This paper was published in July 1997 by the National Strategy Information Center's US Working Group on Organized Crime (WGOC). The WGOC, founded in 1996, brings together governmental and non-governmental specialists to improve analysis and operations against organized crime. It may not be reproduced without the permission of the National Strategy Information Center. Copyright Dorothy E. Denning and William E. Baugh, Jr., 1997. ISSN 1093-7269. All Rights Reserved. Address: 1730 Rhode Island Avenue, NW, Suite 500, Washington, DC 20036, nsic@ix.netcom.com, 202-429-0129, fax: 202-659-5429.

ENCRYPTION AND EVOLVING TECHNOLOGIES
AS TOOLS OF ORGANIZED CRIME AND TERRORISM

Dorothy E. Denning
Professor of Computer Sciences, Georgetown University

William E. Baugh, Jr.
Vice President, Science Applications International Corporation

May 15, 1997

We are at the leading edge of what could become a serious threat to law enforcement and national security: the proliferation and use of robust digital encryption technologies. These technologies will be unbreakable, easy to use, and integrated into desktop applications and network services, including protocols for electronic mail, web transactions, and telephony. This paper discusses their impact on organized crime and terrorism. Focus is on criminal investigations rather than foreign intelligence operations, as information about the latter is mostly classified.

We begin by summarizing actual cases where encryption was encountered, the scope of the problem, and the methods used by law enforcement to deal with it. Our findings suggest that the total number of criminal cases involving encryption world-wide is at least 500, with an annual growth rate of 50-100%.

We then discuss the threat posed by encryption to law enforcement, public safety, and national security. The threat is manifest in four ways: failure to get evidence needed for convictions, failure to get intelligence vital to criminal investigations, failure to avert catastrophic or harmful attacks, and failure to get foreign intelligence vital to national security. Encryption can also delay investigations, increase their costs, and necessitate the use of investigative methods which are more dangerous or invasive of privacy. Most of the investigators we talked with did not find that encryption was obstructing a large number of investigations. They were, however, concerned about the future.

Trends in the encryption market which impact law enforcement are reviewed next. One trend is the increasing integration of extremely strong encryption into commercial desktop applications and networks. The encryption will be easy to use and totally unbreakable. The worst case effect could be to render most communications and stored data immune from lawful access. Another trend, which has a balancing effect, is a growing market for key recovery systems that protect the owners of encrypted data from lost keys. These systems can give law enforcement agencies an alternative method of getting the keys needed to decrypt evidence.

Encryption is not the only technology which adversely affects law enforcement. We next describe other tools besides encryption, including cloned cell phones and steganography, that can be used to evade the police, conduct surveillance, or intrude into computers and networks. Many of these tools are enhanced by encryption.

Finally, we discuss encryption policy options, including export controls and domestic regulations in the United States and elsewhere, and their impact on crime and law enforcement. We review the Clinton Administration's encryption program to promote key recovery technologies through liberalized export controls, key recovery standards, and a voluntary licensing regime for key recovery agents.

In focusing on the seamy side of encryption and other technologies, we do not mean to imply that they are inherently bad or that their use should be restricted. Encryption in particular can be critical for safeguarding sensitive information. Business needs access to strong encryption to protect against espionage by competitors and foreign governments [Freeh 96]. Law enforcement needs encryption to safeguard sensitive communications relating to investigations. Individuals need it to protect their private communications and records. Encryption policy must facilitate the sale, export, and use of strong encryption for legitimate purposes.

Not all cryptographic technologies pose a threat to society. It depends on whether the cryptography is used for confidentiality or authentication. The societal threat arises primarily with confidentiality services -- what we refer to as encryption. Authentication technologies enhance investigations by ensuring the integrity and authenticity of evidence and its source. They are at least as important to electronic commerce and information security as encryption, perhaps even more so. Most computer intrusions result either from inadequate authentication or from design and configuration flaws that are not addressed by any form of cryptography.

Our central claim is that the impact of encryption on crime and terrorism is at its early stages. It is critical that we watch the situation closely and respond intelligently. Encryption policy must effectively satisfy a range of interests: information security, public safety, law and order, national security, the economic competitiveness of industry in a global market, technology leadership, and civil liberties. Meeting all of these interests is enormously challenging, but it is crucial that we find ways of protecting both freedom and order.

COMPUTERS AND NETWORKS IN CRIME

For organized crime, computers are indispensable to daily operations and staying competitive. As in any enterprise, they are used to manage financial records, personnel records, transactions, and other information assets. Although low-level drug dealers are generally not into computers, the cartels behind them are fully automated. DEA agents cracking down on Columbia cartel cells found computerized personnel records with a morbid twist: associated with each employee was a list of relatives to be pressured, possibly even killed, in the event of "difficulties" [Ramo 96]. A Cali cartel investigation found the phone records of millions of Cali residents stored on an IBM mainframe. The records were cross-checked with calls made to the U.S. Embassy or Ministry of Defense in order to identify those who were cooperating with the government [Ramo 96].

Organized crime is online, using the Internet to plan and coordinate their activities, and facilitate illegal acts. They are also using it to distribute tools and information for committing crimes and acts of terrorism, including instructions for building bombs and other deadly weapons, instructions for building "red boxes" and other devices used to steal telephone services, and software and instructions for hacking into systems. This information is posted on web servers and news groups, and distributed through electronic mail. Criminals use the Internet to distribute pirated software and child pornography, to solicit victims, and to operate scams. There are off-shore web sites for tax evasion. Although we did not identify any Internet "black nets" that traffic in stolen proprietary information of a general nature, such underground networks could operate using encryption and anonymity services [May 96].

Until recently, crimes involving information technology were an exception to normal criminal patterns. Now, it is common to find computers and other information technologies supporting a wide range of crimes. Ken Citarella, prosecutor with the Westchester County, New York District Attorney's Office, reported that in their jurisdiction, the use of a computer as a filing cabinet for records of criminal activity has become routine. Bill Caelli, a professor with the Queensland University of Technology's Information Security Research Centre, noted that according to a recent anecdote, during most arrests related to computer crime investigations in a Northern England region, armaments have been found on the premises under investigation. He interprets this as one indication that the use of information technology in criminal activity has reached the mainstream. The use of guns in England is unusual; the combination of guns and computers suggests these are serious cases involving organized crime or drugs.

ENCRYPTION IN CRIME AND TERRORISM

Our research has found that encryption is being used as a tool for hiding information in a variety of crimes, including fraud and other financial crimes, theft of proprietary information, computer crime, drugs, child pornography, terrorism, murder, and economic and military espionage. We did not hear about many cases where criminals had exploited weak encryption systems to their advantage, for example, to steal proprietary information. However, a British blackmailer intercepted encrypted transactions transmitted by a bank in the U.K. After breaking the code, he successfully extorted 350,000 from the bank and several customers by threatening to reveal the information to the Inland Revenue [Grabosky 97].

Terrorism

Aum Shinri Kyo (Supreme Truth). On March 20, 1995, the Aum Supreme Truth cult dropped bags of sarin nerve gas in the Tokyo subway, killing 12 people and injuring 6,000 more [Kaplan & Marshall 96]. They had developed a variety of weapons of mass destruction, both chemical (sarin, VX, mustard gas, cyanide) and biological (botulism, anthrax, Q fever). They were attempting to develop a nuclear capability and a "death ray" that could destroy all life. Shoko Asahara and his followers used murder, kidnapings, extortion, torture, poison, electric shocks, drugs, imprisonment, and wiretaps to acquire assets, control defections, and attack their enemies. Among the tens of thousands of members were some of Japan's brightest scientists and doctors. The cult had stored their records on computers, encrypted with RSA. Authorities were able to decrypt the files after finding the key on a floppy disk. The encrypted files contained evidence that was crucial to the investigation, including plans and intentions to deploy weapons of mass destruction in Japan and the United States.

Bolivian terrorists assassinate four U.S. Marines. A few years ago, AccessData Corporation of Orem, Utah, assisted in an encryption case involving a military sting operation [Thompson 97]. A Bolivian terrorist organization had just assassinated four U.S. Marines, and the company was asked to decrypt files seized from a safe house. They had twenty four hours. They decrypted the custom-encrypted files in twelve, and the case ended with one of the largest drug busts in Bolivian history. The terrorists were caught and put in jail.

Ramsey Yousef, World Trade Center and Manila Air bombings. Ramsey Yousef was part of the international terrorist group responsible for bombing the World Trade Center in 1993 and a Manila Air airliner in late 1995. When his laptop computer was seized in Manila, the FBI found that some of the files were encrypted. These files, which were successfully decrypted, contained information pertaining to further plans to blow up eleven U.S.-owned commercial airliners in the Far East [Freeh 97]. While useful to the investigation, much of the information was also available in unencrypted documents. Also, because Yousef and others were arrested, decryption was not essential to averting the scheduled catastrophes.

Terrorist attacks on businesses. A terrorist group that was attacking businesses and state officials used encryption to conceal their messages. At the time the authorities intercepted the communications, they were unable to decrypt the messages, although they did perform some traffic analysis. Later they found the key on the hard disk of a seized computer, but only after breaking through additional layers of encryption, compression, and password protection. The messages were said to have been a great help to the investigating task force.

