Hard Drive Encryption Software

We examine some of the products which provide add-on encryption under Windows.

By Phil Morris

A fair amount of data stored on your average business PC can be classed as "sensitive", ie, information that you or your customers wouldn't want to fall into the wrong hands. Operating system password protection is a natural and obvious way to protect the data on these machines, but is this type of password protection enough?

What if, for example, a burglar steals a desktop PC using Windows 95? There's minimal password protection built into the OS so what happens to the sensitive company information on the machine? Chances are that the data will be backed up as a matter of course and the thief won't realise what he has so will simply wipe the hard drive and sell the machine, but what if said data falls into the wrong hands? Assuming that the sensitive files aren't themselves password protected it will be all too easy for the thief or someone computer literate to disseminate the information contained within and either make it public knowledge or pass it onto interested parties. Even if the files are password protected via the application there might be other information that is deemed as sensitive or private for one reason or another, such as which Web sites have been visited by the user.

It's also worth remembering that the password protection built into applications is pretty easy to crack. There are plenty of Web sites offering tools to crack passwords on Word, Excel, PKZIP files etc and even Windows and NetWare admin passwords too.

Of course, breaking into a building to steal a PC isn't always the easiest of tasks, but there is an area that is at far greater risk - laptop / notebook computers. These are, in comparison to your average desktop, far easier to liberate due to their portability. It can also be easier to remove their hard drives. Mobile computing is on the increase and there is unlikely to be a reversal in the trend, therefore more laptops / notebooks will be put at risk along with the data contained on them. Attacks on a system via the Internet are of course also possible, especially if the user is connected via a broadband link (so making it easier to steal large files, for example).

So Encrypt It!

One possible answer to the problem is data encryption. This will not of course stop a thief from stealing the machine in the first place, but if the encryption is strong then it should prove extremely difficult if not impossible to retrieve anything from the stolen machine. In this article I will conduct a cursory examination of various methods of encryption that are available in the form of either commercial, freeware or shareware software. I don't intend to go into any depth on how to install the software, what it looks like etc - I am mainly (but not solely) interested in its features, transparency to the user / operator plus whether it has any particularly good or bad points.

Methods Of Implementation

Various methods are available for implementing hard drive encryption but some things should be first considered. For example, ease of use should be a primary concern, as should security. If a system is hard to use then your users probably won't bother using it. Another important consideration is the transparency of the encryption / decryption, achieved by using on-the-fly encryption methods. Your users will not want to have to manually intervene each time a file is opened or closed, they

will simply want to access their files in the usual manner. Any user intervention will be time consuming and could also lead to unwelcome support calls.

There are three essential methods for encrypting data on a hard drive: the complete hard drive can be encrypted; the designated area of data can be encrypted; or individual files and folders can be encrypted. Complete hard drive encryption is a logical and easy choice as, in theory, you simply load the encryption software, set it up as required with the necessary password(s) and use it. Well, almost. The major drawback with this method is that when booting a PC the BIOS needs to read the boot track. If this is encrypted, how can it access it? If it is inaccessible and the PC can't be booted to decrypt the drive then, in a worst case scenario, the hard drive could be rendered unreadable, necessitating a time consuming reformat and reinstallation - also hoping that any important data has been backed up.

Some PC BIOSes will incorporate features to work around this issue, as will some software, while another option is to use a smart-card or similar which will be required to give access to the drive. There are though some obvious restrictions with this method, one being that once the machine has been booted literally anyone can access the encrypted data, in other words the encryption doesn't take place on a per-user basis. Said data also cannot be easily backed up in an encrypted form to other storage devices - if the backed up data has to be unencrypted then it leaves a rather large and obvious hole in the security. These are just some of the negative issues with this method of encryption - there are others which would take too long to discuss here. The Web Resources section of this article contains links to documents which delve further into the matter.

The second method is to use encryption that is restricted to user- or operator-designated files and folders. Such a method is incorporated within Windows 2000 and Windows XP and is called the Encrypting File System (EFS) - see below for more information on EFS. Other programs rely on similar methods, and EFS isn't the only one I am referring to here. The obvious major drawback with such a method is that it isn't exactly completely transparent to the user - if set up in a logical manner then it can be made easier to use and there are obvious benefits from being able to encrypt single files and folders.

