Encrypting the Private Files on Your Computer
Presentation by Eric Moore, CUGG
June 12, 2010

I. File Encryption Basics
   A. Encryption replaces data within a file with "ciphertext" which resembles random data
   B. May be applied at the file, folder, or drive level
   C. Access requires providing a password or "key"
   D. Provides protection of sensitive data from prying eyes
   E. May be an integrated part of the operating system or a third-party add-on product

II. Encrypting File System (EFS)
   A. Overview
      i. Feature of NT File System (NTFS)
         a. Automatically installed with Windows
         b. Works behind the scenes (transparent to the user)
         c. May be applied to individual files or entire folder contents
      ii. Fully supported in Windows Vista/7 Ultimate and Enterprise
      iii. Partially supported in other Windows versions—user can only decrypt files
      iv. Not supported in Windows 95, 98, or non-Windows operating systems
      v. Uses RSA encryption
   B. How EFS Works
      i. Encrypted files are accessible only the owner and designated recovery agent(s)
      ii. Encrypted files are displayed in green text
      iii. Encrypted files cannot be copied to non-NTFS volumes without proper credentials
      iv. Changes to a file in an encrypted folder are automatically encrypted
      v. Changes to a file not otherwise in an encrypted folder may not be encrypted
   C. Limitations
      i. Cannot encrypt the Windows OS partition
      ii. Any file in computer memory is not encrypted
      iii. Encryption does not carry over to:
         a. Non-encrypted folder
         b. Non-NTFS volume (FAT, FAT32)
         c. CD, DVD, flash drive, backup tape
            - Exceptions: flash drives and external hard drives that are formatted with NTFS
      iv. Slows file access; not appropriate for frequently modified files

v. Incompatible with NTFS compression (only one or the other may be used on a particular file)
vi. Files may still be deleted, moved, or renamed by anyone with appropriate permissions
vii. Files are not encrypted when transmitted over a network connection or by e-mail

D. Best Practices
i. Encrypt entire folder contents rather than individual files
ii. Recommended folders/files to encrypt:
a. My Documents
b. Temp files
c. E-mail stored on your computer (consult with the vendor as to where on the hard drive your e-mail is stored)
d. Paging file
iii. Back up and remove the recovery certificate
a. Reason: You will need it if Windows is unbootable, your account is deleted, or your password is changed by the administrator
b. Where: Store it in a secure place; make a back up copy to be safe

III. BitLocker
A. Overview
i. Only available in Windows Vista/7 Ultimate and Enterprise
ii. Encrypts entire system partition (usually the "C" drive)
iii. System Requirements
a. 1.5 GB partition to store the encryption key
b. Trusted Platform Module (TPM) 1.2 microchip and BIOS support
- Supported in many 2006 and newer laptops
- Alternative: USB flash memory drive
iv. Uses AES encryption

B. Installation Steps
i. Create two partitions: 1.5 GB (S:) and another for Windows (C:)
ii. Install Windows to the system partition, C:
iii. Enable the TPM in BIOS
iv. Turn on TPM support with TPM Management Console (`tpm.msc`)
a. Alternative: Use a flash drive
v. Enable BitLocker through the BitLocker control applet
vi. Store the recovery key password on a USB drive

C. How It Works
i. Must provide a PIN or flash driver before Windows will boot
ii. Cannot bypass with the Recovery Environment
iii. Cannot bypass by placing the drive in another computer
a. It will appear as an unformatted drive/partition of 0 MB

D. Advantages

i. Uses AES, an industrial-strength encryption technology
ii. User must provide PIN or flash drive before Windows will boot
iii. Recovery possible only if you have:
    a. Drive label
    b. System drive letter
    c. BitLocker encryption date
    d. Key file name
iv. Files on a BitLocker partition may be compressed with EFS for an additional layer of security

E. Limitations
i. Backups are not encrypted
ii. Files copied to other media such as USB flash drives are not encrypted
iii. Setup is for the technically savvy; must be comfortable with partitioning utilities and installing Windows
iv. Only available in more expensive versions of Windows
v. Only secures the system partition
    a. Exception: BitLocker To Go for Windows 7 can secure USB drives

