

The following article appeared in the German magazine Network Computing on April 10, 2003 and was translated by Utimaco Safeware:

Report Card: Hard-disc encryption

		Utimaco	WinMagic	IT-SEC	Pointsec Mobile Techn.	PC Guardian	CyProtect
Feature	Weighting	SafeGuard Easy 3.10.2	SecureDoc 3.1	IT-SEC- Notebook 6	Pointsec PC 4.0	Encryption Plus Hard Disk	CyProtect Disk Encryption
Drive encryption	50 %	5	5	3	3	2	1
Access control	30 %	5	4	3,5	3,5	2	2
Price	20 %	3	3,5	4,5	3,5	4	5
Result		4,6	4,4	3,45	3,25	2,40	2,1
		A	A-	C+	C+	D	D

Lost In Seconds

In just a few seconds, a laptop can be stolen or hacked - and valuable information changes its owner. Network Computing has tested various solutions for data protection.

Stop reading this article, get yourself a cup of coffee and come back — if your laptop still is where you left it, you can consider yourself a lucky dog. A survey among 503 security experts resulted in 134 reports about laptop thefts. The losses per theft amounted from US \$ 11,766 up to nearly US \$ 88,000, whereby the biggest part of the damage was caused by the loss of proprietary information. And now imagine that all private data is lost forever or, even worse, is published in the Internet. And now, please think about the fact that you will have to explain to your boss why the business secrets of your company can be found in the internet.

No doubt, laptops are comfortable, but prone to hacker attacks and theft. We will look at three aspects of laptop security: protection of software and communication channels, hardware protection and protection of data. Of course, conventional desktop PCs can benefit from the discussed security measures as well — even heavy tower computers already vanished into thin air.

Administrators and users both should keep in mind that there is no 100 % protection from attacks and losses. However, anti virus software, firewalls or authentication software make attacks more difficult, just as recovery services, VPN tunnels or hard-disk-encryption.

Secure Communication Channels

Basically, a secure remote computing makes sure that the users cannot be attacked, cannot spread viruses themselves and communicate with the company network over secure connections. For this, all laptop users first need Personal Firewalls which protect from the usual attacks. Personal Firewalls can also "hide" a PC by making sure that it does not answer to connection requests or pings. To do this, they block ports and protocols, carry out host-based intrusion detection or decide which applications are able to access the Internet. Firewalls which can be centrally administered are to be preferred as the end users should not make decisions themselves which could affect security — the administrator gives the guidelines which the users have to follow.

Firewalls with application control are better in blocking Trojans than firewalls which only block ports. This is due to the fact that Trojans can work by making outgoing connections over general ports. Of course, Firewalls alone do not protect from viruses. For this, an anti-virus software is required, preferable a package which frequently seeks after new signature definitions.

In the next step for the software protection, it has to be verified whether the user is legitimate. For this, there are several options. One of them is to enforce the user to enter a login password as soon as the system is booted or after there was no user input for a while. If passwords do not seem secure enough for the administrator, he, of course, has the option to use biometric authentication solutions, e.g. fingerprint or speech analyses. However, the administrator should consider that many biometric devices have to be connected to serial interfaces or USB ports, where the laptop users can easily damage or lose them. Meanwhile, Acer, Micron-PC and various other manufacturers are offering laptops with built-in fingerprint scanners.

Speech analysis as access protection sounds like a good solution, as many laptops already have built-in microphones, but this solution can become a problem as well. In noisy environments, it might be impossible for the PC to catch the sound. A heavy cold could also lead to increased helpdesk calls.

