COURSE TECHNOLOGY
CENGAGE Learning™

MCTS Guide to Microsoft Windows 7

Chapter 7
Windows 7 Security Features

Objectives

- Describe Windows 7 Security Improvements
- Use the local security policy to secure Windows 7
- Enable auditing to record security events
- Describe and configure User Account Control
- Describe the malware security features in Windows 7
- Use the data security features in Windows 7
- Secure Windows 7 by using Windows Update

Windows 7 Security Improvements

- Major security improvements in Windows 7 are:
  - Malware protection
  - Easier deployment of alternative authentication methods
  - Enhanced network protection
  - Data protection for stolen hard drives
  - AppLocker for software restriction

Malware Protection

- Malware
  - Malicious software designed to perform unauthorized acts on your computer
- User Account Control (UAC)
  - Feature implemented in Windows 7 to control malware
  - Prompts users when software attempts to take administrative control
- Windows Defender
  - A real-time spyware monitor to prevent the installation of and remove spyware

Malware Protection (cont'd.)

- Spyware
  - A threat to privacy; makes systems unstable
- Internet Explorer has been modified to run in a limited state (protected mode)
  - User files cannot be modified
- A phishing filter has also been added
  - Prevents unauthorized Web sites from stealing log-on credentials and other personal information

Malware Protection (cont'd.)

- Windows service hardening
  - Most Windows exploits used to install malware are the result of flaws in Windows services
  - Windows services have been changed as follows:
    - Each service is given a SID number
    - Services run with a lower privilege level by default
    - Unnecessary privileges for services have been removed
    - Windows Firewall can control network access based on service SIDs
    - Services are isolated and cannot interact with users

Alternative Authentication Methods

- Username and password
  - Most common method for authentication
- Windows 7 makes smart cards easier to manage
- Development of additional authentication methods for Windows, such as biometrics, has been simplified

Network Protection

- Windows 7 is protected on networks by:
  - Enhanced firewall
  - Network Access Protection (NAP)
- Firewall can control both inbound and outbound network packets
- NAP prevents unhealthy computers from accessing the network
  - An unhealthy computer is one that has outdated antivirus signatures or is missing security updates

Data Protection

- NTFS file system provides data protection by using permissions on files and folders
  - NTFS permissions can be easily circumvented when you have physical access to a computer
- BitLocker Drive Encryption
  - Encrypts the contents of a partition and protects the system partition

AppLocker for Software Restrictions

- AppLocker simplifies the management of software restrictions
  - By implementing simpler rules than were available in software restriction policies

Security Policies

- Windows 7 includes a local security policy
  - Can be used to control many facets of Windows
  - Can be accessed in the Local Security Policy in Administrative Tools
- Local security policy categories
  - Account policies
  - Local policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Public Key Policies

Security Policies (cont'd.)

- Local security policy categories (cont'd.)
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Local Computer
  - Advanced Audit Policy Configuration
- The local security policy is part of a larger Windows management system called Group Policy
  - Can be implemented on a local computer, but is typically part of a domain-based network

Security Policies (cont'd.)

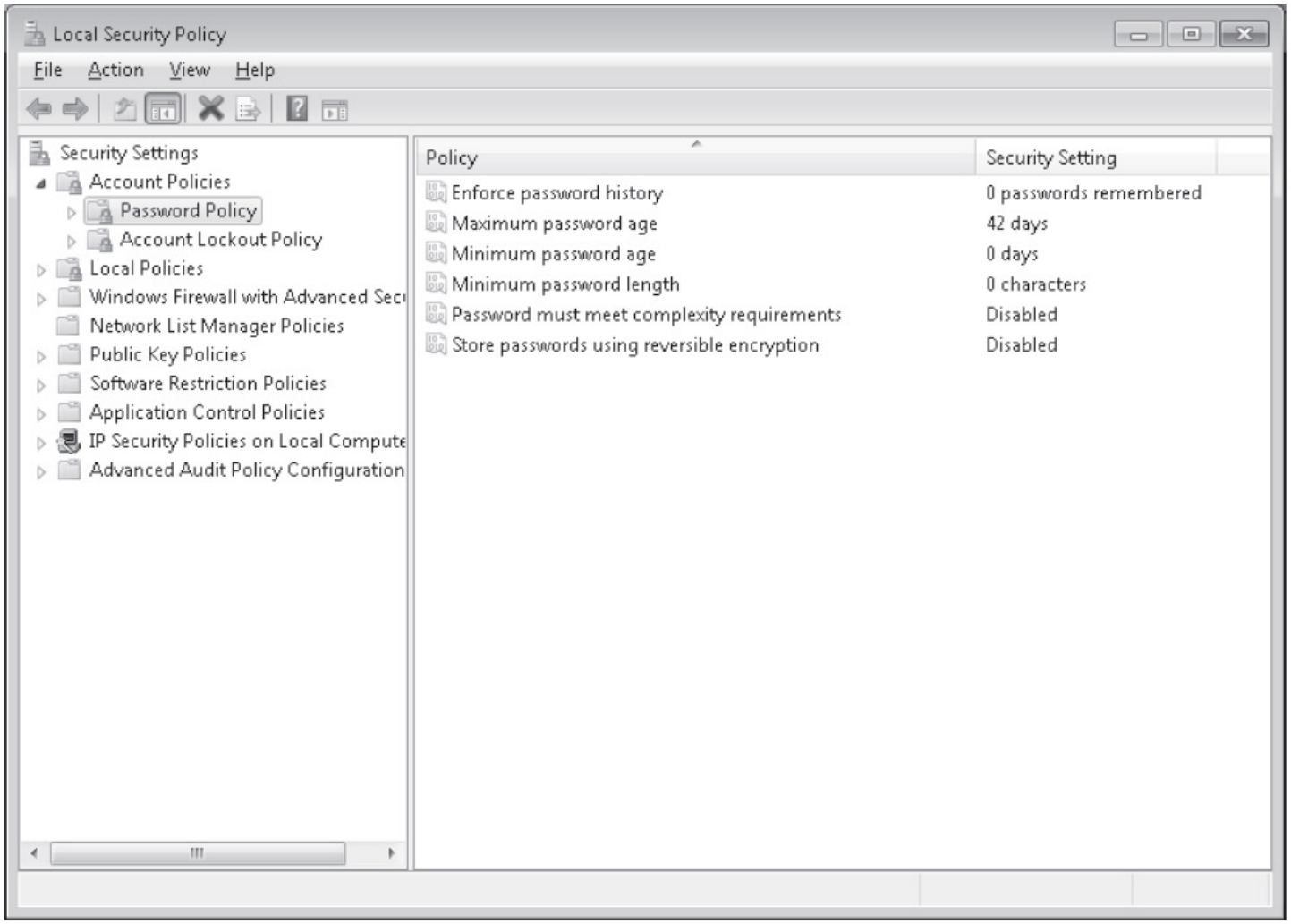

Figure 7-1 Local Security Policy

Courtesy Course Technology/Cengage Learning

Account Policies

- Contain the password policy and the account lockout policy
- Do not affect domain accounts
- Must be configured at the domain level
- Password policy
  - Controls password characteristics for local user accounts
  - Available settings
    - Enforce password history
    - Maximum password age
    - Minimum password age

Account Policies (cont'd.)

- Password policy (cont'd.)
  - Available settings (cont'd.)
    - Minimum password length
    - Password must meet complexity requirements
    - Store passwords using reversible encryption
- Account lockout policy
  - Prevents unauthorized access to Windows 7
  - Can configure an account to be temporarily disabled after a number of incorrect log-on attempts

Account Policies (cont'd.)

- Account lockout policy (cont'd.)
  - Available settings
    - Account lockout duration
    - Account lockout threshold
    - Reset account lockout counter after

Local Policies

- Local policies are for:
  - Auditing system access
  - Assigning user rights
  - Configuring specific security options
- Auditing lets you track when users log on and which resources are used
- User rights control what system task a particular user or group of users can perform
- Specific security options are a variety of settings that can be used to make Windows 7 more secure

Local Policies (cont'd.)

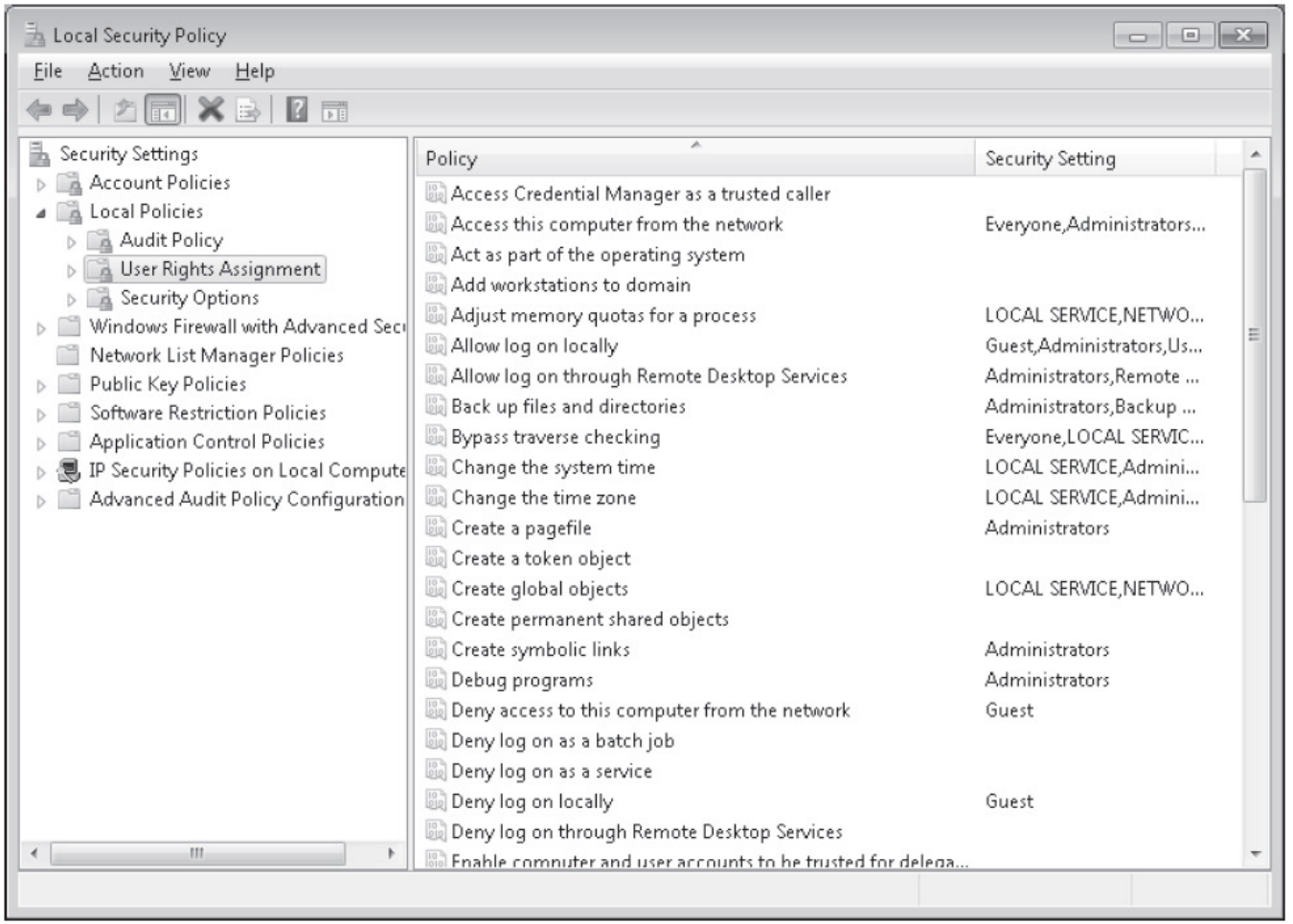

Figure 7-2 User Rights Assignment settings

Courtesy Course Technology/Cengage Learning

Local Policies (cont'd.)