F. Suggested Use
i. Protect the system partition with BitLocker
ii. Use EFS, TrueCrypt, or other encryption software to protect other partitions
iii. May make most sense for a laptop that frequently travels

IV. TrueCrypt
A. Overview
i. Made by TrueCrypt Foundation
ii. Free open-source encryption software for Windows 7/Vista/XP/2000, Mac OS X, and Linux
iii. Uses:
    a. Create a virtual encrypted disk (no partitioning required)
    b. Encrypt an entire partition or storage device such as a USB flash drive or hard drive
    c. Encrypt your Windows partition
    d. Create a hidden volume or operating system for plausible deniability
        - Free space is always filled with random data, so no one can prove you have hidden data in said volume
iv. Encryption is transparent to the user
v. Optimized so file decryption begins before the entire file is loaded into RAM
vi. Supported algorithms: AES-256, Serpent, and Twofish
vii. Supports keyfiles
    a. May improve protection against brute force attacks
    b. May be stored on a secure device such as a security token or smart card

c. Multiple users may access the volume, each with a different password
d. Shared access (multiple users must present their keyfiles before mounting the volume)

B. Virtual Encrypted Disk
i. May be used as another disk on your computer, although the contents are actually stored within a file
ii. May be created on any drive for which you have permission to create and modify files
iii. "Mounting" the virtual disk requires a password or keyfile
iv. After working with files, dismount it to lock other users out

C. Encrypted Volume
i. Encrypt existing contents or erase and reformat
ii. Can create a new partition on a hard drive
iii. Unless mounted, it appears to Windows to be an unformatted device

D. System Encryption
i. Encrypt the system partition (C: drive)
ii. When computer starts, the TrueCrypt Boot Loader screen prompts for your password
iii. Computer can also be booted from a TrueCrypt Boot Disk (CD or DVD)
iv. Unless the password or key file is provided, it appears to Windows to be an unformatted device

E. Limitations
i. Can only encrypt a system drive with nothing but primary partitions; logical partitions are not supported
ii. Cannot encrypt a system disk converted to a dynamic volume
iii. Passwords can only consist of printable ASCII characters (text, numbers, punctuation)
iv. Issues with system encryption of Windows XP systems
v. Volume Shadow Copy is only supported for system encryption
vi. Encrypted systems cannot be upgraded (for example, from Windows XP to Windows Vista)
vii. Files transferred over the network or by e-mail are not encrypted
viii. File copied to non-encrypted volumes are not encrypted
ix. Cannot open encrypted data on a computer that doesn't have TrueCrypt

V. AxCrypt

A. Overview
i. Made by Axantum Software AB
ii. Free open-source encryption software for 32- and 64-bit versions of Windows
iii. Double-click to edit or view the file
iv. Automatic re-encryption after modification
v. Can create executable encrypted files

vi. AES encryption with 128-bit keys
vii. Supports keyfiles

B. Advantages
   i. Any encrypted file may be saved to any other media or shared by e-mail without losing privacy
   ii. Creating an executable allows the file to be used on other Windows computers that do not have AxCrypt
   iii. Easy to install
   iv. Fully integrated with Windows Explorer; no configuration necessary
   v. Integrated file shredder (securely delete files)
   vi. Encrypted files may be given anonymous names

C. Limitations
   i. Cannot encrypt folders
   ii. Cannot encrypt entire partitions

VI. Concluding Thoughts

A. Whenever possible, do not store sensitive information on your hard drive. Store it on removable media such as a flash drive that is kept in a secure place.
B. Encrypt flash drives that you frequently use away from home.
C. Encrypt your backups
D. Encrypt your e-mail communications with a product such as PGP
E. Be aware that access to encrypted data and programs will be slower than without encryption
F. No encryption technology is 100% secure
   i. New methods for cracking or circumventing encryption are being developed
   ii. Computers are becoming faster every year
G. Use strong passwords
H. Avoid password reuse—use different passwords for different drives and products
I. For added security, use a multilayered encryption approach
   i. Use EFS within a TrueCrypt volume
   ii. Use AxCrypt to encrypt files within an EFS folder or TrueCrypt volume
   iii. Use EFS/AxCrypt on a BitLocker volume
   iv. Et cetera...

