WHITEPAPER

ELCOMSOFT
PROACTIVE SOFTWARE

CONTENTS

WHAT IS EFS?

One of the innovations in the Microsoft Windows 2000 and the NTFS 5.0 file system was the Encrypting File System (EFS) technology, which is designed to quickly encrypt files on the computer hard drive.

NTFS by itself has built-in protection. However, as is frequently the case, it very quickly required additional security. The reason was the wide-spread use of NTFSDos-type utilities, which made it easy to circumvent the NTFS security system, gaining access to it through DOS, thus ignoring the set access rights.

The EFS system uses both public and private key encryption and CryptoAPI architecture. EFS can use any symmetrical file encryption algorithm from the following list: Microsoft Windows 2000 used DESX, Windows XP used 3DES, and Windows XP SP1, 2003 and the new Windows Vista use AES.

File encryption does not require the user to execute any preliminary operations. During the first encryption of the file, an encryption certificate and a private key are automatically issued for the user.

One of the distinguishing convenient features of EFS is that the files remain encrypted when they are transferred to a different folder or to a different NTFS drive. If the transfer is to a different file system, the files are automatically decrypted. When the user adds new files to an encrypted folder, they are automatically encrypted. There is no need to decrypt a file before using, since EFS is embedded in the operating system and will execute this function automatically, while observing all security measures.

The creators of EFS have also ensured against the loss of the private key by the user, for example as a result of OS reinstallation, or when new user accounts were created. Here, the specially-designed EFS Recovery Agent can be used to decrypt files. In Windows 2000 the Recovery Agent is represented by either local administrator (when working on a stand-alone computer) or domain administrator (if the computer operates within a domain). In Windows XP and above this had to be done manually.

In this White Paper we will assess the advantages and disadvantages of EFS technology and also review the different options for restoring encrypted data using EFS, in the event of password loss or system failure.

EFS ADVANTAGES AND DISADVANTAGES

EFS technology makes it so that files encrypted by one user cannot be opened by another user if the latter does not possess appropriate permissions. After encryption is activated, the file remains encrypted in any storage location on the disk, regardless of where it is moved. Encryption is can be used on any files, including executables.

The user with permission to decrypt a file is able to work with the file like with any other, without experiencing any restrictions or difficulties. Meanwhile, other users receive a restricted access notification when they attempt to access the EFS encrypted file.

This approach is definitely very convenient. The user gets the opportunity to reliably and quickly (using standard means) limit access to confidential information for other household members or colleagues who also use the computer.

EFS seems like an all-around winning tool, but this is not the case. Data encrypted using this technology can be entirely lost, for example during operating system reinstallation.

We should remember that the files on disk are encrypted using the FEK (File Encryption Key), which is stored in their attributes. FEK is encrypted using the master key, which in turn is encrypted using the respective keys of the system users with access to the file. The user keys themselves are encrypted with the users' password hashes, and the password hashes use the SYSKEY security feature.

This chain of encryption, according to EFS developers, should reliably protect data, but in practice, as explained below, the protection can be ultimately reduced to the good old login-password combination.

Thanks to this encryption chain, if the password is lost or reset, or if the operating system fails or is reinstalled, it becomes impossible to gain access to the EFS-encrypted files on the drive. In fact, access can be lost irreversibly.

Regular users do not fully understand how EFS works and often pay for it when they lose their data. Microsoft has issued EFS documentation that explains how it works and the main issues that may be encountered when encrypting, but these are difficult for regular users to understand, and few read the documentation before starting to work.

DATA CAN BE LOST FOR GOOD

Let's figure out in what situations can EFS-encrypted data can be lost. How dangerous can a situation be? We'll take it from the top.

HOW CAN ONE LOSE ACCESS TO EFS-ENCRYPTED DATA?

Almost all of us have encountered a situation where it was necessary to fully reinstall Windows. This may have been due to the operating system's functioning being disrupted by software failure, a virus attack, or a mistake made by an inexperienced user, the system password for a user account was lost or a user profile was deleted. In this case, all encrypted data in the old configuration would most likely be lost.