- User rights assignment settings
  - Allow log on locally
  - Back up files and directories
  - Change the system time
  - Load and unload device drivers
  - Shut down the system
- Security options settings
  - Devices
  - Interactive logon
  - Interactive logon
  - Shutdown

AppLocker

- Used to define which programs are allowed or disallowed in the system
- Used in corporate environments where parental controls are not able to be used
- Enhancements over software restriction policies:
  - Rules can be applied to specific users and groups rather than all users
  - Default rule action is deny to increase security
  - Wizard to help create rules.
  - Audit only mode for testing that only writes events to the event log

AppLocker (cont'd.)

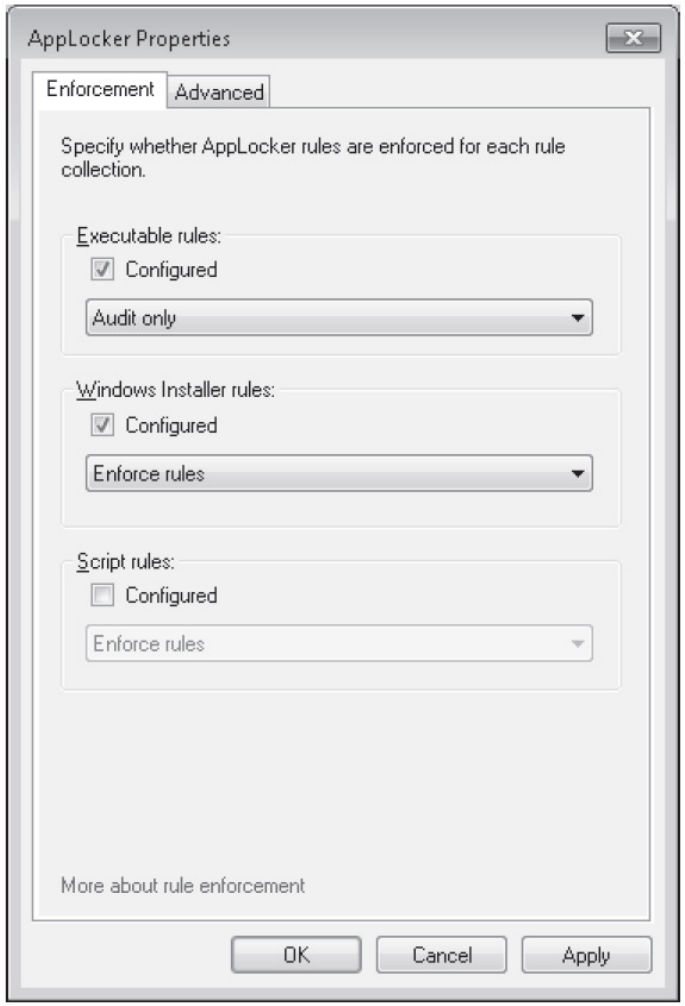

Figure 7-3 Configuring AppLocker enforcement

Courtesy Course Technology/Cengage Learning

AppLocker (cont'd.)

- You can audit or enforce AppLocker rules
  - Relies on the configuration of appropriate rules and the Application Identity service
- Rule Collections
  - Executable
  - Windows Installer
  - Scripts
  - DLL

AppLocker (cont'd.)

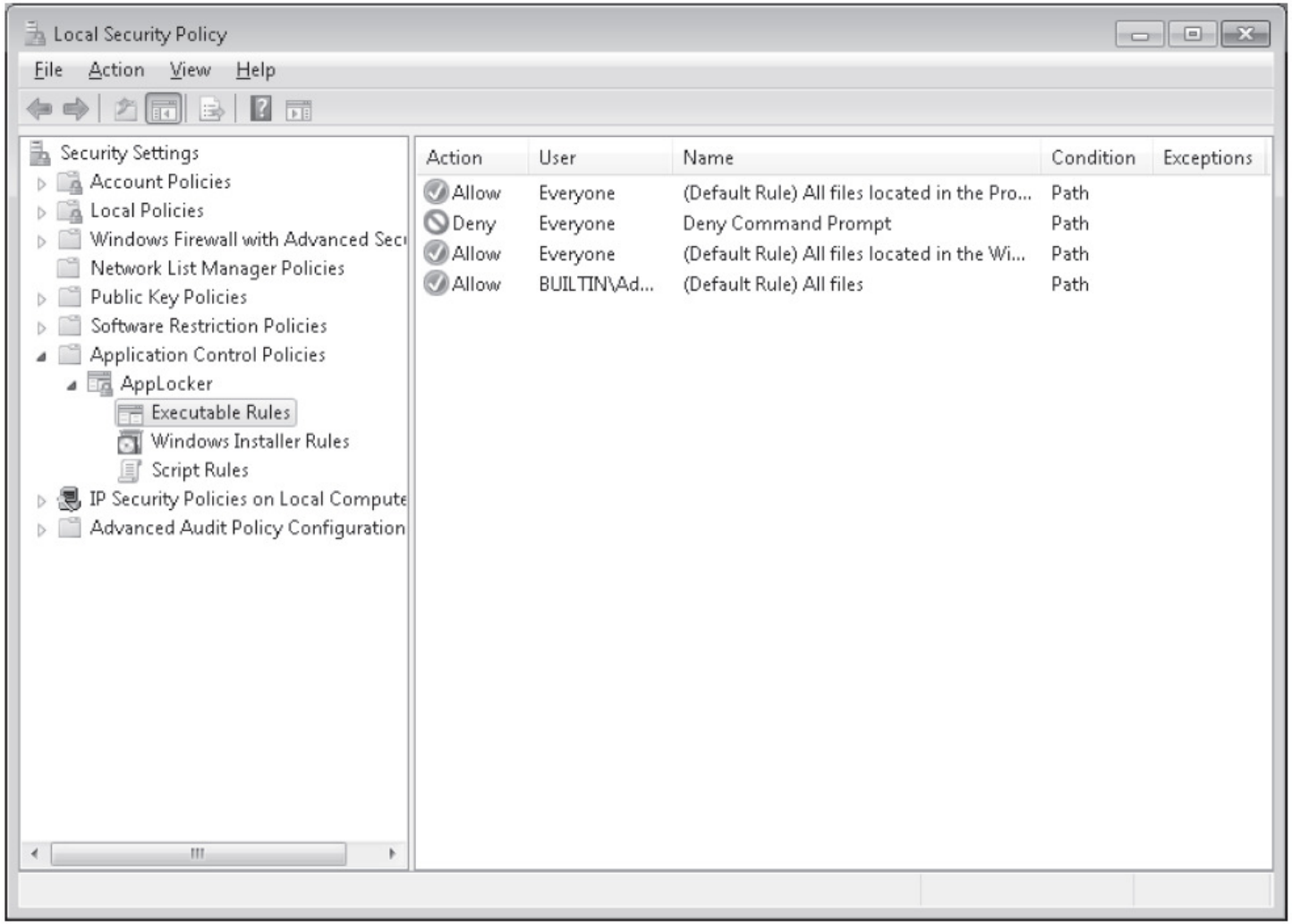

Figure 7-4 Applocker rule collections

Courtesy Course Technology/Cengage Learning

AppLocker (cont'd.)

- Rule Permissions
  - Each rule contains permissions that define whether the rule allows or denies software the ability to run
- Rule Conditions
  - Define the software that is affected by the rule
  - Three conditions that can be used:
    - Publisher
    - Path
    - File hash

AppLocker (cont'd.)

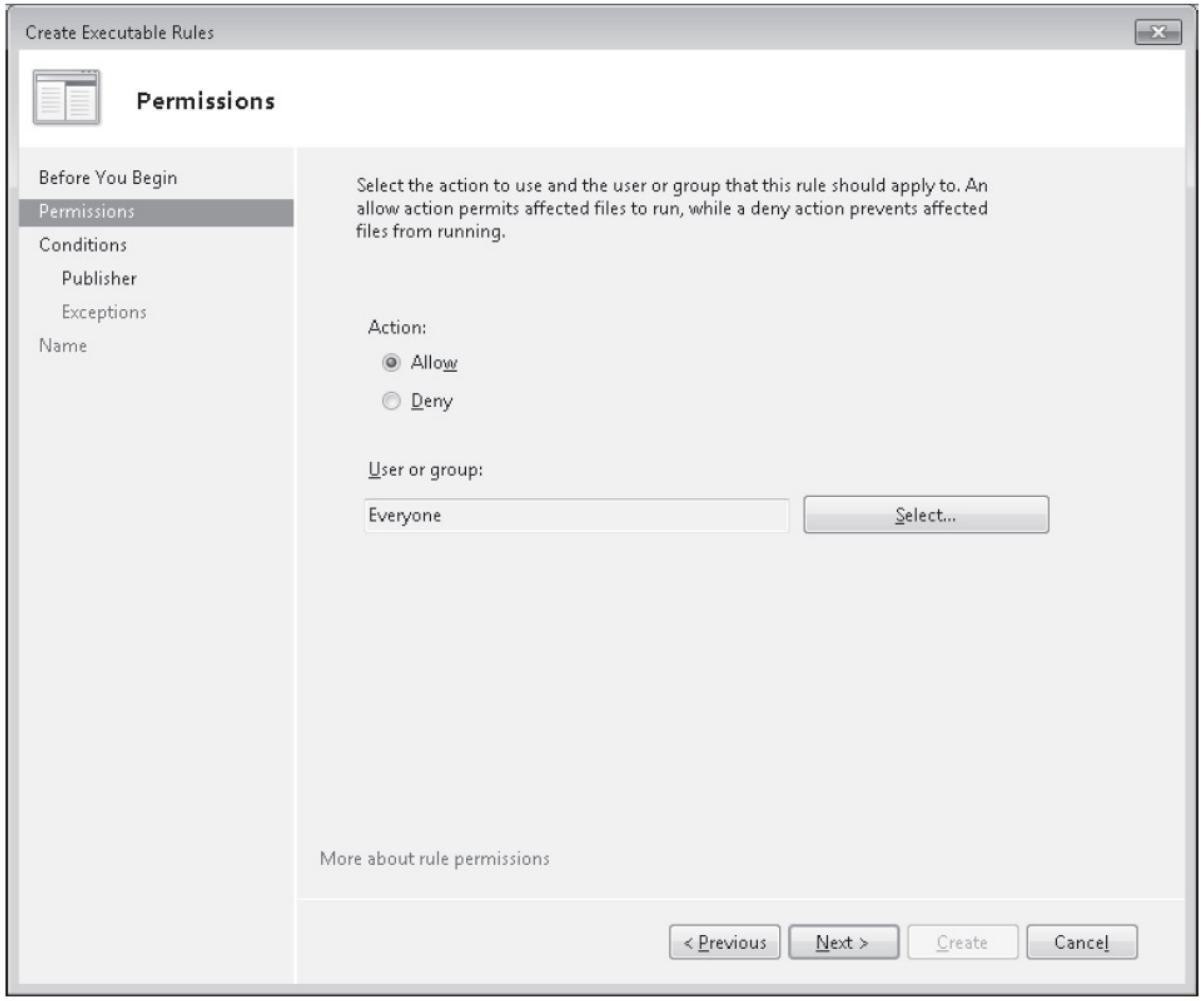

Figure 7-5 AppLocker rule permissions
Courtesy Course Technology/Cengage Learning

AppLocker (cont'd.)