New York Subway Bomber. In 1995, John Lucich was assigned to the Manhattan District Attorney's Office to assist with the investigation of the New York subway bomber, Mr. Leary. Mr. Leary was eventually found guilty and sentenced to 94 years in jail for setting off fire bombs in the New York subway system. He had applied his own form of encryption to numerous files on his computer, and Mr. Lucich was given the computers for analysis. After failing to break the encryption themselves, the files were sent to outside encryption experts. These efforts also failed. Eventually, the encryption was broken by a federal agency. The files contained child pornography and personal information, which was not particularly useful to the case. However, investigators retrieved other evidence from the computer that was used at trial.

Cryptoviral extortion. Cryptoviruses, a new form of financial terrorism, are said to have been introduced into at least nine business systems in London [McCormack 96]. These fragments of malicious code are like other viruses, except they encipher data rather than damaging the target system in other ways. In these cases, the viruses enciphered critical banking records and files. The companies were subsequently contacted by hackers demanding up to 100,000 for the key.

There is a rumor that the French police have been unable to decrypt the hard disk on a portable belonging to a member of the Spanish/Basque ETA, a terrorist organization. We have also heard that some terrorist groups are using high-frequency encrypted voice/data links with state sponsors of terrorism, and we received one anonymous report of a group of terrorists encrypting their e-mail with Pretty Good Privacy (PGP).

Organized Crime

Dutch organized crime. Dutch organized crime gets technical support from a group of skilled hackers who today use PGP and PGPfone to encrypt their communications. The hackers at one time supplied the mobsters with palmtop computers on which they installed Secure Device, a Dutch software product for encrypting data with IDEA. The palmtops served as an unmarked police/intelligence vehicles database. In 1995, the Amsterdam Police captured a PC in possession of one organized crime member. The PC contained an encrypted partition, which they were unable to recover at the time. Nevertheless, there was sufficient other evidence for conviction. The disk, which was encrypted with a U.S. product, was eventually decrypted in 1997 and found to be of little interest.

Multi-site gambling enterprise. A significant gambling enterprise operated multiple sites linked by a computer system, with drop-offs and pick-ups spanning three California counties. The head of the enterprise managed his records with a commercial accounting program, using a codeword to encrypt the files. The software manufacturer refused to assist law enforcement in breaking the code. However, the police were able to crack the codeword by exploiting weaknesses in the system. The encrypted files contained the daily take on the bets, payoffs, persons involved, amounts due and paid or owed, and so forth. After breaking the code, they printed the results of four years of bookmaking, which resulted in a plea of guilty to the original charges and a sizeable payment of back taxes, both state and federal [McMahon 97].

Theft, fraud, and embezzlement of funds. An encryption case occurring in Vilseck, West Germany involved theft, fraud, and embezzlement of U.S. defense contractor and U.S. government funds over the three year period 1986-1988. The crooks had stored financial records relating to their misdeeds on a personal computer. When investigators seized the computer, they found that the hard disk had been password protected. After using hacker software to defeat the password protection, they found that some of the files listed in the directory had been encrypted. They then found the encryption program on the hard disk and used it to decrypt the files. The encryption program was unsophisticated and available from the U.S. The password-protected and encrypted evidence was deemed valuable as a condensed source of investigative leads and in obtaining a confession. Sufficient other evidence was available that the prosecution would have been successful using other records [Price 97].

National drug ring. The Dallas Police Department encountered encryption in the investigation of a national drug ring which was operating in several states and dealing in Ecstasy [Dallas 97]. A member of the ring, residing within their jurisdiction, had encrypted his address book. He turned over the password, enabling the police to decrypt the file. Meanwhile, however, the subject was out on bond and alerted his associates, so the decrypted information was not as useful as it might have been. The detective handling the case said that in the ten years he had been working drug cases, this was the only time he had encountered encryption, and that he rarely even encountered computers. He noted that the Ecstasy dealers were into computers more than other types of drug dealers, most likely because they are younger and better educated. They are using the Internet for sales, but they are not encrypting electronic mail. The detective also noted that the big drug dealers were not encrypting phone calls. Instead, they were swapping phones (using cloned phones) to stay ahead of law enforcement.

Cali cartel. The Cali cartel is reputed to be using sophisticated encryption to conceal their telephone communications. Communications devices seized from the cartel in 1995 included radios that distort voices, video phones which provide visual authentication of the caller's identity, and instruments for scrambling transmissions from computer modems [Grabosky 97].

Italian Mafia. Maria Christina Ascents, who runs the Italian state police's crime and technology center, said that the Italian mafia is increasingly looking to use encryption to help protect it from the government [Ramo 96]. She cited encryption as their greatest limit on investigations, and noted that instead of hiring cryptographers to create their codes, mobsters download copies of PGP off the Internet.

Drugs and possible counterfeiting. A police department in Maryland encountered an encrypted file in a drug case. Allegations were raised that the subject had been involved in document counterfeiting and file names were consistent with formal documents. Efforts to decrypt the files failed, however, so the conviction was on the drug charges only [Schmidt].

Many investigators reported that in organized crime and economic crime cases, the subjects typically used encryption systems that were ready-at-hand, namely those supplied with word processing, spreadsheet, and other applications software such as Word, WordPerfect, Excel, and Lotus. Encryption in these cases was used mainly to conceal financial, procurement, and other business records. It was generally broken. However, as illustrated by the cases involving the Cali cartel, Italian mafia, and Dutch organized crime, some of the more powerful groups have access to sophisticated methods of encryption.

Espionage

Aldrich Ames spy case. Ames was a CIA agent eventually convicted of espionage against the United States. He had encrypted his computer files using standard commercial off-the-shelf software. The investigator handling the computer evidence was able to decrypt the files using software supplied by AccessData Corporation [Thompson 97]. Failure to recover the encrypted data would have weakened the case.

Insider theft of proprietary software. An employee of a company copied proprietary software to a floppy disk, took the disk home, and then stored the file on his computer encrypted under PGP. Evidently, his intention was to use the software to offer competing services, which were valued at tens of millions of dollars annually (the software itself cost over a million dollars to develop). At the time we heard about the case, the authorities had not determined the passphrase needed to decrypt the files. Information contained in logs had led them to suspect the file was the pilfered software.

Kevin Poulson. Kevin Poulson was a skilled hacker who rigged radio giveaways, "winning" Porsches, trips to Hawaii, and tens of thousands of dollars in computer cash. He also burglarized telephone switching offices and hacked his way into the telephone network in order to determine who was being wiretapped and to install his own. In his book about Poulson's crime spree, Jonathan Littman reported that Poulson had encrypted files documenting everything from the wiretaps he had discovered to the dossiers he had compiled about his enemies [Littman 97]. The files were said to have been encrypted several times using the "Defense Encryption Standard" [sic]. According to Littman, a Department of Energy supercomputer was used to find the key, a task which took several months at an estimated cost of hundreds of thousands of dollars. The result yielded nearly ten thousand pages of evidence.

Pedophiles and Child Pornographers

International pedophile ring. Authorities in the U.K. sentenced a Durham priest to six years in jail for sexually assaulting minors and distributing child pornography [Akdeniz]. The priest was part of an international pedophile ring that communicated and exchanged images over the Internet. When authorities seized his computers, they found files of encrypted messages. We learned from an inside source that the messages had been enciphered using the built-in encryption for Psion Series 3 Word (no relationship to Microsoft Word) documents. The encryption was successfully broken, however, the decrypted data did not affect the case.

Child pornography and possible corporate espionage. A 15 year old boy came to the child abuse bureau of the Sacramento County Sheriff's Department with his mother, who desired to file a complaint against an adult who had met her son in person, befriending the boy and his friends and buying them pizza. The man had sold her son $500-$1000 worth of hardware and software for $1.00 and given him lewd pictures on floppy disks. The man subsequently mailed her son pornographic material on floppy disk and sent her son pornographic files over the Internet using America Online. After three months of investigation, a search warrant was issued against a man in Campbell, California and the adoption process of a 9 year old boy was stopped. Eventually, the subject was arrested, but by this time he had purchased another computer system and traveled to England to visit another boy. Within ten days of acquiring the system, he had started experimenting with different encryption systems, eventually settling on PGP. He had encrypted a directory on the system. There was information indicating that the subject was engaged in serious corporate espionage, and it was thought that the encrypted files might have contained evidence of that activity. They were never able to decrypt the files, however, and after the subject tried unsuccessfully to put a contract out on the victim from jail, he pled no contest to multiple counts of distribution of harmful material to a juvenile and the attempt to influence, dissuade, or harm a victim/witness [Kennedy 97].

Several law enforcement agents reported that they had encountered encrypted e-mail and files in cases involving pedophiles and child pornography, including the FBI's innocent images investigation. In many cases, the subjects were using PGP to encrypt files and e-mail. The investigators thought this group favored PGP because they are generally educated, technically knowledgeable, and heavy Internet users. PGP is universally available on the Internet, and they can download it for free.

What is Encountered and How Much

Law enforcement and investigative agencies have encountered a variety of encryption methods, including the Data Encryption Standard (DES), the International Data Encryption Algorithm (IDEA), the RSA public-key cryptosystem, various proprietary algorithms, and home-brewed methods. The encryption has been used to conceal telephone communications, electronic mail, Internet chat and telephony, individual files, boot sectors, and entire disks. In some cases, the encryption was part of a commercial application or network service; in others, it was a stand-alone product for file or communications encryption. No single algorithm or product has dominated all cases.