Consider the following typical scenarios in detail:

1. **The system is not booting due a component having been replaced or failed or due to operating system failure.** For example, the motherboard is out of order, the boot sector is damaged, system files are corrupted, some "half-baked" updates or a different unstable piece of software was installed. In this case, the hard drive can be connected to a different computer and the data can be read off it, but if it is EFS encrypted, this would not work.
2. **The system administrator at the company or the user has reset the user password.** In this case, access to EFS-encrypted data would also be lost.
3. **The user profile was deleted.** In this case, the files (and the user keys) may still be on the disk, but the system cannot see them, even if the user is recreated with the same name, a different ID will be assigned to the account, which is used in the encryption process. In this situation, access to the data encrypted using EFS will also be lost.
4. **The user is migrated to a different domain** (is authenticated through a different server). If the user encryption keys were stored on the server at the times of the migration (usually this is the case), then an unprofessional migration can result in the loss of access to the EFS-encrypted data.
5. **System reinstallation.** In this case, access to EFS-encrypted data would naturally be lost. If a backup copy of the entire system disk is made at the time, or at least of the user profile ("Documents and Settings"), then access could be restored with the use of special software, but only if the keys are not damaged.

It is fairly common for the system itself to be stored on one disk, while encrypted files are stored on a different disk. When the administrator reinstalls the operating system, usually a backup of just the disk with the data is made and then the system is reinstalled. Obviously, in this case the keys are lost and with them goes the access to encrypted data.

It should be said that there is a straightforward way to avoid this situation, if before using EFS the EFS Recovery Agent is set up, but this, just like the workings of EFS in general, are too complicated for the average user, as demonstrated below.

WHAT IS THE EFS RECOVERY AGENT?

The EFS Recovery Agent is a user with permission to decrypt data, encrypted by another user, if the latter lost the encryption certificate keys or if the user's account was deleted, but the encrypted data is needed.

As a rule, the Recovery Agent is the Administrator, but it can also be a different user. There can be multiple Recovery Agents. In order to assign Recovery Agent permissions to a user, first Recovery Agent certificates need to be created using the command **"Cipher /R: filename"**, where "filename" is the path and name of the created certificates without the extension.

After this, the user will be asked to enter a password to protect the private key and to confirm it (the password is not displayed in the console on entry). Then two files are created with the specified name: ***.cer** and ***.pfx**. These contain the public and private certificate keys, respectively. Now the certificate must be added to the user's personal storage, specified by the Recovery Agent (this step can be skipped, then the Recovery Agent can do it later, when the recovery functions need to be used) importing the file *.pfx (double-click on the file icon to launch the certificate import wizard). Here, the administrator had to open the "Local Security Settings" snap-in (Start - Run - secpol.msc), select "Public Key Policy - EFS" and in the menu "Action" select "Add Data Recovery Agent." The "Add Recovery Agent Wizard," will open, and on the second page one must click on "View folders" and select the *.cer file created earlier.

In order to restore access to the encrypted files after system reinstallation or after a private key had been lost, the Recovery Agents' private keys must be kept in a secure location or (if they are not assigned), the private keys of all users using EFS, by exporting them from the "Private" depository of the "Certificates" snap-in (certmgr.msc). In Windows Vista, there is finally a way to store the keys on a smart card, which is much more reliable in terms of security.

It is clear that this kind of safety measure with the use of the EFS Recovery Agent contradicts its intended principle of simplicity and requires non-trivial, from the average user's point of view, though routine for an administrator, actions and manipulations. It is no surprise that few use it.

It should be noted that if the administrator tried to reset the account password for a local user, the user will lose all private certificates and with them the access to EFS-encrypted files (a corresponding warning will appear when this action is attempted). The same will happen if the local administrator, using special means, tried to force a password change (i.e., without entering the old password).

