

Index

• Numerics •

48-bit recovery option, 192
128-bit encryption, 173, 188
256-bit encryption, 173, 188
256-bit recovery option, 192

• A •

About.com identity-theft site, 330
Access Control Entry (ACE), 105
access control list (ACL), 109
access control model, 335
access levels, 40
access management
 with auditing and logging, 124–132
 discussed, 96, 103
 to floppy, 299
 with NTFS permissions, 111–116
 object-level security, 96–97, 103–111
 to Registry, 116–124
 system security settings, 96
access point (AP). *See also* wireless access point
 in discovery process, 218–219
 and SSID values, 235
 username and password for, 232
account(s)
 built-in, 83–87
 defined, 81
 managing, 81–83
 password-protected, 286
 SAM, 299
account-lockout policy, 297–298
ACE (Access Control Entry), 105
ACL (access control list), 109
action pane, 206
Active Directory (AD)
 and domain network, 207, 296–297
 Domain Profile, 207
 password policies, 296–297
Active Server Pages (ASP), 250
ActiveX
 defined, 241, 335
 and DHTML, 246
 disabling, 250
 and HTML, 241
 and IE7, 15, 241–243
 in Internet Zone, 250
 object caching, 253
 properties of, 256
 security risks of, 236
 threat of, 243
 typically installed, 255
ActiveX Opt-In
 and automatic downloads, 256
 defined, 242, 257
 options, 242–243
 and security risks, 243
acts of God (natural threat-sources), 32
AD. *See* Active Directory
ad hoc (peer-to-peer) wireless network
 defined, 335
 discussed, 219, 230–232, 320
Add button
 for ACEs, 114
 in File Sharing Wizard, 99
Add text (File Sharing Wizard), 98, 99
Admin Approval mode
 administrators in, 69–70
 for built-in administrators, 59–61
 defined, 335
 disabled, 60
 elevation prompt for administrators in,
 61–63
 enabled, 60, 61
 Local Security Policy, 59–63
 and Standard User mode, 55–57
 and UAC, 69–70
administrative templates
 custom, 303
 discussed, 302
 interface, 303–304
 and Registry, 302
 settings, 303

- administrative username, 232–233
- Administrator (account), 83–84
 - in Admin Approval mode, 61–63, 69–70
 - built-in, 59–61, 300
 - common tasks of, 55
 - elevation prompt for, 61–63
 - sharing, 98
 - Standard Users versus, 55
- Administrators (group), 82, 84
- .adm, 303
- Advanced Encryption Standard (AES), 173, 188
- Advanced Security applet
 - Getting Started section with, 211–213
 - and Resources pane, 213–214
 - Windows Firewall with, 205–214
- Advanced tab (Windows Firewall), 204–205
- adware, 260
- AES (Advanced Encryption Standard), 173, 188
- alert(s)
 - for application installations, 65
 - when program is blocked, 203
 - in Windows Defender, 270–271
 - in WSC, 50
- allow
 - access, 214
 - connection, 212
 - secure connections, 212
 - Unicast Response, 210
- Allowed Items, 274–275
- anonymous enumeration, 299
- ANONYMOUS LOGON, 84
- antispymware, 261
- antivirus software
 - discussed, 325–326
 - and firewalls, 328
 - in mobile devices, 322
- AP. *See* access point
- application installations
 - alerts for, 65
 - backing up, 141
 - by malicious programs, 65
- Apply To, 114, 115
- archive folder, 151
- ASP (Active Server Pages), 250
- asymmetric encryption
 - defined, 335
 - discussed, 160–161
 - and symmetric encryption, 163
- @RISK: The Consensus Security Alert (newsletter), 329
- attachment
 - in e-mail, 318
 - in instant messaging, 321
- Audit Account Logon Events, 126
- Audit Account Management, 126
- Audit Logon Events, 126
- Audit Object Access, 126, 130
- audit policy, 298
- Audit Policy Change, 126
- Audit Privilege Use, 126–127
- Audit Process Tracking, 127
- Audit System Events, 127
- auditing
 - access management with, 124–132
 - defined, 105, 125
 - discussed, 105, 124–125
 - and logging, 124–132
 - of NTFS objects, 130–131
 - of objects, 130–132
 - passive, 131
 - policies, 124–129
 - of Registry objects, 131
 - of service objects, 131
- AuditPol.exe, 298
- Authenticate Communications between Computers section (Getting Started), 211
- Authenticated Users, 83, 85, 106
- authentication, 81–82, 335
- authorization, 335
- Auto Start, 265
- automatic (scheduled) scan, 269, 270
- Automatic Updating
 - and ActiveX Opt-In, 256
 - discussed, 44
 - managing, 45–46
 - monitoring, 45
 - and WSC, 44–46