The third method is arguably the best, with it being the most secure, most transparent and least likely to have any major disadvantages in everyday use or support. This involves creating a dedicated "virtual" drive which is encrypted and solely contains encrypted data. Such virtual drives (also known as containers) are rela-

"There are three essential methods for encrypting data on a hard drive: the complete hard drive can be encrypted; the designated area of data can be encrypted; or individual files and folders can be encrypted."

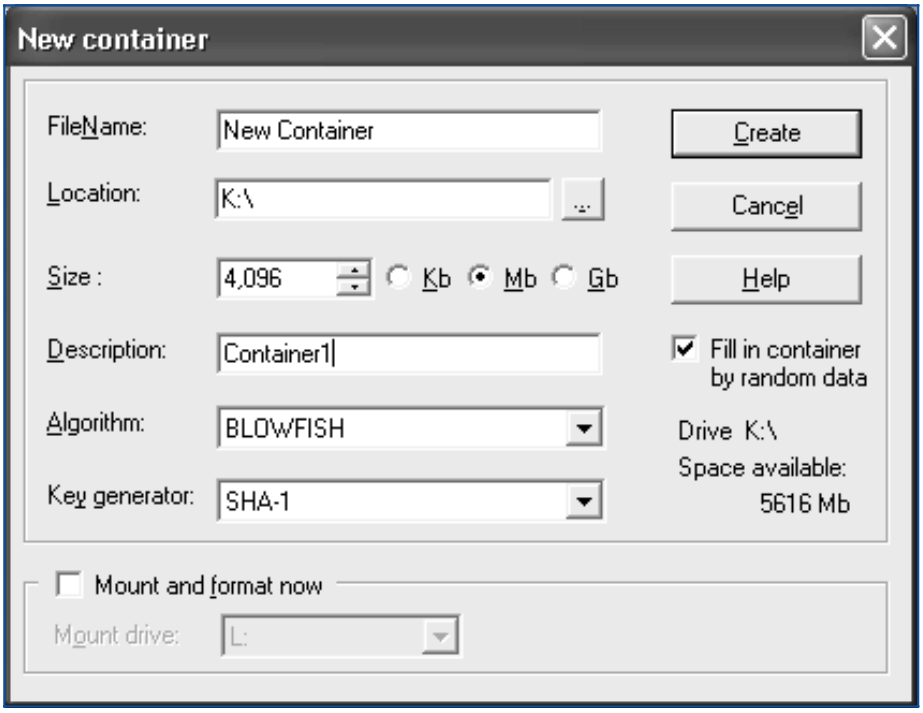

Figure 1 - BestCrypt v.7 - creating a new container.

tively easy to back up and in the process retain the encryption - that way the data remains secure.

Depending on the software, Smartcards can also be used to provide access to the encrypted data, or the access can be solely password-reliant. More than one user can access the PC, as each user can have their own private container(s) and consequently their own passwords. This method is also transparent to the user when opening / closing files so making it easy to use once installed by a support engineer / operator etc. PC Support is not a problem as an engineer can access the PC without needing to see the users' data (depending on the problem of course) while being able to easily backup the container if required. Virtual drives are definitely the most widely used forms of encryption, being utilised by many of the more popular hard drive encryption packages.

Microsoft EFS

For those PCs that run either Windows 2000 or Windows XP some built-in encryption is available in the form of Microsoft's EFS. Once either of the aforementioned operating systems is installed no further software installation is required to enable EFS, but there's a potential problem: the partition with the data to be encrypted must be formatted as NTFS - FAT32, FAT16 etc will not support EFS so if for some reason it is not possible to convert the partition to NTFS then a third party encryption product will need to be employed.

EFS allows the encryption of files or folders as required and protects them by means of a randomly generated File Encryption Key which is unique to each file. This key is matched with a public / private key in order to provide access to the files or folders in question. In order to increase the security of EFS it is recommended that 128-bit encryption is used. No manual user intervention is required during the file encryption / decryption process as it all takes place transparently during hard disk writes and reads. If a folder is encrypted then all files and directories created within it are also automatically encrypted, while encryption of just one file requires a decision to be made whether the folder containing it also needs to be encrypted.