Consequently, the risk of losing the most important data, encrypted using EFS technology, when there is a system failure or due to an administrator/user error, is rather high and must always be taken into consideration.

WHAT TO DO IN CASE OF SYSTEM FAILURE?

The typical situation in which access to EFS-encrypted data is lost takes place when the connection between the operating system and the keys physically located on the disk (cf. situations described in section "How can one lose access to EFS-encrypted data?") is lost. In this case do not give up, there is a solution. There is high probability that access to the data can be restored. But if the keys had been deleted from the disk and no backup copy of the user profile or the user's certificates had been made, then the data is indeed unrecoverable.

Practice shows that even the export/import of the profile or the certificates proves to be effective: the keys do reappear in the system, but access to the encrypted data is not restored.

If you find yourself in this situation and the EFS-encrypted data has become inaccessible despite the keys having been saved, then it is possible to use a specialized piece of software, which is highly likely to help restore access to the data.

POSSIBLE ACTIONS TO TAKE

Here we will try to describe the various possible actions that could be taken in this situation. You have a few options:

1. Boot using the working user account with administrator privileges, if it exists, and continue with the installation of the special decryption software.
2. Physically disconnect the hard drive and install it on a different workstation running decryption software.
3. Boot up using a different operating system, installed on the same machine, if it is installed, or install it specifically for this purpose.

Most importantly, you need to gain direct access to the disk. If following the first route, this is possible only for users with administrator permissions. This is why when the backup/working user account is insufficient you can try to expand the account permissions.

DATA DECRYPTION SCHEME

Once direct access to the disk has been obtained, it is possible to move on to the next step – directly decrypting and restoring the data. This can be done according to the following plan:

1. Search for and try to decrypt all keys on the hard drive of the problem computer.
2. Search for encrypted files on the hard drive and try to decrypt them.

One of the most effective tools, designed to decrypt EFS-protected data, is the Advanced EFS Data Recovery tool. It can be used to decrypt data on a problem computer, even in the case where some of the user key records are corrupted.

The possibilities and features of Advanced EFS Data Recovery are presented in detail below.

ADVANCED EFS DATA RECOVERY

EFS Data Recovery (AEFSDR) is a specialized software program for decrypting files, encrypted using EFS technology in Microsoft Windows 2000 and Windows XP, Windows 2003 Server and the new Windows Vista environments.

This software tool can be used to decrypt files in record time, even when the system does not load or when some of the encryption key records are corrupted.

Even if the system user database is protected using SYSKEY, Advanced EFS Data Recovery still makes it possible to decrypt the files. In Windows 2000 it is possible to decrypt all files, even if the administrator and user passwords are not known.

Advanced EFS Data Recovery uses a two-step process:

1. The first step is to search for all EFS keys (private and master) and try to decrypt them. The first step involves decrypting at least one key, required for decryption the rest of the files. In Windows XP and above this may require that the user password be entered into AEFSDR, which was used to encrypt the files, or the Recovery Agent password. First the program tries to do this automatically, for example trying to extract the password from cache or system files, checking simple combinations (such as password=username) and then conducts an attack using a medium-sized built-in dictionary.