Automatically Deny Elevation Requests,
63–64

AutoPlay and AutoRun
of CD/DVDs, 285
policies, 304

availability, 20, 36

• **B** •

backing up

advanced methodologies, 140
application information, 141
with Backup and Restore, 151–154
with Backup Files Wizard, 152–153
business information, 141
on CD, 152
with CompletePC Backup, 139, 154–157

discussed, 135

on DVD, 152

encryption keys, 170

files, 138–139, 146, 152–153

folders, 138–139, 146

on hard disk, 152

options for, 137–140

organization for, 150–151

and partitioning, 174

preserving data by, 147–150

private keys, 170

reasons for, 136–137

requirements for, 140–144

with Shadow Copy, 139–140

with shadow copy, 157

storage media for, 142

strategy planning for, 145–147

supported devices for, 140

system data, 141

with System Restore, 137–138, 147–149

third-party software for, 327–328

Backup and Restore Center

defined, 335

discussed, 151–154

Backup Files Wizard, 152–153

Backup Log Automatically When Full, 129

Backup Operators, 84

BATCH, 84

BCWipe (Jetico), 333

binary behaviors

and DHTML, 246

in IE7, 246

BIOS

and BitLocker, 173

changes to, 180

BitLocker

additional security with, 187

advanced options, 181–182

basic options, 179–181

and BIOS, 173

data recovery, 191–194

and data theft, 171–173

defined, 17, 172, 335

disabling, 195–196

discussed, 171–173

encryption with, 16–17, 188–189

folders, recovering, 191–192

and Group Policy Object Editor, 178, 191

interface, 179, 195

methods, 188–189

options for recovery, 192–194

and PIN, 183–186

preparing system for, 174–178

Prevent Memory Overwrite, 189–191

recovering data, 191–194

for removable media, 196

requirements for, 173–174

setting up, 178–187

and startup key, 186–187

and TPM, 173, 179, 182–187

weaknesses of, 196

BitLocker Drive Encryption, 194, 304

blocking

alerts, 203

connections, 201, 208, 209, 212

of file downloads, 13

of inbound connections, 201, 208

of programs, 203

with spyware removal tools, 327

Bluetooth, 322

boot protection, 172

broadband Internet, 313. *See also* wireless
network

broadband router, 314

built-in account, 83–87

built-in administrator, 59–61, 300
 built-in group (special identity), 83–87
 built-in identity, 83–87
 business information
 backing up, 141
 protection of, 21

• C •

Cancel button (File Sharing Wizard), 100
 caution, 215
 CD
 AutoPlay and AutoRun, 285
 backing up on, 152
 deny write access to, 292
 CD-ROM access, 299
 cellphone. *See* mobile device
 Change (permission), 78
 Change button, 115
 Change Scope button, 203
 Change Settings, 46
 Check for Updates, 45
 Check Names, 92
 Check this Web site, 245
 child object, 109, 111
 children, controls for, 12
 Classic View (UAC), 59
 Clear All button, 115
 code, 10
 Cogswell, Bryce, 332
 common sense, 24
 Communications, Secure in, 9, 10
 company financials, 21
 CompletePC Backup (system image)
 backing up with, 154–155
 description, 146
 discussed, 139, 154–157
 restoring, 155–156
 and shadow copies, 156–157
 Components (Windows), 304
 compressed files, 162
 compressed folder, 162
 computing, 1, 12
 confidentiality, 36–37
 configuration policy, 301
 Consent, Prompt for, 61, 63
 console tree, 206
 Container Only check box, 115
 Contributor (permission), 100

Control Panel, 303
 Co-Owner (permission), 100
 Credentials, Prompt for
 in Administrator mode, 62
 in Standard User mode, 63
 cross-domain scripting protection, 15–16
 cross-domain security
 defined, 257
 and IE7, 243–244
 scripting attacks, 15–16, 243–244
 Currently Running Programs, 276
 custom scan, 11, 268
 customer information, 21

• D •

DACL (Discretionary Access Control List),
 104, 105
 data. *See also* sensitive information
 backing up, 147–150
 in BitLocker, 191–194
 and EFS, 167–168
 organizing, 150–151
 preserving, 147–150
 recovering, 167–168, 191–194
 on removable media, 286–288
 removing, 286–287
 System Restore for, 147–149
 Data Recovery Agent, 163
 data scrubber program, 288
 data theft, 171–173
 DDoS (Distribute Denial-of-Service), 317–318
 decryption, 336
 Default, Secure by, 9, 10
 Default Action (Definition-Based), 271, 272
 Default View (UAC), 59
 Defender. *See* Windows Defender
 definition files, 262–263, 269
 deny write access, 292
 Deployment, Secure in, 9, 10
 Design, Secure by, 9, 10
 Desktop, 303
 detect application installations
 disabled, 65
 for elevation prompts, 65–66
 enabled, 65
 device
 installation, 290–291
 usage, 292