To give an example of the encryption process within Windows XP, a file or folder can be encrypted by simply right clicking on the item in question, selecting Properties, clicking on the General tab then the Advanced button and selecting "Encrypt contents to secure data". Permanent decryption of the data can be achieved by effectively reversing the aforementioned encryption process.

Besides the fact that there is the requirement for an NTFS formatted partition, EFS has some other limitations. Firstly, because the encryption is effectively tied to the user's account, if someone knows the user's password then any encrypted data can be accessed - after all, the operating system doesn't know that the wrong person is

"For those PCs that run either Windows 2000 or Windows XP some built-in encryption is available in the form of Microsoft's EFS."

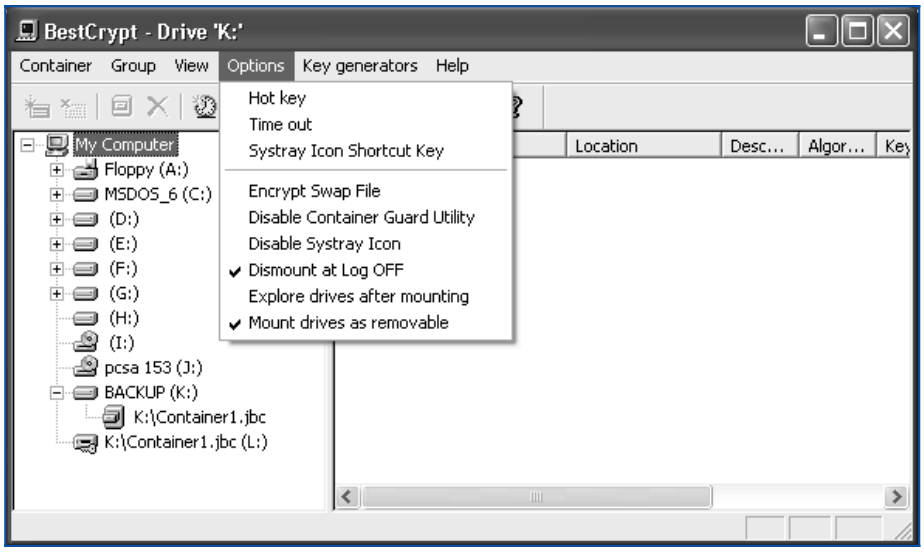

Figure 2 - BestCrypt v.7 control panel showing options.

gaining access to private files. The local Administrator can of course also access any encrypted files.

Compressed files and folders cannot be encrypted - if encryption is attempted on such then the file or folder is automatically uncompressed. Also, files that have the System attribute set cannot be encrypted, neither can files in the systemroot directory structure. Caution is also advised when re-installing the operating system because EFS uses the unique SID - re-installing the OS will generate a new SID, so rendering any encrypted files and folders inaccessible. Therefore always decrypt any encrypted files and folders before re-installing the OS.

Other vulnerabilities relevant to the Windows 2000 implementation are discussed at securityfocus.com (a link is provided in the Web Resources section), there is also a link to an article that gives a step by step breakdown of the encryption process.

Despite the disadvantages, EFS has some obvious advantages - firstly it comes free with wither Windows 2000 or XP. Secondly, as it is built-in it doesn't require a separate installation, so perhaps causing less support hassle in some respects. Overall though and despite the criticisms (which should be borne in mind) EFS is a worthwhile addition to Windows 2000 and XP and should provide a useful additional level of security on users' PCs.

BestCrypt

The Finnish firm Jetico produces a hard disk encryption product called BestCrypt, currently compatible with Windows 9x, Me, NT, 2000 and Linux (earlier versions also supported DOS and Windows 3.x, these versions are now freeware). At the time of writing Windows XP is only supported by the version 7 beta, but for the purposes of this review I will concentrate on non-beta version 6.