For the connection to the company network, the magic word is "encryption". First of all, it has to be found out what has to be encrypted. If all users only access web-based programs, HTTPS will do. E-mail can be encrypted by SSL over IMAP or POP3. This makes e-mail exchange over the Internet more secure, as the entire session from the host to the e-mail server is encrypted. There are two main forms of e-mail encryption: S/MIME and IMAP/POP3 over SSL which both meet different requirements. S/MIME encrypts and signs the message, but not the session. IMAP/POP3 over SSL protects the login and the session, but with the next hop, the data can already be transferred into clear text. IMAP over SSL is very simple and does not require user intervention, but is not supported by all kinds of client software. If the entire traffic has to be encrypted or several programs do not support encryption, VPN is an option. Virtual private networks allow remote users to access internal network resources without making these resources accessible to the public.

By the way, Split-Tunnelling should be switched off so that all network traffic can go through the VPN, and not just the traffic meant for the company network. Several VPN Clients are delivered in a bundle with a Personal Firewall, possibly facilitating installation and management. Most VPN Clients support the integration with smartcards, USB Tokens or biometric devices for the handling of certificates and authentication.

Of course, all these Firewall, anti virus, authentication and VPN solutions mean more work for the helpdesk and more software to be kept up to date. Maybe these solutions even require separate administration server and management interfaces. Such aspects have to be considered in a cost analysis.

The Seventh Commandment

Theft is a reality of life since the first caveman took the dinosaur steak of his neighbour from the campfire. With laptops, the case is similar. It only takes a few seconds, if, in a crowded airport terminal, a strange hand grabs the laptop and vanishes with it forever. Just as quickly, the laptop bag is forgotten in the baggage rack of a plane.

A lost laptop can be considerably more valuable than the hardware. How valuable are the data stored on the laptop? If they were not secured, numerous hours of work are possibly lost. Several laptops also contain private information or sensible company secrets which possibly are worth millions if the wrong persons get hold of them.

Different products are available to protect the laptop, from cable locks to motion detectors. But none of these products can guarantee a 100% protection from theft — they only make theft more difficult. Most laptops are made of relatively soft plastic and only have a small slot for locks. We have found out that, with a simple screwdriver, the case often can be opened wide enough to remove the lock. A palm-sized gas burner is able to melt the plastic material. Although a laptop with a hole in one side will be worth less than an intact device, the components of the systems can nevertheless be sold individually — and a thief who is only interested in the data will not care about physical damage at all. Laptops with a hardened plastic case are recommendable; e.g. the »Omnibook 6000« by Hewlett Packard with a magnesium-boosted case.

Once the thief has stolen the laptop, little can be done about it. If laptops are purchased over online auctions or computer exchanges, it is hardly of interest whether the good was stolen, unless the original owner has installed theft recovery software (see Network Computing 5/2003). However, there are restrictions in the efficiency of such programs.

The hardware may be history after a theft, but the data can remain protected if it had been encrypted. Individual files and file folders can be encrypted, but complete hard-disks as well. For Windows 2000 and Windows XP users who want to encrypt individual files, the Encrypted File System (EFS) Utility is available immediately. The user just has to click on the respective file with the right mouse button in the Windows Explorer and to activate the encryption in the file features. The fact that a file is encrypted by far does not mean that it is not available in a non-encrypted form in another place of the hard-disk. EFS only works with individual files and file folders and not with the complete hard-disk. It encrypts neither Temp files, printer spoolers nor the Swap file. Microsoft recommends encrypting the Temp directory, but then the Swap file remains unprotected as well. By »EnCase« tool by Guidance Software, we have found parts of a big text file in a Windows Swap file, which had been encrypted before by EFS.

To delete a file does not mean that it is removed as well. The deleting procedure only removes the pointers to the protected location of the file. Only when the file is overwritten, it is actually deleted. Many of the files deleted before can be overwritten by the user de-fragmenting the hard-disk. Programs like Wipeinfo in the Norton Utilities or »BCWipe« by Jetico delete files and then overwrite every sector the files had required.

File or file folder-based encryption programs have the drawback that the decision whether to encrypt or not is in the hand of the users. But these can easily forget to encrypt a document after work. The only way for actually protecting data is to use programs which encrypt the complete hard-disk. Moreover, these programs have the advantage of even encrypting deleted files, so that nobody needs to worry about overwriting. There are not many systems of that kind, but we have tested some of them.