Further Reference

Encrypting File System

The Encrypting File System (TechNet article)
http://technet.microsoft.com/en-us/library/cc700811.aspx

What is Encrypting File System (EFS)?
http://windows.microsoft.com/en-us/windows-vista/What-is-Encrypting-File-System-EFS

Best Practices for the Encrypting File System
http://support.microsoft.com/kb/223316

Create a Recovery Certificate for Encrypted Files
http://windows.microsoft.com/en-US/windows-vista/Create-a-recovery-certificate-for-encrypted-files

Recover Encrypted Files or Folders
http://windows.microsoft.com/en-us/windows-vista/Recover-encrypted-files-or-folders

Back up Encrypting File System (EFS) Certificate
http://windows.microsoft.com/en-us/windows-vista/Back-up-Encrypting-File-System-EFS-certificate

Prevent Data Theft with Vista's EFS and BitLocker (TechRepublic article)
http://articles.techrepublic.com.com/5100-10878_11-6162949.html

Share Encrypted Files (Windows Vista)
http://windows.microsoft.com/en-US/windows-vista/Share-encrypted-files

Certificates: frequently asked questions
http://windows.microsoft.com/en-US/windows-vista/Certificates-frequently-asked-questions

Special Edition Using Microsoft Windows Vista by Robert Cowart and Brian Knittel (Que Publishing, 2007)

BitLocker

Explore the Features: BitLocker Drive Encryption
http://www.microsoft.com/windows/windows-vista/features/bitlocker.aspx

What's the difference between BitLocker Drive Encryption and EFS?

http://windows.microsoft.com/en-US/windows-vista/Whats-the-difference-between-BitLocker-Drive-Encryption-and-Encrypting-File-System

BitLocker To Go for Windows 7 (TechRepublic article)
http://blogs.techrepublic.com.com/window-on-windows/?p=1176

BitLocker Drive Encryption Step-by-Step Guide for Windows 7
http://technet.microsoft.com/en-us/library/dd835565(WS.10).aspx

Enable/Disable BitLocker Drive Encryption in Windows 7 (includes pictures)
http://www.techtalkz.com/windows-7/515981-enable-disable-bitlocker-drive-encryption-windows-7-a.html

How to enable/disable BitLocker Drive Encryption in Windows 7
http://www.windows7home.net/how-to-enabledisable-bitlocker-drive-encryption-in-windows-7/

Paul Thurrot's SuperSite for Windows: BitLocker To Go
http://www.winsupersite.com/win7/ff_bltg.asp

Enable BitLocker without TMP chip in Windows 7
http://nogitech.wordpress.com/2009/07/09/enable-bitlocker-without-tpm-chip-in-windows-7/

Special Edition Using Microsoft Windows Vista by Robert Cowart and Brian Knittel (Que Publishing)

TrueCrypt

Product Web Site
http://www.truecrypt.org/

Online Documentation
http://www.truecrypt.org/docs/

AxCrypt

Product Web Site
http://www.axantum.com/

Online Documentation
http://www.axantum.com/AxCrypt/Default.html

Strong Passwords

Microsoft's recommendations for creating strong passwords
http://www.microsoft.com/protect/fraud/passwords/create.aspx

How to Create Strong Passwords That You Can Remember Easily
http://www.makeuseof.com/tag/how-to-create-strong-password-that-you-can-remember-easily/

Gibson Research's Password Generator (online utility)
https://www.grc.com/passwords.htm

Strong Password Generator (online utility)
http://strongpasswordgenerator.com/

PC Tools Random Password Generator (online utility)
http://www.pctools.com/guides/password/

E-mail Encryption

Pretty Good Privacy (PGP)
http://www.pgp.com/

GNU Privacy Guard (GnuPG)
http://www.gnupg.org/

Miscellaneous

Windows Volume Shadow Copy
http://en.wikipedia.org/wiki/Shadow_Copy

Advanced Encryption Standard (AES)
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Rivest-Shamir-Adleman (RSA) encryption
http://en.wikipedia.org/wiki/RSA

Serpent Encryption Algorithm
http://en.wikipedia.org/wiki/Serpent_encryption_algorithm

Twofish Block Cipher
http://en.wikipedia.org/wiki/Twofish

How to Format USB Drive and Memory Stick with NTFS
http://www.online-tech-tips.com/computer-tips/format-usb-ntfs/