The FBI's Computer Analysis Response Team (CART) forensics lab reported that encryption was encountered in 2% of 350 submissions to the headquarters component in 1994 and 5-6% of 500 submissions (25-30 cases) in 1996. This represents a quadrupling of cases from 1994 to 1996, which averages out to an annual doubling or growth rate of 100%. A submission could be anything ranging from a single floppy disk to several boxes of disks or complete systems. CART also estimated that about 5-6% of the 1,500 cases handled in the field involved encryption, the largest categories being child pornography and computer crime cases. This corresponds to about 75-90 cases. It does not include cases handled by other federal law enforcement agencies, including the Drug Enforcement Administration (DEA), Treasury (Secret Service, Customs, and IRS), or state and local law enforcement agencies. It also excludes national security cases (foreign intelligence, counter-intelligence, and defense cases) and cases involving intercepts of encrypted telephone communications. In his March 19 testimony before the Senate Committee on Commerce, Science, and Transportation, FBI Director Louis Freeh reported that the number of requests for decryption assistance pertaining to communications interceptions had risen steadily over the past several years [Freeh 97].

One private consultant who has assisted law enforcement agencies in Canada and the U.S. with cases involving encryption and other access restriction methods reported that he had helped with 5 cases in 1995, 8 in 1996, and 3 within the first two months of 1997. Another U.S. consultant said he helped with 4 cases in 1996. Brian Deering, a computer specialist with the National Drug Intelligence Center, reported that they had assisted with about 6 cases during the past year and half. The NDIC assists in large-scale, multi-agency investigations for the FBI, DEA, customs, and other federal agencies. The Air Force Information Warfare Center encountered 5 cases with encryption in 1996. These are cases with severe consequences to ongoing military operations and represent about 10% of all cases handled by the center.

Bill Caelli reported that the Queensland University of Technology's Information Security Research Centre had been asked to assist in decryption activities for law enforcement agencies around the world about once every few months over the last 18 months or so. He said it had been reputed that in Northern England, in almost all cases involving seizures of computer evidence during the last six months, pertinent files on the hard disk were found encrypted. He said that there was substantial evidence of the same phenomena in Australia.

There is no central database recording the number of encryption cases handled nationally or globally, or indeed even the number of computer forensics cases. Mark Pollitt, program manager of CART, estimates there are at least 5,000 computer forensics cases nationally, up to a maximum of 10,000. World-wide, he estimates anywhere from 10,000 up to 20,000 cases. If about 5% of those involve encryption, then the total number of cases would be 250 to 500 nationally and 500 to 1,000 globally. Eric Thompson, president of AccessData Corporation, estimates that the total number of cases involving encryption is on the order of 1,000 to 5,000. The rate of 5,000 would be about a quarter to one half of all computer forensics cases globally. This is a higher percentage than reported by

CART for the U.S., but it is lower than the near 100% figure attributed to recent cases in Northern England. Thompson also estimates that at least 100-200 are child pornography cases involving just PGP.

Due to the increased use of computers and networks combined with the increased availability of encryption, the number of cases involving encryption is growing and will continue to do so. We estimate an annual growth rate of at least 50-100%. Table 1 gives 5-year estimates for the number of cases globally involving encryption given that the number of cases in 1996 is 250 or 500 nationally and 500, 1,000 or 5,000 globally; and given that the growth rate is 29%, 50%, or 100%. The extremely conservative rate of 29% represents a projected growth rate in the use of encryption by business; it was estimated from a survey of 1600 U.S. business users conducted by the U.S. Chamber of Commerce Telecommunications Task Force. The table shows that in five years, there could be anywhere from a few thousand to over 150,000 cases.

Breaking the Codes

As illustrated in some of the preceding cases, even when encryption is encountered in an investigation, it does not necessarily mean that law enforcement agencies are locked out. They have several options for getting access to the plaintext.

Consent. Law enforcement agencies can ask the subject for the key or, in the case where the key is stored on disk encrypted under a password (or passphrase), the password. In many cases, subjects have cooperated with the police and disclosed their passwords. One question that frequently arises is whether a court can compel the disclosure of plaintext or keys, or whether the defendants are protected by the Fifth Amendment. Philip Reitinger, an attorney with the Department of Justice Computer Crime Unit, studied this question and concluded that a grand jury subpoena can direct the production of plaintext or of documents that reveal keys, although a limited form of immunity may be required [Reitinger 96]. He leaves open the question of whether law enforcement can compel production of a key that has been memorized but not recorded. He also observes that faced with the choice of providing a key that unlocks incriminating evidence or risking contempt of court, many will choose the latter and claim loss of memory or destruction of the key.

Key recovery system. Key recovery refers to a capability whereby authorized persons can, under prescribed conditions, obtain access to the key needed to decrypt information through a process other than the normal channel by which the key is distributed to the intended recipient. The decryption key is recovered using information stored with the ciphertext together with information held by a trusted agent, which could be an officer of the organization owning the data or a third party. The primary objective is to protect organizations and individuals using strong encryption from loss or destruction of encryption keys, which could render valuable data inaccessible. In the case of communications, they also allow an organization to monitor an employee's conversations when there is probable cause the employee is engaged in misconduct or illegal activity, or to review taped conversations in the event of a lawsuit or discovery of illegal activity. Although the greatest demand for key recovery is with stored data, some organizations also want key recovery for communications systems.

Key recovery systems can accommodate lawful investigations by proving authorities with a means of acquiring the keys needed. If the keys are held by a third party, this can be done without the knowledge of the criminal group under investigation. Of course, if criminal enterprises operate their own recovery services, law enforcement may be no better off, as they will likely need the cooperation of the criminals to get keys.

Exploiting a weakness in the system. It is often possible to obtain the key needed to decrypt data by exploiting a weakness in the encryption algorithm, implementation, key management system, or some other system component. Indeed, there are software tools on the Internet for cracking the encryption in many commercial applications. One site on the World Wide Web lists freeware crackers and products from AccessData Corporation and CRAK Software for Microsoft Word, Excel, and Money; WordPerfect, Data Perfect, and Professional Write; Lotus 1-2-3 and Quattro Pro; Paradox; PKZIP; Symantex Q&A, and Quicken [Bokler 97].

Thompson reported that they had a recovery rate of 80-85% with the encryption in large-scale commercial commodity software applications [Thompson 97]. He also noted that 90% of the systems are broken somewhere other than at the crypto engine level, for example, in the way the text is pre-processed.

Brute force. In those cases where there is no shortcut attack, the key might be determined through a brute force search, that is, by trying all possible keys until one is found that yields known plaintext or, if that is not available, meaningful data. The effort required to do this grows significantly with the length of the key, as each additional bit doubles the number of candidates to try.

In January, 1997, a 40-bit key was broken in 3.5 hours by a Berkeley student, Ian Goldberg. He used a network of 250 computers capable of testing 100 billion keys per hour in a known plaintext attack (the plaintext and ciphertext were provided in a challenge cipher from RSA Data Security). In February 1997, a student at the Swiss Federal Institute of Technology, harnessed the power of 3,500 computers on the Internet to break a 48-bit key (another RSA challenge). The key was found after 312 hours (13 days), with the networked machines achieving a peak search rate of 1.5 trillion keys per hour. In his testimony before the Senate in March, 1997, William Crowell, Deputy Director of the National Security Agency, observed that it would have taken the Berkeley student 9 trillion times the age of the universe (about 15 billion years) to decrypt a 128-bit key with his 250 workstations [Crowell 97]. Even if all 260 million personal computers of the world were put to the task, it would take an estimated 12 million times the age of the universe.

Table 2 shows the number of key bits that can be broken in a second, day, week, or year under various assumptions about processor speed and number of processors available. A processor speed of 100,000 keys/second corresponds roughly to the average rate of each individual workstation in the Berkeley and Swiss-led attacks; 1 million keys/second is a hypothetical rate often used in brute force projections. A speed of 30 million keys/second is the estimated speed using a Field Programmable Gate Array (FPGA) chip, while 200 million keys/second might be achieved with an Application-Specific Integrated Circuit (ASIC) chip [Blaze 96]. These correspond to optimal conditions with state-of-the-art technology. The table shows the results for up to 1,000,000 processors, however, it should be noted that we are unaware of any actual task ever using more than a few tens of thousands of processors simultaneously. Each factor of 1,000 improvement in processor speed or number of processors allows one to search over an additional 10 bits in the same amount of time; a factor of 10 allows one to search over an additional three bits approximately.

The entries in the table were calculated on the worst-case assumption that it was necessary to exhaustively try each possible bit combination before finding the correct key. Adding 1 bit to these values gives the key lengths that can be cracked on an average-case assumption where the key is found half-way through the key space. In practice, an actual attack might take longer if the attacker does not know the method and does not have known plaintext.

Table 2 shows that to break a 56-bit DES key would require, for example, 1 million of the Berkeley workstations running for 1 week or about 10,000 running for 1 year. Alternatively, the key might be broken using 10,000 FPGA chips or 1,000 ASIC chips in 1 day. The table also shows that breaking key sizes on the order of 64-bits is a considerable stretch. Even with a year, it would take over 10,000 FPGA chips or over 1,000 ASIC chips. Under the most optimistic conditions, the longest key size that one could conceive of breaking is 72 bits, and that would require a year and a million special purpose chips.

Since the early days of computing, technology improvements have followed Moore's law, with processing power doubling about every 18 months. We can use the table to project into the future, every 18 months cracking keys that are one bit longer within the same period of time. After 30 years, for example, one could crack keys that are 20 bits longer than can be cracked today; after 60 years, one could crack keys that are 40 bits longer. At this rate, it will be 84 years before one could conceive of cracking a 128-bit key within a year's time. For all practical purposes, 128-bit keys are totally uncrackable within our lifetime.