Encryption Software for Hard-Disks

To protect files, they can either be individually encrypted — file by file of the complete file folder — or a program encrypts the complete hard-disk. Each method has its advantages: If individual files are encrypted by third party software, the user can assume that, when the files are transferred over the network, they only can be opened by the users which have the password and have loaded this software. Otherwise, the encryption of the complete hard-disk prevents data theft if the computer is stolen. Network Computing has taken a closer look at several hard-disk encryption programs: »CyProtect Disk Encryption« by Cyprotect, »iT_SEC_notebook« by IT-SEC, »Encryption Plus Hard Disk« by PC Guardian, »Pointsec PC 4.0« by Pointsec Mobile Technologies, »SafeGuard Easy 3.10.2« by Utimaco and »SecureDoc 3.1« by Winmagic.

The method of encryption on file level is well-known. Conventional encryption patterns include Advanced Encryption Standard (AES), Blowfish and 3DES with key lengths of 56 to 256 bits. All kinds of products for the encryption of individual files and complete file folders are available, including shareware and freeware offers. Several encryption products require that the data is decrypted by the same computer (or key)

which has also been used for the encryption. Other products allow the encryption and decryption with one password. The method actually is determined by the requirements of the users. However, numerous file and file folder encryption products are available on the market, but they are only slightly different from each other.

To protect temporary files, Swap files and printer spools as well, the user has to encrypt the complete hard-disk. As actually the complete disk including the operating system is encoded, the encryption software has to be loaded before the operating system. Normally, the boot loader loads the operating system after the PC has been booting and carrying out the memory test. If now a hard-disk encryption software is installed, it modifies the boot loader which then boots the encryption software and no longer directly Windows. The encryption software authenticates the user and loads Windows if the authentication is successful. Of course, this procedure is much more complicated than the simple encryption of files and file folders. The purpose of the disk encryption products is to protect the data from a thief which lays his hands on the hard-disk and not to protect the data when they are copied or transferred.

The six tested disk encryption products automatically load while the computer is booting and require a user authentication by means of a user name/password or token. Then, they are encrypting the hard-disk. As the operating system is encoded itself, an authentication has to be made before the system is booting. If a user forgets his password, the administrator normally is able to reset it.

The files remain on the hard-disk in an encrypted form, but indeed are transferred over the network in clear text and copied to mobile data media or not-encrypted partitions/drives. Our analysis of the hard-disk after the encryption showed that in fact the complete disk, apart from a little bootstrap code, was encrypted. Features which should be considered at the purchase are multi user support, recovery key, overwriting by administrators, centralized management and integration with PKI and tokens additional to the authentication by user names/password.

There is a difference between the complete drive encryption and a virtual drive encryption. Software which carries out a virtual drive encryption creates an individual encrypted file on a drive which is presented to Windows as a logical, mountable drive. Emulation software (e.g. a Virtual PC on Macintosh computers) and Disk Imaging products have been working this way for years. These virtual drives offer the same level of protection as the encryption on the file folder level — in other words, the Swap file and the temporary files are not encrypted. Here, one has to be careful as the product marketing mostly does not explain this clearly.

WinMagic SecureDoc 3.1

Securedoc encrypts hard-disks by DES, 3DES and AES. Moreover, the product allows the encryption of individual disks by the same key or a key which is used by several users. In the test, we were also able to encode two disks with two different

keys. The advantage is that, by this, data can be protected and can also be hidden from different departments of the organization.

It is a common activity that disks can be encrypted and be shared by a group. Otherwise, the encryption of the disks can also be made for individual users. Instead of being stored on the hard-disk, the encoding key can also be stored on a disk which, apart from the username and the password, for encryption requires this disk as a token as well. Another feature which supports this password is the locking of drives. This way, the access to drives can be prevented. Indeed, the practical value of this feature is challenged when considering that files can simply be loaded via HTTP or FTP. The 3.2 version is based on the PKCS-11 standard and e.g. works with »Datakey-330-PKI« tokens or »iKey 2000« by Rainbow Technologies and over smartcards with PKI solutions by Entrust, Verisign or Baltimore.