- Rule Exceptions
  - Define software that the rule does not apply to

Other Security Policies

- Windows Firewall with Advanced Security
  - Used to configure the new firewall in Windows 7
  - Lets you configure both inbound and outbound rules
  - Can be used to configure IP Security (IPsec) rules
- Network List Manager Policies control how Windows 7 categorizes networks
- Public Key Policies has a single setting for the Encrypting File System (EFS)
- IP Security Policies on Local Computer are used to control encrypted network communication

Security Templates

- Security templates are .inf files that contain:
  - Settings that correspond with the Account Policies and Local Policies in the local security policy
  - Settings for the event log, restricted groups, service configuration, registry security, and file system security
- Edited by using the Security Templates snap-in
- Security templates are used by Security Configuration and Analysis tool and Secedit

Security Templates (cont'd.)

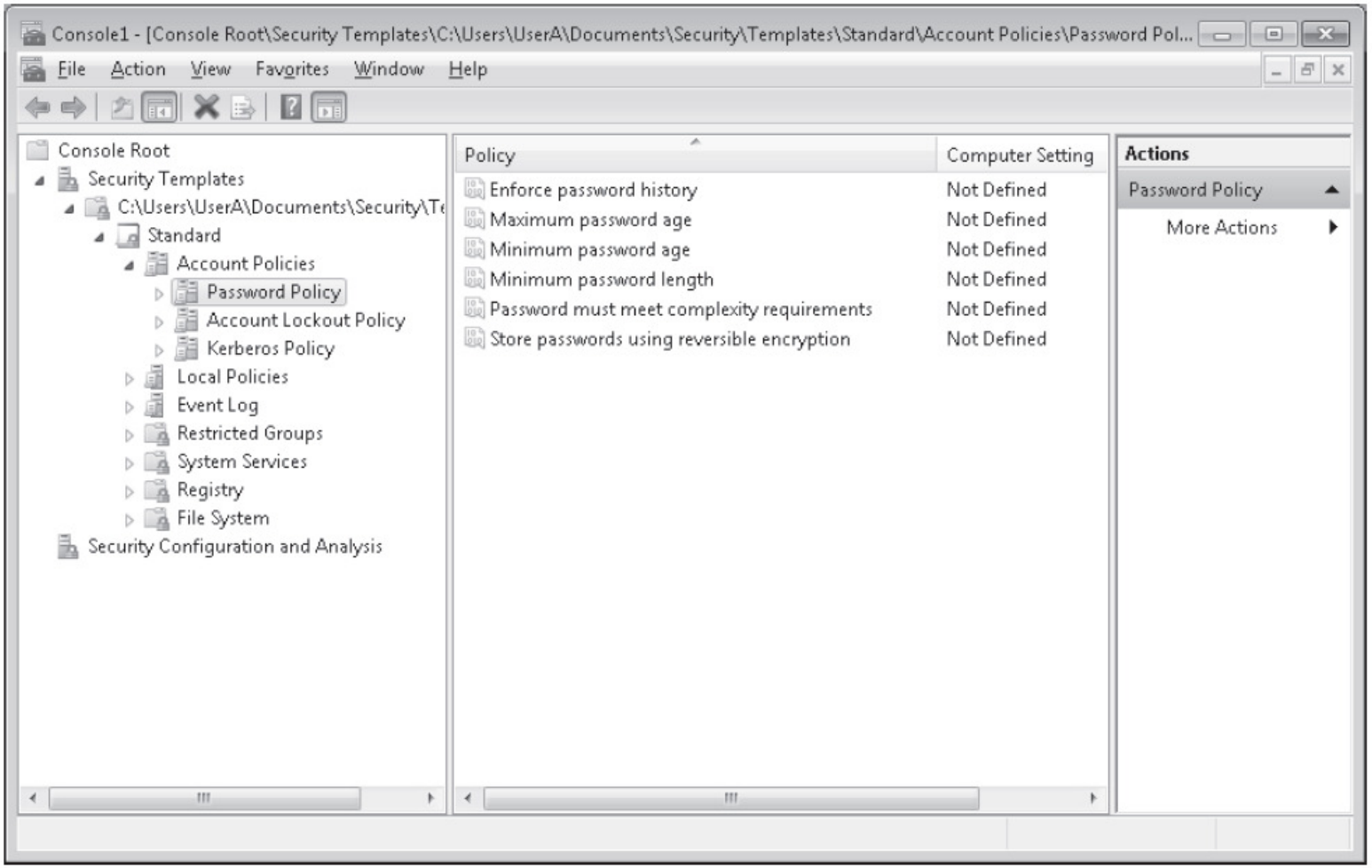

Figure 7-8 Security Templates MMC snap-in

Courtesy Course Technology/Cengage Learning

Security Templates (cont'd.)

- Tasks you can perform with the Security Configuration and Analysis tool
  - Analyze
  - Configure
  - Export

Auditing

- Auditing
  - Security process that records the occurrence of specific operating system events in the Security log
- Every object in Windows 7 has audit events related to it
- Auditing is enabled through the local security policy or by using Group Policy
- Once the audit policy is configured
  - The audited events are recorded in the Security log that is viewed by using Event Viewer

Auditing (cont'd.)

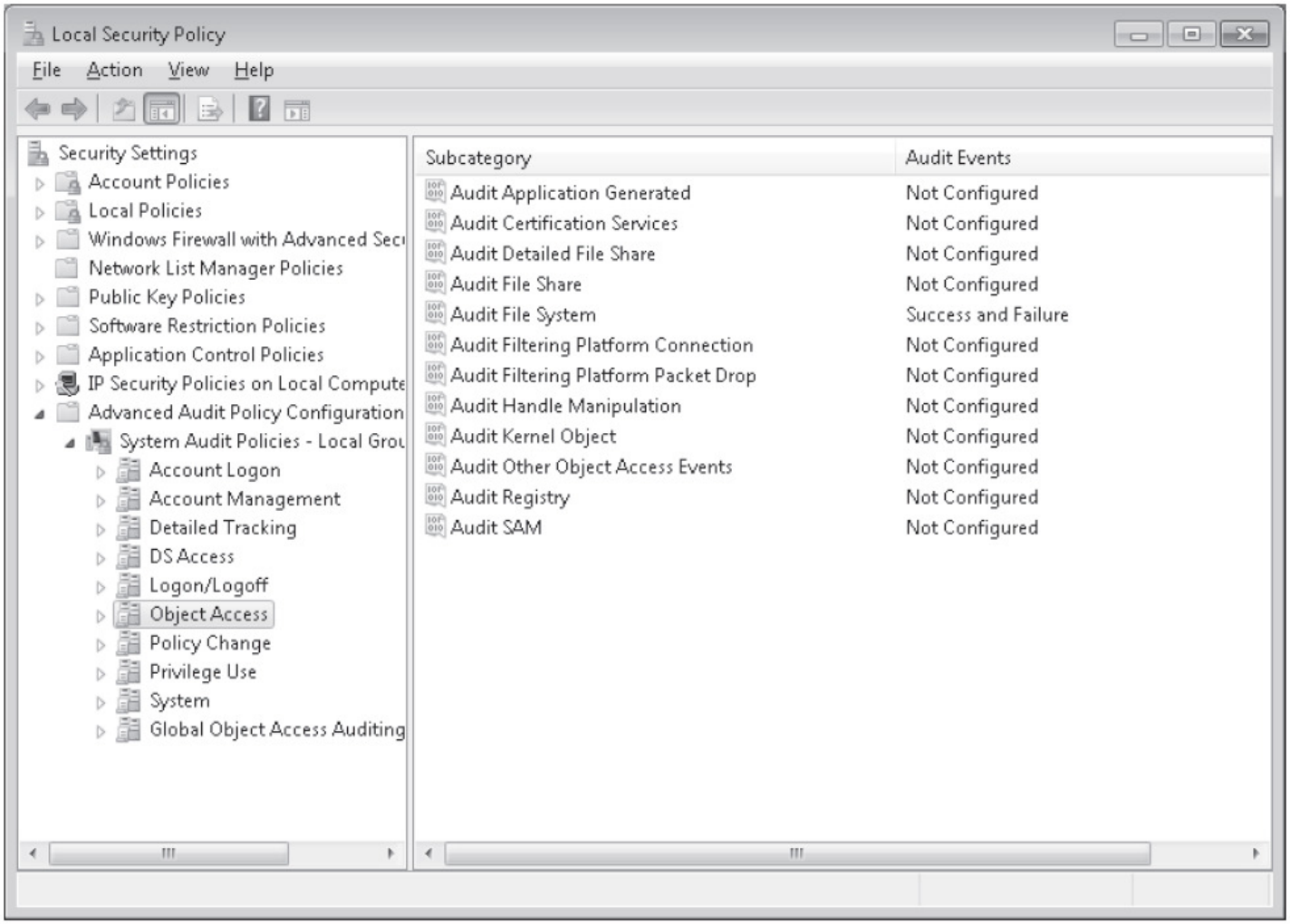

Figure 7-9 Advanced Audit Policy

Courtesy Course Technology/Cengage Learning

Table 7-1 Event categories for advanced audit policy settings

Event Category	Description
Account Logon	Tracks when users are authenticated by a computer. If a local user account is used, the event is logged locally. If a domain user account is used, the event is logged at the domain controller. Account Logon events are not audited by default.
Account Management	Tracks when users and groups are created, modified, or deleted. Password changes are also tracked. Success events for user management are audited by default. Success and failure events for group management are auditing by default.
Detailed Tracking	Tracks how a computer is being used by tracking application activity. This includes identifying the creation and termination of processes, encryption events, and RPC events. No events are audited by default.
DS access	This category is not relevant for Windows 7 and is not audited by default. It is used only for domain controllers.
Logon/Logoff	User activity events, including local and domain logons, at the local computer. This category is similar to, but different from, audit account logon events. Logging on with a local account generates both an account logon event and a logon event on the local computer. Logging on with a domain account generates an account logon event at the domain controller and a logon event at the workstation where the logon occurred. Success event for logon, logoff, account lockout are audited by default. Failure events for logon are also audited.
Object Access	Tracks access to files, folders, printers, and registry keys. Each individual object being accessed must also be configured for auditing. Only files and folders on NTFS-formatted partitions can be monitored. Object access is not audited by default.
Policy Change	Tracks changes to user rights assignments, audit policies, and trust policies. Success events for audit policy changes and authentication policy changes are audited by default.
Privilege Use	Tracks when tasks are performed that require a user rights assignment, such as changing the system time. You can define which categories of privilege use are audited. None are audited by default.
System	Tracks when system events occur, such as restarting the system. By default success and failure events are audited for system integrity and other system events. Only success events are audited for security state change.
Global Object Access	Provides an easy way to specify that all access to files or registry keys should be audited. This avoids the need to configure auditing at the file, folder, or registry key level after enabling auditing for object access to files or registry keys. However, this must still be used in combination with auditing enabled for object access. This category does not appear when using auditpol.exe.

Auditing (cont'd.)

