7.4.9 File Encryption Facts

Encryption of files, directories, and hard drives provides an additional level of data security. File encryption is part of a layered defense strategy and helps to protect confidential data in the event that system data is hacked, lost, or stolen. There are different methods that can be used to encrypt data or entire hard drives.

This lesson covers the following topics:

- Encrypting File System (EFS)
- PGP and GPG
- BitLocker
- Database encryption

Encrypting File System (EFS)

The Encrypting File System (EFS) was introduced with NTFS version 3 and has been included in every version of Windows since Windows 2000 except for in the Home editions. EFS provides an easy and seamless way for users to encrypt files on their Windows computers. EFS is only used to encrypt individual files and folders.

EFS combines the speed of symmetric encryption with the convenience of asymmetric encryption, using a process called key encapsulation. The process for a user to encrypt a file is as follows:

1. The user accesses Properties and from the General tab clicks **Advanced**. From there, the user selects Encrypt contents to secure data.
2. Windows generates a pseudo-random number called the File Encryption Key (FEK). Windows uses the FEK with the AES encryption algorithm to encrypt the file.
3. The FEK is then encrypted using the user's public key. The encrypted FEK is stored in the file's header in a special location called the Data Decryption Field (DDF).
4. The decryption process is the opposite. The user's private key is used to first unlock the DDF and get the FEK. The FEK is then used to decrypt the file.

The encryption and decryption process relies on the user's password being kept safe. If the user account becomes corrupted or the password is forgotten, any encrypted files are lost. To help remedy this, a data recovery agent (DRA) can be set up. The DRA is simply another account that can decrypt the encrypted files.

- The DRA used to be automatically configured as the system administrator in older versions of Windows. Nowadays, it is no longer automatically set up.
- A local DRA for an individual workstation can be configured through the machine's Group Policy settings.
- A domain-wide DRA can be configured in Active Directory. Only a domain administrator can set up a domain-wide DRA.

Additional security considerations are:

- Decryption keys can be backed up to an external USB drive. This ensures access even if the Windows system completely crashes.

- A file is automatically unencrypted when it is moved or copied to a non-NTFS formatted device or media. A file is also automatically unencrypted when you copy a file over the network using the SMB Protocol.
- Key security relies on the user having a strong password and following proper password security protocols.

PGP and GPG

GNU Privacy Guard (GPG) is an encryption tool that encrypts emails, digitally signs emails, and encrypts documents. GPG is an implementation of the Pretty Good Privacy (PGP) Protocol. PGP is a commercial product that is now owned by Symantec and makes products that can be used to protect laptops, desktops, USB drives, optical media, and smartphones.

Both PGP and GPG do the following:

- Follow the OpenPGP standard (RFC 4880) for encrypting and decrypting data.
- Combine asymmetric and symmetric cryptography. The process is as follows:

1. GPG/PGP generates a random symmetric key and uses it to encrypt the message.
2. The symmetric key is then encrypted using the receiver's public key and sent along with the message.
3. When the recipient receives a message, GPG/PGP first decrypts the symmetric key with the recipient's private key.
4. The decrypted symmetric key is then used to decrypt the rest of the message.

GPG supports many common algorithms including RSA, DSA, 3DES, IDEA, MD5, SHA, and more. AES is used by default.

PGP can use either RSA or the Diffie-Hellman algorithm for asymmetric encryption and IDEA for symmetric encryption.

BitLocker

BitLocker was introduced in Windows Vista and is used to encrypt an entire volume, not just individual files and folders. BitLocker is designed to protect all data on a volume even if the hard drive is moved to another computer.

BitLocker Options	Description
Partitions/volumes	When setting up BitLocker, the hard disk must be configured with two partitions – the System and Boot. • The system partition (system volume) contains the boot loader. This is a piece of software responsible for booting the operating system. This partition holds the boot sector and is marked active. • The boot partition (boot volume) is the partition that contains the operating system folder and all personal files and programs. With BitLocker, only the boot partition is encrypted.

Encryption options	When setting up BitLocker, you can choose how much of the drive should be encrypted. Options include: ▪ Encrypt used disk space only - Introduced with Windows 10, this option only encrypts the portion of the drive that is currently in use. As data is written to the drive, it is encrypted. This method speeds up the encryption process and is recommended for new drives. ▪ Encrypt entire drive - This is recommended for drives that are already in use. However, this process can take a very long time depending on the size of the drive. This process encrypts all data, even data that may have been deleted but still remains hidden on the drive.
TPM chip	BitLocker utilizes the computer's Trusted Platform Module (TPM) chip. The TPM chip is built onto the motherboard and generates and stores encryption keys to protect boot files. If the hard drive is moved to another computer, the encryption keys won't match and the data on the drive cannot be accessed. (The TPM chip must be at least version 1.2 for BitLocker to use it.) BitLocker can be enabled without a TPM chip, but boot files will not be encrypted. To use BitLocker without the TPM chip, the user will need to use a startup USB key or have a system volume password enabled to boot into Windows. This option is enabled through the following policy: Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives
Data recovery	During the process of enabling BitLocker, Windows generates the recovery key. The recovery key is different from the user-generated password that is created during the setup process. This is a randomly generated key that can be used to recover data in the following instances: ▪ Moving the hard drive to a new system ▪ Changes are made to startup files ▪ BitLocker goes into a locked state The recovery key is extremely important and should be backed up in multiple places. BitLocker gives the following options to back up the key: ▪ Personal Microsoft Account ▪ USB flash drive ▪ File (the file cannot be saved to an encrypted drive) ▪ Print the key out ▪ If the computer is on an Active Directory network, the recovery key can be saved in Active Directory A special user account called the data recovery agent (DRA) can be created and can decrypt any encrypted data drive on the network. If the hard drive contains the operating system files, it will need to be installed on another system as a data drive before the DRA can decrypt it.

Database Encryption

Today, many organizations store sensitive data such as customer billing information in databases.

Keeping this data encrypted helps protect it if a hacker ever gains access to the database. Databases consist of multiple tables that use columns and rows to store data.

The following table describes the three main methods of data encryption:

Database Encryption Method	Description
Transparent Data Encryption (TDE)	TDE encrypts the entire database and all backups. ▪ Encrypts data at rest, which is data not being currently used. ▪ This method is called transparent because when an authorized user needs to access the data, it is automatically decrypted so the user does not see the process or need to do anything extra.
Column-level encryption	Column-level encryption allows the administrator to encrypt each column separately. ▪ Each column is encrypted using a different key, which increases security. ▪ Column-level encryption causes a hit to the performance of the database.
Application-level encryption	In application-level encryption, the program that is used to create or modify the data is responsible for encrypting the data. ▪ Data is encrypted before it goes into the database. ▪ The resources required to set up this method can be prohibitive.