MARKETPLACE

Nov 12, 1990

Data encryption a vital step in keeping data secrets safe

BY SIMSON L. GARFINKEL
SPECIAL TO CW

If you think secret messages are just for James Bond and international spies, think again. If you are not using data encryption to protect financial or medical records or other confidential information stored in your computer, you may be putting that information at risk of tampering.

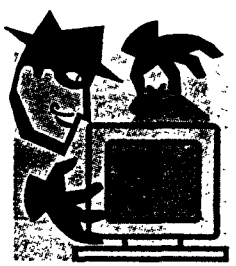
An encryption system is effective in protecting data on a disk and data being transmitted around the world. Encryption also reduces the chances of data being altered without your knowledge.

Encryption systems work by transforming a message into another message using a mathematical function and a special encryption password called the "key." If you encrypt the same message with two different keys, you get two different encrypted messages. If the encryption system is good, it is nearly impossible to translate the encrypted message back into the original message without knowing the key.

"Oil companies use it for transmitting oil exploration data from the oil well back to the main computer," says Samuel S. Wagstaff, a professor of computer science at Purdue University. "They don't want [their competitors] to benefit from the information."

Layers of protection

Encryption provides additional layers of protection for computers shared by many users. Unauthorized users may be able to access files, but if they don't know the key used to encrypt the files, it won't do them any good.



For this reason, encryption also protects data from being tampered with, says Dorothy Denning, a computer security expert at Digital Equipment Corp.'s Software Research Center in Palo Alto, Calif. Even if attackers manage to bypass your computer's security system, they won't be able to view confidential information without the encryption key. Although the attackers may be able to delete files, they can't forge encrypted documents because the forged documents won't decrypt properly.

Because encryption thwarts data tampering, it's also used for financial transactions transmitted over vulnerable channels, Denning says. Furthermore, she says, encryption can protect programs from attack by viruses. A virus that modifies an encrypted program won't run after the program is decrypted.

There are currently two basic types of encryption systems in use: "private key" and "public key" systems. Private-key encryption uses the same password to encrypt and decrypt the message. One of the most common private-key encryption systems is the Data Encryption Standard, better known as DES, developed by IBM in the 1970s.

Public-key encryption uses one key to encrypt a message (called the public key) and another key to decrypt the message. One of the most popular public key systems is RSA (for its creators, Rivest, Shamir and Adleman), which uses keys calculated from prime numbers that are hundreds of digits long.

There are a variety of encryption products on the market today. Some are programs that automatically encrypt data when it is saved onto disk and that decrypt it when the data is loaded back into an application program. Other programs are stand-alone and must be run in a separate step, leaving the decrypted data on the computer's hard disk. Some systems use special-purpose encryption hardware to speed the encryption process. Encrypting modems are also available and can be set to automatically encrypt everything sent over a telephone line.

Picking an encryption system is complicated by the fact that none is perfect: every system can be broken, according to Wagstaff. "Some of them can be broken in one or two days, some may take 100 years. Some can be broken for $1,000, while some of them might cost a billion dollars to break. You have to estimate the power of your enemy and how much power your enemy is willing to spend to break your cipher," he says.

Extra power needed

Encryption is not without its problems, however. It takes time and computer power to encipher and decipher a message. Generally, the more secure the encryption system, the longer it takes.

Another danger is forgetting your key. If your encryption system is any good, losing your key means that you've also lost your data.

Encryption software is fundamentally different than other applications. With a spreadsheet or a word processor, it's easy to tell if the program is functioning properly. But if you're not a cryptography expert, how do you tell if a proprietary encryption algorithm is easy to break?

Cryptologia magazine published articles in 1987 demonstrating the ease of cracking the encryption systems used by several popular IBM Personal Computer programs. "I've seen enough encryption schemes cracked that I would be very suspicious of a proprietary one," Denning says. Instead, she adds, companies should rely on well-known and well-tested systems such as DES and RSA.

Garfinkel is a free-lance writer and computer consultant based in Cambridge, Mass.

Any buying, selling or leasing concerns you'd like to have addressed in Marketplace? Call Cathy Duffy, associate editor at *Computerworld*, at (800) 343-6474 or fax at (508) 875-8931.