Hiding Crimes in Cyberspace[1]

Dorothy E. Denning and William E. Baugh, Jr.

July 1999

[To appear in *Information, Communication and Society*, Vol. 2, No 3, Autumn 1999, and in *Cybercrime*, B. D. Loader and D. Thomas (eds.), Routledge, 1999.

INTRODUCTION

The growth of telecommunications and electronic commerce has led to a growing commercial market for digital encryption technologies. Business needs encryption to protect intellectual property and to establish secure links with their partners, suppliers, and customers. Banks need it to ensure the confidentiality and authenticity of financial transactions. Law enforcement needs it to stop those under investigation from intercepting police communications and obstructing investigations. Individuals need it to protect their private communications and confidential data. Encryption is critical to building a secure and trusted global information infrastructure for communications and electronic commerce.

Encryption also gives criminals and terrorists a powerful tool for concealing their activities. It can make it impossible for law enforcement agencies to obtain the evidence needed for a conviction or the intelligence vital to criminal investigations. It can frustrate communications intercepts, which have played a significant role in averting terrorist attacks and in gathering information about specific transnational threats, including terrorism, drug trafficking, and organized crime (White House 1995). It can delay investigations and add to their cost.

The use of encryption to hide criminal activity is not new. The April 1970 issue of the FBI Law Enforcement Bulletin reports on several cases where law enforcement agencies had to break codes in order to obtain evidence or prevent violations of the law. None of the cases, however, involved electronic information or computers. Relatively simple substitution ciphers were used to conceal speech.

Digital computers have changed the landscape considerably. Encryption and other advanced technologies increasingly are used, with direct impact on law enforcement. If all communications and stored information in criminal cases were encrypted, it would be a nightmare for investigators. It would not be feasible to decrypt everything, even if technically possible. How would law enforcement agencies know where to spend limited resources?

We address here the use of encryption and other information technologies to hide criminal activities. Numerous case studies are presented for illustration. We first examine encryption and the options available to law enforcement for dealing with it. Next we discuss a variety of other tools for concealing information: passwords, digital compression, steganography, remote storage, and audit disabling. Finally we discuss tools for hiding crimes through anonymity: anonymous remailers, anonymous digital cash, computer penetration and looping, cellular phone cloning, and cellular phone cards.

ENCRYPTION IN CRIME AND TERRORISM

This section describes criminal use of encryption in four domains: voice, fax, and data communications; electronic mail; files stored on the computers of individual criminals and criminal enterprises; and information posted in public places on computer networks.

Voice, Fax, and Real-Time Data Communications

Criminals can use encryption to make their real-time communications inaccessible to law enforcement. The effect is to deny law enforcement one of the most valuable tools in fighting organized crime - the court-ordered wiretap. In March 1997, the director of the Federal Bureau of Investigation, Louis J. Freeh, testified that the FBI was unable to assist with 5 requests for decryption assistance in communications intercepts in 1995 and 12 in 1996 (US Congress 1997a). Such wiretaps can be extremely valuable as they capture the subjects' own words, which generally holds up much better in court than information acquired from informants, for example, who are often criminals themselves and extremely unreliable. Wiretaps also 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. Communications intercepts have also been useful in terrorism cases, sometimes helping to avoid a deadly attack. They have helped prevent the bombing of a foreign consulate in the United States and a rocket attempt against a U.S. ally, among other things (ibid).

There is little case information in the public domain on the use of communications encryption devices by criminal enterprises. 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 and Smith 1997).

We understand that some terrorist groups are using high-frequency encrypted voice/data links with state sponsors of terrorism. Hamas reportedly is using encrypted

Internet communications to transmit maps, pictures, and other details pertaining to terrorist attacks. The Israeli General Security Service believes that most of the data is being sent to the Hamas worldwide center in Great Britain (IINS 1997).

The lack of universal interoperability and cost of telephone encryption devices - several hundred dollars for a device that provides strong security - has likely slowed their adoption by criminal enterprises. The problems to law enforcement could get worse as prices drop and Internet telephony becomes more common. Criminals can conduct encrypted voice conversations over the Internet at little or no cost. This impact on law enforcement, however, may be balanced by the emergence of digital cellular communications. These phones encrypt the radio links between the mobile devices and base stations, which is where the communications are most vulnerable to eavesdroppers. Elsewhere, the communications travel in the clear (or are separately encrypted while traversing microwave or satellite links), making court-ordered interception possible in the switches. 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.

Hackers use encryption to protect their communications on Internet Relay Chat (IRC) channels from interception. They have also installed their own encryption software on computers they have penetrated. The software is then used to set up a secure channel between the hacker's PC and the compromised machine. This has complicated, but not precluded, investigations.