Security is assured by the use of four encryption algorithms, these being: Blowfish in Cipher Block Chaining mode; Russian Federal Standard GOST 28147-89 in Cipher Feedback mode; USA Federal Standard DES in Cipher Block Chaining mode; and Twofish in Cipher Block Chaining mode. Additional encryption modules are also available to download from Jetico's Web site. Supported file systems are FAT12, FAT16, FAT32 and NTFS.

In use, BestCrypt operates differently from Microsoft's EFS - instead of allowing you to encrypt anything you desire, it requires the creation of a "container" where all the encrypted data will be stored. This container (more than one can be created) is really just a large file created on some free space on your hard drive. The container is effectively a virtual disk and will support any unused drive letter. The data can then be accessed as if it is present on a real drive, so ensuring that any applications don't experience difficulties accessing the data.

Container Size

"BestCrypt operates differently from Microsoft's EFS - instead of allowing you to encrypt anything you desire, it requires the creation of a "container" where all the encrypted data will be stored."

Container size is limited by the operating system in use - as an example, 2 GB is the limit with FAT16, while NTFS allows up to 64 GB. Once created, a container cannot be resized. When the container is created the operator decides on the type of algorithm to be used, the size and the key generator - after that a drive letter is assigned and the new virtual drive is mounted and formatted. As the container is simply a file it can of course be backed up with the encryption remaining intact, plus the containers can be created on network disks which can then in turn be shared with other users on any operating system - that includes Unix variations, Linux, Windows 3.x, Windows 9x, Windows NT/2000 and Novell.

In addition to the creation of containers on network drives, they can also be created on any removable media (except floppy disks). Any data written to the container is encrypted on the fly, conversely data is decrypted on-the-fly too. To access the data the relevant container has to be opened so requiring a password to be input - in use containers don't have to remain in this open state, if they are disconnected/closed then any resident data is rendered inaccessible until they are re-opened with the password. You can set a timeout after which the container is dismounted, thus avoiding the problem of users leaving the office and forgetting to render their BestCrypt containers inaccessible to passers by.

One interesting point to note if your users are in the habit of losing passwords is

that BestCrypt does not incorporate a backdoor password, so if a user loses a password the data can not be recovered. On a different point entirely, besides running from the GUI, BestCrypt can also be run from the command line, a feature that is useful if, after all these, years, you still prefer to type in your commands instead of using a pretty GUI. This also makes it easy to add icons to the desktop which will mount or dismount your encrypted drive with a single click (though of course you will also need to enter the password when mounting). A Development Kit is also available to download and this is freeware.

BestCrypt 7 adds some useful new features: new swap file encryption; hidden containers; containers can now be mounted from sub-folders instead of being limited to the root; containers can be organized in separate groups via the BestCrypt control panel; the Rijndael encryption algorithm has been added and new passwords can be added to existing containers.

A trial download of BestCrypt is available from Jetico's site (see the Web Resources section), and is fully functional but expires after 30 days. After the software has expired any encrypted data is rendered read-only unless the software is subsequently registered.

This brief summary of just some of its features only scratches the surface, but suffice it to say that BestCrypt is a very professional piece of software and has garnered high praise in a number of reviews. I would certainly recommend it to those looking for a fast, flexible, secure third-party encryption tool.

It is also worth mentioning another Jetico product called BCWipe that can be installed during the BestCrypt installation - as the name implies, this securely deletes files and is compatible with Windows 9x, Me, NT and 2000.

ScramDisk

ScramDisk is a free disk encryption program and like BestCrypt is a product that has been highly rated in a number of reviews. The free version of ScramDisk is only for Windows 9x and Me. Features mentioned here will relate to version 3 of the software.

The basic operating principles of ScramDisk are similar to BestCrypt, in other words free space is allocated to a container which is assigned a password. When mounted, this container becomes a virtual drive which is then allocated an available drive letter. Whenever someone wishes to access this drive the password is entered. The password is generated by use of the mouse - the program requires random data to generate the password and this is generated by moving the mouse when requested, so creating the master key. You might have seen this process in use in other programs. The secure handling of the passwords is rather interesting as whenever a password is entered it is cached in "locked memory", therefore memory which isn't swapped out to the swap file.