With many encryption systems, for example PGP, the key corresponds to or is computed from a passphrase chosen by the user. In that case, it may be easier to brute force the password than the key because it will be limited to ASCII characters and be less random than an arbitrary stream of bits. Eric Thompson reports that the odds are about even of successfully guessing a password [Thompson 97]. They use a variety of techniques including Markov chains, phonetic generation algorithms, and concatenation of small words.

Other methods. In some cases, it might be possible to get a key through some other method, for example, an informant or a court-ordered wiretap on the subject's communications.

IMPACT OF ENCRYPTION ON LAW ENFORCEMENT AND NATIONAL SECURITY

The Threat

The threat posed by encryption to law enforcement, public safety, and national security can be broken down into four components:

Failure to get evidence needed for convictions. If criminals conceal their communications and stored records with unbreakable encryption, it may be impossible to obtain the evidence needed for a conviction. One consultant said their inability to decrypt a hard disk was a "show stopper" for the case. In the child pornography/economic espionage and drug/counterfeiting cases described earlier, the subjects were convicted, but not of the crimes that were believed to be concealed by encryption. In March, FBI Director Freeh testified that they were unable to assist with 5 requests for decryption assistance in communications intercepts in 1995 and 12 in 1996 [Freeh 97]. Such wiretaps can be extremely valuable as they capture the subjects' own words and reveal plans and intentions. They have provided crucial evidence in cases involving organized crime, drugs, fraud, public corruption, murder, and other crimes [Freeh 94, pp. 6-20].

Failure to get intelligence vital to criminal investigations. Encryption can frustrate communications intercepts, which provide valuable information regarding the intentions, plans, and members of criminal conspiracies, and in providing leads in criminal investigations. Drug cartels and organizations rely heavily on communications networks; monitoring of these networks has been critical for identifying those at the executive level and the organizations' illegal proceeds [Freeh 94, p. 12]. Encryption can hide evidence of crimes which may be more serious than those leading to an investigation. Encryption can also conceal information regarding the victims of crimes. In pedophile cases, the inability to decrypt a diary, address book, or electronic mail message can make it impossible to identify potential victims in need of psychological counseling.

Failure to avert catastrophic or harmful attacks. A significant number of terrorist acts and murders have been avoided through the effective use of electronic surveillance, including the bombing of a foreign consulate, a rocket attack against a U.S. ally, the shooting down of a commercial airliner with a stolen military weapon system, an attack on a nuclear power facility, and a rocket attack against an FBI field office [Freeh 94, pp. 17-18]. If the communications in these cases had been encrypted, the planned catastrophes might not have been averted. Even if the codes had been cracked, doing so might have taken too long for the results to be useful, especially if the keys changed with each message or phone call. The 3,500 computers used to break the 48-bit key over a 2-week period, for example, would be totally inadequate against terrorists sending encrypted messages every hour even if all they used were 48-bit keys. More likely, they would be using 128-bit keys.

Failure to get foreign intelligence vital to national security. Communications intercepts conducted as part of foreign intelligence operations provide information critical to national security, including intelligence in support of military operations; intelligence about political and economic powers hostile to the U.S., particularly those with weapons of mass destruction; and intelligence about specific transnational threats to national security, including weapons proliferation, terrorism, drug trafficking, organized crime, illicit trade practices, and environmental issues of great gravity [Clinton 95]. This includes intercepts conducted under the Foreign Intelligence Surveillance Act (FISA), which have provided information crucial to the United States, the National Security Council, the intelligence community, the Department of Defense, and the State Department [Freeh 94, p 20-21]. Encryption can cut off access to these vital sources of information.

In 1994, the FBI's organized crime/drugs section reported that every major FBI organized crime investigation had relied upon electronic surveillance [Freeh 94, p. 8]. The program manager stated: "The loss or impairment of the capability to conduct court-ordered electronic surveillance would catastrophically impair federal and state law enforcement agencies' ability to effectively investigate organized criminal groups." The potential effects include increased organized crime and terrorism; substantial loss of life; substantial economic harm to business, industry, labor unions, and society generally; increased corruption of legitimate business and labor unions; increased availability of illegal drugs; undetected and unprosecuted public corruption and fraud against the government; and unprosecuted terrorist acts and criminal cases of all kinds [Freeh 94, p. 22].

Some methods of electronic surveillance are relatively unaffected by encryption, including pen registers, trap/trace devices, and electronic bugs. The greatest impact is with intercepts of call content, which to be effective must be done without the knowledge of the subjects. There are circumstances when encryption does not prevent access to call content, for example, when it is used only on the radio link of a cellular call, allowing access at a base station or switch, or when it is relatively weak and breakable. However, even weak encryption can preclude real-time access, which may be critical to averting a disaster or planned event.

Everyone we talked to agreed that in the majority of criminal cases involving encryption of files and disks, authorities have been able to decrypt the data, usually by getting the password/key from the subject or by cracking a weak system. Where they have failed, they have generally been able to make a case through other evidence such as hard copies of encrypted documents, other paper documents, unencrypted conversations and files, witnesses, and information acquired through other surveillance technologies such as bugs. The encrypted evidence is but one piece of the case. In some cases, information stored in an encrypted file on one machine would be found in the clear on the same machine or that of a conspirator. Most of the investigators we talked with were unaware of any cases that were entirely derailed because of encryption. As one law enforcement officer said, when they know that a case involves encryption, they approach it differently. Nevertheless, everyone forecasted a major problem with encryption which would only grow worse.

Other Effects of Encryption

Even when encryption does not stop an investigation, it can impact a case in several ways.

Delayed investigations. Encryption has delayed investigations by months or longer while computer forensics analysts have determined the systems used, the files to be decrypted, and available vendor support and tools. The problems are aggravated when an entire disk is encrypted, so that even the software used is hidden from view.

Increased costs. We were told about one case which cost a half million dollars to get the key; in the Poulson case, Littman reported compute costs in the hundreds of thousands of dollars. These examples, however, represent the extreme end. In many instances, law enforcement is able to use reasonably priced commercial cracking tools or in-house expertise and methods. But even then, dealing with encryption can add to the personnel and travel costs of an investigation. As the number of computer and encryption cases increases, the personnel and computing resources required by law enforcement to deal with encryption will obviously increase as well.

Increased danger and invasion of privacy. If investigators encounter unbreakable encryption while up on a wiretap, they may pursue other methods of surveillance, including hidden microphones, cameras, and other sensors installed on the subject's premises. Undercover operations are another alternative. These methods are generally more dangerous both to the subject and to law enforcement, more invasive of the subject's privacy, and more expensive.

Market Trends and Impact

The encryption market is exploding in response to the growing use of the Internet and Intranets for sensitive communications and for electronic commerce. The following summarizes some of the market trends [Denning 97].

Worldwide proliferation. As of December 1996, Trusted Information Systems of Glenwood, Maryland, identified 1393 encryption products worldwide produced and distributed by 862 companies in at least 68 countries [TIS 96]. Of these, 823 (56%) are produced in the U.S. The remaining 570 (44%) are produced in 28 different countries. Encryption software is also proliferating as freeware on the Internet. The widespread use of PGP is due in part to its availability on Internet file and web servers worldwide.

Easy to use, ready at hand, and unbreakable. Strong encryption is being integrated into commercial applications and network protocols where it will be easy to use and often automatic. Word processing, spreadsheet, database, electronic mail, Internet telephony, and other software applications will offer users encryption methods that use 128-bit keys or longer. They will be impossible to crack by brute force. Firewalls and other network services will use unbreakable encryption to implement secure networks, untappable by law enforcement as well as everyone else. The result of this trend is that commercial applications which were once breakable by law enforcement may no longer be. Although the U.S. and most other countries restrict exports of strong encryption, this has not prevented its availability worldwide. In some instances, foreign companies are exporting encryption with keys long enough to be uncrackable. For example, Siemens Nixdorf is exporting 128-bit encryption for web browsers and web servers.

Multiple methods. Many encryption products support a variety of encryption methods, including methods based on open standards. Interoperability between products is achieved not by universal adoption of any single method, but rather by protocols that negotiate to find the strongest method they have in common. Because there is no single standard, law enforcement must be prepared to handle a plethora of different methods.

Global interoperability. Through open standards, the high-grade domestic products of one country can be designed to interoperate with those of another. This enables global interoperability at a high level of security even if the products providing such security are not readily exported. Also, in some cases the cryptographic strength provided by an exportable product can be brought to the level of a domestic product through a foreign-made security plug-in. For example, foreign users of Netscape's or Microsoft's 40-bit web browser can install a 128-bit plug-in (SafePassage) that acts as a proxy between their 40-bit browser and a 128-bit web server [O'Reilly 96]. This trend tends to nullify the effect of export controls.

Key recovery. The preceding trends will generally help users protect their information assets, while making criminal investigations more difficult. A trend that is expected to facilitate investigations is the adoption of key recovery systems. However, if organized crime groups operate their own key recovery facilities, investigators could be worse off because the encryption will be much stronger, possibly uncrackable, and the criminals might not cooperate with the authorities. Moreover, with wiretaps, which must be performed surreptitiously to have value, investigators cannot go to the subjects and ask for keys to tap their lines. Key recovery systems also could encourage the use of encryption in organized crime to protect electronic files, as criminal enterprises need not worry about loss of keys.

