu, http://www.ece.cmu.edu/~peha

time, codes can be broken, which means an unauthorized observer can determine the secret key. The question is whether breaking a code would take a month, or a decade, or a billion years. The more possible values for that key, the longer it takes. Thus, a common measure for the strength of a code is the number of bits (1's or 0's) in the key. Increasing the number of bits by one doubles the number of possible keys, and typically doubles the expected amount of time to break the code.

The time it takes to break a code depends as much on the processing speed of computers as the number of bits in a key. For over five decades, computer processing speeds have doubled every 1.5 to 2.5 years. Thus, a code that took a thousand years to break with the computers available in 1960 would take 1 year to break with the computers available in 1980, and a few hours to break with the computers available in 2000. It is necessary to increase the strength of encryption systems on a regular basis.

Section 3: Encryption Policy Objectives

Encryption in the wrong hands is extremely dangerous - an observation that has long driven US policy. Even the Roman Empire used encryption for military communications. Probably the most dramatic example of the military significance of encryption in this century is the tremendous strategic advantage gained by allied forces in World War II when they broke the "unbreakable" German Enigma code. Given this experience, it is no surprise that encryption was treated as a munitions throughout the cold war, and the State Department attempted to keep encryption away from unfriendly governments and terrorist organizations much the way it would with missile technology.

Law enforcement agencies also have reason for concern about encryption. They may attempt to search computer records that are encrypted, or to wiretap a telephone line. A number of infamous criminal groups have been found to use encryption, including the group responsible for the nerve gas attack on the Tokyo subway, Bolivian terrorists who assassinated four US Marines, Ramzi Yousef who planned to sabotage 11 American Airlines flights, the Cali drug cartel, and the Italian Mafia. Only one in 300 convictions in the US includes evidence from wiretapping, and few if any cases have ever been impeded by encryption, but this may change as encryption becomes more common. That is the fear of law enforcement.

It is not just criminals, terrorists, and foreign governments that can make use of encryption. US citizens and legitimate businesses can use encryption to protect their communications from competitors and from organized crime. Encryption can protect personal privacy rights when it is applied to medical records, spending histories, and credit ratings. Government agencies can protect sensitive and classified information from foreign governments. Encryption can protect critical civilian infrastructure, such as the banking system, telephone network, electric power grid, and air traffic control systems from vandals and terrorists. Encryption can even address fraud, tax evasion, identity theft, and other information-based crimes of the rising electronic marketplace. Indeed, electronic commerce will never reach its potential without effective encryption. Thus, encryption can improve public safety.

Companies that produce computer and communications systems or components thereof also have a great stake in the encryption debate. While encryption packages may not be a large market by themselves, encryption is an important part of many larger systems. For example, the encryption system used to protect patient records is a small aspect of a hospital information system, but its absence may cost the system designer a sale.

A recent study by the National Research Council identified three primary policy objectives:

1. Broad availability of cryptography to all legitimate elements of US society to support confidentiality and authentication, protect information security, and prevent information crimes.
2. Continued economic growth and leadership of key US industries and businesses in an increasingly global economy, including but not limited to US computer hardware, software, and communications companies.
3. Public safety and protection against threats - access to information of foreign parties hostile to the US, and criminal elements within the US.

There is an inherent tension between the first two objectives of making encryption available for legitimate uses, and objective 3 of making it hard to obtain.

Section 4: Current Availability of Strong Encryption

As described in Section 2, the strength of an encryption system is typically measured in the number of bits in its secret keys. Today's commercial encryption systems range from 40 bits to 128 bits or more. How much is enough? How much is too much? As will be described further in later sections, some current policies are designed to limit the availability of encryption systems with 56 or more bits.

As early as 1971, IBM was prepared to develop a 128-bit encryption product. After consultations with the National Security Agency (NSA), they instead produced the 56-bit Data Encryption Standard (DES), which became an industry standard for many years. Some have suggested that 56-bit encryption was selected because NSA could break it. Even if they couldn't break it in the early 1970's, they can now. In 1997, an ad hoc group made their computers available over the Internet whenever they were idle to help break a 56-bit code. They succeeded in just five months. In July 1998, a group from the Electronic Frontier Foundation built a computer that can break 56-bit encryption in just a few days. Thus, 56 bit encryption is no longer particularly secure. DES is still an important industry standard, but it can be used in an enhanced mode that offers the equivalent of 116 bit encryption.

