LAW ENFORCEMENT'S NEW WEAPONS FOR ELECTRONIC DETECTION SPUR PRIVACY PROPONENTS TO STRIKE BACK, SAYS PART 2 OF THIS TWO-PART ARTICLE

# Encryption wars: shifting tactics

MICHAEL A. CALOYANNIDES
Mitretek Systems

THE GROWING AVAILABILITY of powerful encryption has in effect rewritten the rule book for creating, storing, and transmitting computer data. People everywhere rightly regard confidentiality as essential for conducting business and protecting personal privacy. But governments worldwide have been sent into a spin, for fear secret encryption keys will add to the weapons of terrorists and other criminals. Some nations have even attempted to control the technology by constructing a maze of regulations and laws aimed at blocking its import, export, and/or use. Such bans have largely failed, though. [See Part 1 of this article, *IEEE Spectrum*, April, pp. 39–43].


[1] Nearly two dozen satellite terminals at the Menwith Hill facility in northern England are allegedly used by the U.S. National Security Agency to intercept satellite and radio communications worldwide. The site is said to be part of the global surveillance effort known as Echelon.



0018-9235/00/$10.00©2000 IEEE

In recent years, the war over encryption has moved beyond controlling the technology itself. Now, some governments are granting law enforcement agencies new powers and funding the development of new tools to get at computerized data, encrypted or otherwise. Rising to that challenge, privacy proponents are striking back with new techniques for hiding data and preserving anonymity in electronic communications.

## CONFESS UP!

One legal tact being used by states is to require owners of encrypted files to decrypt them when asked to by authorities. So far, only Singapore and Malaysia have enacted such laws, with Britain and India about to follow suit.

In Britain, two recent bills would give law enforcement officers the authority to compel individuals to decrypt an encrypted file in their possession under pain of a two-year jail term. Further, anyone given such a command would have to "keep secret the giving of the notice, its contents, and the things done in pursuance of it" on penalty of a five-year jail term. The bills define encryption extremely broadly, even including what some consider to be mere data protocol.

Along similar lines, the Clinton administration drafted the Cyberspace Electronic Security Act (CESA), which it sent to Congress last September. This proposed legislation would allow the use of search warrants or court orders to gain "lawful access" to encryption keys or decrypted plaintext.

Straightforward though it seems, the approach is technically flawed. After all, a suspect may truly be unable to decrypt an encrypted file. He or she may have forgotten or lost the key. Or, if public-key encryption was used, the sender of a file will have the key used to encrypt the file, but rarely, if ever, the decryption key, which remains the exclusive property of the intended recipient. If symmetric key encryption was used, and the sender's hard disk crashes, the key will likely be wiped out along with all the other stored data. This flaw in the legislation was demonstrated by a British group, which mailed an ostensibly incriminating document to a government official and then destroyed the decryption key, making it impossible for that official to decode the file, even if "compelled."

Moreover, according to the latest version of CESA, police would be at liberty to present a text in court and claim it was the decrypted version of an encrypted file, without revealing to the defendant exactly how they arrived at the plaintext. This means that "the defendant can have a hard time defending himself, and makes it a lot easier for the police to fabricate evidence," observed Bruce Schneier of Counterpane Security Inc. in his October 1999 electronic newsletter *Cryptogram*. "The ability to receive a fair trial could be at stake."

## ESCROWED ENCRYPTION

Another controversial scheme for letting law enforcement in on encrypted data is known as escrowed encryption. Here, a third party is appointed by the state to keep a copy of the decryption keys—in escrow, as it were—for the state to use to decrypt any file sent to or by any user. In other words, encrypted files would be protected—except from the state.

Needless to say, many people abhor the mere idea. Even if a sound case could be made for revealing the decryption key to government personnel, what is to prevent them from reusing that key in the future, to look at other documents by the same user? Further, drug traffickers, terrorists, and others of most concern to law enforcement are the least likely to use encryption that is openly advertised as readable by the government.

Then, too, given the transnational nature of the Internet, a global key-escrow system would need to be established. Sovereign states, with their own interests to protect, would object to such a system; this in fact happened with the escrow scheme known as the Clipper Chip, which was heavily promoted by the U.S. government but largely dismissed by other states. The logistics of who keeps the escrowed keys, who has authority to demand their release, under what conditions, and so on, becomes unwieldy when vast numbers of encryption keys, states, and legal systems are involved.