If not carefully designed, key recovery systems are potentially an avenue of crime for information thieves. It is critical that these systems have sufficient safeguards to protect against compromise and abuse.

Educated public. More and more students are graduating with the knowledge and skills to use, evaluate, and develop encryption systems.

Even outside the academic community, the level of awareness and expertise is increasing, aided in part by the Internet. For some Internet users, the use of encryption may become routine. Anti-government militia groups operating in the U.S. are advocating the use of encryption to prevent government surveillance.

Among this growing body of encryption experts are those who are participating in criminal activity or who are willing to sell their skills to organized crime groups. One consultant told us that he did not discriminate on the basis of occupation. Organized crime groups of the future will have in-house or ready access to expertise on encryption and other information technologies. Most people we talked with expected organized crime groups to hire the talent needed to evade law enforcement.

OTHER TECHNOLOGIES AS TOOLS OF CRIME

As the population has become increasingly computer literate, the number of cases involving computer searches and seizures has also increased. We noted earlier that the headquarters component of the FBI Computer Analysis Response Team handled about 500 cases in 1996. This is a 140% increase over the 350 cases handled in 1994.

One of the challenges facing investigators is handling disks with gigabytes of data. The encryption problems are compounded if files are encrypted with different products or under different keys. It may not even be clear which files are worthwhile to access. Another challenge is handling data dispersed across local area networks and Intranets. In some cases, investigators have had to seize entire networks. A third challenge is handling new communication technologies.

Concealment Technologies

The modern day criminal has access to a variety of tools for concealing information besides encryption:

Password protection. Criminals, like law abiding persons, often password protect their machines to keep others out. In one gambling operation with connections to New York's Gambino, Genovese, and Colombo crime families, bookies had password-protected a computer used to cover bets at the rate of $65 million a year [Ramo 96]. After discovering that the password was one of the henchmen's mother's name, the cops found 10,000 digital betting slips worth $10 million. We received a report of another gambling case where the bookie had password-protected his computer. Again, the police were able to get the password. Passwords are also used to control access to data stored on backup tapes.

Digital compression. Digital compression is normally used to reduce the size of a file or communication without losing information content, or at least significant content. The greatest reductions are normally achieved with audio, image, and video data; however, substantial savings are possible even with text data. Compression can benefit the criminal trying to hide information in two ways. First, it makes the task of identifying and accessing information more difficult for the police conducting a wiretap or seizing files. Second, when used prior to encryption, it can make cracking an otherwise weak cipher difficult. This is because the compressed data is more random in appearance than the original data, making it less susceptible to techniques that exploit the redundancy in languages and multimedia formats.

Steganography. Steganography refers to methods of hiding secret data in other data such that its existence is even concealed. One class of methods encodes the secret data in the low-order bit positions of image, sound, or video files. There are several tools for doing this, many of which can be downloaded for free off the Internet. With S-tools, for example, the user hides a file of secret data in an image by dragging the file over the image. The software will optionally encrypt the data before hiding it for an extra layer of security. S-tools will also hide data in sound files or in the unallocated sectors of a disk.

Anonymous remailers. Using an anonymous remailer, someone can send an electronic mail message without the receiver knowing the sender's identity. The remailer may keep enough information about the sender to enable the receiver to reply to the message by way of the remailer. Some remailers also provide encryption services (typically using PGP) so that messages sent to and from the remailer can be encrypted. Anonymous remailers allow persons to engage in criminal activity while concealing their identities.

Anonymous digital cash. Digital cash enables users to buy and sell information goods and services. It is particularly useful with small transactions, serving the role of hard currency. Some methods allow users to make transactions with complete anonymity; others allow traceability under exigent circumstances, for example, a court order. Total anonymity would afford criminals the ability to launder money and engage in other illegal activity in ways that would circumvent law enforcement.

Remote storage. Criminals can hide data by storing it on remote hosts, for example, a file server at their Internet Service Provider (ISP). Jim McMahon, former head of the High Technology Crimes Detail of the San Jose Police Department, reported that he had personally seen suspects hiding criminal data on non-local disks, often at ISP locations, but sometimes on the systems of innocent third parties with poor security, leaving them open to intrusions and subsequent abuse. We also heard of cases where software pirates had stashed their pilfered files in hidden directories on systems they had hacked.

Floppy disks. Criminals also can hide data on floppy disks which are kept separate from the main computers. Don Delaney, a detective with the New York State Police, reported that in one recent Russian organized crime case involving more than $100 million in state sales tax evasion, money laundering, gasoline bootlegging, and enterprise corruption, they had to obtain amendments to their search warrants in order to seize disks and records from handbags and locked briefcases in the offices at two locations. After an exhaustive six month review of all computer evidence, they determined that the largest amount of the most damaging evidence was on the disks. The crooks did their work in Excel and then saved it on floppy disk. The lesson they learned from this was to execute the search warrant with everyone present and look for disks in areas where personal property is kept. As storage technologies continue to get smaller, criminals will have even more options for hiding data. A time may come when they can store data on tiny microdots that can be hidden anywhere.

Audit disabling. Most systems keep a log of activity on the system. Perpetrators of computer crimes have, in many cases, disabled the auditing or deleted the audit records pertaining to their activity. The hacking tool RootKit, for example, contains Trojan horse system utilities which conceal the presence of the hacker and disable auditing. ZAP is another tool for erasing audit records. Both of these can be downloaded for free on the Internet.

Cellular phones and cloning. Drug lords, gangsters, and other criminals regularly use "cloned" cell phones to evade the police. Typically, they buy the phones in bulk and discard them after use. A top Cali cartel manager might use as many as 35 different cell phones a day [Ramo 96]. In one case involving the Colombia cartel, DEA officials discovered an unusual number of calls to Colombia on their phone bills. It turned out that cartel operatives had cloned the DEA's own number! Some cloned phones, called "lifetime phones," hold up to 99 stolen numbers. New numbers can be programmed into the phone from a keypad, allowing the user to switch to a different cloned number for each and every call. With cloning, whether cellular communications are encrypted may have little impact on law enforcement, as they do not even know which numbers to tap.

Cellular phone cards. A similar problem occurs with cellular phone cards. These pre-paid cards, which are inserted into a mobile phone, specify a telephone number and amount of air time. In Sweden, phone cards can be purchased anonymously, which has made wiretapping impossible. The narcotics police have asked that purchasers be required to register in a database that would be accessible to the police [Minow 97]. A similar card is used in France, however buyers must show an identification card at the time of purchase. In Italy, a pre-paid card must be linked to an identity, which must be linked to an owner.

The emergence of digital cellular communications is potentially a benefit to both users and to law enforcement. This is because digital cell phones use stronger methods of authentication to protect against cloning, and they use link encryption for privacy. Traffic is encrypted between a cell phone and a base station, but the signals otherwise travel in the clear (or are separately encrypted while traversing microwave or satellite links). The advantage to users is that they can protect their local over-the-air communications even if the parties they are conversing with are using phones with no encryption or with incompatible methods of encryption. The benefit to law enforcement is that plaintext can be intercepted in the base stations or switches. Although there are devices for achieving end-to-end encryption with cellular phones, they are more costly and require compatible devices at both ends.

Hacking and Surveillance Tools

Dutch organized crime has an information warfare division that combines muscles, brains, know-how, guts, and money to achieve their goals. The division works for anyone willing to pay them. They work in cell structures, loosely coupled, and hard to get. The Amsterdam police faced severe information warfare attacks when investigating two major drug organizations, known as the cases of "Charles Z." and "De Hakkelaar." Police officers were observed, threatened, and intimidated; houses of District Attorneys and police officers were burglarized; rumors spread to discredit DA's and the investigation; PC's and diskettes were stolen and published during the trials. In short, everything was done to obstruct justice and the trials, though some were convicted.

Surveillance and hacking tools used by organized crime include:

Wiretapping tools. Organized crime groups have used signals intelligence against federal and state law enforcement agencies. In the mid 1980's, authorities in Texas and Florida found facilities equipped with signals monitoring equipment, including scanners and multiple receivers. The targeted frequencies included local and federal law enforcement: single channel VHF and UHF radio. The apparent purpose was to provide indications and warnings of counter-narcotics activities, including detection of drug transactions and impending raids. Intercept logs and other written records revealed that the facilities were operated by former Army and Navy security personnel [Blanchard 97].

Dutch organized crime was found tapping the phone lines of safe houses and the homes of high police officials. They had built receivers to monitor nation-wide pager networks. Intercepted information was fed into a database where it was further processed to determine, for example, which special units were cooperating with each other.

Colombian police and DEA agents raiding the Cali headquarters of one trafficking operation found signal-scanning equipment to intercept phone calls, fax messages, and air-traffic-control operations [Ramo 96]. The DEA also discovered drug-laden Colombian jets which had been outfitted with air-to-air signal interceptors to monitor the routes of U.S. military jets flying over the Gulf of Mexico and the Caribbean Sea [Ramo 96].

In 1990, Legion of Doom hackers were convicted of breaking into phone company switches and monitoring the communications of whomever they pleased. Kevin Poulson, who was mentioned earlier in conjunction with his use of encryption, roamed the switches of telephone networks, wiretapping movie stars, associates, and even the federal wiretappers. Between 1989 and 1991, he had access to nearly every federal and national security wiretap in California [Littman 97].