Electronic Mail

Law enforcement agencies have encountered encrypted e-mail and files in investigations of pedophiles and child pornography, including the FBI's Innocent Images national child pornography investigation. In many cases, the subjects were using Pretty Good Privacy (PGP) to encrypt files and e-mail. PGP uses conventional cryptography for data encryption and public-key cryptography for key distribution. 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. Investigators say, however, that most child pornography traded on the Internet is not encrypted.

One hacker used encrypted e-mail to facilitate the sale of credit card numbers he had stolen from an Internet service provider and two other companies doing business on the Web. According to Richard Power, editorial director of the Computer Security Institute, Carlos Felipe Salgado Jr. had acquired nearly 100,000 card numbers by penetrating the computers from an account he had compromised at the University of California at San Francisco. Using commonly available hacking tools, he exploited known security flaws in order to go around firewalls and bypass encryption and other

security measures. Boasting about his exploits on Internet Relay Chat, Salgado, who used the code name SMAK, made the mistake of offering to sell his booty to someone on the Internet. He conducted on-line negotiations using encrypted e-mail and received initial payments via anonymous Western Union wire transfer. Unknown to him, he had walked right into an FBI sting. After making two small buys and checking the legitimacy of the card numbers, FBI agents arranged a meeting at San Francisco airport. Salgado was to turn over the credit cards in exchange for $260,000. He arrived with an encrypted CD-ROM containing about 100,000 credit card numbers and a paperback copy of Mario Puzo's The Last Don. The key to decrypting the data was given by the first letter of each sentence in the first paragraph on page 128. Salgado was arrested and waived his rights. In June 1997, he was indicted on three counts of computer crime fraud and two counts of trafficking in stolen credit cards. In August, he pled guilty to four of the five counts. Had he not been caught, the losses to the credit card companies could have run from $10 million to over $100 million (Power 1997).

We were told of another case in which 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 to determine who was talking with whom. 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. We also received an anonymous report of a group of terrorists encrypting their e-mail with PGP.

Stored Data

In many criminal cases, documents and other papers found at a subject's premises provide evidence crucial for successful prosecution. Increasingly, this information is stored electronically on computers. Computers themselves have posed major challenges to law enforcement, and encryption has only compounded these challenges.

The FBI found encrypted files on the laptop computer of Ramsey Yousef, a member of the international terrorist group responsible for bombing the World Trade Center in 1993 and a Manila Air airliner in late 1995. 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 (US Congress 1997a). Although much of the information was also available in unencrypted documents, the case illustrates the potential threat of encryption to public safety if authorities cannot get information about a planned attack and some of the conspirators are still at large.

Successful decryption of electronic records can be important to an investigation. Such was the case when Japanese authorities seized the computers of the Aum Shinrikyo cult - the group responsible for gassing the Tokyo subway in March 1995,

killing 12 people and injuring 6,000 more (Kaplan and Marshall 1996). 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 said to be crucial to the investigation, including plans and intentions to deploy weapons of mass destruction in Japan and the United States.

In the Aum cult case, the authorities were lucky to find the key on a disk. In other cases, the subjects turned over their keys. For example, the Dallas Police Department encountered encrypted data in the investigation of a national drug ring which was operating in several states and dealing in Ecstasy. 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 were using the Internet for sales, but they were 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 - see later discussion) to stay ahead of law enforcement (Manning 1997).[2]

In many cases, investigators have had to break the encryption system in order to get at the data. For example, when the FBI seized the computers of CIA spy Aldrich Ames, they found encrypted computer files, but no keys. Fortunately, Ames had used standard commercial off-the-shelf software, and the investigator handling the computer evidence was able to break the codes using software supplied by AccessData Corporation of Orem, Utah. The key was Ames's Russian code name, KOLOKOL (bell). According to investigators, failure to recover the encrypted data would have weakened the case. Ames was eventually convicted of espionage against the United States (CSI 1997).[3]

Code breaking is not always so easy. In his book about convicted hacker Kevin Poulsen, Jonathan Littman reported that Poulsen had encrypted files documenting everything from the wiretaps he had discovered to the dossiers he had compiled about his enemies. 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 that took several months at an estimated cost of hundreds of thousands of dollars. The effort apparently paid off, however, yielding nearly ten thousand pages of evidence (Littman 1997).

A substantial effort was also required to break the encryption software used by the New York subway bomber, Leary. In that case, the result yielded child pornography and personal information, which was not particularly useful to the case.

Investigators, however, retrieved other evidence from the computer that was used at the trial. Leary was found guilty and sentenced to 94 years in jail.

Timeliness is critical in some investigations. Several years ago, a Bolivian terrorist organization assassinated four U.S. Marines, and AccessData was brought in to decrypt files seized from a safe house. With only twenty four hours to perform this task, 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 (CSA 1997). In such cases, an effort that requires months or years to complete might be useless.

In other cases, the ability to successfully decrypt files proved unessential, as when a Durham priest was sentenced 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 U.K. authorities seized his computers, they found files of encrypted messages. The encryption was successfully broken, however, the decrypted data did not affect the case.

