COURSE TECHNOLOGY
CENGAGE Learning

A+ Guide to Managing and Maintaining Your PC, 7e

Chapter 20
Security Practices

Objectives

- Learn how to protect against and remove malicious software
- Learn how to implement security using Windows
- Learn how to use BIOS security features

Controlling Access to Computer Resources

- Types of access control
  - Controlling access to data folders and files
  - Hiding network resources
  - Using encryption technologies
    - Windows Encrypted File System (EFS)
    - BitLocker Encryption
  - Using BIOS features to control security

Controlling Access to Data Folders and Files

- Permissions are assigned to individual user accounts or user groups
  - Vista user accounts: Administrator, Standard, Guest
  - Windows XP accounts: Administrator, Guest, Limited, Power User, Backup Operator
  - You can also create account groups
- Access control based on job descriptions
  - Create user group for each job class and assign data permissions
- Default user groups
  - Authenticated Users, Everyone, Anonymous users

Controlling Access to Data Folders and Files (cont'd.)

- Applying Concepts example:
  - Controlling access to files and folders
    - Step 1: Create folders, user accounts, and user groups
    - Step 2: Set permissions for local users
    - Step 3: Share the folders on the network
    - Step 4: Test and go live

Controlling Access to Data Folders and Files (cont'd.)

- Tips on using shared folders
  - Monitor user permissions: consider read-only access
  - Use Advanced Security Settings box
  - Subfolder assigned inherited permissions
    - Change via parent folder
  - Permissions manually set for a subfolder or file
    - Override inherited permissions
  - Ensure each user account needs a password
  - Remote computer users need same user account and password

Controlling Access to Data Folders and Files (cont'd.)

- Tips to troubleshoot problems
  - Verify Vista Network and Sharing Center settings
  - Verify Windows XP Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks
  - Verify local user accounts and passwords match on local and remote computers
  - Verify remote user is assigned share permissions to access the file or folder
  - Place users in the same workgroup for performance
  - Map network drives for heavily used shared folders

Hidden Network Resources and Administrative Shares

- Enhance security for a computer
  - Disable File and Printer Sharing
  - Hide a shared folder: $ at end of folder name
  - Make Windows XP personal folders private
  - Local share: folders on a computer shared with others using a folder's Properties box
  - Administrative shares: folders shared by default on a network that administrator accounts can access
    - %systemroot% folder: most likely C:\Windows
    - Any volume or drive: \\BlueLight\C$
  - Do not share all the drives on all computers

Encrypting Files and Folders

- Encrypting File System (EFS) certificate
  - Required to decrypt the files
- NTFS file system
  - Used on drive holding the encrypted file or folder
- EFS encryption
  - Public key and private key created
  - Recovery key created for administrator use
    - Unlock encrypted file or folder if user key not available

Encrypting Files and Folders (cont'd.)

- Encrypt a file or folder
  - Right-click folder or file, select Properties
  - In General tab click Advanced button
  - Check Encrypt contents to secure data, click OK
    - In Properties window click Apply
    - Make choice about encrypting subfolders

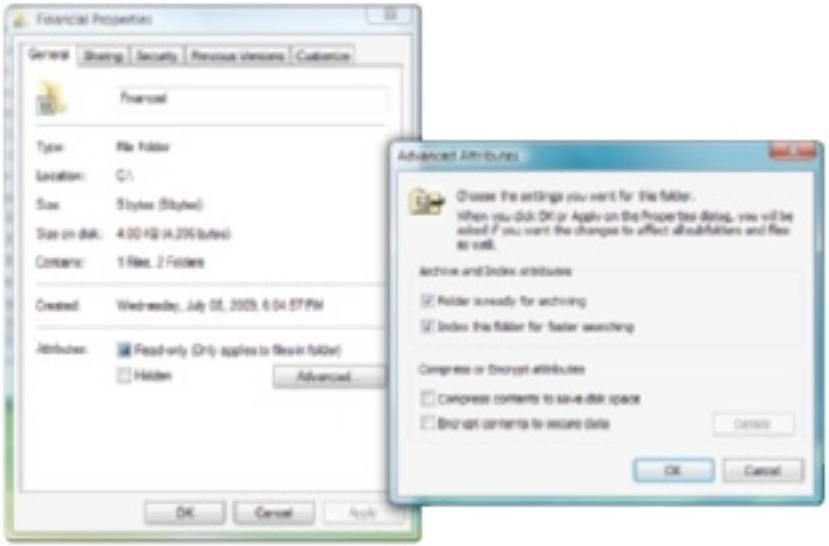

Figure 20-17 Encrypt a file or folder using the Properties box
Courtesy: Course Technology/Cengage Learning

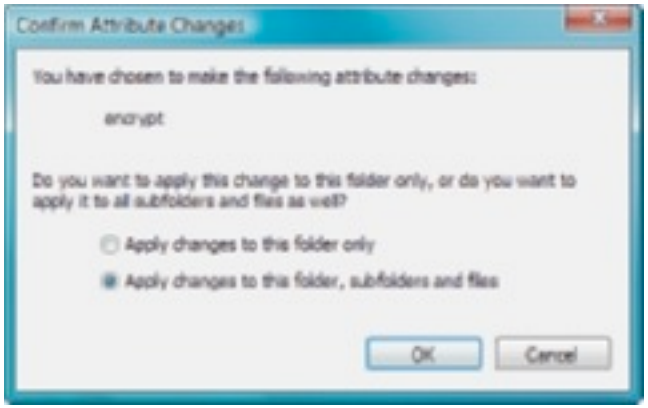

Figure 20-18 Encryption can apply to subfolders or just to the one folder
Courtesy: Course Technology/ Cengage Learning

Encrypting Files and Folders (cont'd.)