In view of such concerns, official support for escrowed encryption has all but died in the United States and elsewhere.

## GLOBAL SURVEILLANCE

The ineffectiveness of legal constraints on encryption appears to have persuaded many governments to change direction. They are instead seeking to capitalize on the unencrypted nature of most digital traffic and to derive information by monitoring that traffic. Even encrypted messages tend to leave unencrypted who is communicating with whom and when.

Officially, most states deny the existence of electronic surveillance networks. But extensive claims of their existence persist. Echelon and FIDNet are two such alleged intelligence-gathering efforts that have been frequently described in the mainstream press and debated in official hearings by government legislatures.

Echelon is, according to the Washington, D.C.–based Federation of American Scientists, a global network that "searches through millions of interceptions for pre-programmed keywords on fax, telex, and e-mail messages" [Fig. 1]. In his book *Secret Power: New Zealand's Role in the International Spy Network*, Nicky Hager asserts that the international eavesdropping system "is designed primarily for non-military targets," and claims that "every word of every message intercepted gets automatically searched—whether or not a specific telephone number or e-mail address is on the list."

Last June, Duncan Campbell, a British researcher who first broke the story of Echelon's existence back in 1988, submitted a report on the network to the European Parliament's Science and Technology Options Assessment (STOA) Panel. According to Campbell's report, a group known as the International Law Enforcement Telecommunications Seminar is involved in coordinating and sponsoring Echelon-related activities. Since the report's release, public inquiries have been launched by politicians on both sides of the Atlantic, including Representative Bob Barr (a Republican from Georgia and a former Federal prosecutor) and the UK's Glyn Ford, a Labor Member of Parliament.

The same sort of public inquiries have been made about the Federal Intrusion Detection Network (FIDNet) that the U.S. National Security Council has proposed creating. It would monitor traffic on both government and commercial networks, with the stated goal of safeguarding the critical U.S. information infrastructure. Although the House Appropriations Committee did away with funding for it last summer, FIDNet supporters continue to push the program, arguing that it would not intrude on individuals' communications. Meanwhile, a number of civil rights groups, including the Electronic Privacy Information Center (EPIC), in Washington, D.C., and the American Civil Liberties Union, based in New York City, have challenged FIDNet's constitutionality. According to David Sobel, general counsel for EPIC, the plan "demonstrates that privacy concerns are being swept under the carpet." [But see "Is privacy a right?" on p. 49.]

## COMPUTER FORENSICS

As society relies increasingly on computers, the amount of crime perpetrated with the machines has risen in kind. To law enforcement's delight, electronic records have proved to be a fertile ground for detectives. Indeed, in their present shape, computers, the Internet, and e-mail are the most surveillance-friendly media ever devised.

This development has given rise to an entirely new industry: computer forensics. Its purpose is not only to find out what files are stored in a computer, but also to recover files that were created with, stored in, sent by, received from, or merely seen by that

computer in the past, even if such files were subsequently "deleted" by the user.

The ability to resurrect electronic paper trails from supposedly deleted files stems in large part from the features built into many computer programs. For example, the DELETE command in most software does not delete. It merely marks the space that such a file occupied in a disk as being available in the future to be overwritten. (If it really deleted, then UNDELETE commands would not work.) Also, many Windows applications save temporary versions of a file being worked on, just in case the computer crashes. Even if a user were to deliberately overwrite the original file, the temporary version still lurks in some part of the disk, often with an unrecognizable name and occasionally even invisible from the conventional directory.

Electronic paper trails are also left behind by the FAST SAVE function, which saves the latest version of a word-processing document as the original plus the sequence of changes made to it. A recipient of the electronic end result can see how the document evolved over time—not the kind of information most people care to share.

Internet-related applications, like many other software programs, do a lot of internal housekeeping that involves writing information onto the hard disk. For example, the popular Web browser Netscape Navigator creates a file called netscape.hst, which gives a chronological listing of almost everything its user has done with the browser since it was installed.

Simply surfing the Web pushes other data into computer memory, in the guise of "cookies" and as documents "cached" on one's disk. Web sites visited can also learn the visitor's Internet service provider, Web browser, and a lot more. A remote Web site could even gain full access to a visitor's hard disk, depending on how aggressive that remote site elects to be and how extensive the protective measures taken by the visitor.