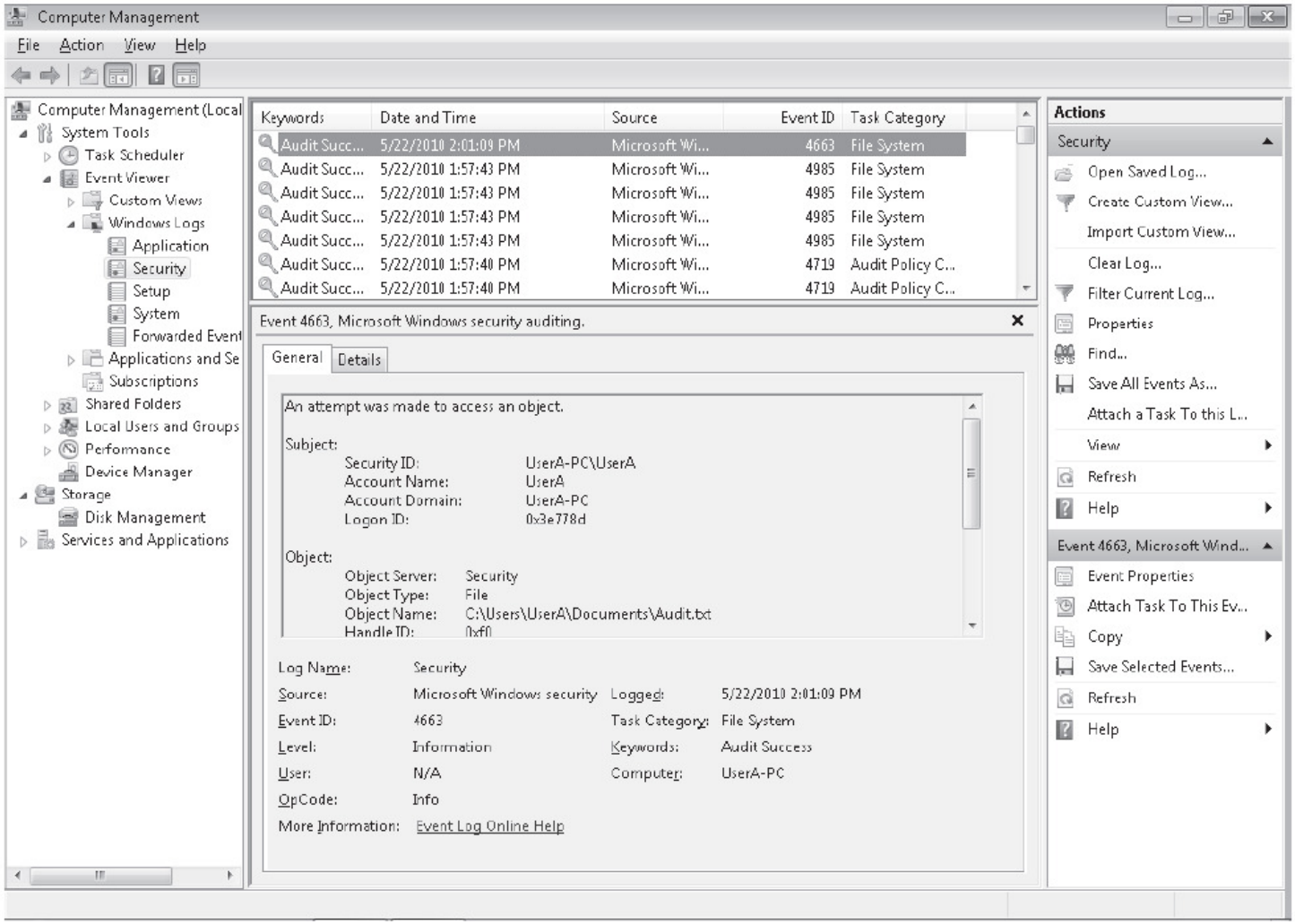

Figure 7-10 Windows Security log

Courtesy Course Technology/Cengage Learning

User Account Control

- User Account Control (UAC)
  - Feature introduced in Windows Vista that makes running applications more secure
- Security is enhanced by reducing the need to log on and run applications using administrator privileges
- When UAC is enabled and an administrative user logs on
  - Administrative user is assigned two access tokens
    - Standard user privileges
    - Administrative privileges

User Account Control (cont'd.)

- Standard user access token is used to launch the Windows 7 user interface
- Admin Approval Mode
  - Ensures that the access token with administrative privileges is used only when required
- Application Information Service
  - Responsible for launching programs by using the access token with administrative privileges

Application Manifest

- Application manifest
  - Describes the structure of an application
  - Includes required DLL files and whether they are shared
- Applications that are not designed for Windows 7 and which require administrative privileges
  - Do not properly request elevated privileges
  - Fix it by using the Application Compatibility Toolkit

UAC Configuration

- Windows 7 introduces a simplified interface for managing UAC
- UAC is configured by using either:
  - Windows 7 Local Security Policy
    - For small environments
  - Group Policy
    - For larger environments

UAC Configuration (cont'd.)

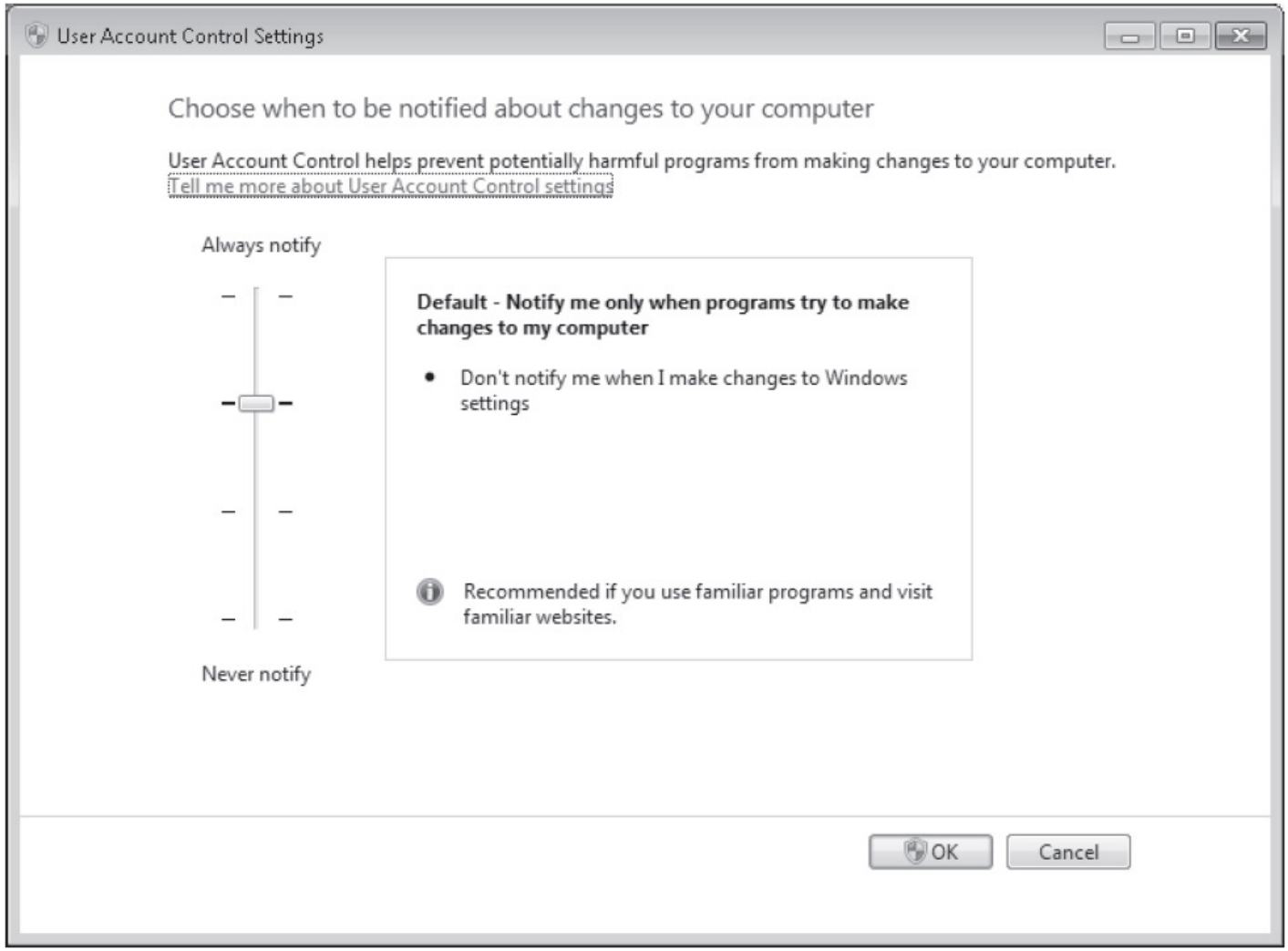

Figure 7-11 UAC settings

Courtesy Course Technology/Cengage Learning

Table 7-2 UAC configuration options

Option (User Account Control:)	Description
Admin Approval Mode for the Built-in Administrator account	Used to enable or disable Admin Approval Mode for the built-in administrator account. The default configuration is disabled.
Allow UIAccess application to prompt for elevation without using secure desktop	This configuration allows UIAccess programs, such as Remote Assistance, to automatically disable the screen dimming that normally occurs when a UAC prompt is displays. This is a less secure configuration but can speed up screen drawing over slow connections. This is disabled by default.
Behavior of the elevation prompt for administrators in Admin Approval Mode	Used to configure the elevation prompt for Administrators only. The default configuration is to prompt for consent for non-Windows binaries. However, you can also configure a prompt for administrative credentials instead of a simple approval. You can also disable the prompt. Entirely disabling the prompt effectively disables UAC for administrators because applications can then request elevation to administrative privileges and are automatically approved. However, applications do run with standard user privileges until they request elevation.
Behavior of the elevation prompt for standard users	Used to configure the elevation prompt for standard users only. The default configuration is to prompt for credentials. You can also select Automatically deny elevation requests, in which case the user must manually use Runas to elevate the privileges of the application.
Detect application installations and prompt for elevation	Used to automatically detect whether an application is being installed and generate a prompt to elevate privileges. The default configuration is enabled. If this option is disabled, then many legacy application installations will fail.
Only elevate executables that are signed and validated	Used to limit privilege elevation to only applications that are digitally signed. The default configuration is disabled, which allows older unsigned applications that require administrative privileges to be elevated.
Only elevate UIAccess applications that are installed in secure locations	Used to force applications using the UIAccess integrity level in their application manifest to be located from a secure location. Secure locations are C:\ProgramFiles\ and C:\Windows\System32 and their subfolders. The default configuration is enabled.
Run all administrators in Admin Approval Mode	Used to limit all user processes to standard user privileges unless they are elevated to administrator privileges. The default configuration is enabled. When this option is disabled, UAC is disabled for administrators and standard users.
Switch to the secure desktop when prompting for elevation	Used to secure communication between the elevation prompt and other processes. When enabled, the UAC elevation prompt is limited to communication with processes that are part of Windows 7. This prevents malware from approving elevation. The default configuration is enabled.
Virtualize file and registry write failures to per-user locations	Used to enable non-UAC compliant applications to run properly. Applications that write to restricted areas are silently redirected to space in the user profile. The default configuration is enabled.

Malware Protection

- Windows 7 includes the following features to protect computers from malware:
  - Windows Defender
  - Microsoft Security Essentials

Windows Defender

- Windows Defender
  - Antispyware software included with Windows 7
- Spyware
  - Software that is silently installed on your computer, monitors your behavior, and performs actions based on your behavior
- Windows Defender provides two levels of protection:
  - On-demand scanning
  - Real-time scanning
- Scanning use signatures to identify spyware

Windows Defender (cont'd.)

