Global Information Assurance Certification Paper

Chuck “Spence” Fasching
SANS Security Essentials
GSEC Practical Assignment
Version 1.2e
“A Discussion of Best Practices for Microsoft’s Encrypted File System”

Introduction

Organizations are purchasing laptops and network connected desktop computers for their users everyday. This allows users to work on the road and bring their work home with them. It allows for the easy sharing of files across the network. It also introduces a new level of risk to organizational data. Laptops that are stolen may have sensitive organizational data on them. Network connected computers are at risk whenever the power is turned on. The challenge to the security professional is to mitigate the risk associated with mobile and network computing and protect organizational assets.

This paper discusses using Microsoft’s Encrypted File System to mitigate the risk associated with mobile and network computing. Specifically, it addresses file system security in relation to encryption and EFS. It will discuss many of the best practices, as recommended by Microsoft and other sources. The goal is to bring a level of understanding to the “why” behind the best practice recommendations and how they may affect an organization.

Assumptions

This paper assumes the reader has a good working knowledge of general security practices. Many of the ideas presented here are based on sound general security practices that have been applied to data encryption. It is also assumed that the reader understands the basics of Public/Private key encryption and encryption in general.

EFS General Information

Microsoft’s Encrypted Files System was designed to encrypt data on hard disks, preventing modification and viewing of that data from un-authorized sources. EFS is closely integrated with NTFS. This integration is so close that it prevents encrypted files from being written to the paging file and can encrypt temporary copies during file creation. By using Microsoft’s CryptoAPI, a public-key encryption scheme, all files are encrypted with a random key, or file encryption key. This key is different and not reliant upon the users public/private key pair, which decreases the risk of cryptanalysis attacks. EFS provides for data recovery of encrypted files in case of certificate / key loss. EFS can not be enabled unless at least one recovery key has been configured.

Best Practices

Avoid using print spool files in your print server architecture, or ensure that print spool files get generated in an encrypted folder.

When files are written to the print spool, they are written to a different location than the data originally was stored. These files are then (temporarily) subject to copying in clear text or modification. By encrypting the print spool folder, the risk to the files is reduced.

Data protection is not just file encryption.

Follow best practice when it comes to file security. Just because a file is encrypted, and can not be modified, does not mean a malicious user can not delete that file. Ensure that the correct file system permissions are assigned to all files. This will reduce the risk of accidental or malicious deletion of files.

Designate two or more recovery agent accounts per Organizational Unit (OU), depending on the size of the OU. Designate two or more computer for recovery, one for each designated recovery agent account, and give permissions to appropriate administrators to use the recovery agent accounts.

Agents that are added after initial implementation will not be able to recover files that were encrypted before their creation. When a file is encrypted via EFS, there are two fields tagged to the file – the Data Decryption Field (DDF) and the Data Recovery Field (DRF). The DDF is used by the owner of the file for decryption and the DRF is used by recovery agents for recovery. If the recovery agent is not in the DRF at the time of encryption, it will not be able to recover the file. By having two recovery agents (a primary and a backup) in the initial implementation, it is assured that one of the agents will be able to recover the file, even if on of the agent certificates becomes lost or corrupted.

Do not destroy recovery certificates or private keys when recovery agents are changed (which should occur periodically). Keep all of them, until all files that may have been encrypted with them are updated.

Take this a step further – never destroy recovery certificates or private keys used by recovery agents if it can be avoided. This will mitigate the risk of losing data if a user has “fallen out of the loop” and not had their encrypted files updated properly. Again, user education here is a must. By educating the users, they are less likely to fall out of the loop and update their files as needed.

Encrypt the "My Documents" folder for all users (%user profile%\My Documents).

The goal of this best practice is to ensure that the common locations that users store files are encrypted. If an organization has file servers that users regularly save data to, these should be encrypted also (unless the data is meant to be shared by other persons in the organization). The basic premise is that any common location that users store files should be encrypted by default. The organization's training program should also include a section on informing users of this policy, so that they may enable encryption for any "non-standard" data locations.

Establish a roaming profile policy.

Roaming profiles are downloaded during the logon process. By default, user's private keys are stored in their profile. The organization should take steps to mitigate the risk of private keys be subverted during the logon process. At first glance this may seem easy – simply encrypt the stream by enabling an IPSec policy on the domain controller. The organization must ensure that IPSec and tunneling are turned on both the client (desktop / laptop) and the Domain Controllers. This will ensure that the download of the roaming profile is indeed encrypted on the wire.

For organizations that have high-risk data, use smart cards, tokens or some other form of two-factor authentication.

Once again this really boils down to enforcing strong authentication. Smart cards can even be programmed to hold EFS credentials – eliminating the need to store them locally. This will further protect encrypted files – users will need to know their PIN and use the smart card for authentication to EFS. This does increase the complexity of the organization's security, and once again, a training program should be implemented.