- Decrypting methods
  - File's Properties box General tab
    - Click Advanced
    - Uncheck Encrypt contents to secure data
  - Move file or folder
    - To another computer on the network, a flash drive, a FAT volume
  - Cipher command in a command prompt window
    - Used to encrypt, decrypt, or recover encrypted file when the certificates lost
    - Example: cipher /d C:\filename.ext

Encrypting Files and Folders (cont'd.)

- Back up EFS certificates
  - Stand-alone computer EFS encrypting process
    - Generates a self-signed digital certificate used for encryption
    - Contains public key needed to decrypt the file or folder
    - Create backup copy of the certificate and private key
  - Certificates are managed using Certificate Manager (certmgr.msc) console

Encrypting Files and Folders (cont'd.)

- Give other local users access to your encrypted files
  - Requires addition of another user's certificate to the encrypted files
  - Other user can export certificate for installation onto local users computer
    - Export only the certificate (not the private key)
    - Certificate file without private key has a .cer file extension and is not password protected
    - Install (import) certificate on local computer, add the certificate to each selected encrypted file

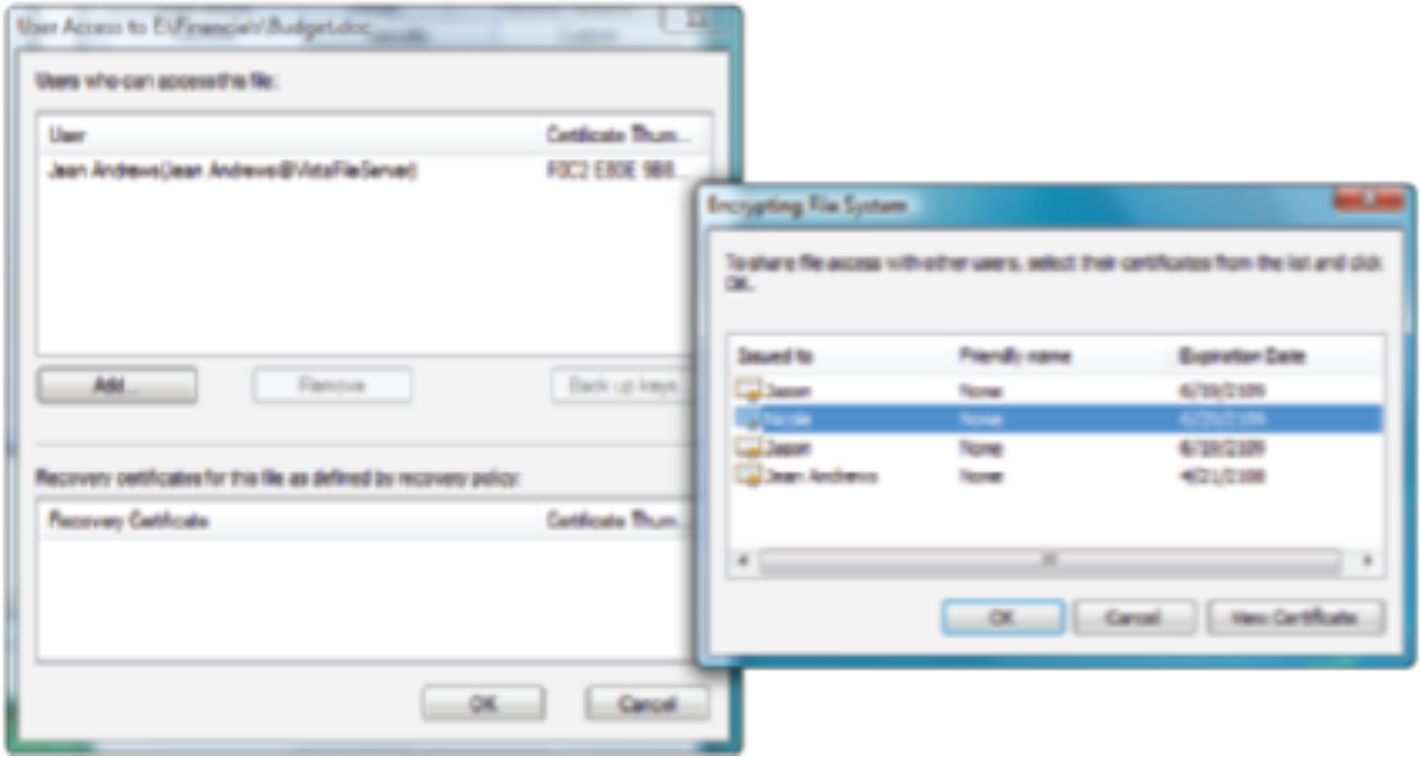

Figure 20-24 Add an installed certificate to a file
Courtesy: Course Technology/Cengage Learning