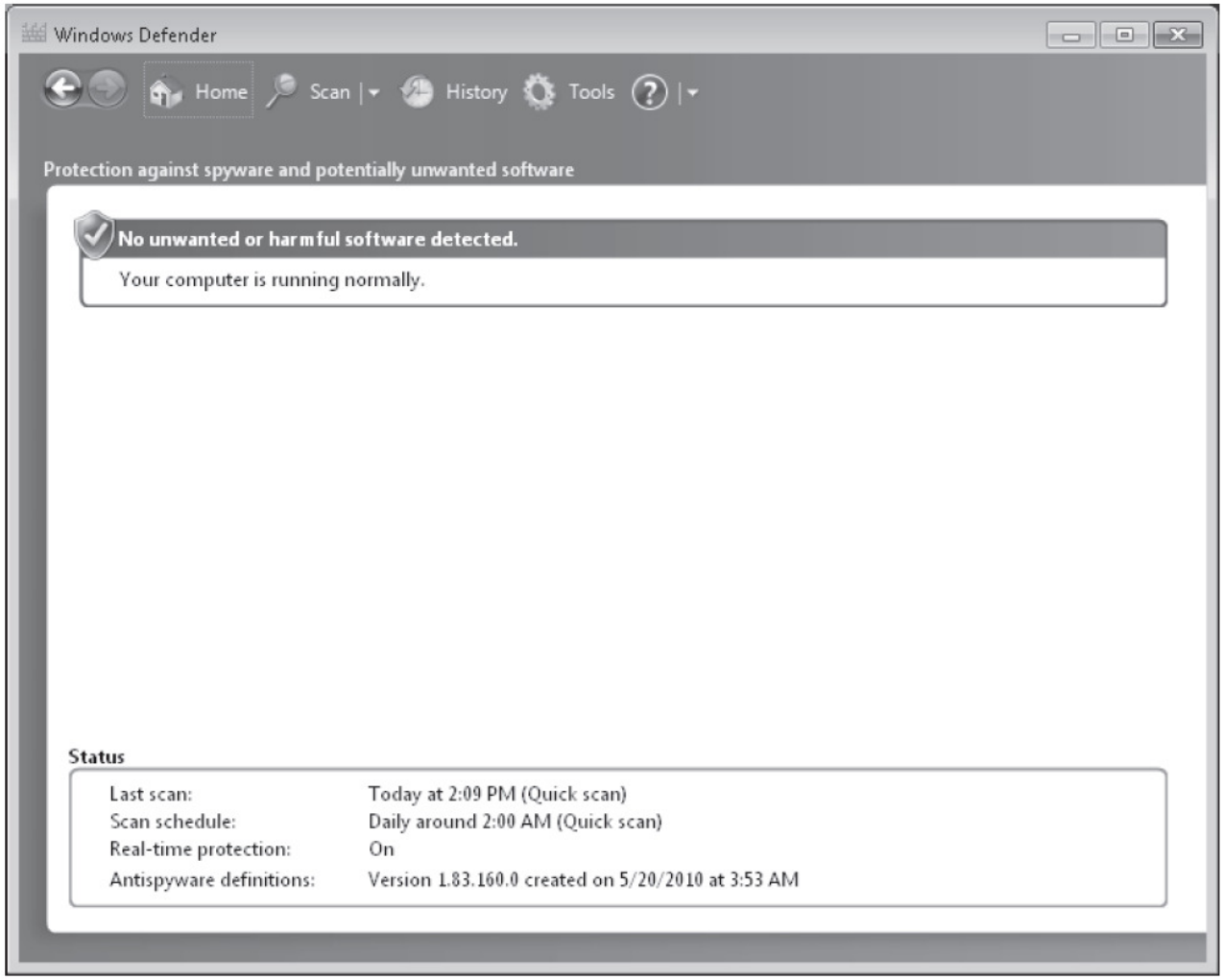

Figure 7-12 Windows Defender

Courtesy Course Technology/Cengage Learning

Windows Defender (cont'd.)

- On-Demand Scanning
  - Windows Defender can perform ad hoc scanning
    - When you suspect that spyware is present on your computer
  - Windows Defender can also perform scheduled scans
- Real-Time Scanning
  - Constantly monitors your computer and alerts you when spyware attempts to install
  - Better than on-demand scanning because you are preventing the problem rather than fixing it

Windows Defender (cont'd.)

- Real-Time Scanning (cont'd.)
  - Protects the following areas:
    - Downloaded files and attachments
    - Programs that run on my computer
- Windows Defender Alert Levels
  - Severe or High
  - Medium
  - Low

Windows Defender (cont'd.)

- Windows Defender Actions
  - When malware is detected, it can be quarantined, removed, or allowed
  - You can define default actions that are applied for severe, high, medium, and low alerts

Microsoft Security Essentials

- Viruses are a different type of software than spyware
- Some of the things viruses can do:
  - Send spam from your computer to the internet
  - Capture usernames and passwords for Web sites, including online banking
  - Steal enough personal information for identity theft
  - Allow others to remote control your computer and use it as a launching point for illegal activities
- Windows 7 does not include any software to protect your computer from viruses

Data Security

- NTFS permissions
  - Most basic level of data security in Windows 7
  - Stop logged-on users from accessing files and folders that they are not assigned read or write permission to
- Relatively easy to work around NTFS permissions
  - When you have physical access to the computer
- To secure data on desktop computers and laptops, encryption is required
  - Windows 7 includes Encrypting File System (EFS) and BitLocker Drive Encryption

Encryption Algorithms

- Encryption makes data unreadable
  - Decryption makes data readable again
- Symmetric encryption
  - Same key to encrypt data and decrypt data
  - The key is a long number that is very hard to guess
  - Symmetric encryption is strong and fast
    - Good for encrypting large volumes of data such as files
  - Used by both EFS and BitLocker Drive Encryption
  - Biggest problem is securing the key

Encryption Algorithms (cont'd.)

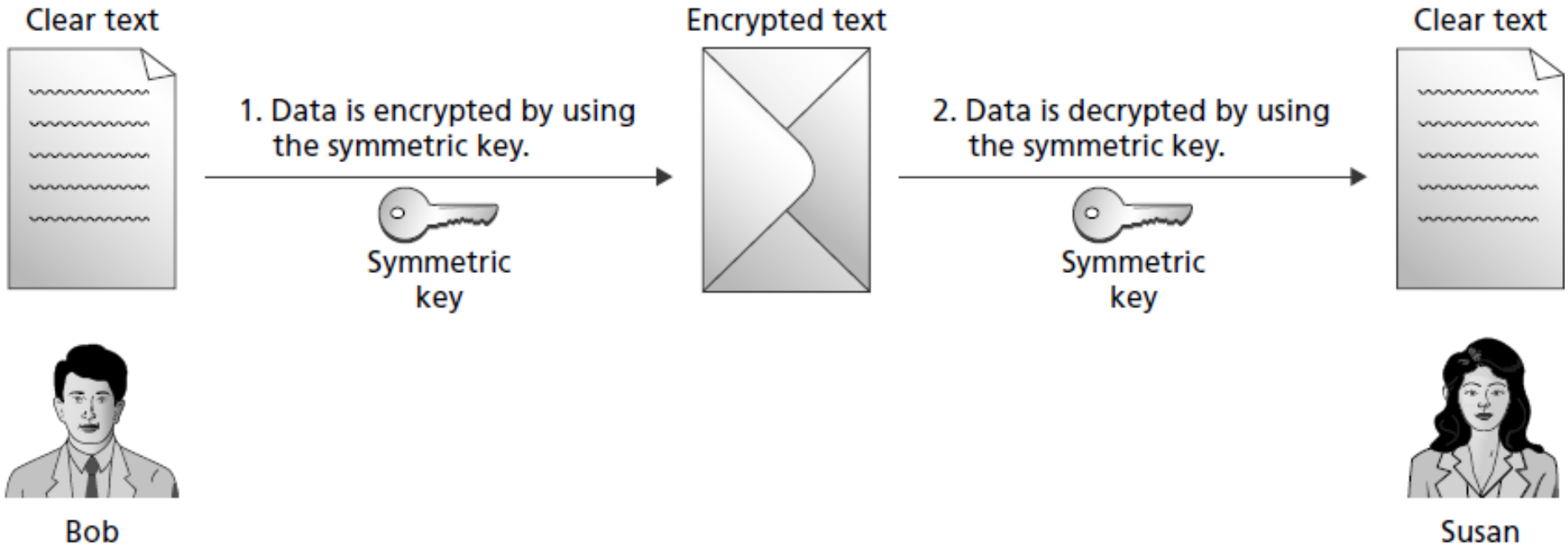

Figure 7-13 Symmetric encryption

Courtesy Course Technology/Cengage Learning

Encryption Algorithms (cont'd.)

- Asymmetric encryption
  - Uses two keys to encrypt and decrypt data
    - Data encrypted by one key is decrypted by the other
  - Keys are part of a digital certificate
  - Digital certificates are obtained from certificate authorities
  - Requires more processing power and is less secure than symmetric encryption
  - Use symmetric encryption to encrypt the data and then use asymmetric encryption to protect just the symmetric key

Encryption Algorithms (cont'd.)

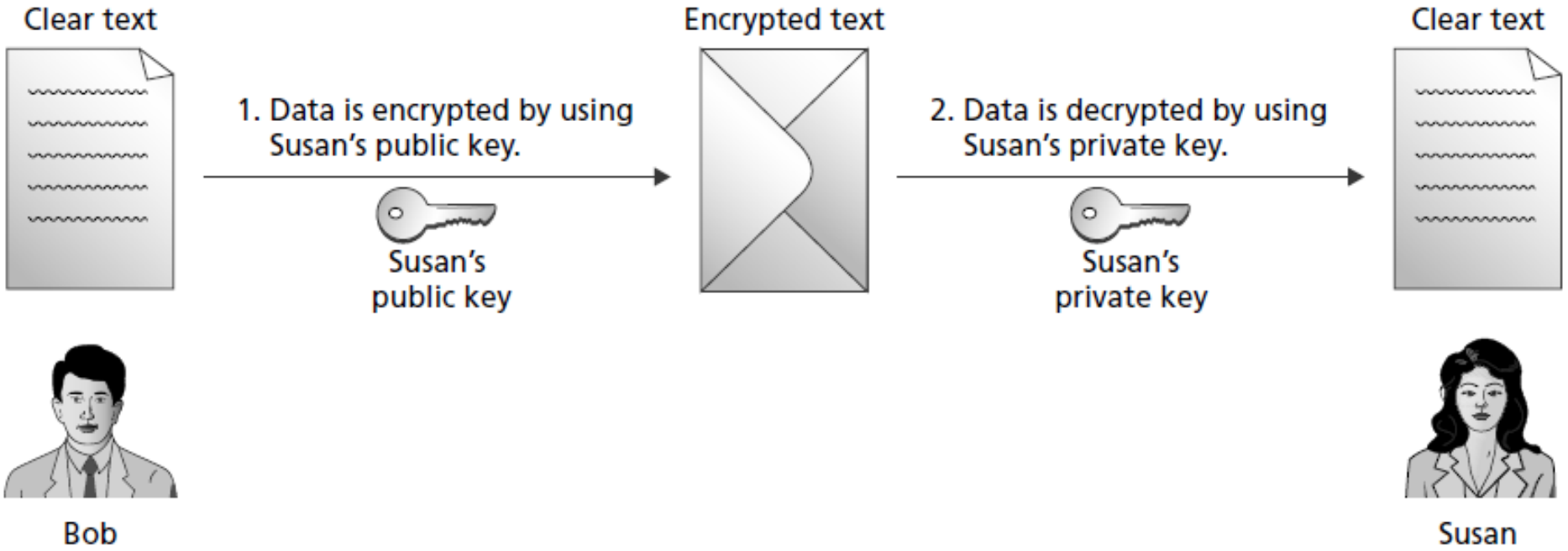

Figure 7-14 Asymmetric encryption

Courtesy Course Technology/Cengage Learning

Encryption Algorithms (cont'd.)