Software tools now make it fairly straightforward to get a computer to cough up information that its owner may not realize is there. Not to be outdone, computer programmers have developed numerous tools that can defeat most computer forensics tools. While such counter-forensics programs will remove most traces of sensitive data from a computer, it is extremely difficult to remove *all* traces that may have been left behind. In the absence of a thorough schooling in the esoteric details of computers, the odds favor the competent computer forensics investigator.

Also favoring the forensics expert are new laws legalizing the accessing of computers by law enforcement agencies. Last December, for example, the Australian Parliament passed a bill giving the Australian Security Organization the power to obtain warrants to access computers and telecommunications services "if necessary deleting or altering other data in the target computer...[and] to conceal the fact that anything has been done under the warrant." And as of this February, Dutch authorities are now permitted to use bugging devices in computers to retrieve text.

## COUNTERMEASURES

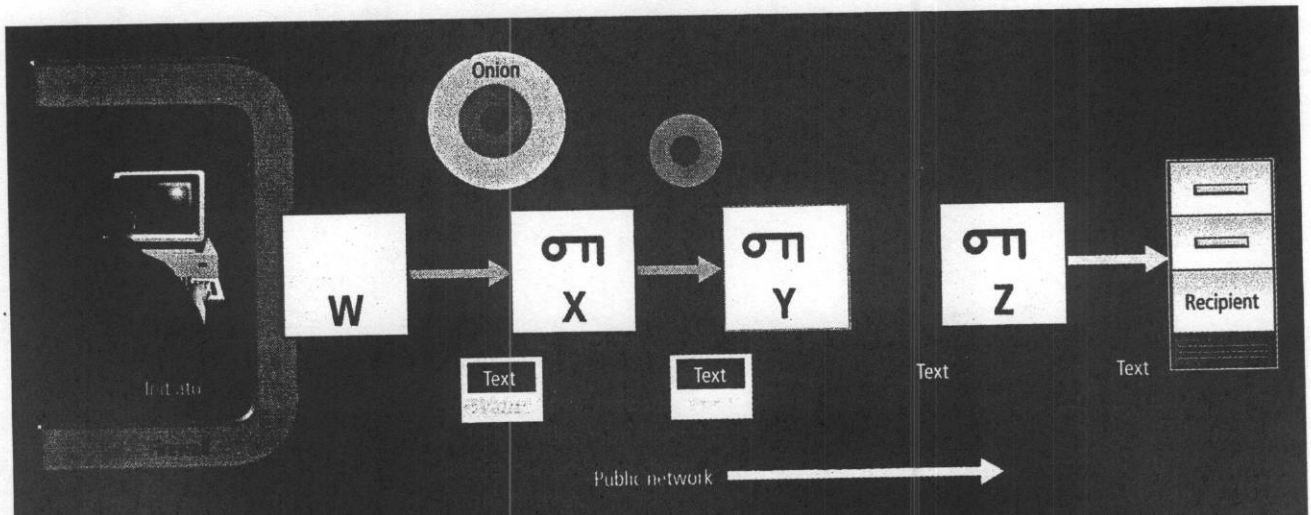
The various legal roadblocks and technical wizardry contrived by governments and law enforcement to block encryption's spread have, of course, curbed neither the need for the technology nor the ingenuity of privacy-loving programmers. As a result, a number of countermeasures have been engineered to augment or replace encryption. Among them are anonymizers, which conceal the identity of the person sending or receiving information, and steganography, which hides the information itself.

The need for anonymity in a democratic society has long been recognized, to shield whistleblowers and political dissenters from retaliation, to protect the records of medical patients, and so on. Less dramatic situations also justify anonymity, such as placing a personal ad or seeking employment through the Internet without jeopardizing one's current job. To be sure, anonymity can be exploited by sociopaths seeking to avoid accountability for their actions. But, in general it serves a useful social function.

Anonymous and pseudonymous remailers are computers accessible through the Internet that launder the true identity of an e-mail sender. Most are operated at no cost to the user. A pseudonymous remailer replaces the sender's e-mail address with a false one and forwards the message to the intended recipient. The recipient can reply to the sender's pseudonymous address, which, in turn, forwards the response to the sender's true address.

Anonymous remailers come in three flavors: cypherpunk, mixmaster, and Web-based. Cypherpunk remailers strip away the message header, which describes where the message came from and how it got there, before forwarding the message to the recipient. Conceivably, someone with physical access to such a remailer's phone lines could correlate the incoming and outgoing traffic and make inferences.