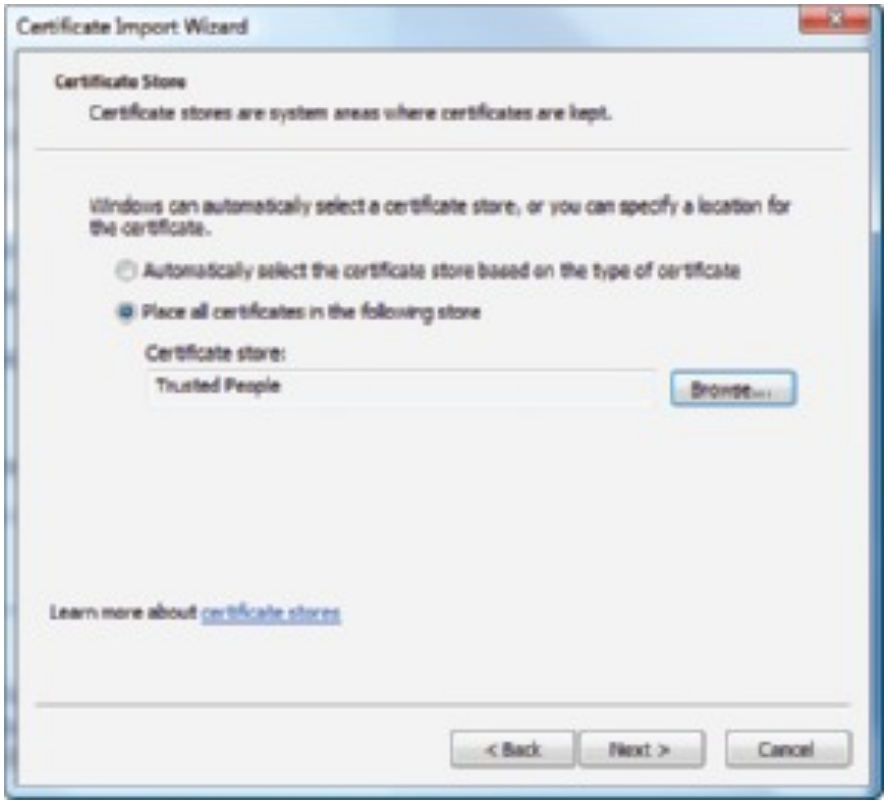

Figure 20-25 Place another person's certificate in your Trusted People store. Courtesy: Course Technology/Cengage Learning

Encrypting Files and Folders (cont'd.)

- Solve problems with encrypted files
  - No access after new version of Windows
    - Use backup copy of certificate
  - No access to file encrypted by another user
    - Other person must add user's certificate to the file
  - No access after Windows Easy Transfer process
    - Export certificate from original computer, install it on the new computer, and add certificate to the files
  - Encrypt contents to secure data check box dimmed
    - Encryption not supported

Encrypting Files and Folders (cont'd.)

- Solve problems with encrypted files (cont'd.)
  - Advanced button missing on General tab of a file or folder properties box
    - Volume not using the NTFS file system
  - Certificate corrupted and no backup certificates exist
    - Recover the file using a recovery certificate
    - Must be logged on as an administrator
    - Process includes using Cipher command to create a recovery certificate, using Group Policy to install recovery certificate, using another Cipher command to add recovery certificate to encrypted file

Using BitLocker Encryption

- Encrypts entire Vista Enterprise/Ultimate volume and any other volume on the drive
  - Works in partnership with file and folder encryption
- Three ways to use BitLocker Encryption
  - Computer authentication
  - User authentication
  - Computer and user authentication
- Provides great security at a price
  - Risk chance of TPM failure
  - Risk losing all copies of the startup key

Supporting BIOS Security Features That Affect Access Control

- Power-on passwords
  - Supervisor password
    - Required to change BIOS setup
  - User password
    - Required to use the system or view BIOS setup
  - Drive lock password
    - Required to access the hard drive
  - Set in BIOS setup utility
  - BIOS reset jumpers
    - Used if supervisor password is set and forgotten

Supporting BIOS Security Features That Affect Access Control (cont'd.)

- Support for intrusion-detection devices
  - Installed inside computer case
    - Connected to motherboard pins
    - Intrusion-detection BIOS setup feature must be enabled
  - Not a recommended best practice for security
- Support for a TPM chip
  - Installing BitLocker Encryption initializes TPM chip
    - Configures TPM chip and turns it on
    - Temporarily turning off BitLocker turns off TPM chip
    - Be careful clearing TPM chip

Quick Quiz #1

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True
- 2. _____ permissions are attained from a parent object.

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True
- 2. _____ permissions are attained from a parent object.
- Answer: Inherited

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True
- 2. _____ permissions are attained from a parent object.
- Answer: Inherited
- 3. Permission _____is when permissions are passed from parent to child.

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True
- 2. _____ permissions are attained from a parent object.
- Answer: Inherited
- 3. Permission _____is when permissions are passed from parent to child.
- Answer: propagation

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True
- 2. _____ permissions are attained from a parent object.
- Answer: Inherited
- 3. Permission _____is when permissions are passed from parent to child.
- Answer: propagation
- 4. True or False: Local shares are folders shared by default on a network that administrator accounts can access.

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True
- 2. _____ permissions are attained from a parent object.
- Answer: Inherited
- 3. Permission _____is when permissions are passed from parent to child.
- Answer: propagation
- 4. True or False: Local shares are folders shared by default on a network that administrator accounts can access.
- Answer: False

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True
- 2. _____ permissions are attained from a parent object.
- Answer: Inherited
- 3. Permission _____is when permissions are passed from parent to child.
- Answer: propagation
- 4. True or False: Local shares are folders shared by default on a network that administrator accounts can access.
- Answer: False
- 5. _____ Encryption locks down a hard drive by encrypting the entire Vista volume and any other volume on the drive.

Quick Quiz #1

- 1. True or False: Windows XP uses simple file sharing by default.
- Answer: True
- 2. _____ permissions are attained from a parent object.
- Answer: Inherited
- 3. Permission _____is when permissions are passed from parent to child.
- Answer: propagation
- 4. True or False: Local shares are folders shared by default on a network that administrator accounts can access.
- Answer: False
- 5. _____ Encryption locks down a hard drive by encrypting the entire Vista volume and any other volume on the drive.
- Answer: BitLocker

Dealing with Malicious Software

- Learn to recognize symptoms indicating a system has been infected with malicious software
- Learn about the strategies used to deal with malware
- Learn a step-by-step plan to clean up an infected system
- Learn how to protect a system from getting malware

Malware Symptoms

- Malicious software warnings
  - Many pop-up ads when surfing the Web
  - Slow system
  - Excessive disk accesses
  - Drive access lights flashing
  - Strange or bizarre error messages
  - Less memory available
  - Strange graphics on monitor
  - System cannot recognize CD or DVD drive
  - Filenames have weird characters or large file sizes

Malware Symptoms (cont'd.)