- Hash encryption
  - One-way encryption
    - It encrypts data, but the data cannot be decrypted
  - Used to uniquely identify data rather than prevent access to data
  - Sometimes hash values for data are called fingerprints
  - Used for storing passwords
  - When passwords are stored as only a hash value, it is impossible to decrypt the password

Encryption Algorithms (cont'd.)

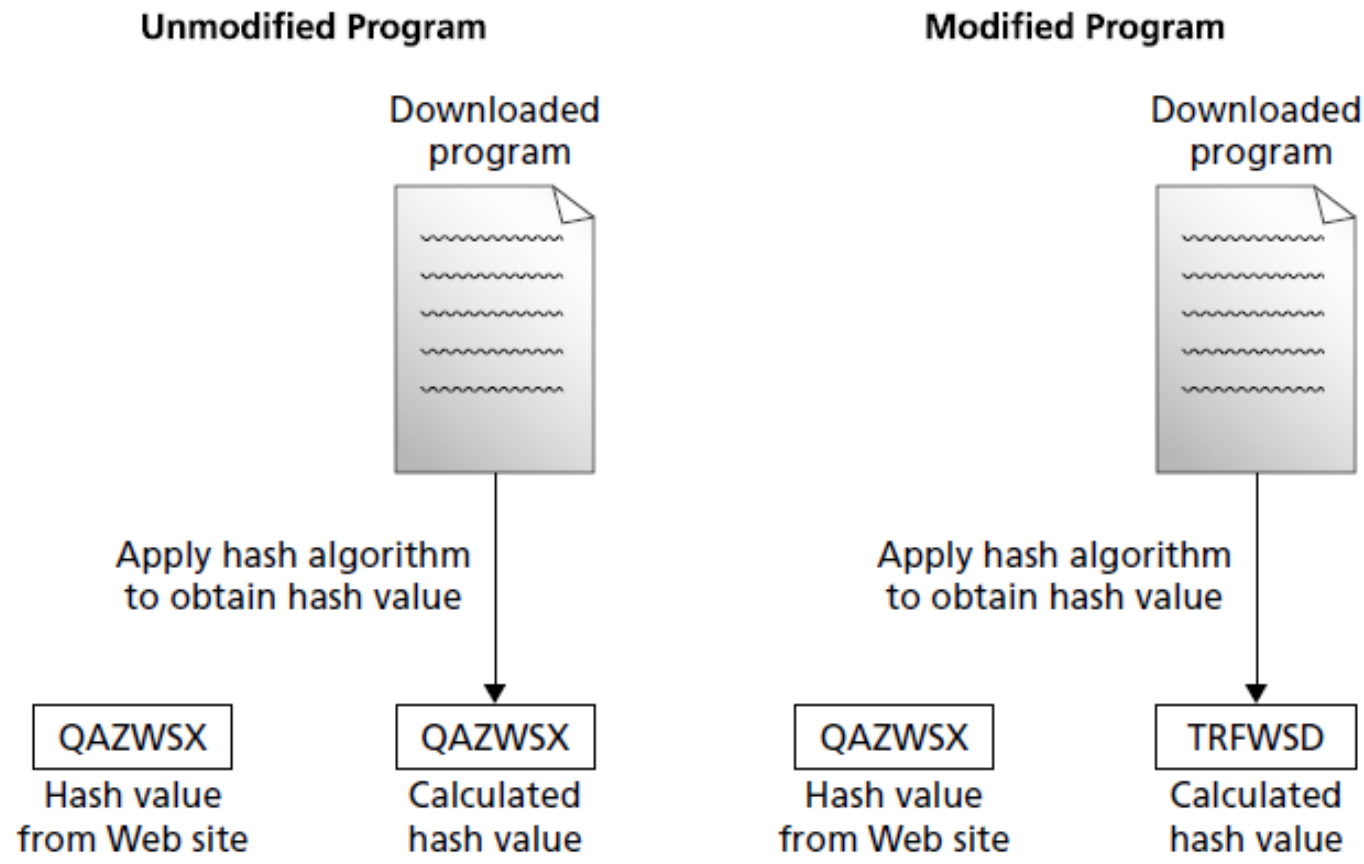

Figure 7-15 Using a hash value to verify software integrity

Courtesy Course Technology/Cengage Learning

Encrypting File System

- Encrypting File System (EFS)
  - First included with Windows 2000 Professional
  - Encrypts individual files and folders on a partition
  - Suitable for protecting data files and folders on workstations and laptops
  - Can also be used to encrypt files and folders on network servers
- File or folder must be located on an NTFS-formatted partition

Encrypting File System (cont'd.)

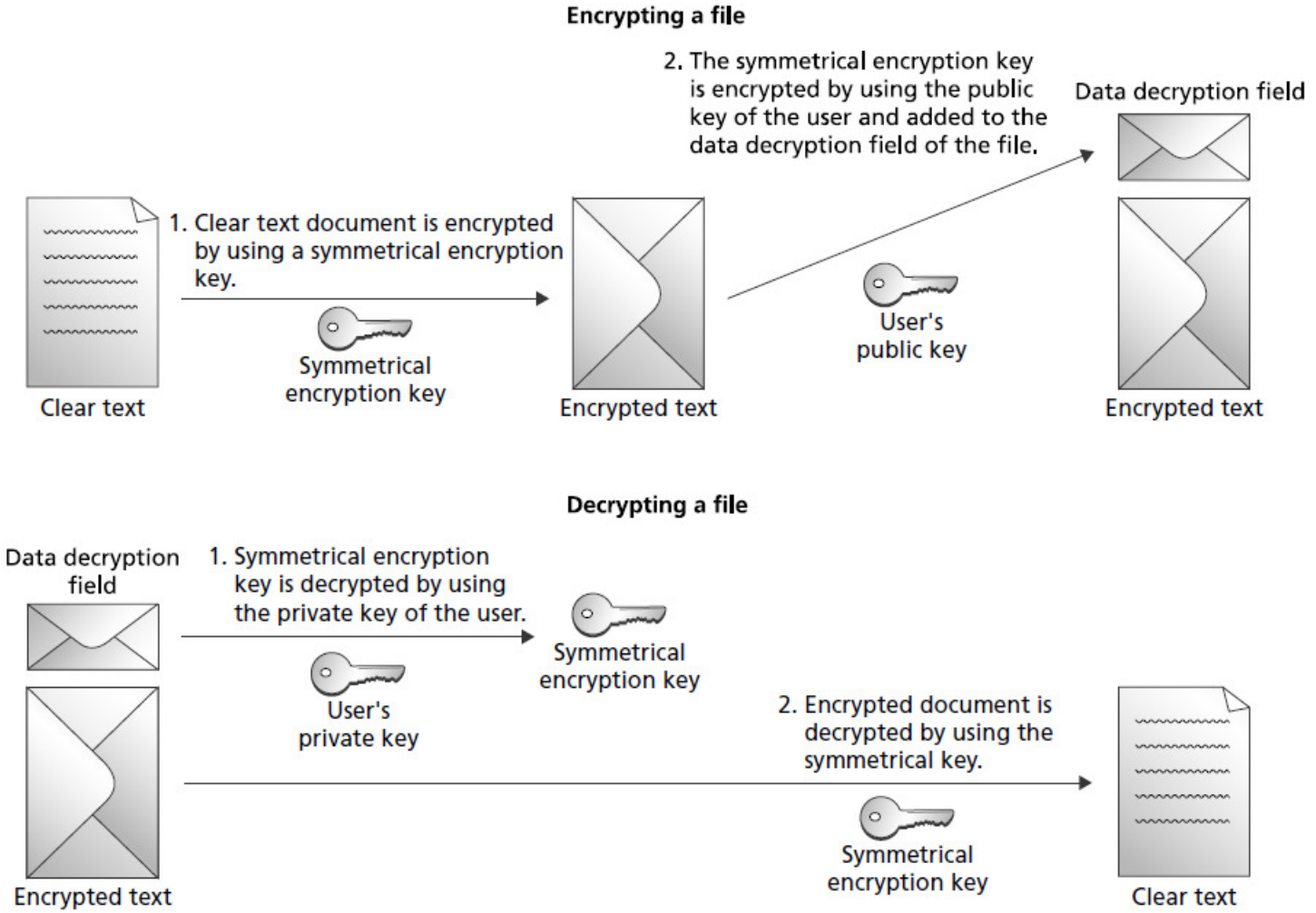

Figure 7-16 EFS encryption and decryption process

Courtesy Course Technology/Cengage Learning

Encrypting File System (cont'd.)

- To use EFS, users must have a digital certificate with a public key and a private key
  - Windows 7 can generate one for you
- From the user perspective, encryption is a file attribute
- Files can also be encrypted using the command-line utility Cipher
- Lost encryption keys
  - If a user loses the EFS key, then an encrypted file is unrecoverable with the default configuration

Encrypting File System (cont'd.)

Figure 7-17 Advanced Attributes of a file

Courtesy Course Technology/Cengage Learning

Encrypting File System (cont'd.)

- Lost encryption keys
  - Some ways EFS keys may be lost
    - The user profile is corrupted
    - The user profile is deleted accidentally
    - The user is deleted from the system
    - The user password is reset
  - In User Accounts, there is an option to manage file encryption certificates
    - Allows you to view, create, and back up certificates
  - Creating a recovery certificate allows the files encrypted by all users to be recovered if required

Encrypting File System (cont'd.)

- Lost encryption keys (cont'd.)
  - Steps for creating and using a recovery certificate
    - Create the recovery certificate
    - Install the recovery certificate
    - Update existing encrypted files
- Sharing Encrypted Files
  - Steps to work with encrypted files on multiple computers
    - Encrypt the file on the first computer
    - Export the EFS certificate, including the private key from the first computer

Encrypting File System (cont'd.)

- Sharing Encrypted Files (cont'd.)
  - Steps to work with encrypted files on multiple computers (cont'd.)
    - Import the EFS certificate, including the private key on the second computer
    - Open the encrypted file on the second computer
  - Steps to share encrypted files with other users
    - Export the EFS certificate of the first user, but do not include the private key
    - Import the EFS certificate of the first user into the profile of the second user as a trusted person
    - Second user encrypts file and shares it with first user

Encrypting File System (cont'd.)

- Moving and Copying Encrypted Files
  - Encrypted files behave differently when copied or moved
  - Rules for moving and copying encrypted files
    - An unencrypted file copied or moved to an encrypted folder becomes encrypted
    - An encrypted file copied or moved to an unencrypted folder remains encrypted
    - An encrypted file copied or moved to a FAT partition, FAT32 partition, or floppy disk becomes unencrypted
      - If you have access to decrypt the file

Encrypting File System (cont'd.)