Mixmaster remailers avoid that problem by using stronger encryption and tricks for frustrating traffic analysis, such as padding messages to disguise their true length. But even mixmasters can be compromised. For example, through a concerted effort, it would be possible to detect a correlation between Mr. A sending an encrypted message through a remailer, and Ms. B receiving a message at some variable time afterwards.




[2] The Onion Router is a clever scheme for communicating anonymously over the Internet in real time. The onion is a layered, encrypted set of instructions that establishes the connection between the initiator and recipient. The actual message, also encrypted, can then be sent through. Although the onion shown here shrinks as it moves through the network, in actuality it gets padded with random data at each step, to better thwart traffic analysis.

# Is privacy a right?

Encryption proponents often support their views by citing the individual's right to privacy. But to what extent is such a right protected by law? The answer varies widely from country to country. Most countries, with the notable exception of totalitarian regimes, legally protect both personal records and communications to some extent, with of course carefully worded exclusions in the cases of suspected but nebulously defined "crimes."

Even states with a long history of democracy tend to interpret their obligation to ensure domestic tranquility as superseding the citizen's right to privacy. These same countries may protect the privacy of a citizen from other citizens but not from the government itself. Interestingly, some languages (such as Greek) do not even have a word for "privacy," even though its essence may be ingrained into the culture.

The U.S. Constitution does not explicitly protect privacy. Most likely, the framers of the constitution saw privacy rights as conflicting with other constitutional guarantees. The first amendment, for example, blocks the government from restricting expression, even though that expression might also compromise the privacy of others.

When the Federal government has tried to protect individual privacy, it has often ended up at odds with the First Amendment; in court, privacy rights almost never win against the First Amendment. Collection and dissemination of information, especially about public figures, is hardly ever restricted by the Supreme Court. There is, however, some implicit constitutional protection for certain private activities, such as freedom to practice one's religion.

In general, what little protection of individual privacy there is at the Federal level relates to procedures rather than substance, as in the Fourth Amendment's prohibition of "unreasonable search and seizure." Of course, what is "unreasonable" is in the mind of the beholder, and the beholder changes with time. Back in 1928, for example, the Supreme Court decreed, in *Olmstead v. the United States,* that Federal wiretapping did not amount to an unreasonable search because it did not involve a physical trespass.

The Federal Communication Act of 1934 made wiretapping illegal, but a subsequent reading of the law restored wiretapping's legitimacy, as long as the wiretapped information was kept within the executive branch.

The Fifth Amendment prevents the government from taking private property for public use without due process and compensation. In 1984, the Supreme Court decreed that this protection extends to data, too. Even so, the protection is minimal at best; it is not an outright prohibition against seizure by the state.

When it comes to data held by the government, the 1974 Federal Privacy Act stipulates that government agencies can only store "relevant and necessary" personal information about individuals. This stipulation is obviously vague and therefore subject to abuse.

A number of states have their own privacy laws. Unfortunately, many of these are also vaguely worded and have ended up being tested in state courts time and again. In Hawaii, for example, it is illegal to "invade privacy," unless there is a "compelling State interest." Arizona, likewise, makes it illegal for one to be "disturbed in his private affairs except under authority of law." California, in 1974, declared privacy an "inalienable right," yet in 1994 the state ruled that mandatory drug testing of college athletes was not an invasion of privacy.

**The U.S. Constitution does not explicitly protect privacy**

In the United States, private individuals have almost never won lawsuits against other private parties for privacy violations. In general, such claims have to be framed in terms of loss of property, rather than simple loss of privacy. But who owns personal information? Are a patient's medical records owned by that person or by the medical doctor or hospital or insurance company?

U.S. courts have often stated that the information is owned by whoever went to the trouble and expense to collect and store it. Even the Supreme Court has stated that any expectations of privacy must derive their legitimacy from laws governing real or personal property.

Given such a flimsy legal framework for the protection of privacy, it follows that the only substantive means an individual in the United States has to protect the privacy of his/her data is to encrypt it in a secure manner.

### ACROSS THE ATLANTIC

In contrast to the United States, Western European countries have strong legal protection of individual privacy. Ironically, this protection is possible precisely because those governments have fewer legal limitations placed upon them by their respective constitutions.

On the one hand, no European nation has a constitutional guarantee of freedom of expression or freedom of the press. As a result, the press in Europe has time and again been muzzled by courts appealing to "higher" principles, and there are laws prohibiting the broadcast of "harmful programming." On the other hand, this same broad authority to intervene in communications and information makes it possible to legislate privacy.