- Malicious software warnings (cont'd.)
  - Files constantly become corrupted
  - OS boots and hangs
  - Antivirus software displays one or more messages
  - Receive email indicting an infected message sent
  - Task Manager shows unfamiliar processes
  - Browsing issues
    - Changed home page or toolbars
  - Cannot access AV software sites
  - Messages about macros

Strategies for Dealing with Malware

- General plan
  - Install antivirus software on each computer
    - Download updates and run regularly
    - Review item in quarantine file
  - Reinstall hard drive using an image
  - Install data on network drives
  - Monitoring network for unusual activity with software
    - Quarantine suspicious computers
- This plan may be harder to implement in a small business

Step-By-Step Attack Plan

- Plan to clean up an infected system
  - General cleanup
    - Use antivirus and antiadware software
  - Windows tools
    - Check out the system
    - Verify malware remnants removed
    - Ensure system in tip-top order

Step-By-Step Attack Plan (cont'd.)

- Step 1: Quarantine an infected system
  - Prevent spreading of malware
    - Immediately disconnect from network
    - Download antivirus software
      - Disconnect other computers while infected computer connected
      - Connect infected computer directly to the ISP
      - Boot into Safe Mode with Networking
    - Before cleaning up infected system back up data to another media

Step-By-Step Attack Plan (cont'd.)

- Step 2: Run AV software
  - Virus programming characteristics
    - Can hide from antivirus (AV) software
    - Can block downloading and installing of AV software
  - Antivirus programming characteristics
    - Scans for what it knows
    - Uses heuristic scanning
    - Looks for distinguishing characteristics

Antivirus Software	Web Site
AntiVirus + AntiSpyware by Trend Micro (for home use)	www.trendmicro.com
Avast by ALWIL Software (home edition is free)	www.avast.com
AVG Anti-Virus by AVG Technologies	www.avg.com
BitDefender Antivirus	www.bitdefender.com
ClamWin Free Antivirus by ClamWin (open source and free)	www.clamwin.com
F-Secure Anti-Virus by F-Secure Corp.	www.f-secure.com
Kaspersky Anti-Virus	www.kaspersky.com
Malwarebytes (free version available)	www.malwarebytes.org
McAfee VirusScan Plus by McAfee Associates, Inc.	www.mcafee.com
Norton AntiVirus by Symantec, Inc.	www.symantec.com
Panda Antivirus Pro	www.pandasecurity.com
Windows Live OneCare by Microsoft	onecare.live.com
Worry-Free Business Security by Trend Micro (for networks)	www.trendmicro.com

Table 20-1 Antivirus software and Web sites

Step-By-Step Attack Plan (cont'd.)

- Step 2: Run AV software (cont'd.)
  - Antivirus software purchase considerations
    - Automatic downloads: upgrades and signatures
    - Manual download capability
    - Automatic execution at startup
    - Word-processing macro detection
    - Automatic Internet file download monitoring
    - Schedule automatic scans and allow manual scans
    - Scanning for other types of malware
    - Software installation while system in Safe Mode without Internet access

Step-By-Step Attack Plan (cont'd.)

- Step 2: Run AV software (cont'd.)
  - Infected computer without AV software
    - Use another computer with antivirus software
    - Verify remote computer software firewall has maximum protection and antivirus software is up to date and running
    - Network the computers
      - Share infected computer drive C
    - Map network drive from remote computer to infected computer drive C
    - Perform virus scan on remote computer drive C

Step-By-Step Attack Plan (cont'd.)

- Step 2: Run AV software (cont'd.)
  - Infected computer without AV software (cont'd.)
    - No other computer with antivirus software available
      - Purchase antivirus software
      - Start installation
      - Scan for infections before installing software
      - Determine what to do with problems
      - Reboot
      - Allow software to update itself, scan again
    - Do not download purchased software from infected computer

Step-By-Step Attack Plan (cont'd.)

- Step 3: Run adware or spyware removal software
  - Specifically dedicated to removing adware or spyware
    - Better than antivirus software
    - May need to run removal product more than once
    - May need to run more than one product

Adware and Spyware Removal Software	Description
Ad-Aware by Lavasoft (*www.lavasoft.com*)	One of the most popular and successful adware and spyware removal products. It can be downloaded without support for free.
Spybot Search & Destroy by PepiMK Software (*www.safer-networking.org*)	Does an excellent job of removing malicious software and it's free.
Spy Sweeper by Webroot Software, Inc. (*www.webroot.com*)	Very good product but does require you pay a yearly subscription.
Windows Vista includes Windows Defender (*www.microsoft.com/windows/products/winfamily/defender*)	Antispyware software embedded in the OS.

Table 20-2 Removal software

Step-By-Step Attack Plan (cont'd.)

- Step 4: Clean up what's left over
  - Antivirus or antiadware software
    - May not delete files
    - May leave orphaned entry in registry or startup folders
    - Check Antivirus or antiadware software Web site for instructions to manually clean things up

Step-By-Step Attack Plan (cont'd.)

- Step 4: Clean up what's left over (cont'd.)
  - Respond to any startup errors
    - Use MSconfig.exe
    - Program launched from registry
      - Back up and delete registry key
    - Program launched from startup folder
      - Move or delete shortcut or program in the folder
  - Research malware types and program files
    - Several Web sites offer virus encyclopedias
    - Check things out carefully

Step-By-Step Attack Plan (cont'd.)

- Step 4: Clean up what's left over (cont'd.)
  - Delete files
    - Try to delete program file using Windows Explorer
    - Empty the Recycle Bin
    - May have to remove hidden or system file attributes

Command	Explanation
cd \	Make the root directory of drive C the current directory.
dir INT0094.exe	The file does not appear to be in the directory.
attrib INT0094.exe	The file is actually present but hidden.
attrib –h –s INT0094.exe	Remove the hidden and system attributes of the file.
dir INT0094.exe	The dir command now displays the file.
del INT0094.exe	Delete the file.