Even when decrypted material has little or no investigative value, considerable resources are wasted reaching that determination. If all information were encrypted, it would be extremely difficult for law enforcement to decide where to spend precious resources. It would not be practical or even possible to decrypt everything. Yet if nothing were decrypted, many criminals would go free.

Some investigations have been derailed by encryption. For example, at one university, the investigation of a professor thought to be trafficking in child pornography was aborted because the campus police could not decrypt his files. In another case, 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.

At Senate hearings in September 1997, Jeffery Herig, special agent with the Florida Department of Law Enforcement, testified that they were unable to access protected files within a personal finance program in an embezzlement case at Florida State University. He said the files could possibly hold useful information concerning the location of the embezzled funds (US Congress 1997b).

Herig also reported that they had encountered unbreakable encryption in a U.S. Customs case involving an illegal, world-wide advanced fee scheme. At least 300 victims were allegedly bilked out of over $60 million. Herig said they had encountered three different encryption systems. Although they were able to defeat the

first two, they were unsuccessful with the third. The vendor told them that there no backdoors. “Although I have been able to access some of the encrypted data in this case,” Herig said, “we know there is a substantial amount of incriminating evidence which has not been recovered” (ibid).

In early 1997, we were told that Dutch organized crime had received encryption support from a group of skilled hackers who themselves used PGP and PGPfone to encrypt their communications. The hackers had 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 the 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.

There have been a few reported cases of company insiders using encryption as a tool of extortion. The employees or former employees threatened to withhold the keys to encrypted data unless payment was made. In these cases, encryption is not used to conceal evidence of crimes, but rather to intimidate the organization. We are not aware of any extortion attempts of this nature that succeeded.

The use of encryption by the victims of crime can also pose a problem for law enforcement. At hearings in June 1997, Senator Charles Grassley told of an 11-year-old boy in the Denver area who committed suicide after being sexually molested. The boy had left behind a personal organizer, which investigators believed might contain information about the man whom his mother believed molested him. The organizer was encrypted, however, and the police had been unable to crack the password. The investigation had been on hold since February 1996.

In April 1998, the FBI’s Computer Analysis Response Team (CART) forensics laboratory started collecting data on computer forensics cases handled at headquarters or in one of the FBI’s field offices. As of December 9, they had received 299 examination reporting forms, of which 12 (4%) indicated use of encryption.[4] This is slightly lower than CART’s estimate of 5-6% for 1996 (Denning and Baugh 1997). There are at least three possible explanations. One is that the 1996 estimate, which was made before the FBI began collecting hard data, was somewhat high. A second is that as computers have become more common and user friendly, they are increasingly being used by criminals who lack the knowledge or skills to encrypt their files. Hence, the percentage of computer forensics cases involving encryption is staying about the same or decreasing even as the total number of forensics cases (and encryption cases) is growing. A third is that the early reports are skewed; as more come in, the percentage could approach 5-6%.

Public Postings

Criminals can use encryption to communicate in secrecy through open forum such as computer bulletin boards and Internet Web sites. Although many people might see the garbled messages, only those with the key would be able to determine the plaintext.

This technique was used by an extortionist who threatened to kill Microsoft president and chief executive officer Bill Gates in spring 1997.[5] The extortionist transmitted his messages to Gates via letter, but then asked Gates to acknowledge acceptance by posting a specified message on the America Online Netgirl bulletin board. Gates then received a letter with instructions to open an account for a Mr. Robert M. Rath in a Luxemburg bank and to transfer $5,246,827.62 to that account. The money was to be transferred by April 26 in order "to avoid dying, among other things." Gates was reminded that April 26 was his daughter's birthday. The letter came with a disk, which contained an image of Elvira and the key to a simple substitution cipher. Gates was told to use the code to encrypt instructions for accessing the Rath account via telephone or facsimile. He was then to attach the ciphertext to the bottom of the image and post the image to numerous image libraries within the Photography Forum of America Online (AOL). The graphic image with ciphertext was uploaded to AOL at the direction of the FBI on April 25. Figure 1 shows the image as posted and translation code.

Although Gates complied with the requests, he did not lose his money. The extortion threat was traced to Adam Quinn Pletcher in Long Grove, Illinois. On May 9, Pletcher admitted writing and mailing the threatening letters (there were four altogether) to Gates.

LAW ENFORCEMENT OPTIONS

The majority of investigations we heard about were not stopped by encryption. Authorities obtained the key by consent, found it on disk, or cracked the system in some way, for example, by guessing a password or exploiting a weakness in the overall system. Alternatively, they used other evidence such as printed copies of encrypted documents, other paper documents, unencrypted conversations and files, witnesses, and information acquired through other, more intrusive, surveillance technologies such as bugs. We emphasize, however, that these were cases involving computer searches and seizures, not wiretaps. This section discusses the options available to law enforcement for dealing with encryption.