With European unification, the trend is toward a uniform set of standards. In the Common Position of the European Parliament, which went into effect in 1998, Article 1 states that there is a "fundamental right to privacy with respect [to] the processing of personal data." The fact that the European Union (EU) classifies privacy as a basic right makes it extremely hard to challenge.

Another article in the same document prohibits EU members from giving personal data to nonmember countries that "fail to ensure an adequate level of protection." Although this position does not yet carry the weight of law, some European countries have refused to provide marketing data, or any other data that identifies individuals, to the U.S. government or U.S. companies.

The European Convention on Human Rights also protects privacy to some degree. Among other things, it prohibits states from intercepting citizens' e-mail or Internet calls or covertly tampering with citizens' computers. In 1998, the British parliament, in approving a variation of this convention, established an enforceable right to privacy. Even so, cryptographer Brian Gladman has speculated that the country's government may resort to implanting Trojan horse software in select individuals' computers, to get around any encryption being used. If implemented, such a practice would possibly violate Britain's 1990 Computer Misuse Act, though it would comply with the 1994 Intelligence Services Act.

—*M.A.C.*

Web-based anonymizers range from sites offering conventional anonymizer services, to others where the connection between the user's computer and the anonymizer is itself encrypted with up to 128-bit encryption. The job is done using the standard Secure Socket Layer (SSL) encryption, built into all Web browsers of recent vintage.

For extra privacy, a message may be routed through a series of remailers. Two popular remailer software packages, Private Idaho and Jack B. Nymble, enable the sender to do this automatically.

The Onion Router project (see the site at www.onion-router.net) of the Naval Research Laboratory in Washington, D.C., offers another way to string together remailers. What's more, it allows anonymized and multiply encrypted Web browsing in real time.

Onion routing is a two-stage process. As shown in Figure 2, the initiator instructs router W (in this case, a proxy server at the firewall of a secure site) to create an onion, which consists of public-key–encrypted layers of instructions. Router X peels off the first layer of the onion, which indicates the next step in the path and supplies a symmetric decrypting key for use when the actual message comes through later.

The onion then goes to Routers Y and Z, depositing keys at each stop. Once the connection is established, the encrypted message is sent through and successively decrypted, arriving at the recipient as plaintext. To respond, the recipient sends the message to Router Z, which encrypts the text, onion-style, and sends it back through the already established path.

## HIDING DATA

The microdot used by German spies during World War II to transmit strategic information is an example of steganography, used to hide data in plain view. The microdot consisted of a greatly reduced photograph of a page of text, which was pasted over a period in an otherwise innocuous document. A more modern application is the digital watermark, for identifying official copies of copyrighted images and recordings. Unlike encryption, which hides the content of a message in an obvious manner, steganography hides the mere existence of anything hidden.

The commercially available computer-based steganography programs popular today rely on three techniques:

- Merging the information to be hidden into a "cover" sound file by changing the least significant bit of each digitized sample of the file. The resulting file sounds the same to the human ear and is the same length as the original file.
- Merging the information to be hidden into a cover image file by changing the least significant bit of the digitized value of the brightness of each pixel. Typical images use 256 levels of brightness, with 8 bits per pixel for black-and-white images and 8 bits for each of the three primary colors (red, green, and blue) per pixel for color images. A lot of data can lurk in a 1024-by-768–pixel image [Fig. 3].
- Hiding data in the areas of a computer floppy disk or hard drive that are normally not accessed. A computer disk is divided into clusters, each of which holds from 512 bytes to over 32 000 bytes. When a file is saved, it uses a portion of one or more clusters; because DOS and Windows store only one file per cluster, the space left over between the end of a file and the end of the cluster (called the slack) is available to hide data in. This scheme is extremely easy to detect, however.

NEIL F. JOHNSON, GEORGE MASON UNIVERSITY

**[3] Steganography [above] is the science—or in this case, the art—of hiding data in plain view. Commercial software can easily embed information, which may or may not be encrypted, within otherwise benign digital audio and video files.**

The most commonly used commercial steganography software tools are Hide and Seek, Steganos, StegoDos, White Noise Storm, S-Tools for Windows, Jpeg-Jsteg, and Stealth. For Unix computers, there is SFS (Steganographic File System).