ESN/MIN scanners. The process of producing cloned cell phones begins by intercepting the Electronic Serial Number (ESN) and Mobile

Identification Number (MIN) of legitimate phones when they are in use. These numbers are snatched from the airwaves with special scanners and later programmed into phones. Some of these devices encrypt the intercepted ESN/MIN pairs before saving them in storage. This makes it more difficult for the authorities to prove that the device was used to store compromised ESN/MIN pairs.

Packet sniffers. Packet sniffers are frequently used to harvest user names and passwords transmitted over computer networks. In many instances, a sniffer is installed on a machine which has been hacked by the sniffer's owner. In such cases, the sniffer may store the passwords in a hidden file in order to avert detection. Periodically, the contents of the file are e-mailed back to the hacker. Investigators have found sniffers which encrypted the passwords and routed them through an anonymous re-mailer to avoid tracking.

Other hacking tools. These include war dialers for finding dial-in ports, password crackers, network scanners such as SATAN and the Internet Security Scanner for locating network vulnerabilities (these are also used by system administrators to patch their security holes), and miscellaneous scripts and programs for launching attacks against information systems. All of these tools can be downloaded from numerous hacking sites on the web.

Other Security Technologies

Encryption, password protection systems, and network scanners are useful tools against criminal intruders. As we have seen, they are also useful to the crook. In fact, the same could be said of all information security technologies. In the hands of organized crime, they will make the task of law enforcement more difficult. The same mechanisms that keep out hackers and corrupt insiders can keep out investigators making a surreptitious entry or seizing computer evidence.

ENCRYPTION POLICY OPTIONS

The following outlines policy options and their likely impact on crime. For a discussion of a broader range of options, see the National Research Council's report on encryption [CRISIS 96].

Export Controls

Encryption policy in the U.S. and most other major industrial countries has been based on restricting exports of encryption technology, but not imports or domestic use. Notable exceptions are France and China, which have also controlled domestic use of encryption.

Although the exact regulations have changed over the years, U.S. policy has been to allow export of products which reasonably afforded government access, while severely limiting export of those which are totally inaccessible. Until the end of 1996, the policy was realized by granting general licenses for products using 40-bit keys, and requiring individual licenses for products using longer keys [Commerce 96a].

Products using extremely long keys, for example, 128-bit RC4 or Triple-DES with 112 or 168-bit keys, were generally not exportable at all.

At the end of 1996, the regulations were amended to include ready export of products with an acceptable key recovery system [Commerce 96b]. For such products, key length is not a factor as the government can get access to plaintext through the key recovery system. Trusted Information Systems, for example, has been granted approval to export 128-bit encryption with its patented RecoverKeyTM technology. Because many vendors have not yet built key recovery systems, the government is also allowing exports of 56-bit DES or equivalent to vendors with plans to implement key recovery in their products by the end of 1998. Several vendors have received export approvals for DES-based products under the regulations.

In May 1997, the Commerce Department announced that it will allow export of non-recoverable encryption with unlimited key length for products that are specifically designed for financial transactions, including home banking [Commerce 97]. They will also allow exports, for two years, of non-recoverable general-purpose commercial products of unlimited key length when used for interbank and similar financial transactions, once the manufacturers file a commitment to develop recoverable products. The reason key recovery is not required with financial transactions is that financial institutions are legally required and have demonstrated a consistent ability to provide access to transaction information in response to authorized law enforcement requests.

Impact of export controls on crime and law enforcement. It is extremely difficult to assess the impact of export controls on crime as we cannot know what the current state would be if there had not been such controls. We can, however, make four general observations:

First, export controls have not prohibited the proliferation and use of encryption sufficient to protect against most eavesdroppers and intruders. The reason today's communications are vulnerable to cellular scanners, packet sniffers, and other surveillance tools is not because of weak encryption, but rather because they are not encrypted at all. If packet sniffers had to break even a 40-bit key to harvest a single password, their use would plummet. This is not to say that one could not build tools to crack weak encryption or that users should settle for weak encryption, only that the most common attacks today could have been prevented using exportable encryption. This is particularly true now that encryption of unlimited strength can be exported with key recovery.

Second, export controls have made it more difficult for businesses and law enforcement agencies operating outside the U.S. to get strong encryption from the U.S. to protect their communications. A law enforcement officer in a foreign country complained that it took him a year and a half to get a U.S. product; when it finally arrived, the strongest methods had been removed. Meanwhile, their communications were targeted by members of organized crime. The Administration has taken steps to expedite the licensing process; it is vital that such efforts continue.

Third, export controls have not prevented determined criminals and terrorists from getting access to unbreakable cryptography. They can obtain such encryption from products produced domestically, products made in countries with lax controls, and products distributed over the Internet.

Fourth, export controls have likely slowed down the spread of unbreakable encryption to organized crime groups. Many criminals use whatever encryption comes with standard commercial products that are approved for export. These products might have incorporated unbreakable methods were it not for export controls.

Lifting export controls. Many people in the private sector have been arguing for years that export controls harm the competitiveness of U.S. industry in the global market and make it more difficult for consumers and businesses to get products with strong encryption. As a result of their extensive lobbying efforts, three bills were introduced in 1996 to liberalize export controls on encryption, two in the Senate and one in the House of Representatives. Although none of the bills was brought to the floor for a vote, all three were reintroduced in February 1997. The current bills are as follows:

> S. 376, the "Encrypted Communications Privacy Act of 1997," introduced by Senator Leahy with Senators Burns, Murray, and Wyden as co-sponsors.
>
> S. 377, the "Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997," introduced by a bi-partisan group of seventeen senators led by Senators Burns and Leahy.
>
> H.R. 695, the "Security and Freedom Through Encryption (SAFE) Act of 1997," introduced by Representative Goodlatte with over eighty co-sponsors. It was passed by the House Judiciary Committee on May 14.

These bills would all lift export controls on encryption software independent of whether the products provide key recovery. In addition, there have been three lawsuits challenging the constitutionality of export controls on encryption software (see [Denning 97] for a summary).

Although we cannot know with any certainty the effects of lifting export controls, it seems inevitable that removing barriers to international trade would likely promote the availability and use of all forms of encryption, both domestically and internationally, as any regulations on encryption impose a hurdle to vendors and corporations operating in a global market. Thus, one effect of lifting export controls is likely to be increased availability and use of encryption to protect sensitive information from organized crime.

In trying to assess the impact of lifting export controls on investigations of crime and terrorism, the task is more difficult. On the one hand, the increased availability of strong encryption, indeed any form of encryption, could make the task of law enforcement more difficult. On the other hand, because there is a market demand for key recovery systems, law enforcement agencies would likely be able to get keys in many cases, particularly situations involving stored data where the user demand for key recovery is greatest, and those involving independent recovery agents. As noted earlier, if organized crime groups holds their own keys, then the task of acquiring keys might be no easier than it is without a built-in key recovery system.

The Clinton Administration, which has been opposed to lifting all controls, has argued that export controls will at the very least ensure that all exportable encryption products, including those used to protect communications, will have key recovery systems operated by acceptable key recovery agents. Because many, perhaps most, vendors will build a single product line for both domestic and international customers, the benefits to law enforcement will be felt domestically as well as internationally. However, some vendors told us they would develop products only for the domestic market so that their products could offer strong, government-proof encryption. Key recovery would be completely optional.

Although the argument is often made that no organization would trust their data to encryption software acquired on the Internet, this is not entirely supported by evidence, as many individuals in business, government, and academia download software from the Internet. PGP has been downloaded and used by criminal and law-abiding organizations alike. Distribution of software via the World Wide Web is becoming commonplace by major vendors.

On April 18, the Department of Commerce announced the formation of a President's Export Council Subcommittee on Encryption. The subcommittee is to advise the Secretary on matters pertinent to the implementation of an encryption policy that supports the growth of commerce while protecting the public safety and national security. The subcommittee is to consist of approximately 25 members representing the exporting community and government agencies responsible for implementing encryption policy.

Domestic Regulations

Domestic regulations can range from licensing mechanisms aimed at facilitating the voluntary adoption of key recovery systems to laws banning methods of encryption that do not afford government access.

Voluntary Licensing of Key Recovery Services. The Clinton Administration has drafted a bill intended to promote the establishment of a key management infrastructure (KMI) with key recovery services. The bill is based on the premise that in order to fully support electronic commerce, encryption products must interface with a KMI which issues and manages certificates for users' public keys. The bill would create a program under the Secretary of Commerce for registering certificate authorities and key recovery agents wishing to participate in the KMI enabled by the act. Certificate authorities registered under the act would be permitted to issue certificates for public encryption keys only if the corresponding decryption keys were stored with a registered key recovery agent (private signature keys would not be stored). Participation in the registered KMI would be voluntary. Certificate authorities could operate without registration, and encryption products could interface with infrastructures supported by unregistered CA's. Users would be free to acquire certificates from unregistered CA's without depositing their keys

The bill specifies the conditions under which recovery information can be released to government agencies or other authorized parties independent of whether the key recovery agents are registered, and criminalizes various acts relating to the abuse of keys or the KMI. The bill also establishes liability protections for key recovery agents acting in good faith. Certificate authorities and key recovery agents registered under the act will be required to meet minimum standards for security and performance.

The Commerce Department has also begun the process of creating a standard for the KMI. Together with the bill, the standard aims to facilitate the establishment of reliable and trustworthy certificate authorities and key recovery services, and the use of strong encryption in conjunction with such services. A Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal KMI was established in the fall of 1996 to provide recommendations for such a standard. The standard will provide a framework for the KMI and for encryption products that use KMI services. The Commerce Department is coordinating ten pilot projects to use key recovery within the federal government.