Getting Key From Subject

In many cases, subjects have cooperated with the police and disclosed their keys or passwords, sometimes as part of a plea bargain. One hacker who had encrypted his files with the Colorful File System confessed to his crimes and revealed his CFS passphrase:

ifyoucanreadthisyoumustbeerikdale--**oragoodcypherpunk

He (Erik) wanted to speed the process along. The decrypted files contained evidence that was important to the case.[6]

A question that frequently arises is whether a court can compel the disclosure of plaintext or keys, or whether the defendants are protected by the 5th 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 1996). He left open the question of whether law enforcement could compel production of a key that has been memorized but not recorded. He also observed 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.

In People v. Price in Yolo County, California Superior Court prosecutors successfully compelled production of the passphrase protecting the defendant's PGP key. In this case, however, the key was not sought for the purpose of acquiring evidence for conviction, but rather to determine whether the defendant's computer should be released from police custody. He had already been convicted of annoying children and wanted his computer back. The police argued it should not be released as
there was reason to believe it contained contraband, specifically PGP-encrypted files containing child pornography. This determination was based on the existence of a pair of files named "Boys.gif" and "Boys.pgp" (when PGP encrypts a plaintext file, it automatically gives the ciphertext file the same name but with the extension ".pgp").[7]

The defendant was unsuccessful in arguing a 5th Amendment privilege. The prosecution argued that the contents of the file had already been uttered and, therefore, were not protected under the 5th Amendment. As long as prosecutors did not try to tie the defendant to the file by virtue of his knowing the passphrase, no incrimination was implied by disclosing the passphrase.

To handle the passphrase, a court clerk was sworn in as a special master. An investigator activated the PGP program to the point where it prompted for the passphrase. He left the room while the defendant disclosed the passphrase to the special master, who typed it into the computer. The investigator was then brought back into the room to hit the Enter key and complete the decryption process. As expected, child pornography fell out. The judge then ordered the computer, its peripherals, and all diskettes destroyed. The defendant argued that the computer contained research material, but the judge admonished him for commingling it with the contraband.

Getting Access Through a Third Party

Some encryption products have a key recovery system which enables access to plaintext through a means other than the normal decryption process. The key needed to decrypt the data is recovered using information stored with the ciphertext plus 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.

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. Indeed, they 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 could also encourage the use of encryption in organized crime to protect electronic files, as criminal enterprises need not worry about loss of keys.

Because of the potential benefits of key recovery to law enforcement, the Clinton Administration has encouraged the development of key recovery products by offering an export advantages to companies making such products. Beginning in December 1996, products with key recovery systems could be readily exported with unlimited key lengths. The Administration has retained restrictions on non-recoverable products that use keys longer than 56 bits, but even here export controls have been liberalized to allow ready export under certain conditions.

Breaking the Codes

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 Corp. 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.[8]

Eric Thompson, president of AccessData, reported that they had a recovery rate of 80-85 per cent with the encryption in large-scale commercial commodity software applications. He also noted that 90 per cent of the systems are broken somewhere other than at the crypto engine level, for example, in the way the text is pre-processed (CSI 1997). A passphrase or key might be found in the swap space on disk.

In those cases where there is no shortcut attack, the key might be determined by 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. Keys are represented as strings of 0s and 1s (bits), so this means trying every possible bit combination. This is relatively easy if the keys are no more than 40 bits, and somewhat longer keys can be broken given enough horsepower. In July 1998, John Gilmore, a computer privacy and civil liberties activist, and Paul Kocher, president of Cryptography Research in California, won $10,000 for designing a supercomputer that broke a 56-bit DES challenge cipher in record time, in their case 56 hours or less than three days. The EFF DES Cracker was built by a team of about a dozen computer researchers with funds from the Electronic Frontier Foundation. It took less than a year to build and cost less than $250,000. It tested keys at a rate of almost 100 billion per second (EFF 1998; Markoff 1998).

Unfortunately, criminals can protect against such searches by using methods that take longer keys, say 128 bits with the RC4, RC5, or IDEA encryption algorithm or 168 bits with Triple DES. Because each additional bit doubles the number of candidates to try, a brute force search quickly becomes intractable. To crack a 64-bit key, it would take 10 EFF DES Crackers operating for an entire year. At 128 bits, it is totally infeasible to break a key by brute force, even if all the computers in the world are put to the task. To break one in a year would require, say, 1 trillion computers (more than 100 computers for every person on the globe), each running 10 billion times faster than the EFF DES Cracker. Put another way, it would require the equivalent of 10 billion trillion DES Crackers! Many products, including PGP, use 128-bit keys or longer.

With many encryption systems, for example PGP, a user's private key (which unlocks message keys) is computed from or protected by 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. They use a variety of techniques including Markov chains, phonetic generation algorithms, and concatenation of small words (CIS 1997).