Regardless of US policy, there is no shortage of foreign products available. As of September 1997, there were 653 foreign encryption products available from 29 countries (in addition to the 948 US products). These include 128-bit encryption packages that can be downloaded over the Internet from anywhere in the world.

Section 5: Key Escrow

Some believe that the needs of users for strong encryption and the needs of law enforcement to break that encryption when necessary can both be met through *key escrow* (also known as *key recovery*). All users store their secret keys with one or more trusted third parties. Law enforcement officers are allowed access to these keys if (and only if) a court authorizes a warrant.

Use of key escrow systems could be mandatory or voluntary. The government has considerable power to promote voluntary usage through procurement. Government agencies could purchase these systems, and thereby force government contractors who wish to communicate with the government to do the same. The hope is that others would

buy the system to communicate with those contractors, and the standard would ultimately dominate the market.

Key recovery was initially the cornerstone of the Clinton administration's encryption policy. The US Government adopted the Escrowed Encryption Standard. The National Institute of Standards and Technology (NIST) would develop a family of encryption systems. The first NIST processor to emerge was the *Clipper Chip*, which was designed for telephone systems. Commercial use would be voluntary. The Clipper is built with tamper-proof packaging in specially authorized manufacturing facilities. This prevents users from deliberately changing their keys, thereby defeating the escrow system. An 80-bit key is fixed during the manufacturing process. NIST would hold half of the key, and the Treasury Department would hold the other half. The encryption algorithm itself is classified, so no one can produce a chip that communicate with the Clipper but does not have its key in escrow.

The Clipper was severely criticized for a variety of reasons. First, placing a key in a database somewhere creates a new vulnerability for the encryption system; any one who gains access to the database can break into the system. Would customers be willing to use this chip? Dividing the key in two improves security somewhat, but an 80-bit code can be broken in minutes when half the key is known. Some critics were particularly concerned that the US government held these keys, and argued that it should be in the hands of commercial companies instead. These critics believe that the US government would violate its own procedures, or are concerned that their customers would believe this. This is particularly likely for US companies wishing to sell to foreign companies and governments. Other critics were concerned that the encryption algorithm was classified. Either through oversight or design, NIST might have left a "back door" that would allow knowledgeable users to break the code without going through the escrow agents. Finally, some were more upset with the financial implications than the security implications. Because the Clipper must be implemented in hardware, it is far more expensive than comparable alternatives without key escrow.

Key escrow also raises some new civil rights issues. For example, a warrant allows law enforcement to wiretap for a limited time, but once an escrowed key has been revealed, it is difficult to prevent police from continuing surveillance indefinitely. The international issues are particularly complex. The Clinton administration hopes to establish a global Key Management Infrastructure (KMI) in cooperation with foreign governments. This raises questions of the extent to which one country's law enforcement officers can act in the territory of another, and when evidence obtained abroad (where evidentiary laws may differ) can be used domestically. Such issues must be addressed if key escrow becomes national policy.

Ultimately, Vice President Gore acquiesced to the criticisms of the Clipper on behalf of the Clinton administration, saying that he would like a "more versatile, less expensive system" that can be implemented in software and which "would not rely on a classified algorithm." It will be challenging to create such a system in which users cannot change their keys at will. Mr. Gore also believes that this system "must permit the use of private-sector key escrow agents as one option." Of course, placing such information in private hands solves some problems, and creates others. What if the private company helps protect criminal customers under investigation? What if they surreptitiously sell the keys to criminals? What if they lack the technical expertise or financial stability to operate the key escrow system?

Clipper appears to be dead, but further legislation involving key escrow is likely. FBI Director Louis Freeh told the Senate Judiciary Committee that key escrow should be

required for all encryption products. On the other side, bills have been introduced that would prevent the government from imposing any such mandate, with strong support from industry and civil rights groups. Other bills have been designed to encourage key escrow without requiring it. For example, The Secure Public Networks Act would not allow government funds to be spent on any encryption system without key escrow.

Section 6: Domestic Use

It has long been US policy to allow any type of encryption to be used in or imported into the US, with no limit on strength or mandate for key escrow. This is the stated policy of the Clinton administration. However, as stated in the previous section, FBI Director Louis Freeh shifted the debate by advocating a new domestic encryption policy. There was an attempt to restrict domestic encryption use in 1997, but it was defeated in the House Commerce Committee. The issue may be raised again.