- Moving and Copying Encrypted Files (cont'd.)
  - Rules for moving and copying encrypted files (cont'd.)
    - If you do not have access to decrypt a file, then you get an access-denied error
      - If you attempt to copy or move the file to a FAT partition, FAT32 partition, or floppy disk

BitLocker Drive Encryption

- BitLocker Drive Encryption
  - Data encryption feature included with Windows 7
- An entire volume is encrypted when you use BitLocker Drive Encryption
  - Also protects the operating system
- Designed to be used with a Trusted Platform Module (TPM)
  - Part of the motherboard in your computer and used to store encryption keys and certificates

BitLocker Drive Encryption (cont'd.)

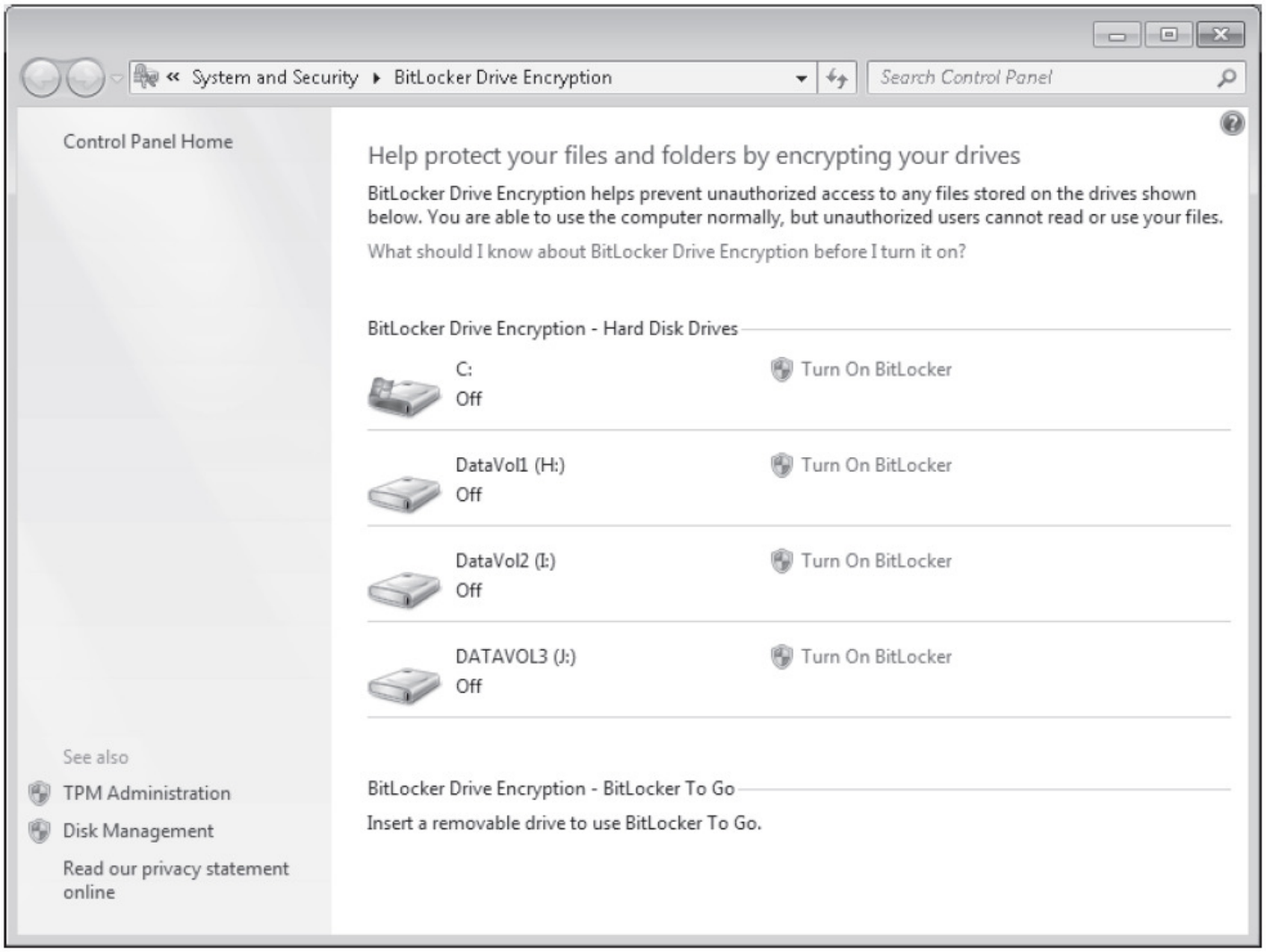

Figure 7-18 BitLocker Drive Encryption

Courtesy Course Technology/Cengage Learning

BitLocker Drive Encryption (cont'd.)

- BitLocker Drive Encryption modes
  - TPM only
  - Startup key
- BitLocker Hard Drive Configuration
  - Hard drive must be divided into two partitions
    - Encrypted partition: the operating system volume
    - Unencrypted system partition: contains necessary files to boot the operating system

BitLocker Drive Encryption (cont'd.)

- BitLocker Encryption Keys
  - Volume Master Key (VMK)
    - Encrypt data on the operating system volume
  - Full Volume Encryption Key (FVEK)
    - Used to encrypt the VMK
- Recovering BitLocker-Encrypted Data
  - A recovery password is generated automatically
  - You can save it to a USB drive or folder, display on the screen, or print

BitLocker Drive Encryption (cont'd.)

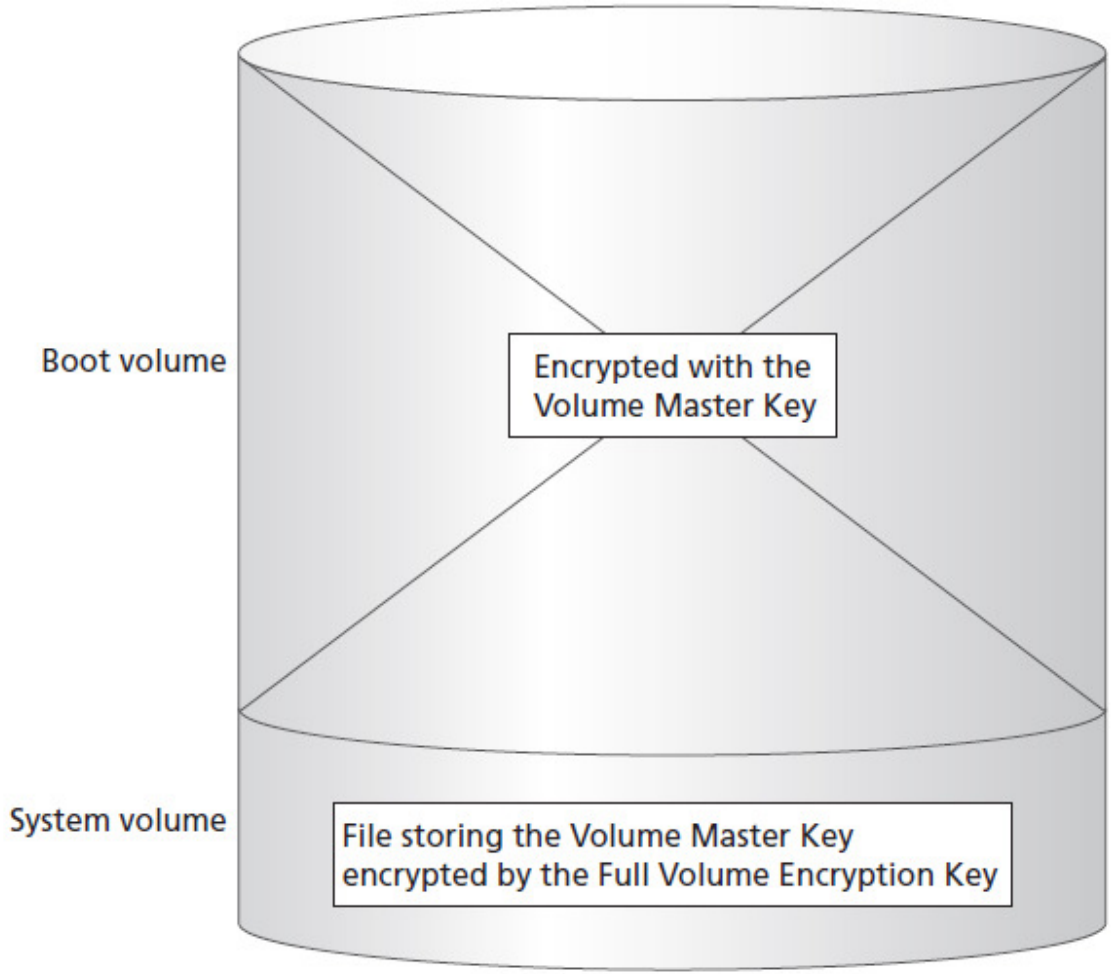

Figure 7-19 BitLocker Encryption Keys

Courtesy Course Technology/Cengage Learning

BitLocker Drive Encryption (cont'd.)

- Recovering BitLocker-Encrypted Data (cont'd.)
  - Recovery password is required when the normal decryption process is unable to function
  - Most common reasons include:
    - Modified boot files
    - Lost encryption keys
    - Lost or forgotten startup PIN
- Disabling BitLocker Drive Encryption
  - Decrypts all of the data on the hard drive and makes it readable again

BitLocker Drive Encryption (cont'd.)

- BitLocker To Go
  - Included with Windows 7
  - Protects data on removable storage such as USB drives
  - Options for unlocking removable storage:
    - Use a password to unlock the drive
    - Use my smart card to unlock the drive

Windows Update

- Scheduling automatic updates with Windows Update
  - The most important security precaution you can take with Windows 7
- When a Windows security flaw is found, the flaw is reported to Microsoft
  - Microsoft releases a patch to fix the problem
- Windows Update categories
  - Important
  - Recommended
  - Optional

Windows Update (cont'd.)