Table 20-3 Commands to delete a hidden system file

Step-By-Step Attack Plan (cont'd.)

- Step 4: Clean up what's left over (cont'd.)
  - Delete files (cont'd.)
    - Open Task Manager
      - Verify process not running
      - End process using Task Manager or Taskkill command
    - Delete all Internet Explorer temporary Internet files
      - Windows Explorer Disk Cleanup
      - Internet Explorer Delete Browsing History box

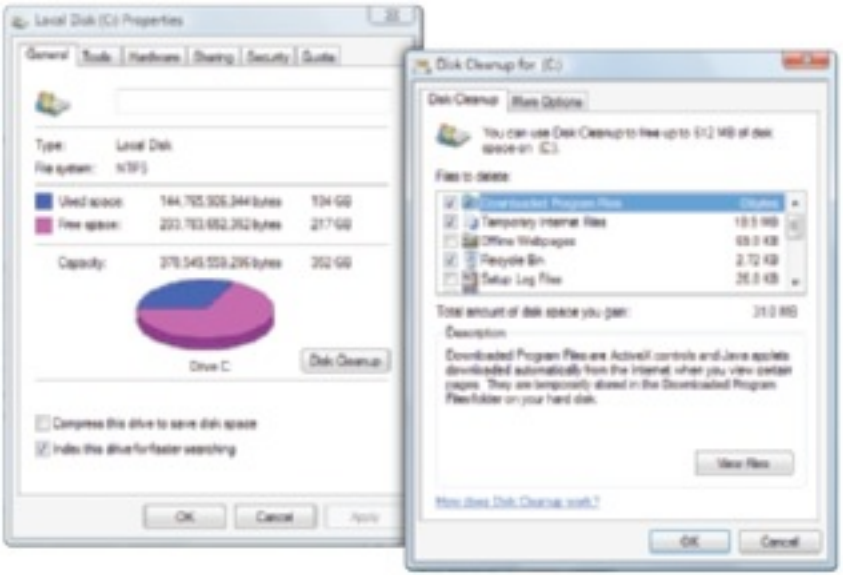

Figure 20-38 Delete all temporary Internet files. Courtesy: Course Technology/ Cengage Learning

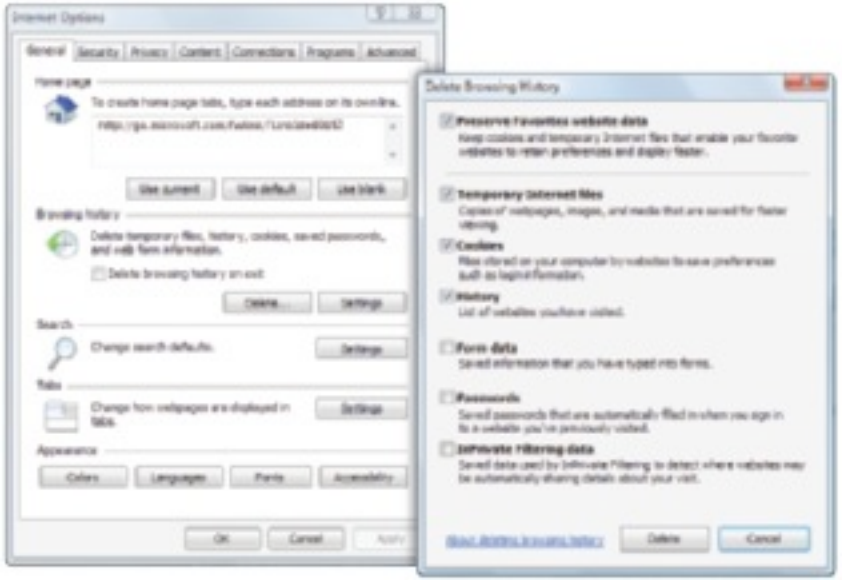

Figure 20-39 Use the Internet Properties box to delete the browsing history. Courtesy: Course Technology/Cengage Learning

Step-By-Step Attack Plan (cont'd.)

- Step 4: Clean up what's left over (cont'd.)
  - Purge restore points
    - Malware can hide in System Restore utility data area
    - To remove malware:
      - Purge data storage area
      - Turn off System Protection, reboot system, and turn System Protection back on
    - If antivirus software reports virus in the C:\System Volume Information_restore folder, purge all restore points

Step-By-Step Attack Plan (cont'd.)

- Step 4: Clean up what's left over (cont'd.)
  - Clean the registry
    - Delete unneeded startup registry keys
    - Use a registry cleaning utility
    - Use Autoruns at Microsoft TechNet
      - Helps in searching for orphaned registry entries

Step-By-Step Attack Plan (cont'd.)

- Step 4: Clean up what's left over (cont'd.)
  - Clean up Internet Explorer
    - Remove unwanted toolbars and home pages
      - Use Programs and Features window or Add or Remove Programs window
      - Uninstall software related to the browser
    - Disable suspicious add-ons
    - Delete unwanted ActiveX add-ons
    - Change home page if necessary

Step-By-Step Attack Plan (cont'd.)