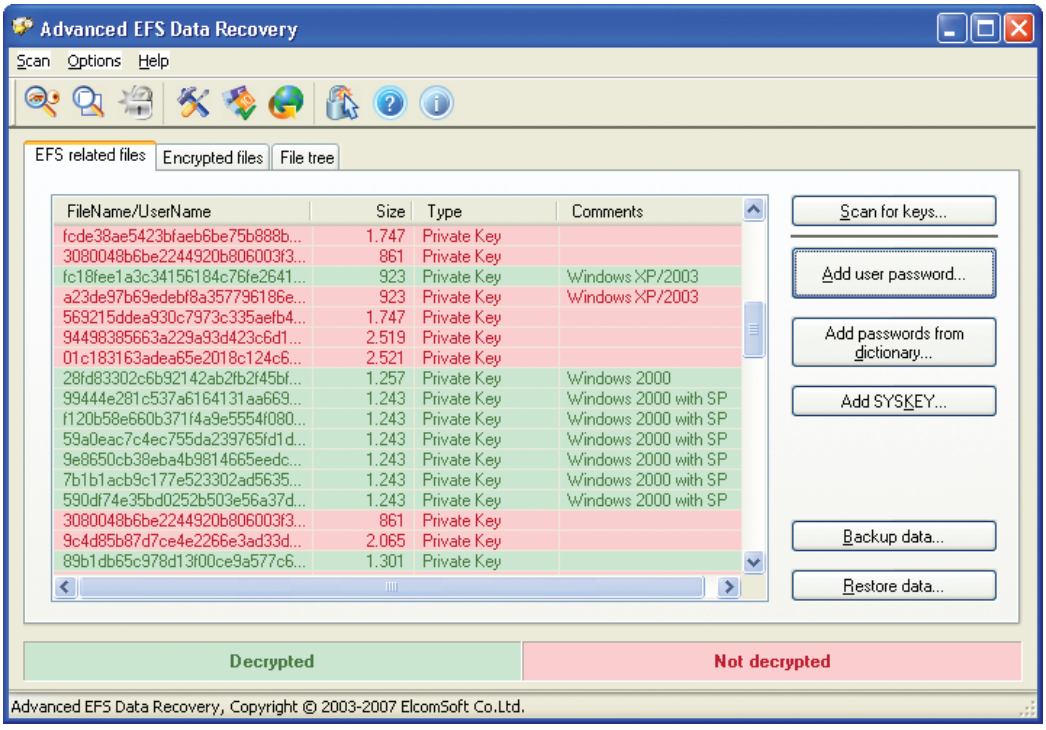

Fig. 1. Tab showing the computer search and decryption of private EFS keys.

2. At the second stage, the program runs a search using the EFS-encrypted files on a hard drive and also attempts to decrypt. If there are few encrypted files and their location is known, the user can manually select these files in the program “File tree” in the interest of saving time.

It may turn out that the keys are stored on the network server, while the files encrypted using those keys are stored locally. In this case, use AEFSDR to first retrieve and decrypt the keys stored on the server and then use the “Backup data” option to save the results to a file and transfer them to the local machine. This way the results of the first stage of the process can be transferred to the machine with the encrypted data to start the second stage of the process.

The file decryption process can take a significant amount of time, so one of the key advantages of Advanced EFS Data Recovery is the ability to manage the system load. The user can chose between three load levels: High, Normal and Low.

Another notable feature is that Advanced EFS Data Recovery fully supports the newest Microsoft Windows Vista operating system as well as Windows Server 2008.

In conclusion, it is important to talk about the effectiveness of the product in question, i.e., the likelihood of successful data decryption. According to the assessment of ElcomSoft experts, Advanced EFS Data Recovery can be used to successfully restore **up to 99%** of EFS-encrypted data, if the user keys are retrieved, which is a very high success rate.

You can download a trial version of Advanced EFS Data Recovery here.

