15.3.3 Disk and Email Encryption Facts

Encryption is an increasingly common practice used for laptops, mobile devices, emails, files, and system backups. Encryption is often required for legal and security measures. Due to the complexity of encryption and the ever-growing amounts of data involved, the impact on performance may be an issue. This is especially a concern with mobile devices where performance is a top priority and the need for encryption is greater. Performance may have to be impacted when the need for data security is of greater importance or legally required.

This lesson covers the following topics:

- Disk encryption
- Disk encryption tools
- Email encryption
- Email encryption tools

Disk Encryption

Disk encryption software or hardware protects data stored on disk by converting it into an unreadable code. Disk encryption works on entire hard drives just as encryption works on files or messages. Using a disk encryption program, you can protect any information you copy onto the disk. The three advantages of disk encryption are:

- The location of data stored on a disk is protected because the disk cannot be viewed by unauthorized users. The location is protected using cryptography, passphrases, or hidden volumes.
- Volume encryption works even when the OS is not active.
- All data you burn to a Blue-ray, DVD, or backup disk is safeguarded.

Disk Encryption Tools

Disk encryption tools include the following:

Tool	Description
VeraCrypt	VeraCrypt is software for establishing and maintaining an encrypted volume for data storage devices. VeraCrypt uses on-the-fly encryption, meaning the data is automatically encrypted immediately before it is saved and decrypted immediately after it is loaded. It requires no user intervention.
Symantec Drive Encryption	Symantec Drive Encryption provides organizations with complete, transparent drive encryption for all data, including user files, swap files, system files, and hidden files on laptops, desktops, and removable media.
Windows Encrypting File System (EFS)	EFS is a proprietary function of the Windows operating system.
BitLocker	Bitlocker is a Windows drive encryption feature that offers additional protection of EFS or non-EFS volumes. Bitlocker: - Provides the most protection when used with a Trusted Platform Module (TPM). A TPM is used to validate the integrity of system boot components. - Encrypts all user and system files, including OS, swap, and hibernation files. - Allows recovery keys to be archived to USB, file, print, or Active Directory. - Supports multi-factor authentication.

Email Encryption

Emails can contain sensitive information about the organization that can cause huge losses if infiltrated by unauthorized entities. Encrypting emails can eliminate these threats. Digital signatures are a common encryption method. A digital signature adds increase protection by encrypting the signed email for confidentiality, which also serves as a means of nonrepudiation. Nonrepudiation ensures a sender proof of delivery, and the recipient is assured of the sender's identity. Hashing the message can also be used to protect message integrity.

Email Encryption Tools

Tool	Description
Secure Sockets Layer (SSL)	SSL is an Application layer protocol developed for managing the security of message transmission on the internet. It uses RSA asymmetric, or public key, encryption to encrypt data transferred over SSL connections. Within the client message, there are a few components you should be aware of: the SSL version, the encryption algorithms, compression algorithms, and key exchange algorithms.
Transport	

Layer Security (TLS)	The TLS protocol establishes a secure connection between a client and a server to ensure the privacy and integrity of information during transmission. It uses the RSA algorithm with 1024 and 2048 bit strengths. TLS is a replacement for SSL. It allows the client and server to authenticate each other, select encryption algorithms, and exchange symmetric keys prior to data exchange. The TLS Record Protocol provides secured connections with an encryption method, such as Data Encryption Standard (DES).
OpenSSL	OpenSSL is an open-source cryptography toolkit that implements SSL and TLS network protocols and the related cryptography standards required by them. The core library, written in the C programming language, implements the basic cryptographic functions and provides various utility functions. Keyczar is an open-source cryptographic toolkit designed to make it easier and safer for developers to use cryptography in their applications. It supports authentication and encryption with both symmetric and asymmetric keys.