- Step 5: Dig deeper to find malware processes
  - Task Manager process examination
    - Most processes are registered as running
      - User name or user account
    - Core Windows processes do not list account
      - Right-click item without a user name
      - Select Perform Administrative Tasks
    - Virus may disguise itself as a legitimate Windows core process
      - Svchost.exe process running under a user name
      - Located somewhere other than C:\Windows\system32

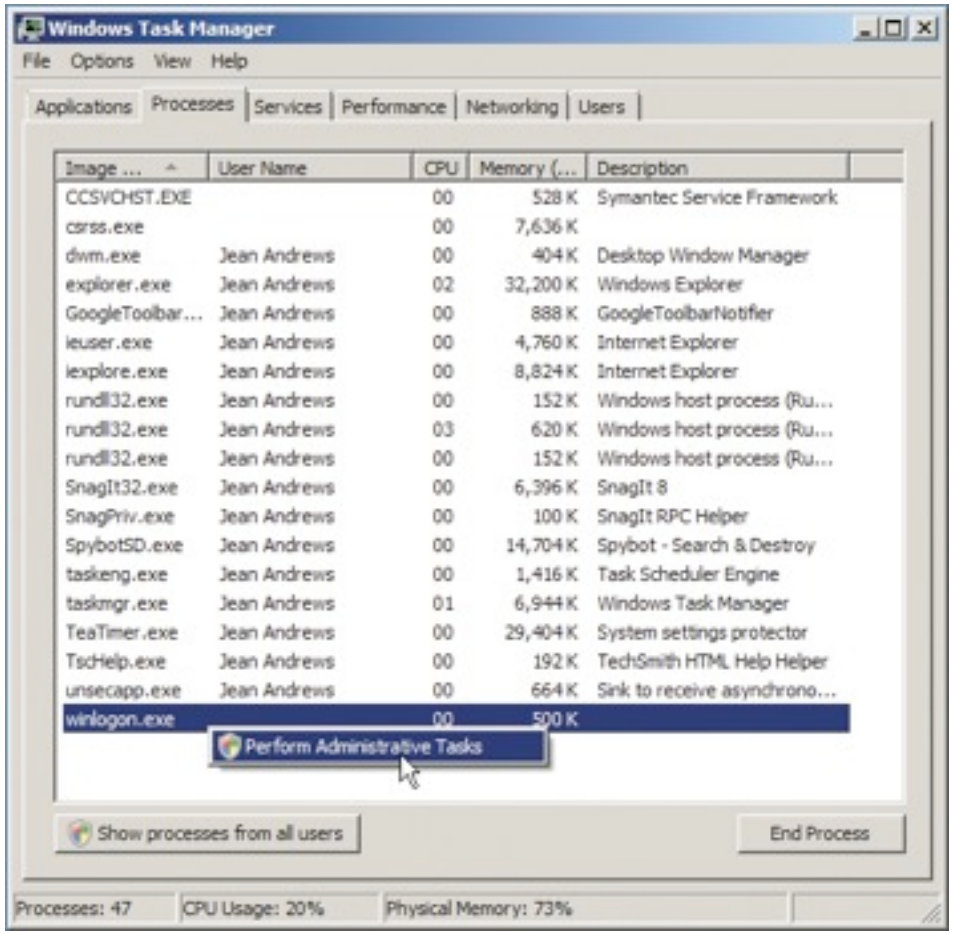

Figure 20-47 Processes currently running under Windows Vista
Courtesy: Course Technology/Cengage Learning

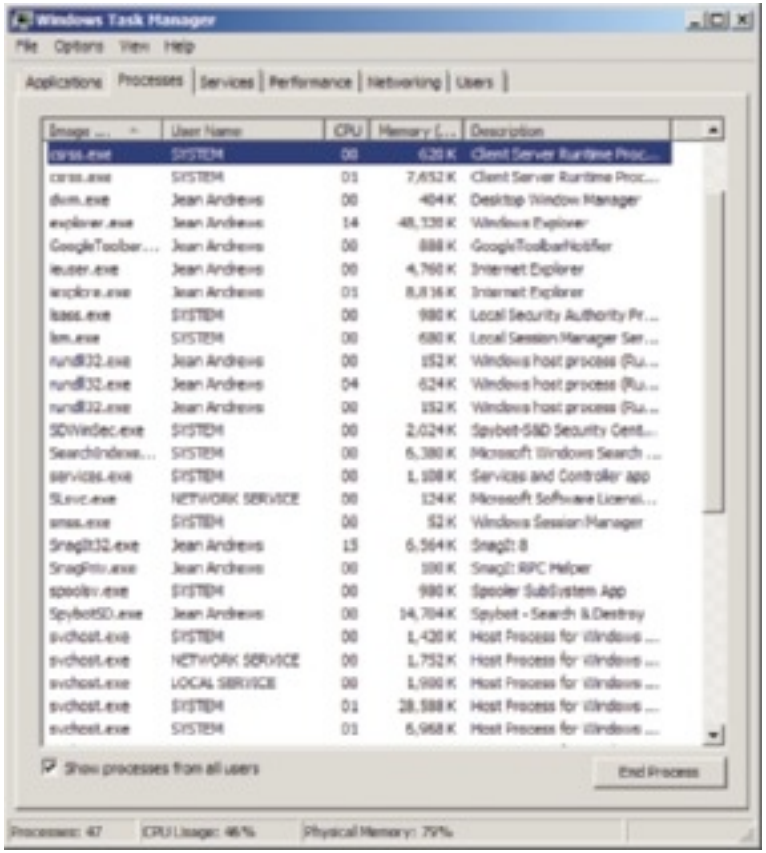

Figure 20-48 Task Manager set to show more information about processes
Courtesy: Course Technology/Cengage Learning

Figure 20-49 Set Task Manager to show the path to a program file
Courtesy: Course Technology/Cengage Learning

Step-By-Step Attack Plan (cont'd.)

