PRODUCT REVIEWS

March 31, 1997 (Vol. 19, Issue 13)

Windows e-mail encryption software

PGP Mail brings strong encryption to 32-bit platforms
By Joe Peschel

The first commercial version of Pretty Good Privacy's PGP Mail was, ahem, pretty good because it made encrypting files easier than enciphering them with freeware PGP. Now PGP Mail 4.5 is designed for Windows 95 and Windows NT 4.0. If you're looking for security through encryption, PGP employs some of the strongest cryptographic algorithms for security. However, you must install the product on each system.

It still includes ViaCrypt's Enclyptor, a floating toolbar that lets you encrypt, decrypt, sign, and verify the contents of the Windows Clipboard. PGP has added a couple of useful buttons to the Enclyptor that let you launch a clipboard viewer, run the default editor, and start the main PGP program.

PGP Mail still includes the corporate-access and corporate-certification keys introduced in ViaCrypt 4.0 Business Edition. The keys allow for corporate access to encrypted messages, an action that many will construe as a violation of privacy. On the other hand, corporate-access keys are easy to defeat because they aren't hard-coded.

PGP Mail supports long file names, integrates with Explorer, and includes plug-ins for Netscape Mail 3.0 and Eudora 3.0.

PGP functions primarily as a public-key encryptor. It uses a public key for encrypting files and a secret key for decrypting them. Two correspondents exchange public keys so that each can encrypt messages with the other's public key. Messages are decrypted with each correspondent's secret key.

Known as an asymmetrical system because it employs two keys, PGP Mail uses two algorithms for the most part. The first, RSA, offers key sizes of as high as 2,048 bits and uses the International Data Encryption Algorithm (128-bit IDEA). To break the RSA key, you must factor large numbers -- a process best left to immortals. PGP Mail uses a third algorithm, MD5, for signatures.

If you're new to cryptography, PGP Mail makes the basics easy. You start by creating a key pair (a secret key and a public key) of anywhere from 768 bits to 2,048 bits. (The default in PGP Mail is 1,024 bits, which strikes a good balance between speed and strength.) If you are already using

freeware PGP 2.6, for example, PGP Mail lets you maintain your current key pair.

I used my freeware PGP key pair when testing PGP Mail. I found it easy to tell the program where the default public and secret keys were located. You can configure PGP Mail to be compatible with previous versions of PGP to communicate with, say, a Version 2.6 user.

PGP Mail automatically inserts the plug-ins for Netscape Mail 3.0 and Eudora 3.0 during installation. PGP Mail, however, cannot prompt users prior to inserting a plug-in.

The plug-ins let you automatically encrypt, decrypt, and verify messages and attachments. PGP Mail includes only a pair of plug-ins, so you'll want to use the Enclyptor to copy text to the Clipboard and encrypt its contents before pasting to another mail program.

Although PGP Mail is cryptographically strong, system and user weaknesses exist. PGP Mail (and PGP) lacks a separate mechanism for securely deleting files. PGP Mail will overwrite the source file of an encrypted file, but it will do so only once. I'd also like to see an option to execute multiple overwrites of slack space, free space, and the Windows 95 swap file.

Finally, the default pass-phrase rule of at least eight letters and no special characters may entice a user to choose an ordinary word as a pass phrase. Such a choice might be vulnerable to "dictionary" attack.

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

What's in PGP Mail 4.5

- Enclyptor floating encryption/decryption toolbar
- Integrated file wipe mechanism
- Plug-ins for Netscape Mail and Eudora
- Private-key encryption with International Data Encryption Algorithm
- Strong public-key encryption
- 32-bit support
- ViaCrypt corporate key access

THE BOTTOM LINE: VERY GOOD

PGP Mail 4.5

PGP Mail is a good choice as an encryption solution for corporate use.

Pros: Plug-ins for Netscape Mail and Eudora; floating encryption bar; backward compatibility.

Cons: Few plug-ins; no separate secure file deletion; controversial corporate key access.

Pretty Good Privacy Inc., San Mateo, Calif.; (888) 747-3011 (toll-free), (602) 944-0773; http://www.pgp.com/products/.

Price: $150; upgrades available.

Platforms: Windows 95, Windows NT 4.0.