Often, investigators will find multiple encryption systems on a subject's computer. For example, PGP might be used for e-mail, while an application's built-in encryption might be used to protect documents within the application. In those cases, the subject might use the same password with all systems. If investigators can break one because the overall system is weak, they might be able to break the other, more difficult system by trying the same password.

To help law enforcement develop the capability to stay abreast of new technologies, including encryption, the Federal Bureau of Investigation proposes to establish a technical support center. The center would maintain a close working relationship with the encryption vendors. The Clinton Administration announced support for the center in its September 1998 update on encryption policy (White House 1998).

One issue raised by the development and use of tools for breaking codes is how law enforcement can protect its sources and methods. If investigators must reveal in court the exact methods used to decipher a message, future use of such methods could be jeopardized.

Finding an Access Point

Another strategy for acquiring plaintext is to find an access point that provides direct access to the plaintext before encryption or after decryption. In the area of communications, a router or switch might offer such access to communications that traverse the switch. If the communications are encrypted on links coming into and going out of the switch, but in the clear as they pass through the switch, then a wiretap placed in the switch will give access to the plaintext communications. We noted earlier how digital cellular communications could be intercepted in this manner, while at the same time offering users considerably greater security and privacy than offered by analog phones that do not use encryption.

Network encryption systems which offer access points of this nature are given an export advantage over those that do not (ibid). The approach was initially called a "private doorbell" approach to distinguish it from one that uses key recovery agents (Corcoran 1998; CISCO 1998). Now it is considered a form of recoverable encryption.

For stored data, Codex Data Systems of Bardonia, New York, advertises a product called Data Interception by Remote Transmission (D.I.R.T.) which is designed to allow remote monitoring of a subject's personal computer by law enforcement and other intelligence gathering agencies. Once D.I.R.T. is installed on the subject's machine, the software will surreptitiously log keystrokes and transmit captured data to a pre-determined Internet address that is monitored and decoded by D.I.R.T. Command Center Software. D.I.R.T. add-ons include remote file access, real-time capture of keystrokes, remote screen capture, and remote audio and video capture. The software could be used to capture a password and read encrypted e-mail traffic and files.

When All Else Fails

The inability to break through encryption does not always spell doom. Investigators may find printed copies of encrypted documents. They may find the original plaintext version of an encrypted file, for example, if the subject forgot to delete the original file or if it was not thoroughly erased from the disk. They may obtain incriminating information from unencrypted conversations, witnesses, informants, and hidden microphones. They may conduct an undercover or sting operation to catch the subject. These other methods do not guarantee success, however.

If there is sufficient evidence of some crime, but not the one believed to be concealed by encryption, a conviction may be possible on lesser charges. This happened in Maryland when police 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.[9]

In another case, 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.[10]

If encryption precludes access to all evidence of wrongdoing, then a case is dropped (assuming other methods of investigation have failed as well). Several cases that had been aborted or put on hold because of encryption were noted earlier.

OTHER TECHNOLOGIES FOR HIDING EVIDENCE

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

Passwords

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 1996). 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.

Another gambling enterprise operated multiple sites linked by a computer system, with drop-offs and pick-ups spanning three California counties. The ring leader managed his records with a commercial accounting program, using a password to control access to his files. Although the software manufacturer refused to assist law enforcement, police investigators were able to gain access by zeroing out the passwords in the data files. They found the daily take on bets, payoffs, persons involved, amounts due and paid or owed, and so forth. The printed files showed the results of four years of bookmaking, and resulted in a plea of guilty to the original charges and a sizeable payment of back taxes, both state and federal.[11]

Passwords are encountered much more often than encryption in computer forensics cases. Of the 299 computer examination reports received by the FBI's CART between April and December 1998, 60 (20 per cent) indicated use of passwords. This was five times as many as had indicated use of encryption.[12]

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. Figure 2 shows the effect of using S-tools to hide a 17-page book chapter inside an image file that is less than four times the size; that is, about a quarter of the file contains a hidden document. The difference between the before and after images is barely noticeable.

There have been a few reported cases of criminals using steganography to facilitate their crimes. One credit card thief, for example, used it to hide stolen card numbers on a hacked Web page. He replaced bullets on the page with images that looked the same but contained the credit card numbers, which he then offered to

associates. This case illustrates the potential of using Web images as "digital dead drops" for information brokering. Only a handful of people need even know the drop exists.

Steganography can be used to hide the existence of files on a computer's hard disk. Ross Anderson, Roger Needham, and Adi Shamir propose a steganographic file system that would make a file invisible to anyone who does not know the file name and a password. An attacker who does not know this information gains no knowledge about whether the file exists, even given complete access to all the hardware and software. One simple approach creates cover files so that the user's hidden files are the exclusive or (XOR) of a subset of the cover files. The subset is chosen by the user's password (Anderson et al 1998).