Steganography does have some weaknesses. For one thing, sending or storing many seemingly harmless images or sound files can in itself raise a red flag, unless the sender's normal routine as, say, a musician or photographer warrants such conduct. And while image and sound files hiding information may seem natural to the eye or ear, the difference may still be detectable by techniques devised to spot such aberrations.

Interestingly, the extent to which hidden information can be detected is related to the popularity of the steganography software used. Law enforcement agencies treat steganography much like a computer virus: once a program hits the market in a big way, tools are developed to detect it. The more extensive the program's use, the more resources are devoted to detecting its footprint.

## THE FUTURE OF ENCRYPTION

Encryption today is as strong as it is because there is no need for it to be any stronger. Of course, the underlying mathematical assumptions might be challenged by a breakthrough, such as a solution to factoring large numbers into their prime-number components. Meanwhile, an encryption method can be strengthened by merely adding bits to the encryption key.

Nevertheless, several schemes under development may eventually find use for electronic communication and storage: elliptic curve encryption; voice encryption (already freely available and used worldwide over the Internet); quantum cryptography; and DNA cryptography.

Few microprocessors have been specially designed to run encryption software. Most personal computers can accommodate the hardware and software requirements of modern encryption, but most hand-held devices, such as 3Com's Palm Pilot, cannot. For these devices, a new class of algorithms, known as elliptic curve encryption, is claimed to provide encryption strength equal to that of the standard algorithms in use today, while using a smaller key and arithmetic that is easier on microprocessors and needs much less memory. Being a new type of encryption, its security has yet to withstand the concerted scrutiny of experts.

Voice encryption is a response to the

increasing flow of audio traffic over the World Wide Web, which has led, among other things, to the merging of strong encryption with Internet telephony. Given appropriate software, anyone today can carry on fully encrypted conversations with any other user connected to the Internet.

Perhaps the most advanced such software is SpeakFreely, which is available worldwide free of charge (see www.speakfreely.org). Some mainstream voice-over-the-Internet services do not offer encryption, though. Instead, they route the data through the company's servers, thereby opening up a security weakness.

Quantum cryptography is not in itself an encryption algorithm. Rather, it is a means for creating and securing the distribution of private keys. Based on the Heisenberg uncertainty principle, the idea is that communicating photons cannot be diverted from the intended recipient to the unsought-for interceptor without creating an irreversible change in the quantum states of the system.

The precepts of quantum cryptography date from the early 1970s, and research has been ongoing for the last decade at universities like Johns Hopkins University, in Baltimore, Md., and the University of Geneva in Switzerland; at U.S. national laboratories such as Los Alamos; and in the corporate sector, at British Telecom and elsewhere.

In DNA cryptography, each letter of the alphabet is converted into a different combination of the four bases that make up human deoxyribonucleic acid (DNA). A piece of DNA spelling out the message to be encrypted is then synthesized, and the strand is slipped into a normal fragment of human DNA of similar length. The end result is dried out on paper and cut into small dots. As only one DNA strand in about 30 billion will contain the message, the detection of even the existence of the encrypted message is most unlikely.

## SHIFTING ATTITUDES

If, as seems likely, encryption and related products will continue to develop for personal and commercial uses, countries will have to rethink their policies toward the technology.

In what may be a sign of things to come, the German government announced last May that it would fund the development and free distribution of open-source encryption software that the government itself will be unable to break (see www.gnupg.org). The Federal Ministry of Economics and Technology released a report stating that Germany "considers the application of secure encryption to be a crucial requirement for citizens' privacy, for the development of electronic commerce, and for the protection of business secrets."

Several months earlier, French Prime Minister Lionel Jospin announced a similar shift, saying that his country would scrap any key escrow plans in favor of free use of cryptography.

In both cases, the motivation seems to have been the realization that protecting data from foreign parties outweighs any law enforcement concerns, and that the use of strong encryption furthers, rather than hinders, national security.

Independently, the Canada government announced last October that it would not seek to regulate the domestic use of encryption. Likewise, the Clinton administration, in announcing the loosening of U.S. cryptography export policy last September [discussed in Part 1 of this article], noted that "Americans will remain free to use any encryption system domestically."


**[4] During the 1999 Internet Convention, held in Hong Kong, police handed out stickers like the one at left to encourage the use of encryption. Official attitudes toward encryption are shifting from deep opposition to outright endorsement.**

The significance of such trends is clear: the global reach of the Internet has made it extremely easy for encryption software to travel between countries, with or without controls, and if one or more major countries elects not to enforce controls, the technology will spread still more easily. Society's transformation into a computer-based economy makes protecting corporate and personal information not only desirable, but necessary.