Implement a network encryption policy.

EFS does support encrypting files on network file servers, but does not protect the data stream. Data will be at risk if a user is copying across a network. By implementing good network data security, an organization reduces the risk that data will be intercepted or tampered with during transit. This applies to network shares as well as remote "trusted" locations. Win200 IPSec with tunneling is a good solution here. By enforcing all communication to be encrypted IPSec, both the data on the fileserver is protected (by EFS) and the data stream is protected (by IPSec).

Implement a strong password policy.

The first step in any strong security environment (whether it is encryption or any other form of security control) is strong authentication. Authentication can take many forms, but in an Active Directory environment, it is generally going to be a

userID matched to a password (something the user has – the userID and something only the user should know – the password). EFS can automatically generate a public-key pair and get that public key certified by a CA (or self signs if there is not CA available). Since this key pair is transparently assigned to the userID, protecting the user's identity is crucial to preventing data theft.

Implement a user-training program.

It is true that EFS can be implemented and used with little to no user intervention. But, it behooves and organization to educate it's users on any security measures that are being put into place. Not all organizations will store private keys or certificates the same way. Some may use smart cards, others simple floppies. It boils down to this: Every organization is different; therefore every organization needs to educate its users on those differences. By training users on an organization's security practices (including file and disk encryption), the organization empowers the user with good security knowledge and practices. A good training program can even get users to embrace security, not view it as a hindrance. By implementing a strong security-training program, an organization closes the gap between their current level of security, and their desired level of security.

Recovery agent certificates should be assigned to special recovery agent accounts that are not used for any other purpose.

This follows the same practice of administrators having their own accounts with "normal" access, and only access administrator accounts when work deems it necessary. Assigning recovery agent (or administrator) access to regular user accounts increases the risk of a recovery agent (or administrator account) being compromised. Be sure that any critical account, whether an administrator account or agent recovery account is protected by strong authentication, such as long passwords / pass-phrases, alpha, numeric and special characters, etc.

Teach users to never encrypt individual files, but only folders.

Programs access and re-write files differently. This best practice will mitigate the risk of a program writing a file to clear text (even temporarily). For example – when Microsoft Word opens a file, it creates a temporary file in the same directory as the original. This is the file the user is actually working with – if only the original file was encrypted, then the temporary file will be written in clear text. If the directory is encrypted, even the temporary file will be encrypted, since the encryption process is transparent to programs at the folder level.

The private keys associated with recovery certificates are extremely sensitive. They should be generated either on a computer that is physically secured, or their certificates should be completely exported to a PFX file, protected under a strong password, and stored on a secure floppy disk.

The reasons behind this practice are straight forward, if not obvious. If a malicious user were to capture the organization's recovery key, then that malicious user could potentially subvert private organizational data. To expand upon this, if the keys are being stored on a physically secured system, then that system should not have network access or at least be on a secure network or VLAN. The machine (or disks) should be in a secure location, such as a locked rack, room or cabinet. If a recovery certificate is generated on a non-secure machine, it should be immediately copied to removable media and removed from the hard disk of the generating machine. When data recovery is needed, the recovery agent can access the secure disk, load it on the system, recover the data and then immediately delete the certificate from the recovered system. Another way to approach this is by requiring users to use a recovery station. Any files that need to be recovered are copied to the station, recovered, and then copied to their original location. The files on the recovery station are then deleted. This will limit the exposure of these files in their decrypted form. Although these steps will increase the work required when recovering data, it will help mitigate the risk of the organization's recovery key falling into the wrong hands. Key recovery, hopefully, will not be an everyday occurrence.

Use an NTFS only policy.

Since EFS only works on NTFS file systems, when an encrypted file is copied to a FAT or FAT32 file system, it is decrypted. By ensuring that all directories are NTFS, the organization also ensures the data is protected, not only by EFS but also by regular NTFS file permission setting.

Users should encrypt the temp directory.

For the very same reasons that users should encrypt folders instead of files, user should encrypt any temporary directory that they know their programs use. Many programs use c:\temp as a default location to write temporary files. This directory should at least be encrypted.

Conclusion

In conclusion, Microsoft's Encrypted File System is a great way for mitigating risk associated with private data in a Microsoft Environment. Although this paper is not an implementation guide to EFS, by following and understanding these best practices, an organization can ensure that their implementation of EFS has indeed mitigated that risk.

References

http://www.infosecuritymag.com/articles/february01/features_applied_crypto.shtml

http://support.microsoft.com/support/kb/articles/q223/3/16.asp

http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=15741&Key=Encrypting%20File%20System%20%28EFS%29

http://www.win2000mag.com/Articles/Index.cfm?ArticleID=19721&Key=Encrypting%20File%20System%20%28EFS%29

http://support.microsoft.com/support/kb/articles/Q254/9/49.ASP

Windows 2000 Server Documentation

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event