13.8.2 File Encryption Facts

Encryption is the process of scrambling data to make it unreadable except to those who have the required key to unlock the obscured data. You should be familiar with the following types of encryption.

Method	Description
File Encryption	File encryption encrypts individual files so that only the user who created the file can open it. ▪ The Encrypting File Service (EFS) on Windows systems encrypts individual files. Windows automatically decrypts a file when the file owner accesses it. ▪ With EFS, you can add other users who are also allowed to access the encrypted file. ▪ EFS is available only on NTFS partitions. Moving an encrypted file to a non-NTFS partition removes the encryption. ▪ Files remain encrypted and inaccessible even when the drive is moved to another computer or if another operating system is used. This is because the encryption keys needed to decrypt the file do not exist on these other systems. ▪ Encryption cannot be used together with compression (you can use either, but not both).

Disk Encryption	Whole disk encryption encrypts the entire contents of a hard drive, protecting all files on the disk.
	▪ During system startup, a special key is required to unlock the hard disk. Without the key, data on the drive is inaccessible. Providing the key allows the system to decrypt files on the hard drive.
	▪ You cannot access the contents of an encrypted drive by moving it to another computer because the encryption keys needed to decrypt the data do not exist on the other computer system.
	▪ Most solutions provide for a backup recovery key that can be used to unlock the drive if the original key is lost. If both the encryption key and the recovery key are lost, data cannot be retrieved.
	▪ BitLocker is a Microsoft solution that provides whole disk encryption. BitLocker is supported on Ultimate or Enterprise editions of Windows.
	▪ You can implement BitLocker with or without a Trusted Platform Module (TPM).
	  ▪ When using BitLocker with a TPM, the key required to use the disk can be stored in the TPM. This means that the computer can boot without a prompt as long as the hard drive is in the original computer.
	  ▪ Without a TPM, the startup key must be stored on a USB drive.
	  On Windows 10, you can also supply a password at system boot to unlock a BitLocker-encrypted drive.
	  ▪ When the startup key is saved in the TPM, you can require an additional PIN or startup key that must be used to start the system.
	▪ You can use BitLocker to encrypt removable storage devices (such as USB flash drives).

Data Transmission Encryption	Data that is sent through a network can potentially be intercepted and read by an attacker. Use some form of encryption to protect data sent through a network. You should be aware of the following solutions to protect data communications. ▪ A virtual private network (VPN) uses an encryption protocol to establish a secure communication channel between two hosts, or between one site and another site. Data that passes through the unsecured network is encrypted and protected. ▪ IPsec, PPTP, and L2TP are common protocols used for establishing a VPN. ▪ Secure Sockets Layer ((SSL) is a protocol that can be added to other protocols to provide security and encryption. For example, HTTPS uses SSL to secure Web transactions. ▪ Use WPA, WPA2, or WEP to secure wireless communications, which are highly susceptible to eavesdropping (data interception). WEP, WPA Personal, and WPA2 Personal use a common shared key configured on the wireless access point and on all wireless clients. ▪ When implementing network services, do not use protocols such as FTP or Telnet that pass logon credentials and data in clear text. Instead, use a secure alternative such as FTP-S or SSH.