PRODUCT REVIEWS

May 5, 1997 (Vol. 19, Issue 18)

Head to Head

Windows encryption software
Puffer utility out-muscles PCCrypto
Briggs Softworks' product sports powerful feature set
By Joe Peschel

An encryption program's security hinges on the strength of its encryption algorithm. Secure encryption products do exist, but you must sort them out from products such as Genio USA's CrypEdit, (see Product Reviews, Dec. 9, 1996, page 117), which uses a weak encryption algorithm. Two newer encryption products, Briggs Softworks' Puffer 2.1 and McAfee Associates' PCCrypto 2.0, both use a strong encryption algorithm.

PCCrypto closely resembles Puffer, because Kent Briggs, the developer of Puffer, designed the initial release of PCCrypto for McAfee. Less expensive and my personal favorite, Puffer offers additional and more robust features. I suspect Puffer's support will likely be better, too, because it comes from the program developer.

PCCrypto, on the other hand, includes the suspect 56-bit DES, a standard that has long been criticized for its small key space. In addition, the product includes a message-recovery mechanism. Both of these features could lead to security breaches.

Puffer was easier to use than Pretty Good Privacy's PGP Mail 4.5 (see Product Reviews, March 31, page 94) and offered more features than PCCrypto for conventional encryption. If you just want to encrypt files and not share them, you have no need for public-key cryptography. Puffer also includes a file-wipe utility, important for security, which PGP Mail lacks.

Encryption and the Blowfish

Encryption algorithms generally can be divided into two types: asymmetric algorithms, which require two keys; and symmetric algorithms, also known as conventional or private-key algorithms. Both Puffer and PCCrypto use 160-bit Blowfish as their conventional, symmetric encryption algorithm.

Blowfish is a fast encryption algorithm that was designed in 1993. Bruce Schneier, the cryptographer from Counterpane Systems, a cryptography consultancy in Minneapolis (http://www.counterpane.com), designed it, and it has survived attack. The Blowfish source code is readily available and has been scrutinized by other cryptographers. Perhaps the algorithm's best feature, at least from a developer's viewpoint, is that Schneier placed it in the public domain so that anyone can use it.

I asked Schneier to look at the technical specifications regarding the changes Briggs made to Blowfish. Although Schneier did not look at the code itself, he read the specifications and found "no problems with the file format, the minor modifications that the designer made to the Blowfish algorithm, or the feature that checks to see if the key is valid."

However, Schneier noted that "there is always the possibility that security vulnerabilities could exist in the implementation."

Originally, McAfee used Briggs' Delphi source code, but in this release the company has rewritten PCCrypto in C++.

Even though conventional symmetric algorithms such as Blowfish are best suited for disk file encryption, both Puffer and PCCrypto provide a way to use the programs with e-mail. Each utility allows you to create self-extracting encrypted files so that the recipient of your e-mail doesn't have to own either of the encryption utilities. You and your correspondent have to agree on a password, which should be communicated by a secure phone or by courier.

Public-key algorithms solve the dilemma of communicating the password, but someone still could intercept your public key and send fraudulent messages with it. If you and your correspondent use the same program, you can exchange passwords to read each other's encrypted files. But, typical Puffer and PCCrypto files aren't compatible.

Message recovery

Puffer and PCCrypto both include an alternative encryption algorithm: Puffer Cipher 1, a 40-bit clone of the RC-4 algorithm. In addition, PCCrypto boasts a couple of features that Puffer lacks: a log file and a message-recovery mechanism. When you encrypt files with PCCrypto, you have the option of creating a log that includes details about the encrypted files, including their passwords. The product then encrypts the log file with a password so that you have only one password to remember.

This takes care of one challenge of key management: keeping track of multiple passwords. But it also might draw a typical user into choosing a simple word for the log's password, leaving the system vulnerable to a brute-force dictionary search.

The message-recovery mechanism in PCCrypto, called PCRecover, lets a system administrator recover messages encrypted by employees. (PCRecover's installation is optional.) The message-recovery mechanism creates an exceptionally small (and potentially risky) 512-bit RSA public key, for which you enter a password to recover messages. (According to McAfee, the version users will receive will create a 2,048-bit key.)

Strangely enough, PCRecover automatically created the key on the floppy disk. I didn't need to seed the key with any random bits, such as keystrokes or mouse movements, to create it. McAfee said the source of the seeded bits is random, but I would have preferred to seed the bits myself.

Although neither product is perfect, I recommend Puffer over PCCrypto for its more robust feature set and use of a more-secure encryption algorithm.

Joe Peschel, a free-lance computer journalist, covers security programs and other utilities for stand-alone systems. He can be reached at jpeschel@aol.com.

Puffer vs. PCCrypto

PCCrypto, the McAfee encryption product, doesn't offer quite the breadth of features as its competitor, Puffer, from Briggs Softworks

PCCrypto 2.0 Puffer 2.1

Encryption options:

160-bit Blowfish yes yes

56-bit DES yes no

Compressed file (LZ-77 compression) no yes

File headers no yes

Contents of its own editor no yes

To clipboard as ASCII text or self-extracting file yes yes

As a binary file or Binary to the program's editor file only yes

Decryption options:

To and from file, File and clipboard, and editor clipboard only yes

Wiping options:

Number of overwrites Once 10 with 0s on
last pass

Text editor no yes

Log file yes no

Message recovery yes no

THE BOTTOM LINE

Both Puffer and PCCrypto deliver strong encryption, but Puffer offers a greater and more robust feature set and uses a more secure encryption algorithm.

PCCrypto 2.0: GOOD

Pros: Strong encryption with 160-bit Blowfish; self-extracting encrypted files; message recovery feature.

Cons: Single-pass file wipe; some security problems with log file; uses 56-bit DES; lacks support for encrypted and compressed files.

McAfee Associates Inc., Santa Clara, Calif.; (800) 332-9966, (408) 988-3832; fax: (408) 970-9727; http://www.mcafee.com.

Price: $65 (retail); $49 (estimated street).

Platforms: Windows 3.1, Windows 95, Windows NT.

Puffer 2.1: VERY GOOD

Pros: Strong encryption with 160-bit Blowfish; good file-wiping routine; supports self-extracting encrypted and compressed files.

Cons: Inherent limitations of conventional algorithms; lacks a log file; no message recovery feature.

Briggs Softworks, Hewitt, Texas; kbriggs@execpc.com;
http://www.execpc.com/~kbriggs

Price: $29, single user; $199, network server; $749, site license.

Platforms: Windows 3.1, Windows 95, Windows NT.