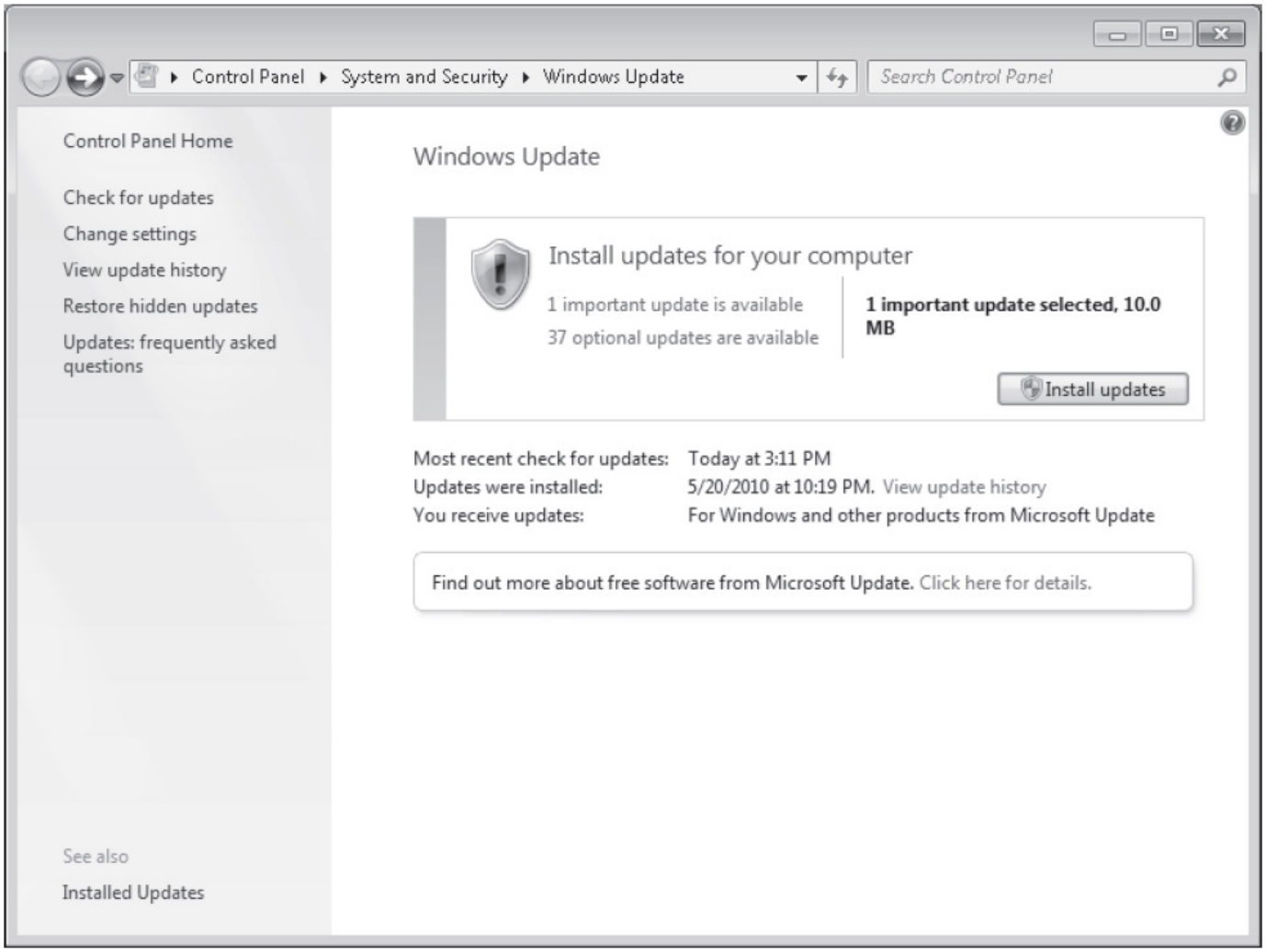

Figure 7-20 Windows Update

Courtesy Course Technology/Cengage Learning

Windows Update (cont'd.)

- Windows Update settings
  - Install updates automatically (recommended)
  - Download updates but let me choose whether to install them
  - Check for updates but let me choose whether to download and install them
  - Never check for updates (not recommended)
- Microsoft Update is an alternative to Windows Update

Windows Update (cont'd.)

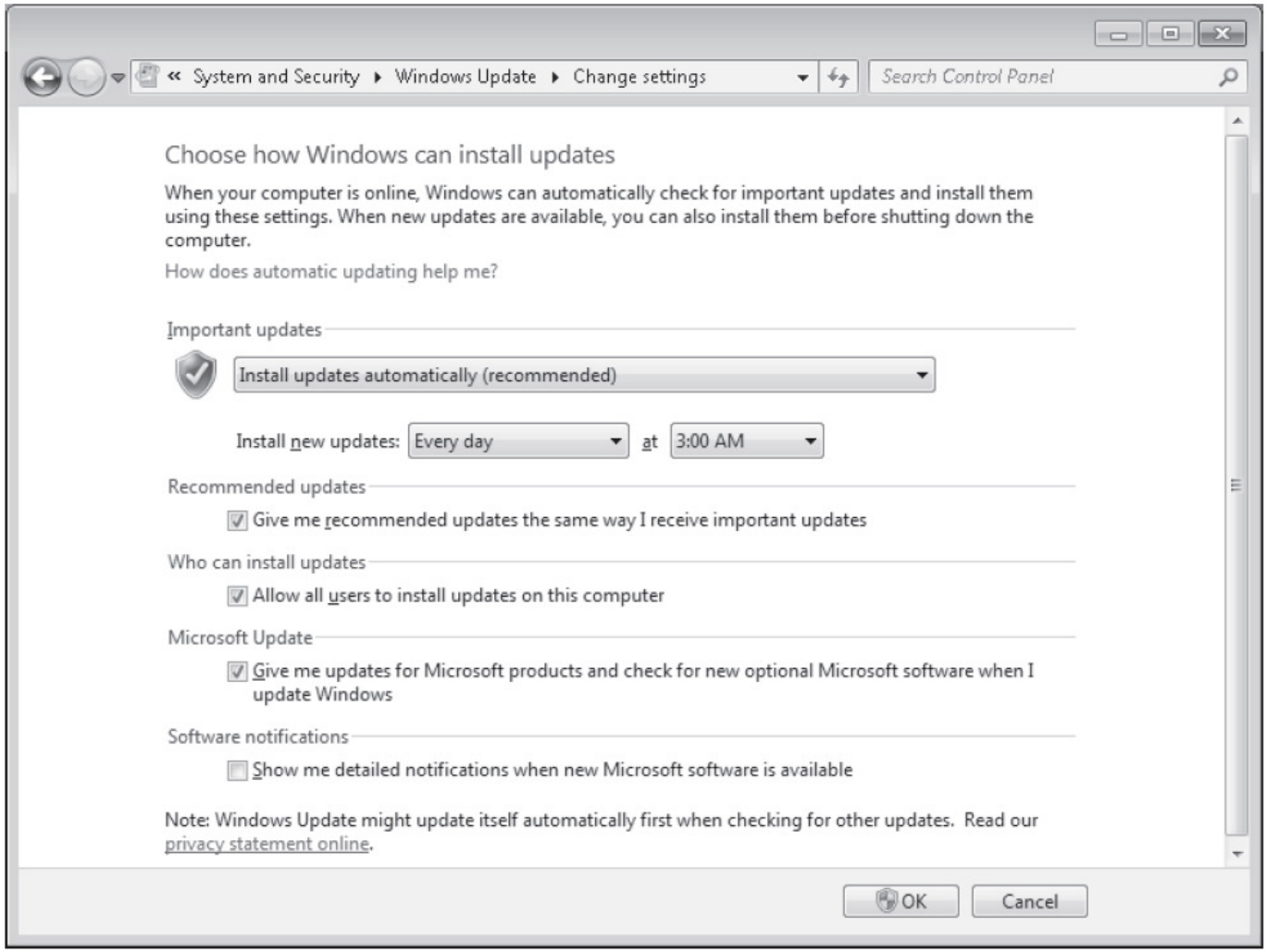

Figure 7-21 Windows Update settings

Courtesy Course Technology/Cengage Learning

Windows Update (cont'd.)

- Windows Update process can be modified to use Windows Server Update Services (WSUS)
  - WSUS allows corporations to test patches before releasing them

Action Center

- Action Center
  - Control Panel applet that lets you quickly check important security settings in Windows 7
- Settings monitored by Windows Security
  - Network Firewall
  - Windows Update
  - Virus protection
  - Spyware and unwanted software protection
  - Internet security settings
  - User Account Control
  - Network Access Protection

Windows Security Center (cont'd.)

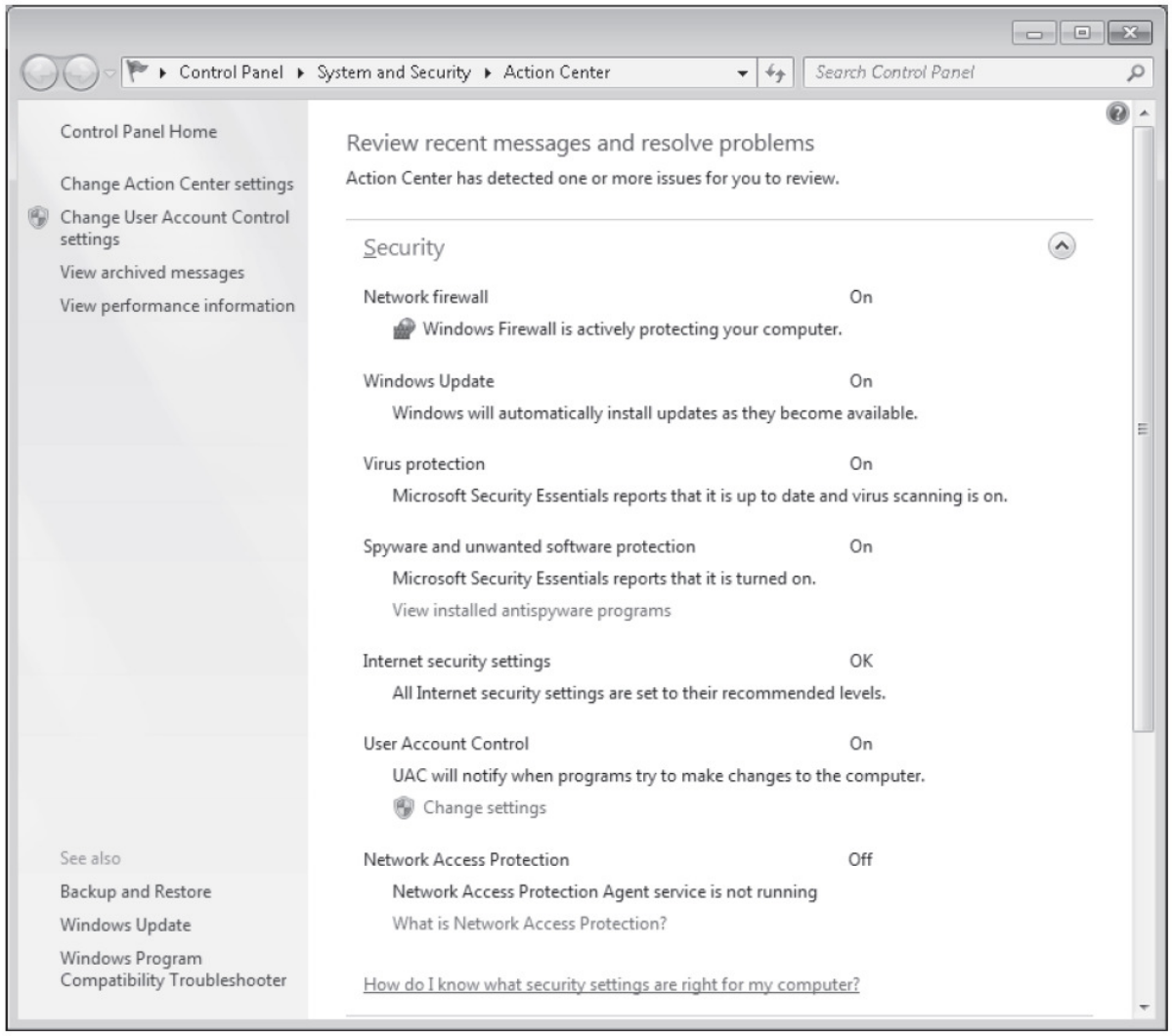

Figure 7-22 Action Center
Courtesy Course Technology/Cengage Learning

Summary

- Windows 7 has new improved security features
- Windows 7 supports various security policies including local security and account policies
- Security templates can be used to configure or analyze Windows 7 security options
- Analyzing and applying security templates is done with Secedit or the Security Configuration and Analysis MMC snap-in
- Auditing is used to record specific operating system events to the security log

Summary (cont'd.)

- UAC increases security by allowing users to log on and perform their jobs with standard user accounts
- Windows Defender is antispyware software
- Microsoft Security Essentials is free antivirus software
- EFS protects individual files by encrypting them
- BitLocker Drive Encryption encrypts an entire partition
- Windows Update ensures that patches are applied to Windows 7 as they are made available