Compatibility

The free version of ScramDisk is only compatible with FAT16 and, more recently, FAT32 (as of version 3). If Windows NT and 2000 users wish to use ScramDisk then it's at a price, namely US$20. This registered version will also support NTFS partitions. Supported encryption algorithms are 3DES, Blowfish, DES, IDEA, MISTY1, Square, Summer (Stream), TEA (16 Rounds) and TEA (32 Rounds). Also included with ScramDisk are shredders, which will securely erase the contents of the swap file and any free disk space if required. As with BestCrypt there is a command line option to support, for example, mounting a volume, plus there are other command line tools. Incidentally, volumes can also be mounted by dragging and dropping an existing volume file onto the running ScramDisk program or it can be done via a menu option.

"ScramDisk is a free disk encryption program and like BestCrypt is a product that has been highly rated in a number of reviews."

The ScramDisk code is based on another encryption program called E4M. Compared to some other encryption programs it has a small storage/memory footprint, consisting solely of an executable and a device driver. On the security side, and as an additional security measure, nothing is written to the registry during either installation or program use. One handy feature is that a batch file can be created, consisting of a file called "ScramDisk". If this is stored in the root directory of the mounted volume it will be found by ScramDisk when it starts (it automatically

searches for this file) and is then executed, so allowing specific configuration options to be selected on startup.

The smallest possible ScramDisk container is 256 KB, while the upper limits vary - under Windows 98 for example the limit is 4 GB. ScramDisk allows the encryption of a whole disk partition, but in addition to this uses steganography (see later in this article) to hide volumes within .WAV audio files.

ScramDisk is described as an "In Progress" work - the source code is available to download from the Web site (listed in the Web Resources section). The author has chosen to remain anonymous, but an email address is available for contacting him, ordering the NT/2000 version of the software, support issues etc.

The resources page on ScramDisk's Web site points to a lot of useful links on Cryptography, PGP, Newsgroups, mailing lists, books etc and is definitely worth a visit. There is even a newsgroup dedicated to this most useful bit of software that is definitely worth trying out.

Encryption Plus Hard Disk And Folders

PC Guardian produces a number of encryption products, two of which are "Encryption Plus Hard Disk" and "Encryption Plus Folders". The former is a commercial package. I'll concentrate on this, although the latter will also receive some attention.

EPHD is an Enterprise product aimed at notebook and desktop computers. It currently only uses one algorithm, namely Blowfish with a 192-bit key - it also protects all the data on the hard drive and isn't reliant on creating a special container unlike the products previously mentioned. Currently supported operating systems are Windows 9x, Me, NT and 2000 - also maybe worth noting is that older 80486-based PCs are not supported. Up to six partitions are supported but not multiple hard drives - if the software detects more than one hard drive in a PC it won't encrypt any of them, but if one is disconnected / removed, the remaining one encrypted and the second drive reconnected all will work just fine. Supported partition types are FAT16, FAT32 and NTFS. The manual advises against converting an encrypted partition from FAT16 to NTFS.

Installation can be selected for either a single PC install or multiple PC install, the difference being that the multiple PC install allows the sharing of the Master Password and Privacy Code. One issue that might interest administrators and support staff is that there are back doors, namely an optional Local Administrator password alongside the Master Password and the user's Daily Password.

Multiple Passwords

This means that you potentially have three passwords to deal with, each of which could be a potential security risk. This of course has its advantages for getting around the problem of lost passwords but the potential disadvantages are obvious. Passwords are managed via the Password Management feature where rules are set which define how users can set up their own passwords, for example an expiry time, minimum password length and any special characters that are specifically required. A special password protected screensaver can also be set, along with the number of guesses that a user can make when entering the password. There is also the provision for a 'one time password' which will allow a user to gain access to a machine where the password has been forgotten.

This article will be concluded in a future edition of PCSA.

"The resources page on ScramDisk's Web site points to a lot of useful links on Cryptography, PGP, Newsgroups, mailing lists, books etc and is definitely worth a visit."

PCSA

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews

A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers

Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software

In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs

There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.