Pointsec Mobile Technologies Pointsec PC 4.0

Pointsec-PC, however, includes less features than Securedoc, but still offers numerous options. The product carries out the encryption via Blowfish or CAST. Pointsec-PC allows the administrator to create several users and groups and offers smartcard integration. As with all tested products, it is possible for the administrator to generate a login password to be used once falls a user should forget his password and therefore it has to be changed. Access to individual partitions can be allowed or denied to the users.

Pointsec-PC does not support removable or mobile media. After the product is installed, the initial encryption process runs in the background while Windows is booting. This means that the users can continue to work while the drive is converted into the encrypted format. Apart from the PC-Guardian product, this was also supported by all other products of the test. Considering the fact that the encryption of a 9 GByte hard-disk took several hours in our test, this surely is a useful feature. In the 4.1 version, Pointsec integrates smartcards by Datakey.

CyProtect CyProtect Disk Encryption

The product name »CyProtect Disk Encryption«, in short Cydisk, is misleading as it actually is a program which carries out virtual drive encryption. On the hard-disk of a Windows 2000 or Windows XP system, Cydisk creates an encrypted image file protected by a password which is allocated a drive letter. Then, this file can be used like any normal drive. The algorithm used for the encryption has been developed by the manufacturer itself and is called polymorphic encryption, in short PMC. PMC works quickly and, according to the manufacturer, is more secure than well-known algorithms like DES or AES.

The program does not encrypt files on the hard-disk — it only carries out the encryption when the file is copied or shifted to the encrypted »drive«. However, Cydisk is able to encrypt complete hard-disk partitions as well. To do this, the program formats the selected partition and integrates into the system in an encrypted form. Of course, the formatting destroys all files on this partition. Fortunately, Cydisk has a protection mechanism which prevents the overwriting of partitions which are

already formatted. Also, an encryption of the partition which contains the operating system is impossible; disks and other portable media cannot be encrypted as well.

The access on encrypted »drives« protects an individual password imaged on 256 Bit binary digits and up to 64 characters of length. This password cannot be reset by an administrator or be overwritten by a master password; i.e. a forgotten password means that the data cannot be accessed any longer. The password query is made while the system is booting. If, at this point of time, no password is entered, the system, however, boots the normal way, but the encrypted drives are only made available when they are integrated into the system by entering the password. Altogether, Cydisk can be operated quite simple, but indeed only offers few features.

PC Guardian Encryption Plus Hard Disk

This product was the easiest one as far as operation and administration is concerned, but also offers less features than most of the competing products. The program is restricted to one user login/password combination per computer. The administrator looks in vain for token support or PKI mechanisms and the product only encrypts the primary hard-disk of the systems.

However, installer packages and password overwriting are available. The product seems rather suitable for individual users or smaller organizations, especially for users who wish a package which is easy in configuration. For bigger organizations which require a good key management, multi user and PKI, the product is not particularly suited.

iT_SEC iT_SEC Notebook

IT-Sec-Notebook is able to encrypt complete hard-disks or individual partitions of computers which execute one of the operating systems Windows NT, Windows 2000 or Windows XP. The program makes the encryption algorithms Blowfish, DES, DESX, XOR and IDEA available for the user. The installation of the program takes about one minute. Then, the computer has to be re-booted and the encryption has to be activated. The encryption as such is time-consuming, but fortunately is made in the background. This way, the user is able to use the computer while the hard-disk or selected partitions are encrypted. The encryption of complete hard-disks or partitions is only possible for hard-disks and partitions which are formatted by the NTFS file system.

IT-Sec-Notebook allows the user the switch on a function called Boot-Security which requires to enter a password before Windows is booted. This function, however, has to be installed before the disk is encrypted. The program requires to enter a key or password before a partition is decrypted or the system is booted.