- Step 5: Dig deeper to find malware processes (cont'd.)
  - Researching processes: Microsoft support site
    - Review core Windows processes automatically launched depending on Windows settings
  - Process Explorer at Microsoft TechNet
    - Identifies how processes relate to each other
    - Useful tool for software developers
    - Used to smoke out processes, DLLs, and registry keys eluding Task Manager

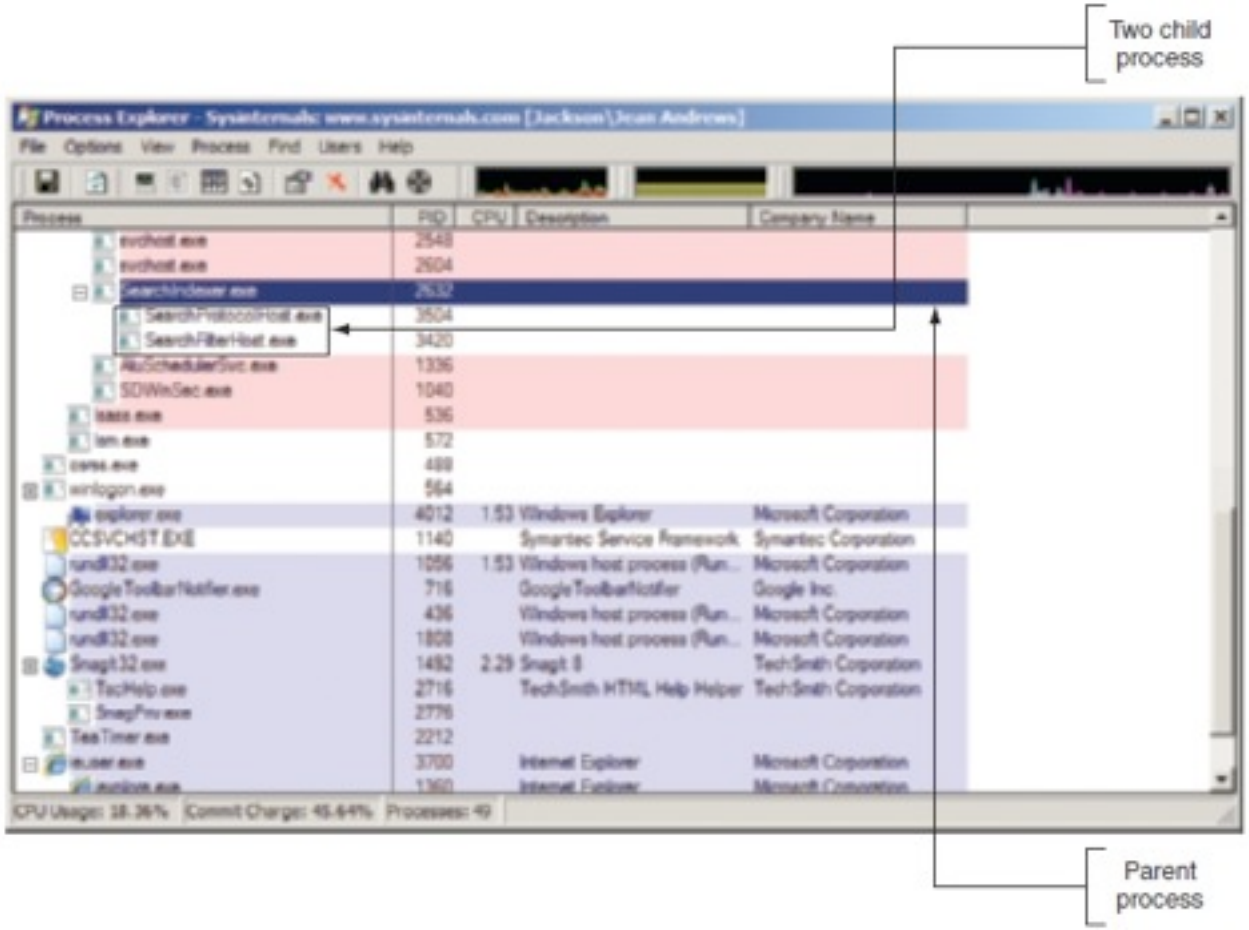

Figure 20-50 Process Explorer color codes child-parent relationships among processes and gives information about processes
Courtesy: Course Technology/Cengage Learning

Step-By-Step Attack Plan (cont'd.)

- Step 6: Remove rootkits
  - Rootkit
    - Program using unusually complex methods to hide itself on a system
    - Designed to keep a program working at root level without detection
      - Can prevent display of running rootkit process
      - May display a different name for the process
      - Filename may not be displayed in Windows Explorer
      - Registry editor may not display rootkit registry keys or display wrong information