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. Eugene Schultz, former manager of the Department of Energy's Computer Incident Advisory Capability, said that a group of hackers from the Netherlands had taken so much information from Defense Department computers that they could not store it all on their own disks. So they broke into systems at Bowling Green University and the University of Chicago and downloaded the information to these sites, figuring they could transfer it somewhere else later.[13] Software pirates have been known to stash their pilfered files in hidden directories on systems they have hacked.

Data can be hidden on removable disks and kept in a physical location away from the computers. Don Delaney, a detective with the New York State Police, told us in early 1997 that in one 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 diskettes. The crooks did their work in Excel and then saved it on floppies. 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.

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.

CONCEALING CRIMES THROUGH ANONYMITY

Crimes can be concealed by hiding behind a cloak of anonymity. A variety of technologies are available:

Anonymous Remailers

An anonymous remailer is a service that allows someone to 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. To illustrate, suppose Alice wishes to send an anonymous e-mail message to Bob. Instead of e-mailing to Bob directly, Alice sends the message to a remailer (an e-mail server), which strips off the headers and forwards the contents to Bob. When Bob gets the message, he sees that it came via the remailer, but he cannot tell who the sender was. Some remailers give users pseudonyms so that recipients can reply to messages by way of the remailer. The remailer forwards the replies to the owners of the pseudonyms. These pseudo anonymous remailers do not provide total anonymity because the remailer knows who the parties are. Other remailers offer full anonymity, but they cannot support replies. All they do is act as a mail forwarder.

A remailer can accumulate batches of messages before forwarding them to their destinations. That way, if someone is intercepting encrypted Internet messages for the purpose of traffic analysis, the eavesdropper would not be able to deduce who is talking to whom.

There are numerous anonymous and pseudo anonymous remailers on the Internet. Some provide encryption services (typically using PGP) in addition to mail forwarding so that messages transmitted to and from the remailer can be encrypted. Users who don't trust the remailers can forward their messages through multiple remailers.

Anonymous remailers allow persons to engage in criminal activity while concealing their identities. President Clinton, for example, has received e-mail death threats that were routed through anonymous remailers. In one case involving remailers, an extortionist threatened to fly a model airplane into the jet engine of an airplane during takeoff at a German airport, the objective being to cause the plane to crash. The threats were sent as e-mail through an anonymous remailer in the United States. The messages were traced to introductory accounts on America Online, but the person had provided bogus names and credit card numbers. He was caught, however, before carrying out his threat.[14]

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 affords criminals the ability to launder money and engage in other illegal activity in ways that circumvent law enforcement. Combined with encryption or steganography and anonymous remailers, digital cash could be used to traffic in stolen intellectual property on the Web or to extort money from victims.

In May 1993, Timothy May wrote an essay about a hypothetical organization, BlackNet, which would buy and sell information using a combination of public-key cryptography, anonymous remailers, and anonymous digital cash.

> 'BlackNet can make anonymous deposits to the bank account of your choice, where local banking laws permit, can mail cash directly ..., or can credit you in 'CryptoCredits,' the internal currency of BlackNet ... If you are interested, do not attempt to contact us directly (you'll be wasting your time), and do not post anything that contains your name, your e-mail address, etc. Rather, compose your message, encrypt it with the public key of BlackNet (included below), and use an anonymous remailer chain of one or more links to post this encrypted, anonymized message on one of the locations listed ..." (May 1996a).

Although May said he wrote the essay to point out the difficulty of "bottling up" new technologies (May 1996b), rumors spread shortly after May's essay appeared on the Internet of actual BlackNets being used for the purpose of selling stolen trade secrets.

In an essay called 'Assassination Politics,' James Dalton Bell suggested using cyber betting pools to kill off Internal Revenue Service (IRS) agents and other 'hated government employees and officeholders' (Bell 1996).[15] The idea was simple: using the Internet, encryption, and untraceable digital cash, anyone could contribute anonymously to a pool of digital cash. The person, presumably the assassin, correctly guessing the victim's time of death wins. After spending nearly two years peddling his ideas on Internet discussion groups and mailing lists, Bell was arrested and pled guilty to two felony charges: obstructing and impeding the IRS and falsely using a social security number with the intent to deceive. In his plea agreement, he admitted to conducting a "stink bomb" attack on an IRS office in Vancouver (McCullah 1997).[16] He also disclosed the passphrase required to decrypt e-mail messages that had been sent to Bell by his associates encrypted under PGP.