- Device Control
 - defined, 288
 - for device installation, 290–291
 - for device usage, 292
 - discussed, 288
 - and Group Policy, 289
 - installation settings of, 288–289
 - for removable media, 286–292
 - usage settings of, 289–290
 - DHCP (Dynamic Host Configuration Protocol), 221, 228
 - DHTML (Dynamic HTML), 246
 - Diffuser, 173, 188
 - diffusion, 188
 - digital certificate
 - defined, 336
 - support for, 161
 - Digital Rights Management (DRM), 80
 - digital signature, 336
 - discovery process, 218–219
 - Discretionary Access Control List (DACL), 104, 105
 - Distribute Denial-of-Service (DDoS), 317–318
 - Do Not Forward policy, 77
 - document, 74
 - Documents folder
 - discussed, 151
 - encryption of, 169
 - files in, 151
 - organization of, 169
 - domain network
 - and Active Directory, 207, 296–297
 - discussed, 219
 - Domain Profile, 207
 - downtime, 136
 - drive-preparation tool, 176–178
 - DRM (Digital Rights Management), 80
 - DVD
 - AutoPlay and AutoRun, 285
 - backing up on, 152
 - deny write access to, 292
 - Dynamic Host Configuration Protocol (DHCP)
 - disabling, 221, 228, 234
 - and wireless networking hardware, 234
 - Dynamic HTML (DHTML)
 - and ActiveX, 246
 - and binary behaviors, 246
- **E** •
- Edit button, for ACEs, 114
 - effective permissions, 105–108
 - EFS. *See* Encrypting File System
 - Elevate without Prompting, 62
 - elevated privilege, 336
 - elevation prompt
 - in Admin Approval mode, 61–63
 - for administrators, 61–63
 - and automatic denial, 63–64
 - defined, 56
 - detect application installations, 65–66
 - and Secure Desktop, 70–71
 - signature checks for, 66–67
 - for Standard Users, 63–65
 - in UAC, 61–68
 - UIAccess, 67–68
 - e-mail
 - attachments, 318
 - MIMC attacks via, 319
 - and mobile devices, 322
 - permissions from, 79
 - security risks with, 318–319
 - employment-related information, 21
 - encrypted file
 - discussed, 162, 163, 168–169
 - in folders, 164
 - sharing, 166
 - Encrypting File System (EFS)
 - and data recovery, 167–168
 - defined, 17, 336
 - discussed, 159, 163
 - encryption with, 16–17
 - for files, 161–163, 162, 166
 - for folders, 161, 164–165
 - and Group Policy, 168
 - protection with, 162
 - and roaming profiles, 170
 - for specific files, 166
 - strategy for use of, 168–170
 - user education for, 168
 - encryption
 - 128-bit, 173, 188
 - 256-bit, 173, 188
 - asymmetric, 160–161, 163, 335
 - with BitLocker, 16–17, 188–189
 - BitLocker Drive Encryption, 194, 304

