PRODUCT REVIEWS

November 24, 1997 (Vol. 19, Issue 47)

Puffer 3.0 acts as secure alternative to PGP Mail

By Joe Peschel

The biggest dilemma for IT professionals in securing e-mail and sensitive files is not deciding whether to encrypt but deciding which encryption program to use. There are plenty of programs available, and many of are them easy to use, but the cryptographic algorithms employed often lack the security of a proven cipher.

Puffer 3.0, from Briggs Softworks, is an easy-to-use encryption program, and it uses proven algorithms. The earlier version of Puffer served best as a file encryptor, using symmetric, or single-password, algorithms. (See Product Reviews, May 5, page 118.) Puffer also let you create self-extracting files for e-mail. Although that method was an effective way of using a symmetric cipher for correspondence, you still needed a secure way to transmit the key.

Briggs has added public-key encryption to Puffer 3.0. A public-key encryption scheme is asymmetrical and uses two algorithms and two keys, one public and one private.

Similar to Pretty Good Privacy's PGP Mail, perhaps the best-known public-key encryption program, users exchange public keys. You encrypt messages with your correspondent's public key and they decrypt with a private key. Likewise, the other user encrypts messages to you with your public key, and you decrypt with your private key.

I tested Puffer's public-key encryption first. Creating the key ring and generating the key was a simple process. You can generate 512-bit, 1,024-bit, or 1,536-bit keys, and you can also set a date for the expiration of the key, which is convenient if you want to change your public key password (of at least 10 characters) often.

I created a 1,536-bit key, which took a few minutes because the number generated underwent primality testing. Puffer will let you speed up the process if you choose to use pre-generated prime numbers. After I created my key I could choose which symmetric cipher to use.

Puffer makes it easy to encrypt files, or to encrypt its own editor's content. Also new is the capability to configure an e-mail client for use with Puffer.

The product now includes a mechanism for message recovery, called secret sharing. This lets a company assign several trustees to recover a message. For instance, you might assign five trustees, requiring that three authorize a recovery operation before recovering a message.

It's an option not everyone will want, but it seems a smaller privacy intrusion than the message recovery in PGP Mail, which allows one person to recover any message. At least with Puffer you can require several trustees.

Puffer still lets you do single-password symmetric encryption with options that let you create self-extracting files, or archives of as many as 1,000 files, though I wish you could easily add to the archives by dragging and dropping. Puffer also still includes its fine Utility tool, which securely wipes files and frees and slacks space.

You won't find any public-key servers for Puffer, yet it's a good alternative to PGP Mail.

Joe Peschel (jpeschel@aol.com) covers security programs and other utilities.

THE BOTTOM LINE: VERY GOOD

Puffer 3.0

Puffer is a reliable encryption program suitable for protecting both e-mail and files.

Pros: Public-key and private-key encryption; secure-wipe utility, secret-sharing message recovery mechanism.

Cons: Difficult to add files to single-password protected archives.

Briggs Softworks, Houston; (800) 242-4755; (713) 524-6394; kbriggs@briggsoft.com; http://www.briggsoft.com.

Price: $29 for single copy; multiple licenses available; downloadable from CompuServe.

Platforms: Windows 95, Windows NT, and Windows 3.1.

Copyright (c) InfoWorld Publishing Company 1997