How then does one balance privacy and confidentiality with security? For governments are undoubtedly obligated to protect their citizens from terrorism and from out-and-out criminality. A partial solution may be to criminalize the use of encryption only in the commission of generally recognized serious crimes and to encourage its use elsewhere.

Attempting to control encryption, however, has proved to be an ineffective means of preventing crime and may actually hurt vital national interests. Similarly, the granting of new policing powers to law enforcement agencies will do less to protect a country's critical infrastructure than building better security technology. And, if greater security is truly what governments are after, then much can be done with the tools already in hand: encrypting all important data and communications makes their illegal retrieval and interception useless to the thief. ◆

## TO PROBE FURTHER

Additional material related to this article can be found on the *IEEE Spectrum* World Wide Web site at www.spectrum.ieee.org.

Nicky Hager's *Secret Power* was published by Craig Potton Publishing, Nelson, New Zealand, 1996. The U.S. government's surveillance efforts are also described in "They are listening to us," *Business Week*, 31 May 1999, pp. 110–11, and in John Markoff's "U.S. Drafting Plan for Computer Monitoring System," *The New York Times*, 28 July 1999.

A good source of information on steganography is the site at www.jjtc.com/Steganography/. Hiding one's identity is discussed at www.stack.nl/~galactus/remailers/index-anon.html and www.anonymizer.com.

Privacy and the Internet are discussed on the Web site at www.cs.berkeley.edu/~daw/papers/privacy-compcon97-www/privacy-html.html. The site at http://jya.com/ crypto.htm has many documents related to encryption and privacy.

*Cryptography and Liberty 2000*, by David Banisar and Wayne Madsen (Electronic Privacy Information Center, Washington, D.C., 2000), surveys the ever-evolving regulation of encryption in 135 countries. A review of cryptography policy in Europe is on the Web at www.modeemi.fi/~avs/eu-crypto.html.

Later this year, the IEEE plans to publish a new standard for implementation of public-key cryptography. Further information is at http://grouper.ieee.org/groups/1363/.

## ABOUT THE AUTHOR

Michael A. Caloyannides is a senior fellow at Mitrek Systems in McLean, Va. He earned his Ph.D. in electrical engineering, applied mathematics, and philosophy from Caltech in 1972 and has worked on information security issues in academia, industry, and government. He can be reached by e-mail at micky@ieee.org.

*Spectrum* editor: Jean Kumagai

# US Picks New Encryption Standard

After four years of work and an international cryptographic competition, the US Department of Commerce's National Institute of Standards and Technology (NIST) has selected an algorithm to serve as the Advanced Encryption Standard (AES).

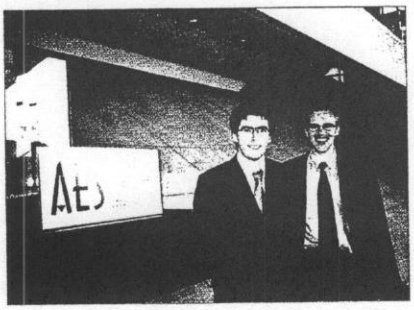
NIST chose the Rijndael (pronounced Rhine-doll) algorithm to become the AES. The algorithm's name was derived from the names of its designers, Belgian cryptographic experts Vincent Rijmen and Joan Daemen.

This standard for encrypting sensitive federal information would replace the Data Encryption Standard. As was the case with DES, companies and agencies worldwide, not just the US government, may also use AES. In fact, some companies are already using Rijndael.

In 1977, the US government adopted DES, which became widely implemented. Now, however, DES is no longer considered strong enough because increases in computing power have made it much easier to crack the algorithm.

"It was becoming clear to us in the mid- to late nineties that it was time for DES to be replaced," says Ed Roback, acting chief of the computer security division at NIST's information technology laboratory.

NIST thus decided to sponsor a global competition to help select the next government encryption standard (http://www.nist.gov/aes). Of the 21 algorithms submitted, 15 met the criteria for further consideration. From these, NIST chose five finalists.



***Vincent Rijmen (left) and Joan Daemen developed the Rijndael algorithm, which the US government recently selected as its official encryption standard.***

"We thought all five had adequate security for the AES," Roback said. An extensive study generated an 800-page report that included public input and commentary. The various key sizes of the algorithms were then tested before NIST made its final selection.