Section 7: Export Control

Much of the policy debate on encryption has focused on export control. Export control is a tool to keep a potentially dangerous tool from foreign hands. In the case of encryption, it is also an indirect method of influencing domestic use. For many US vendors, it is impractical to develop different products for foreign and domestic markets. Moreover, many customers demand products that interoperate across national boarders. Thus, many producers of computer hardware, software, and communications devices design products for both foreign and domestic markets that meet export control restrictions.

For many years, it was illegal to export computer or communications systems that included encryption with keys of more than 40 bits. As described in Section 4, such codes are easy to break. In October of 1996, Vice President Gore announced a new *interim policy*. Regulation of encryption exports was transferred from the State Department to the Commerce Department. It became legal to export any encryption system with a key escrow mechanism built in, regardless of its strength. 56-bit encryption products could be exported after a one-time review, provided that a key escrow system would be implemented by the end of those two years. In the absence of any plans for key escrow, the 40 bit limit would remain. In September of 1998, restrictions were relaxed further; 56-bit encryption products could be exported even without plans for key escrow.

Predictably, the reviews were mixed. Some applauded the administration's moderation in balancing competing policy objectives. Industry critics argued that the restrictions accomplished little, since 128 bit encryption without key escrow is already readily available outside the US. An April 1998 report from the Economic Strategy Institute concluded that the policies imposed at that time (i.e. the 1996 interim policy) would cost the US economy between 35 and 96 billion dollars between 1998 and 2002. Some US companies have overcome these limitations by purchasing foreign products or shifting development activities overseas. For example, in March 1998, Network Associates announced that it would begin contracting all encryption development to a Swiss company.

Export control on encryption also raises some constitutional issues, as an encryption technique is really an idea. Any one who has taken a college programming course can turn that idea into a functioning product. Restricting the transfer of ideas raises free speech concerns. For example, disclosure of an encryption technique to a foreigner would constitute export, even if this disclosure took place within the US. Does speaking about

encryption at an international cryptography conference held in the US constitute illegal export? or is it free speech? In August 1997, a California district court ruled that the Interim Policy (and its predecessor) amounted to prior restraint on free speech. However, the legal question is probably not settled.

It is extremely likely that additional legislation will be proposed to allow US firms to export stronger encryption without key escrow.

Section 8: Summary

Encryption is a powerful information management tool. It allows users to protect the confidentiality of their stored data and their communications, to detect attempts to corrupt that data, and to determine the identity of those with whom they are exchanging information. It thereby shifts the balance of power closer to those in possession of the information, and further from unauthorized users seeking access. This serves the public good if the information is held by a law-abiding citizen, a legitimate company, or a government agency, who can then better protect itself from external threats. This does not serve the public interest if the information is held by a hostile government, a criminal, or a terrorist. Thus, a clash between competing policy objectives is inevitable. The net effect of making strong encryption widely available is open to debate.

Some believe that key escrow offers the appropriate balance between competing objectives. Strong encryption is available, but law enforcement can still eavesdrop on (and impersonate) suspected criminals. The approach of the Clinton administration has been to create a voluntary standard, and promote its use through government procurement policies. However, for reasons of both security and cost, there has been significant resistance to adopting the first voluntary standard - the Clipper. The administration may propose another key escrow system, in an attempt to address the perceived weaknesses of Clipper.

Although there has never been a restriction on domestic use of encryption before, the government could simply prohibit products that use strong encryption, or that do not employ key escrow. Government can also reduce the availability of strong encryption through export control. Because it is sometimes impractical to offer different products for different markets, this also influences encryption availability at home.

Domestic prohibitions deprive law-abiding citizens of strong encryption, and export controls put US industry at a competitive disadvantage. These factors must be balanced with the dangers of strong encryption. Critics argue that such policies also fail to keep strong encryption away from criminals, as foreign encryption products are easily accessible over the Internet and elsewhere. The counter-argument is that when those criminals communicate with legitimate businesses, they must use legal encryption systems which are subject to eavesdropping from authorized law enforcement agents. Moreover, if weak encryption is readily available, many will be too careless or ignorant to seek out strong encryption. (It is trivial to eavesdrop on cellular phones, yet people routinely reveal sensitive information over these phones.)

Encryption issues are likely to resurface in congress in the next two years. When determining a policy, all of the competing objectives should be considered, including crime, civil rights, national defense, and economic competitiveness.