Although Bell did not implement any betting pools, an anonymous message was posted to the Cypherpunks Internet mailing list announcing an Assassination Politics Bot (program) called Dead Lucky that did. The message also listed four potential targets. A related message pointed to an interactive Web page titled Dead Lucky,

which contained the statement 'If you can correctly predict the date and time of death of others then you can win large prizes payable in untaxable, untraceable eca$h.' The page also stated 'Contest will officially begin after Posting of Rules and Announcement of Official Starting Date (Until then it is for Entertainment Purposes Only).' Another anonymous message posted to Cypherpunks had the subject 'Encrypted InterNet DEATH THREAT!!! / ATTN: Ninth District Judges / PASSWORD: sog.' The PGP encrypted message, when decrypted with 'sog,' contained death threats and a claim to authorship of the Assassination Bot. Investigators linked the messages and Bot to an individual by the name of Carl Edward Johnson. In August 1998, a warrant was issued charging Johnson with threatening 'to kill certain law enforcement officers and judges of the United States, with intent to impede, intimidate, or interfere with said officers and judges on account of their official duties.'[17]

Computer Penetrations and Looping

By breaking into someone's computer account and issuing commands from that account, a criminal can hide behind the account holder's identity. In one such case, two hackers allegedly penetrated the computers of Strong Capital Management and sent out 250,000 ads with fraudulent headers that bore the company's name. The ads were for on-line striptease services ('cyber stripping'), computer equipment, and sports betting. SCM filed a $125 million lawsuit against the hackers, demanding penalties of $5,000 per message (Kabay 1997).

Hackers can make it difficult for investigators to discover their true identity by using a technique called looping.' Instead of penetrating a particular system directly, they can enter one system and use that as a springboard to penetrate another, use the second system to penetrate a third, and so forth, eventually reaching their target system. The effect is to conceal the intruder's location and complicate an investigation. In order to trace the connection, investigators need the help of systems administrators along the path. If the path crosses several national borders, getting that cooperation may be impossible.

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 1996). 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.

Digital cellular phones use stronger methods of authentication that protect against cloning. As this technology replaces analog cell phones, cloning may be less of a problem for law enforcement.

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 1997). 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.

CONCLUSIONS

Criminals and terrorists are using encryption and other advanced technologies to hide their activities. Indications are that use of these technologies will continue and expand, with a growing impact on law enforcement. Although the majority of investigations we heard about were not stopped by encryption, we heard about a few cases that were effectively derailed or put on hold by encryption. Even when the encryption was broken, however, it delayed investigations, sometimes by months or years, and added to their cost, in a few cases costing agencies hundreds of thousands of dollars to crack open encrypted files.

Efforts to decrypt data for law enforcement agencies or corporations in need of recovering from lost keys have been largely successful because of weaknesses in the systems as a whole. That success rate is likely to drop, however, as vendors integrate stronger encryption into their products and get smarter about security. It is not possible to break well-designed cryptosystems that use key lengths of 128 bits or more. It is not just a matter of paying enough money or getting enough people on the Internet to help out. The resources simply do not exist - anywhere.

Most of the investigators we talked to said that they had not yet detected substantial use of encryption by large organized crime groups. This can be attributed to several factors, including the difficulty and overhead of using encryption (particularly the personnel time involved) and a general sense that their environments are already reasonably isolated and protected from law enforcement.

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. She cited encryption as their greatest limit on investigations, and noted that instead of hiring cryptographers to create their codes,

mobsters download copies of Pretty Good Privacy (PGP) off the Internet (Ramo 1996).

As the population becomes better educated about technology and encryption, more and more criminals will have the knowledge and skills needed to evade law enforcement, particularly given the ease with which unbreakable, user-friendly software encryption can be distributed and obtained on the Internet. We recommend ongoing collection of data on the use of encryption and other advanced technologies in crime. We need to know how encryption is impacting cases - whether it is broken or circumvented, whether cases are successfully investigated and prosecuted despite encryption, and costs to investigators.

Encryption is a critical international issue with severe impact and benefits to business and order. National policy must recognize not only the threat to law enforcement and intelligence operations, but also the need to protect the intellectual property and economic competitiveness of industry. Encryption policy must also respect consumer needs for encryption and basic human rights, including privacy and freedom of expression. Addressing all of these interests is enormously challenging.

NOTES

[1] The chapter is an update of a study we conducted in 1997 at the invitation of the U.S. Working Group on Organized Crime, National Strategy Information Center, Washington, DC.

[2] Additional information was provided by Detective R. J. Montemayor in the Dallas Police Department.

[3] The key used by Ames was disclosed to us by Robert Reynard on February 18, 1998.

[4] Data provided by CART on December 9, 1998.

[5] United States District Court, Northern District of Illinois, Eastern Division, Search Warrant, Case Number 97-157M, May 8, 1997; United States of America v. Adam Quinn Pletcher, United States District Court, Western District of Washington at Seattle, Magistrate's Docket No. Case No. 97-179M, May 9, 1997.

[6] Byron W. Thompson, presentation at HTCIA/FBI Training Seminar, Perspectives on Computer Crime, November 12-13, 1998.

[7] Information on this case was provided by Fred B. Cotton of SEARCH Group, Inc. Cotton was the investigator who activated the PGP program on the defendant's computer.