NIST will invite public comment until February 2001. The Belgian cryptographers will use this input to revise Rijndael before the secretary of commerce formally approves the algorithm, currently planned for the spring of 2001.

Roback said NIST selected Rijndael in part because "it appears to be consistently a very good performer in both hardware and software across a wide range of computing environments. . . . Its key set-up time is excellent [and its] very low memory requirements make it very well-suited for restricted-space environments."

Rijmen said, "The AES will have standardized key lengths of 128, 192, and 256 bits. Rijndael is more flexible and also allows lengths of 160 and 224 bits." DES used a key length of only 56 bits.

In most circumstances, Daemen said, Rijndael is faster than DES and about 2.5 times faster than the more secure version, called Triple-DES.

The challenge in creating Rijndael's formula, Rijmen said, was to achieve security while using only simple and easy-to-implement instructions.

Under the terms of the AES competition, Rijmen and Daemen will receive no money or royalties for their algorithm and thus must make it freely available.

So why did they enter the AES competition? "We thought that we are the best at what we do," Daemen said. "Now many people think that, too."

Rijmen is conducting postdoctoral research at the Computer Security and Industrial Cryptography lab at the Catholic University of Leuven in Belgium. Daemen is employed at Proton World International, also in Belgium, where he is working on new-generation smart cards. ✱

*—Linda Dailey Paulson*

# Better Software with Open Source?

Open-source software should be used to meet the need for better high-performance-computing software, according to a recent report from the US President's Information Technology Advisory Committee.

"Within high-end computing, we envision using open source for system software, as well as for applications," said Susan L. Graham, committee co-chair and professor of computer science at the University of California, Berkeley.

**Editor: Lee Garber, *Computer*, 10662 Los Vaqueros Circle, PO Box 3014, Los Alamitos, CA 90720-1314; l.garber@computer.org**

NEW COMPUTER VIRUSES YOU SHOULD KNOW ABOUT!

---

Do you have anti-virus protection for these new viruses? You never know when they may strike your system. Be protected!

---

AT&T VIRUS
Every three minutes it tells you what great service you are getting.

MCI VIRUS
Every three minutes it reminds you that you're paying too much for the AT&T virus.

PAUL REVERE VIRUS
This revolutionary virus does not horse around. It warns you of impending hard disk attack - once if by LAN, twice if by C:\

POLITICALLY CORRECT VIRUS
Never calls itself a "virus," but instead refers to itself as an "electronic microorganism."

ARNOLD SCHWARZENEGGER VIRUS
Terminates and stays resident. It'll be back.

GOVERNMENT ECONOMIST VIRUS
Nothing works, but all your diagnostic software says everything is fine.

NEW WORLD ORDER VIRUS
Probably harmless, but it makes a lot of people really mad just thinking about it.

FEDERAL BUREAUCRAT VIRUS
Divides your hard disk into hundreds of little units, each of which does practically nothing, but all of which claim to be the most important part of your computer.

GALLUP VIRUS
Sixty percent of the PCs infected will lose 38 percent of their data 14 percent of the time (plus or minus a 3.5 percent margin or error).

TEXAS VIRUS
Makes sure that it's bigger than any other file.

CONGRESSIONAL VIRUS #1
The computer locks up, screens splits erratically with a message appearing on each half blaming the other side for the problem.

CONGRESSIONAL VIRUS #2
Runs every program on the hard drive simultaneously but doesn't allow the user to accomplish anything.

IRS VIRUS
Takes 33% of your screen as a computing tax.

AIRLINE VIRUS
You're in Dallas, but your data is in Wisconsin.

PBS VIRUS
Your computer stops every few minutes to ask for money.

ELVIS VIRUS
Your computer gets fat, slow and lazy, then self-destructs -- only to resurface at shopping malls and service stations across rural America.

SEARS VIRUS

Your data won't appear unless you buy new cables, power supply and a set of shocks.

JIMMY HOFFA VIRUS
Your programs can never be found again.

KEVORKIAN VIRUS
Helps your computer shut down as an act of mercy.

IMELDA MARCOS VIRUS
Sings you a song (slightly off key) on boot-up, then subtracts money from your Quicken account and spends it all on expensive shoes it purchases through Prodigy.

STAR TREK VIRUS
Invades your system in places where no virus has gone before.

HEALTH CARE VIRUS
Tests your system for a day, finds nothing wrong and sends you a bill for $4,500.