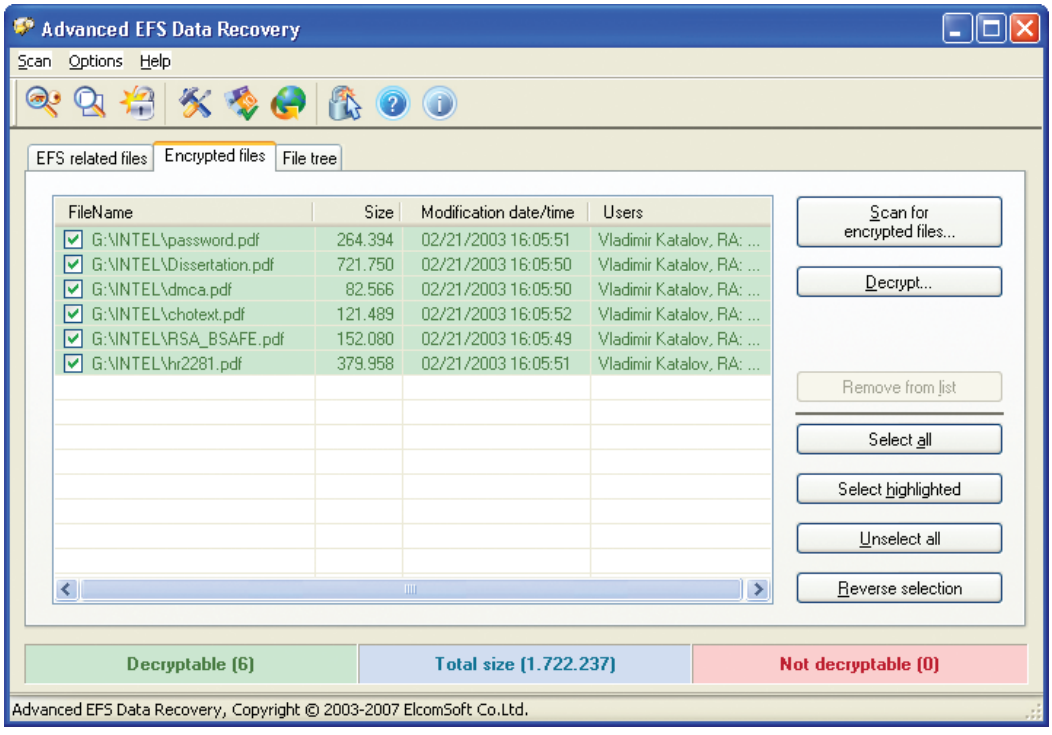

Fig. 2. Tab showing search results and files decryption.

ABOUT ELCOMSOFT

Founded in 1990 in Moscow, Russia, ElcomSoft is a leader in the password/system recovery and forensics market. Thanks to one-of-a-kind technologies, ElcomSoft's products have garnered wide recognition both in Russia and abroad.

ElcomSoft's clients include many well known international companies from the following sectors:

High Tech: Microsoft, Adobe, IBM, Cisco
Governmental: FBI, CIA, US Army, US Navy, Department of Defence
Consulting: Andersen Consulting, Deloitte & Touche, Ernst and Young, KPMG, PricewaterhouseCoopers
Finance: Bank of America, Citibank, Equifax, HSBC, Wells Fargo, J.P.Morgan, Credit Suisse
Telecommunications: France Telecom, BT, AT&T
Insurance: Allianz, Mitsui Sumitomo
Retail: Wal-Mart, Best Buy, Woolworth
Media&Entertainment: Sony Entertainment
Manufacturing: Volkswagen, Siemens, Boeing
Energy: Lukoil, Statoil
Pharmaceuticals: Johnson&Johnson, Pfizer, GlaxoSmithKline, Novartis

ElcomSoft is a Microsoft Gold Certified Partner, Intel Software Partner, as well as a member of the Russian Cryptology Association, the Computer Security Institute (CSI), and the Association of Shareware Professionals (ASP).

ElcomSoft is an acknowledged expert in the password/system recovery and forensics market. The company's technological achievements and opinion leadership is quoted in many authoritative publications. For example: "Microsoft Encyclopedia of Security", "The art of deception" (Kevin Mitnick), "IT Auditing: Using Controls to Protect Information Assets" (Chris Davis), "Hacking exposed" (Stuart McClure).

Visit our website to find out more.

ADDRESS:
Elcomsoft
Zvezdny bulvar 21, office 541
129085 Moscow, Russian Federation

FAX:
US (toll-free): +1 (866) 448-2703
United Kingdom: +44 (870) 831-2983
Germany: +49 18054820050734

WEBSITES:
http://www.elcomsoft.ru
http://www.elcomsoft.com
http://www.elcomsoft.de
http://www.elcomsoft.jp
http://www.elcomsoft.fr