The impact of the program on law enforcement is difficult to predict. If the standard is widely adopted by federal agencies and their contractors, then at the very least it should facilitate investigations of fraud and corruption in certain government-related activities. To the extent that the program is accepted by the private sector, it could further facilitate criminal investigations. However, because the program is voluntary, criminal and law abiding persons alike could opt to use methods of encryption that interface with other public key infrastructures, including infrastructures which do not support key recovery. Indeed, such infrastructures are already emerging in the private sector, which has been developing its own standards. Commercial encryption products will likely support multiple infrastructures, just as they now support multiple encryption algorithms.

Companies offering key recovery services might have incentives to register under the act for liability protection and government endorsement. Further, companies wishing to export their products will have an incentive to use existing key recovery services within the government's KMI or to register their own key recovery services for inclusion in the KMI. Lifting export controls would reduce this incentive.

Controls Relating to the Use of Encryption in Crime. Just as there are penalties associated with the use of weapons in the commission of crimes, penalties could be associated with the use of encryption. The Clinton Administration's proposed bill would add a fine or up to five years of imprisonment for persons knowingly encrypting information in furtherance of the commission of a criminal offense. It would be an affirmative defense to a prosecution that information enabling decryption be stored with a key recovery agent registered under the act. S. 376 and H.R. 695 also include provisions for criminalizing the use of encryption to obstruct justice. Kevin Manson with the Federal Law Enforcement Training Center has suggested the possibility of restricting the use of encryption by convicted felons. Both of these options could increase the likelihood of investigators getting access to plaintext in criminal investigations.

Mandatory Controls on Encryption Products. The Administration's approach to domestic encryption policy has been one based on voluntary measures. They do not propose to mandate that all encryption products support some method of government access. Such mandatory controls might be accomplished through a licensing regime, where the manufacture, distribution, import, and export of unlicensed products is made illegal. Individuals may or may not be permitted to develop their own unlicensed encryption systems for personal use, depending on whether the regulations cover the use of encryption.

Licensing of encryption products would have a positive effect on controlling the distribution and use of unbreakable cryptography. Because many criminals use whatever encryption comes with standard commercial products, it would increase the chances of law enforcement agencies getting access to plaintext communications and stored records in criminal investigations.

If the use of encryption is regulated along with the manufacture and distribution of encryption products, it would be extremely difficult and costly to detect its illicit use. Even if all licensed products were required to insert information into the ciphertext for easy identification, persons intent on circumventing the law could encrypt their messages with an unlicensed product before handing it off to a licensed one. Or, they could encrypt a message with an unlicensed product and then use steganography tools to hide the random stream in sound or image files. Attempting to decrypt intercepted ciphertext to see if it produced plaintext would be fraught with difficulty, as the plaintext itself could be in one of hundreds of different formats and possibly compressed.

Monitoring communications for illicit use of cryptography would also violate existing wiretap statutes, which permit government wiretaps only under a court order based on probable cause of criminal activity and only under strict minimization requirements. Under current laws, detection of the illicit use of encryption would be limited to cases where court orders were obtained for other reasons. If an order to intercept particular communications of a subject or to seize particular computer files is frustrated by encryption, this would be a sign that the subject was most likely using some method of unlicensed encryption. In the case of a computer seizure, the agency would likely find the unlicensed product on the subject's machine.

Even if the use of encryption is not regulated, there are drawbacks to regulating the manufacture and distribution of products. One, which we noted earlier, is that key recovery systems could potentially be abused, either by the government or by the people operating key recovery services. Although it is possible to build in extensive safeguards to protect against such abuses, mandatory key recovery would force users to take risks they might consider unacceptable, particularly with respect to their communications where they might not need key recovery for their own purposes. A second drawback is cost. Establishing a mandatory licensing regime would be expensive and raise the cost of encryption products.

International Policy

The use of encryption is an international issue, both for industry which is concerned about being able to market and use encryption that is strong and globally interoperable, and for governments which recognize the need for encryption but are also concerned about its adverse effects. Other countries have been wrestling with encryption policy, and several are considering strategies based on key recovery technologies.

United Kingdom. The British government considers it essential that security, intelligence, and law enforcement agencies preserve their ability to conduct effective legal interception of communications, while at the same time ensuring the privacy of individuals [DTI 97]. Accordingly, they have issued a draft proposal to license trusted third parties (TTPs) providing encryption services to the general public [DTI 97]. The TTPs would hold the encryption keys of their clients, releasing them only to authorized persons; appropriate safeguards would be established to protect against abuse and misuse of keys. The licensing regime would seek to ensure that TTPs meet criteria for liability coverage, quality assurance, and key recovery. It would allow for relaxed export controls on encryption products that work with licensed TTPs. It would be illegal for an unlicensed entity to offer encryption services to the public, however, the private use of encryption would not be regulated.

France. France has traditionally required licenses to import, export, or use encryption products. In June 1996, a law was passed to waive the licensing requirement on the use of encryption when the keys are held by licensed key recovery agents [France 96]. To get a license, an organization providing key recovery services would have to do business in France and have stock honored by the French government. The service providers would have to be of French nationality.

European Commission. The European Commission has been preparing a proposal to establish a European-wide network of Trusted Third Parties that would be accredited to offer services that support digital signatures, notarization, confidentiality, and data integrity. The trust centers, which would operate under the control of member nations, would hold keys that would enable them to assist the owners of data with emergency decryption or supply keys to their national authorities on production of a legal warrant. The proposal is currently undergoing further consideration within the Commission before it can be brought before the Council of the European Union for adoption. Eight studies and pilot projects are planned for 1987.

OECD. In recognition of the need for an internationally coordinated approach to encryption policy to foster the development of a secure global information infrastructure, the Organization for Economic Cooperation Development (OECD), has recently issued guidelines for cryptography policy [OECD 97]. The guidelines represent a consensus about specific policy and regulatory issues. While not binding to OECD's 29 member countries, they are intended to be taken into account in formulating policies at the national and international level.

The guidelines expound on eight basic principles for cryptography policy: 1) trust in cryptographic methods, 2) choice of cryptographic methods, 3) market driven development of cryptographic methods, 4) standards for cryptographic methods, 5) protection of privacy and personal data, 6) lawful access, 7) liability protection, and 8) international cooperation. The principal of lawful access does not recommend key recovery, but leaves it as an option of member countries: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible."

Whether other countries embrace key recovery will impact the effectiveness of the U.S. key recovery program and, in turn, its impact on criminal investigations. At the same time, it is hard to see how a global key recovery infrastructure can avoid entirely exploitation by organized crime, especially considering the integration of organized crime with governments such as Russia. If key recovery is adopted on a large scale, strong boundaries must be erected between key recovery systems in the U.S. and other countries.

CONCLUSIONS

Encryption is essential in today's information and network age. Encryption policy must facilitate and encourage the use of encryption so that businesses can protect their corporate assets from economic espionage by foreign governments and competitors, so that law enforcement agencies can counter the surveillance activities of organized crime, and so that all organizations and individuals can safeguard sensitive information from criminals and intruders. At the same time, because encryption can be exploited by criminals and terrorists, its completely unfettered proliferation may not be in our national interest. The Clinton Administration and National Research Council reached a similar conclusion, although they recommended different approaches.

The use of encryption by large organized crime groups is still relatively low. This can be attributed to several factors, including the difficulty and overhead of using encryption (particularly the personnel time involved), a concern about losing access to valuable data if something happens to the keys, and a general sense that their environments are already reasonably isolated and protected from law enforcement. Most of the investigators we talked to did not find that encryption was obstructing a large number of investigations. When encryption has been encountered, investigators have usually been able to get the keys from the subject, crack the codes, or use other evidence.

This should not be interpreted to justify complacency, however, as the world is just now moving rapidly to the Internet and Intranets. Encryption is beginning to show up in serious cases involving organized crime and terrorism. It is having an increasing impact on law enforcement, delaying investigations, increasing costs, and preventing access to valuable evidence and intelligence. Unbreakable encryption is spreading and threatening current and future investigations.

What we are witnessing today is the leading edge of what could become a serious problem. Access to unbreakable encryption has the effect of shifting power from the government to the individual and criminal enterprise. As unbreakable encryption becomes increasingly available in standard commercial products and the population becomes better educated about encryption, its use by criminals and terrorists to evade law enforcement could become routine. Law enforcement could find itself unable to investigate or prosecute many serious cases.

The impact of encryption on crime will be strongly affected by the encryption that is integrated into popular desktop software and network servers, particularly that which is pre-installed at the time of purchase. This software will offer strong file encryption and end-to-end message security for electronic mail, web transactions, telephony, and other network traffic. It will be easy to use and globally interoperable. Many criminals will simply use this encryption rather than going to the trouble of installing add-on products which require greater effort to use or have limited interoperability. Even if they use add-ons within their own circles, they may use the integrated encryption when communicating with others.

Key recovery offers an approach to encryption that can potentially meet the security needs of users while also supporting lawful access in criminal and national security investigations. Given user demand for key recovery with stored data coupled with the Administration's program to promote key recovery through liberalized export controls, many commercial products will include some form of key recovery. However, it is still too early to know the extent to which key recovery will be a standard product feature and its use standard practice.