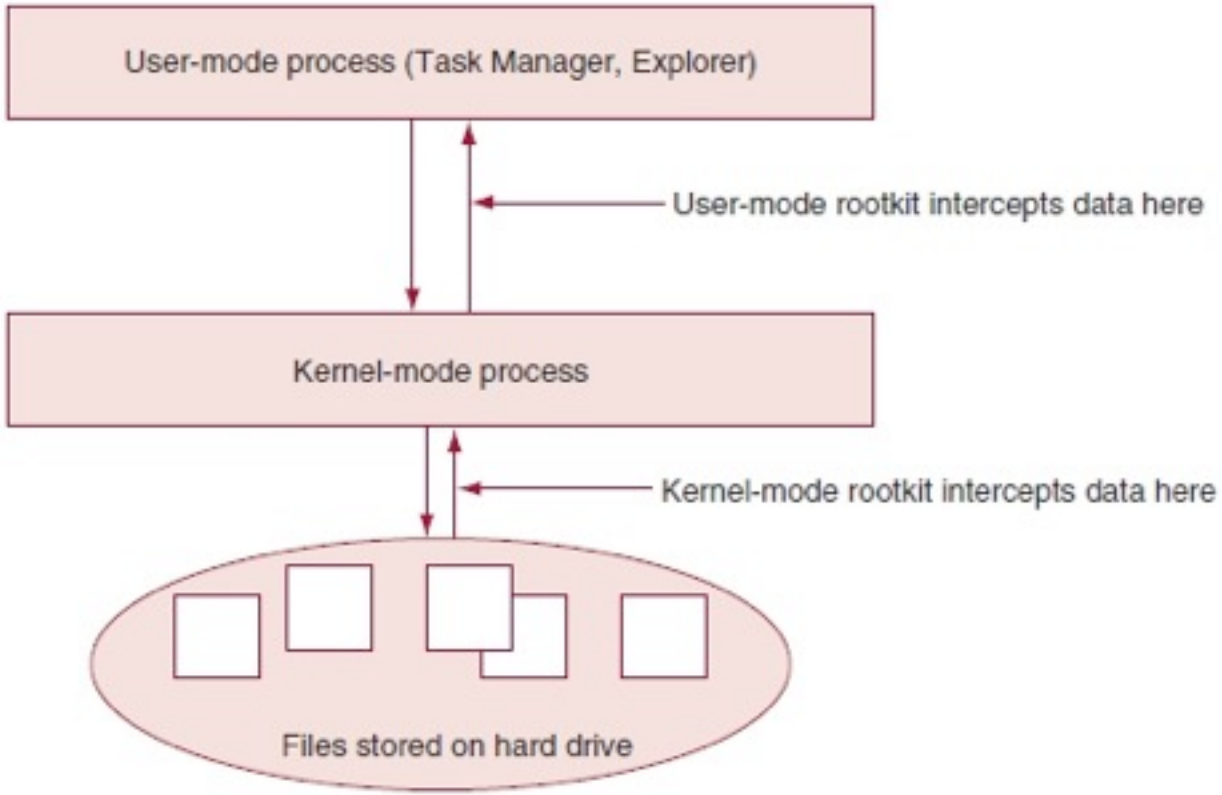

Figure 20-51 A rootkit can run in user mode or kernel mode
Courtesy: Course Technology/Cengage Learning

Step-By-Step Attack Plan (cont'd.)

- Step 6: Remove rootkits (cont'd.)
  - Rootkit not detected if Windows tools infected
  - Antirootkit software
    - Looks for running processes that don't match up with the underlying program filename
    - Compares files, registry entries, processes provided by the OS to the lists it generates from the raw data
    - Good antirootkit programs: RootkitRevealer and BackLight
  - Run antirootkit software from another networked computer

Step-By-Step Attack Plan (cont'd.)

- Step 7: Repair boot blocks
  - Hard drive boot sectors infected or damaged
    - Repair MBR or OS boot record
      - Boot from Vista setup DVD, launch the Recovery Environment, and access command prompt
      - Command bootrec /fixmbr repairs MBR
      - Command bootrec /fixboot repairs OS boot record
  - BIOS code corrupted
    - Virus is unlikely
    - POST "Award BootBlock BIOS ROM checksum error"
      - Use methods to recover from errors when flashing BIOS in Chapter 5

Protect a System against Malicious Software

- Install and run AV software
  - Set software to schedule automatic system scans
- Set Windows to install updates automatically
- Keep a software firewall up and running
- Keep Vista UAC box turned on
- Educate end users
  - Recognizing social engineering situations
  - Locking down workstations
  - Using other security measures

Quick Quiz #2

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined
- 2. True or False: Files constantly becoming corrupted may be a sign of malware.

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined
- 2. True or False: Files constantly becoming corrupted may be a sign of malware.
- Answer: True

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined
- 2. True or False: Files constantly becoming corrupted may be a sign of malware.
- Answer: True
- 3. AV software detects a known virus by looking for distinguishing characteristics called _____, which is why AV software cannot always detect a virus it does not know to look for.

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined
- 2. True or False: Files constantly becoming corrupted may be a sign of malware.
- Answer: True
- 3. AV software detects a known virus by looking for distinguishing characteristics called _____, which is why AV software cannot always detect a virus it does not know to look for.
- 4. Answer: virus signatures

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined
- 2. True or False: Files constantly becoming corrupted may be a sign of malware.
- Answer: True
- 3. AV software detects a known virus by looking for distinguishing characteristics called _____, which is why AV software cannot always detect a virus it does not know to look for.
- 4. Answer: virus signatures
- True or False: The distinction between adware and spyware is slight.

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined
- 2. True or False: Files constantly becoming corrupted may be a sign of malware.
- Answer: True
- 3. AV software detects a known virus by looking for distinguishing characteristics called _____, which is why AV software cannot always detect a virus it does not know to look for.
- 4. Answer: virus signatures
- True or False: The distinction between adware and spyware is slight.
- Answer: True

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined
- 2. True or False: Files constantly becoming corrupted may be a sign of malware.
- Answer: True
- 3. AV software detects a known virus by looking for distinguishing characteristics called _____, which is why AV software cannot always detect a virus it does not know to look for.
- 4. Answer: virus signatures
- True or False: The distinction between adware and spyware is slight.
- Answer: True
- 5. True or False: Malware cannot hide its program files in the data storage area of the System Restore utility.

Quick Quiz #2

- 1. A(n) _____ file is placed in a special directory and cannot be opened.
- Answer: quarantined
- 2. True or False: Files constantly becoming corrupted may be a sign of malware.
- Answer: True
- 3. AV software detects a known virus by looking for distinguishing characteristics called _____, which is why AV software cannot always detect a virus it does not know to look for.
- 4. Answer: virus signatures
- True or False: The distinction between adware and spyware is slight.
- Answer: True
- 5. True or False: Malware cannot hide its program files in the data storage area of the System Restore utility.
- Answer: False

Summary

- To secure a computer and its resources:
  - Control access to data folders and files
  - Hide network resources
  - Encrypt files and folders
  - BitLocker Encryption
    - Encrypt entire Vista volume, any other volume on the drive
  - Use BIOS security features
  - Recognize and deal with malware
  - Protect a system against malware