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

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

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

[11] This case was first reported to us on February 22, 1997 by Jim McMahon, former head of the High Technology Crimes Detail of the San Jose Police Department. We received additional information from Robert Reynard on June 10, 1998.

[12] Data provided by CART on December 9, 1998.

[13] Communication from Eugene Schultz, May 15, 1998.

[14] Presentation by Christoph Fischer at Georgetown University, July 22, 1998.

[15] A version of Bell's essay on Assassination Politics is in Winn Schwartau, *Information Warfare*, 2nd ed., Thunder's Mouth Press, 1996, pp. 420-425.

[16] http://jya.com/jimbell3.htm.

[17] United States of America v. Carl Edward Johnson, Warrant for Arrest, Case No. 98-430M, United States District Court, Western District of Washington, August 19, 1998.

References

Akdeniz, Y., 'Regulation of Child Pornography on the Internet,' http://www.leads.ac.uk/law/pgs/yaman/child.htm.

Anderson, R., Needham, R., and Shamir, A. (1998) 'The Steganographic File System,' presented at the Workshop on Information Hiding, Portland, OR, April 14-17.

Cisco Systems Inc. (1998) 'Thirteen High-Tech Leaders Support Alternative Solution to Network Encryption Stalemate,' Press Release, July 13.

Corcoran, E. (1998) 'Breakthrough Possible in Battle over Encryption Technology,' Washington Post, July 12.p. A8.

CSI (1997) 'Can your crypto be turned against you? An interview with Eric Thompson of AccessData,' Computer Security Alert, No. 167, February.

Denning, D. E. and Baugh, W. E., Jr. (1997) 'Encryption and Evolving Technologies as Tools of Organized Crime and Terrorism,' National Strategy Information Center, Washington, DC, July.

EEF (1998) '"EFF DES Cracker" Machine Brings Honesty to Crypto Debate,' press announcement from the Electronic Frontier Foundation, July 17.

Fischer, C. (1998) Presentation at Georgetown University, July 22.

FBI Law Enforcement Bulletin (1970) 'Crime and Cryptology', April, 13-14.

Grabosky, P. N. and Smith, R. G. (1998) Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, Transaction Publishers.

IINS News Service, (1997) 'Hamas Using Internet for Attack Instructions', Israel, September 28.

Kaplan, D. E. and Marshall, A. (1996) The Cult at the End of the World, Crown Publishers.

Littman, J. (1997) The Watchman: The Twisted Life and Crimes of Serial Hacker Kevin Poulson, Little, Brown and Co.

Manning, W. M. (1997) 'Should You Be on the Net?' FBI Law Enforcement Bulletin, January, 18-22.

Markoff, J. (1998) 'U.S. Data-Scrambling Code Cracked with Homemade Equipment,' New York Times, July 17.

May, T. C. (1996a) 'Introduction to BlackNet,' reprinted in, Ludlow, P (ed), High Noon on the Electronic Frontier, MIT Press, pp. 241-243.

May, T. C. (1996b) 'BlackNet Worries,' in Peter Ludlow, (ed), High Noon on the Electronic Frontier, MIT Press, pp. 245-249.

McCullah, D. (1997) 'IRS Raids a Cypherpunk,' The Netly News, April 4.

Minow, M. (1997) 'Swedish Narcotics Police Demand Telephone Card Database,' Risks-Forum Digest, Vol. 19, Issue 07, April 14.

Power, R. (1997) 'CSI Special Report: Salgado Case Reveals Darkside of Electronic Commerce,' Computer Security Alert, No. 174, September.

Ramo, J. C. (1996) 'Crime Online,' Time Digital, September 23, pp. 28-32.

Reitinger, P. R. (1996) 'Compelled Production of Plaintext and Keys.'

US Congress (1997a) Statement of Louis J. Freeh, Director FBI, before the Senate Committee on Commerce, Science, and Transportation, regarding the Impact of Encryption on Law Enforcement and Public Safety, March 19.

US Congress (1997b) Jeffrey A. Herig, Special Agent, Florida Department of Law Enforcement, "The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry," testimony before the Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information, September 3.

White House (1995) Remarks by the President to Staff of the CIA and Intelligence Community, Central Intelligence Agency, McLean, VA, July 14.

White House (1998) 'Administration Updates Encryption Policy', statement by the Press Secretary and fact sheet, September.

ABOUT THE AUTHORS

Dorothy E. Denning is professor of Computer Science and Communication, Culture, and Technology at Georgetown University. She is author of *Information Warfare and Security*, Addison Wesley, 1999. E-mail: denning@cs.georgetown.edu. Web: www.cs.georgetown.edu/~denning.

William E. Baugh, Jr. is vice president, Science Applications International Corporation, and general manager, Advanced Network Technologies and Security Operations. He is former assistant director, Federal Bureau of Investigation. E-mail: William.E.Baugh.Jr@cpmx.saic.com.