No approach to encryption will be foolproof. Whereas export controls clearly have an impact on product lines, they do not keep unbreakable encryption out of the hands of criminals entirely. Even if non-recoverable methods of encryption were outlawed, determined criminals would find ways of circumventing the controls, either by developing their own systems or by acquiring them through the black market. Encryption software is easy to distribute, and the use of restricted encryption could be camouflaged. However, such laws would make it harder for criminals to acquire and use government-proof encryption.

The impact of encryption on crime is at its early stages. Our companies need strong information protection now, and the market is responding quickly with end-to-end encryption. As the market delivers simple solutions, criminal organizations will use this enterprise-wide cover. It is imperative that we monitor the situation closely so that policy decisions are well informed. We recommend an ongoing study of the effect of encryption and other information technologies on investigations, prosecutions, and intelligence operations. As part of this study, a database of case information from federal and local law enforcement and intelligence agencies should be established and maintained.

Encryption is a critical international issue with severe impact and benefits to business and order. Encryption policy demands our thoughtful and immediate attention, a partnership between business and government, and collaboration with our international colleagues.

REFERENCES

[Akdeniz] Yaman Akdeniz, "Regulation of Child Pornography on the Internet," http://www.cyber-rights.org/reports/child.htm.

[Blanchard 97] This was reported to us by Hugh Blanchard.

[Blaze 96] M. Blaze, W. Diffie, R. Rivest, B. Schneier, T. Shimomura, E. Thompson, M. Weiner, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security," January 1996.

[Bockler] http://www.hiwaay.net/boklr/bsw_crak.html as of February 1997.

[Clinton 95] Office of the Press Secretary, The White House, Remarks by the President to Staff of the CIA and Intelligence Community, Central Intelligence Agency, McLean, VA, July 14, 1995.

[Commerce 96a] This is a simplification. See A Study of the International Market for Computer Software with Encryption, U.S. Department of Commerce and the National Security Agency, Washington, DC, 1996.

[Commerce 96b] Federal Register, Vol. 61, No. 251, December 30, 1996. At http://jya.com/bxa123096.txt.

[Commerce 97] U.S. Department of Commerce News, Bureau of Export Administration, Encryption Exports Approved for Electronic Commerce, May 8, 1997.

[CRISIS 96] Cryptography's Role in Securing the Information Society, Kenneth W. Dam and Herbert S. Lin, eds., National Academy Press, 1996.

[Crowell 97] William P. Crowell, Written Statement to the Senate Committee on Commerce, Science, and Transportation Hearing on S.377 "Pro-Code," March 19, 1997.

[Dallas 97] Walter W. Manning, "Should You Be on the Net?" FBI Law Enforcement Bulletin, January 1997, pp. 18-22. Additional information was provided by Detective R. J. Montemayor in the Dallas Police Department.

[Denning 97] Dorothy E. Denning, "Encryption Policy and Market Trends," February 1997, http://www.cs.georgetown.edu/~denning/crypto/Trends.html.

[Denning & Branstad 96] Dorothy E. Denning and Dennis K. Branstad, "A Taxonomy of Key Escrow Encryption," Communications of the ACM, Vo. 39, No. 3, March 1996, pp. 34-40. At http://www.cs.georgetown.edu/~denning/crypto.

[DTI 97] Licensing of Trusted Third Parties for the Provision of Encryption Services, Public Consultation Paper on Detailed Proposals for Legislation, March 1997, Department of Trade and Industry, DTI reference URN 97/669. At http://www.dti.gov.uk/pubs.

[France 96] A translation and analysis of the French law is available from Steptoe & Johnson at http://www.us.net/~steptoe/france.htm.

[Freeh 94] Statement of Louis J. Freeh, Director Federal Bureau of Investigation, before the Subcommittee on Technology and the Law of the Committee on the Judiciary, United States Senate, and the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary, House of Representatives, March 18, 1994.

[Freeh 96] Statement of Louis J. Freeh, Director Federal Bureau of Investigation, before the Senate Select Committee on Intelligence and Senate Select Committee on the Judiciary, Subcommittee on Terrorism, Technology and Government Information, Hearing on Economic Espionage, February 28, 1996. Free reported that FBI investigations reflect 23 countries engaged in economic espionage activities against the U.S.

[Freeh 97] Statement of Louis J. Freeh, Director Federal Bureau of Investigation, before the Committee on Commerce, Science, and Transportation, United States Senate, regarding the Impact of Encryption on Law Enforcement and Public Safety, March 19, 1997.

[Grabosky 97] P. N. Grabosky and Russell G. Smith, Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, 1997. Information about the English blackmailer was attributed to E. Nicholson, "Hacking Away at Liberty," Times (London), April 18, 1989.

[Kaplan & Marshall 96] David E. Kaplan and Andrew Marshall, The Cult at the End of the World, Crown Publishers, 1996.

[Kennedy 97] This case was reported by Brian Kennedy of the Sacramento County Sheriff's Department.

[Littman 97] Jonathan Littman, The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulson, Little, Brown and Co., 1997.

[May 96] Timothy C. May, "Introduction to BlackNet" and "BlackNet Worries," in High Noon on the Electronic Frontier, Peter Ludlow, ed., The MIT Press, 1996. The articles were written and posted on the Internet in Fall 1993 and February 1994 respectively.

[McCormack 96] Michael McCormack, "Europe hit by cryptoviral extortion," Computer Fraud & Security, June 1996, p. 3.

[McMahon 97] This case was reported to us by Jim McMahon, former head of the High Technology Crimes Detail of the San Jose Police Department.

[Minow 97] Martin Minow, "Swedish Narcotics Police Demand Telephone Card Database," Risks-Forum Digest, Vol. 19, Issue 07, April 14, 1997. The article was a translation and summary of one in the Swedish newspaper, Svenska Dagbladget, April 11, 1997: http://www.svd.se/svd/ettan/ettan_97_04_11/narkotikapolisen.html.

[OECD 97] OECD News Release, OECD Guidelines for Cryptography Policy," March, 1996. http://www.oecd.org/dsti/iccp/crypto_e.html. For an analysis, see Stewart Baker, Background information and a detailed analysis of the OECD Cryptography Policy Guidelines, March 1997. http://www.steptoe.com/pubtoc.htm.

[O'Reilly 96] The State of Web Commerce, O'Reilly & Associates and Netcraft, Ltd., December 1996.

[Price 97] This case was reported to us by Dale Price, who at the time was the senior corporate security official responsible for conducting the investigation on behalf of a major U.S. defense contractor.

[Ramo 96] Joshua Cooper Ramo, "Crime Online," Time Digital, September 23, 1996, pp. 28-32.

[Reitinger 96] Philip R. Reitinger, "Compelled Production of Plaintext and Keys," 1996. http://members.aol.com/TEKALERT/reitinger.html.

[Schmidt] This case was reported to us by Howard Schmidt.

[Thompson 97] "Can your crypto be turned against you? A CSI interview with Eric Thompson of AccessData, Computer Security Alert, No. 167, February 1997, pp. 1+.

[TIS 96] TIS Worldwide Survey of Cryptographic Products, December 1996. http://www.tis.com.

[Wayner 96] Peter Wayner, Disappearing Cryptography, Academic Press, 1996.

GLOSSARY

DES - Data Encryption Standard. An encryption method using 56-bit keys. It was adopted as a federal information processing standard (FIPS) in 1977. The best known method for breaking it is brute force; that is, trying all possible bit combinations. At 56 bits, this is tractable, but time consuming and expensive. Triple-DES iterates DES three times, each time using a different key for a combined key length of 168 bits (the first and third iterations sometimes use the same key for a total of 112 bits). Keys of that length cannot be broken by brute force even under the most optimistic conditions.

IDEA - International Data Encryption Algorithm. An encryption method using 128-bit keys. It was invented by Xuejai Lai and James Massey. The best known method for breaking it is brute force, but this is not possible for 128-bit keys.

Key recovery. A capability whereby authorized persons can, under prescribed conditions, obtain access to the key needed to decrypt information through a process other than the normal channel used to distribute the key to the intended recipient. The decryption key is recovered using information stored with the ciphertext together with information held by a trusted agent, which could be an officer of the organization owning the data or a third party. The term "key escrow" is also used, sometimes synonymously with key recovery, other times to refer to only those methods wherein users' private keys are deposited with a trusted party. See [Denning & Branstad 96] for an overview of methods.

PGP - Pretty Good Privacy. A system that uses IDEA for data encryption and RSA with variable length keys for key distribution and digital signatures. It is available from Internet sites all over the world or as a shrink-wrapped product. It is commonly used for electronic mail and file encryption. PGPfone provides encrypted Internet telephony. PGP was invented by Philip Zimmerman.

RSA. A public-key cryptosystem invented by Ronald Rivest, Adi Shamir, and Leonard Adleman. It is used for distributing message encryption keys and for digital signatures. It can use any length key, but 1,024 bits is common and considered unbreakable. RSA key sizes are much larger than with other encryption methods because a private key can be determined by finding the prime factors of a public key, which is much faster than brute force.

Dorothy E. Denning is Professor, Computer Science Department, Georgetown University, Reiss 225, Washington, DC 20057, ph: 202-687-5703, fax: 202-687-1835, denning@cs.georgetown.edu, http://www.cs.georgetown.edu/~denning.

William E. Baugh, Jr. is Vice President, Information and Technology Systems Sector, Science Applications International Corporation, 8301 Greensboro Drive, Suite 1200, McLean, VA 22102, ph: 703-749-8946, fax: 703-734-5960, WILLIAM.E.BAUGH.JR@cpmx.saic.com.