PRODUCT REVIEWS

October 21, 1996 (Vol. 18, Issue 43)

Windows 95 security utility

A look into Your Eyes Only file protection system
Despite no individual file protection,
its strong cryptography a good start

By Joe Peschel

A good security tool for Windows 95 (itself a weakling when it comes to security) ought to limit access to files, offer file protection, include an auditing log of user activity, and provide a strong cryptographic algorithm to protect sensitive files. Symantec Corp.'s Your Eyes Only for Windows 95, Version 4.0 (YEO), does most of that, except for individual file protection.

Instead of individual file protection, YEO has BootLock and ScreenLock, control mechanisms that prevent unauthorized system access on boot-up and access past the screen saver, respectively. YEO allows you to establish password rules and wipe files, and it lets you set up a primary user who has access to all of the encrypted files of as many as 49 secondary users.

But the most interesting elements of YEO are cryptographic.

Despite its name, which sounds as if this utility might be little more than an encryption toy, YEO provides public key encryption with a twist: You can choose the symmetric algorithm. The algorithms, unlike most, aren't just something Symantec cooked up on its own. This is strong cryptography, primarily licensed from RSA Data Security Inc. (RSADSI) and implemented using that company's Bsafe Toolkit.

With YEO, you can create RSA public keys with sizes between 360 bits and 2,048 bits. Symantec suggests a 768-bit public key. RSADSI, and most cryptographers recommend a key of at least 1,024 bits. I, a professional paranoid, like a 2,048-bit public key, but encryption and decryption are slower.

Unlike Pretty Good Privacy (PGP), which uses RSA with International Data Encryption Algorithm (commonly known as IDEA) as its symmetric cipher, YEO gives you a choice of symmetric -- or private key -- algorithms to chose from. They include the time-worn encryption standard DES and the stronger Triple-DES. The default symmetric algorithm is 128-bit RC4, but you can select 128-bit RC5 or the relatively new Blowfish. Symantec has chosen a 128-bit maximum key size for Blowfish, instead of the 448-bit maximum as designed by Bruce Schneier, a cryptographer at Counterpane Systems Inc., in Oak Park, Ill.

With YEO, you enter your password only once for access to all of your encrypted files. This convenience could be seen as a flaw, as anyone can read your encrypted files if you haven't activated ScreenLock. Once you're in, there's no way to exit YEO short of restarting. You can get to Windows 95 on a YEO-protected machine without the password, but you won't be able to read any of the encrypted files or use YEO's features.

Securing your data

In testing YEO, I used each of the symmetric algorithms with my large RSA key. Each file is encrypted with the symmetric algorithm you choose and RSA for encrypting the message key. By using public key encryption you can share encrypted files by exchanging public keys either with other local users, or across the Internet using e-mail.

YEO, however, doesn't do conventional single private key encryption. The capability for private key encryption, in the manner of PGP, which uses IDEA for conventional encryption, would have been a convenient addition, because the encrypted files are smaller.

YEO attaches itself to Windows 95 Explorer and allows you to encrypt files manually or encrypt the contents of Smart Folders automatically.

Drag a file into a Smart Folder and it will be encrypted. As is the case with the manual encryption process, you can choose the algorithm. Some files, .EXEs, for instance, cannot be automatically encrypted, but you can manually encrypt them.

Encrypted files in a Smart Folder are decrypted by double-clicking the file when you're logged on. When the file within a Smart Folder is closed, it's re-encrypted. In my testing, YEO often failed to re-encrypt open files before I exited Windows 95, a problem that Symantec is correcting.

As I mentioned, the primary user of YEO has access to all files encrypted by secondary users. If you are a secondary user, you might view this as a security hole.

This disk will self-destruct

ScreenLock, the password-protected screen saver, tries to ensure that your system isn't accessed while you're away from your desk. However, an attacker could reset your system while your encrypted files are in plaintext. Enter BootLock, which prevents hard-disk boot-up without a password. It secures the boot block and can't be bypassed by booting to a floppy disk.

Although Symantec won't reveal the algorithm BootLock uses, the company admits that BootLock can be bypassed by an experienced programmer or hacker. Although BootLock uses the same password as YEO proper, a successful bypass of BootLock won't allow access to the encrypted files.

I asked an encryption-testing company, AccessData Corp., to check YEO's vulnerability. Here's its report: "Norton Your Eyes Only appears from our preliminary examination to be a solid product. It appears that the cryptographic implementation of the public/private-key database is solid and is in danger only of a brute-force attack. This attack could be made easy if the algorithm for the log-in ID and password verification is implemented incorrectly. Thus, we are unable to prove at this time that a system protected by Norton Your Eyes Only is safe from attackers. These results are a brief analysis of the product and could change with a more aggressive examination."

The upshot of AccessData's remarks is that the product appears secure within reasonable bounds. Of course, there can be no guarantee that it will always succeed.

In addition to its cryptographic and auditing capabilities, YEO can securely wipe files. Secure Delete will overwrite any file three times with a series of hexadecimal numbers: 0As, 05s, and 03s, before deleting it. There's some controversy about whether three overwrites is a secure wipe; it should be beyond the capability of software-recovery tools, but there are techniques that will recover these wiped files.

Counterpane's Schneier recommends seven overwrites or even burning or shredding the media. The secure wipe will not zero-out a file before deletion, nor will it overwrite the file name or entire clusters.

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

Symantec does more than look the other way when it comes to Windows 95 security

Your Eyes Only components keep files covered

- Add other users
- AuditLog
- BootLock
- Emergency UnLock Disk
- Encrypt, decrypt, and secure wipe
- Encryption
- Network YEO Administrator
- Password rule
- ScreenLock
- SmartLock folders

THE BOTTOM LINE: GOOD

Your Eyes Only for Windows 95, Version 4.0

Your Eyes Only for Windows 95 (YEO) provides a handful of strong cryptographic algorithms for file protection, as well as a mechanism that can block unauthorized access to files. If Symantec were to include a mechanism that protects against individual file tampering in a future version, YEO could be very good.

Pros: Strong public key encryption; automatic file encryption and decryption; supports several users.

Cons: No solid individual file write/read protection; could have stronger secure delete; only for Windows 95; bypassing of BootLock possible.

Symantec Corp., Cupertino, Calif.; (800) 441-7234, (541) 334-6054; fax: (503) 334-7474; http://www.symantec.com.

Price: $90 estimated retail.

Platform: Windows 95.