IT-Sec-Notebook does not offer as many features as e.g. SafeGuard Easy, but the program encrypts disks and selected partitions reliably. The administration is made over a program to be used quiet simple which is available in the system control after the installation. As SafeGuard Easy, IT-Sec-Notebook offers an assistant for the

creation of an emergency disk by which the system can be accessed in case of emergency.

In short, IT-Sec-Notebook is an easy-to-operate program without frills which encrypts hard-disks or individual partitions — not less, but not more as well. By the way, the name of the program is not necessarily to be taken literally as IT-Sec-Notebook also encrypts hard-disks and partitions of normal desktop computers in a reliable way. In the next version which, however, was not available when the test was made, IT-Sec wants to revise the installation procedure completely.



Utimaco SafeGuard Easy

SafeGuard Easy supports various different encryption algorithms, e.g. AES with 128 and 256 Bit, Rijndael-256, DES, DES SB-II, Blowfish-8, Blowfish-16 and STEALTH-40. The product works with all current Windows versions including Windows XP and encrypts complete hard-disks, individual partitions, disk and portable media drives (also Plug-and-Play devices) formatted with one of the file systems FAT-12, FAT-16, FAT-32, HPFS, NTFS or NTFS5. However, SafeGuard Easy supports neither the Dynamic Disk which was introduced first with Windows 2000, nor ATAPI Zip drives and PCMCIA hard-disks.

Moreover, it can be observed that the program does not work when both EIDE and SCSI hard-disks are installed in a system and the boot partition is on the SCSI disk. When the computer is switched on, the SCSI disk is disk 0, but the Windows start changes this allocation the EIDE disk becomes disk 0 — a re-numeration SafeGuard Easy cannot comprehend.

The program encrypts 4 hard-disks maximum and, besides the system user who has all rights in the default, supports up to 14 other users of the individual computer. The SAL feature (secure automatic logon) of the program allows a simultaneous logon of the user to SafeGuard and to the operating system. If, however, the pre boot authentication is switched on, which is absolutely recommendable, the user, nevertheless, has to authenticate himself two times.

If a user starts a computer which has an encrypted hard-disk per system disk, CD-ROM or over another hard-disk, SafeGuard Easy blocks the encrypted disk — it is, however, possible to start the system, but the data remains protected. By request, the program can be configured in a way that it is impossible to start the system anyway.

Info

How Network Computing made the test

For the test, we partly used a Dell Optiplex Dual with 600 MHz. The system executed Windows 2000 and had a SCSI hard-disk. Here, we created a big text file with the objective to find out whether this file still could be found or read after the encryption of the hard-disk. With the Guidance software »EnCase 3.19«, we analyzed each sector of the hard-disk before and after the encryption. The program searches the hard-disk sector by sector so that also data which possibly are left in temporary files, swap files and in the sector slack, can be searched and — if available — can be found. We also worked with an IBM Thinkpad 600. For the hard-disk analysis and the search for files, we used the programs »FileRecovery for Windows« by LC-Tech and Xray 1.21 by Omnixray.

The device/disk encryption can be switched on and off short-term during a session, if the user has the respective right. For the configuration of the encryption and the users, an easy-to-operate administration program without frills is available. An emergency disk can be created in a fast and simple way with the help of the assistant. Another assistant creates configuration files which can be used for installations, de-installations and modifications of existing installations.

Result

To make laptop or notebook theft more difficult and to reduce the effects and costs in case of a successful theft, lots of things can be done. Besides products like firewalls, VPN tunnels and anti virus software which protect the data stored on the computers, a hard-disk encryption is recommendable particularly for mobile computers which can be stolen relatively simple. Our »Reference« award was given to »SafeGuard Easy« by Utimaco, as this encryption software has interesting features and showed a good performance, even if it did not get credits concerning the price. [nwc, dj]