- encryption (*continued*)
 - defined, 336
 - discussed, 16, 159–160
 - of Documents folder, 169
 - with EFS, 16–17
 - for mobile devices, 322
 - for removable media, 287–288
 - removing, from files, 167
 - with RMS, 74
 - of sensitive information, 168–169
 - symmetric, 160, 163, 188, 339
 - with WinZip, 287–288
 - encryption key, 170
 - Enter the Object Names to Select, 92
 - enumeration, anonymous, 299
 - environmental threat-sources, 32
 - event log, 128, 300
 - Event Log key, 124
 - Event Log Readers, 85
 - Everyone (identity), 83, 85
 - Exceptions tab (Windows Firewall), 202–203
 - Exclusion Policies, 75
 - explicit security
 - inherited security versus, 108–111
 - permissions, 111
 - Explorer (Windows), 304
 - eXtensible Rights Markup Language (XRML), 74, 250
- F ●**
- FAT32 permissions, 112
 - file(s)
 - backing up, 138–139, 146, 152–153
 - compressed, 162
 - definition, 269
 - deletion of, 332–333
 - in Documents folder, 151
 - EFS for, 161–163, 166
 - encrypted, 162–164, 166, 168–169
 - and firewalls, 101–102
 - in folders, 164
 - organizing, 151
 - overwrite, 139–140
 - permissions, 112
 - recovering, 167
 - removing encryption from, 167
 - restoring, 153–154
 - secure deletion of, 332–333
 - sharing, 98–102, 166
 - unencrypted, 162
 - File and Folder Backup Wizard, 138–139
 - File Expiration Date, 78
 - File Sharing (Windows), 224
 - File Sharing Wizard, 98–101
 - file-download blocking, 13
 - Files Only option, 130–131
 - Find Now, 93
 - firewall(s). *See also* Windows Firewall
 - advanced, 329
 - and antivirus software, 328
 - discussed, 328–329
 - and hotspots, 224
 - from ISV, 215
 - for mobile devices, 322
 - other types of, 215
 - protection with, 328–329
 - and services, 15
 - sharing, 101–102
 - Firewall Settings, 209
 - Firewall State, 208
 - floppy, access to, 299
 - folder(s)
 - archive, 151
 - backing up, 138–139, 146
 - and BitLocker, 191–192
 - compressed, 162
 - defined, 151
 - Documents, 151
 - EFS for, 161, 164–165
 - organizing, 151
 - permissions, 112
 - public, 101
 - recovering, 168, 191–192
 - removing encryption from, 167
 - restoring, 153–154
 - sharing, 101
 - 48-bit recovery option, 192
 - free space, 178
 - From This Location, 92, 93
 - Full Control (permission), 78, 106
 - full scan, 11, 267, 268

• G •

gadget, sidebar, 331
 gaming restrictions, 13
 General tab (Windows Firewall), 201
 Getting Started section
 with Advanced Security applet, 211–213
 Authenticate Communications between
 Computers section, 211
 discussed, 211
 Monitoring section, 213
 View and Create Firewall Rules section,
 211–213
 GIANT antispymware, 261
 GIANT Company Software Inc., 261
 gpedit.msc, 289, 296, 297. *See also* Group
 Policy Object Editor
 greynet applications, 260
 group(s)
 assigning users to, 94–95
 built-in, 83–87
 creating, 94–95
 defined, 81
 managing, 81–83
 Group Policy
 and Device Control, 289
 and EFS enforcement, 168
 Group Policy Object Editor
 and BitLocker, 178, 191
 defined, 295
 discussed, 295–296
 for local security policies, 296
 for Security Event log, 128–129
 Guest (account), 85

• H •

hard disk
 backing up on, 152
 partitioning, 174–176
 hardware
 discussed, 30
 failure, 136
 protection of, 19–20
 System Restore for, 138
 for wireless networks, 230–232
 hiberfil.sys, 178
 Hibernation, 178
 High alert, 270

HKEY_CURRENT_USER (HKCU), 117, 123
 HKEY_LOCAL_MACHINE (HKLM), 117,
 123–124
 HTML
 and ActiveX controls, 241
 and Internet Zone, 248
 in Internet Zone, 248
 HTTP (HyperText Transfer Protocol), 249
 human element
 of security risks, 39–40
 human threat-sources, 32
 HyperText Transfer Protocol (HTTP), 249

• I •

ICS (Internet Connection Sharing), 320
 identification, 81
 identity, built in, 83–87
 identity theft
 About.com, 330
 defined, 336
 identity-theft site (About.com), 330
 IE7. *See* Internet Explorer 7
 Ignore (threat), 271
 IIS_IUSRS (group), 85
 IM (instant messaging)
 attachments, 321
 MMC attacks via, 319
 security risks with, 321
 inbound connections
 configuring, 208–209
 defined, 207
 Include Inheritable Permissions, 115
 Independent Software Vendor (ISV), 43, 215
 Information Rights Management (IRM)
 discussed, 76
 document protection with, 78–79
 and Microsoft Outlook, 76–78
 and RMS, 76–79
 inheritance, 108–111
 Inherited From, 114
 inherited security, 108–111
 instant messaging (IM)
 attachments, 321
 MMC attacks via, 319
 security risks with, 321
 integrity, 36
 integrity level, 239
 INTERACTIVE (identity), 85–86

- interface
 - administrative templates, 303–304
 - BitLocker, 179, 195
 - Regedit, 118
 - Select Objects, 90–93
 - spyware removal tools, 327
 - of systems, 31
 - of Windows Defender, 11, 262
 - Windows Firewall, 199
 - for Windows Firewall configuration, 18
 - WSC, 42
 - Internet
 - MMC attacks via, 319
 - and mobile devices, 322
 - Internet Connection Sharing (ICS), 320
 - Internet Explorer (IE)
 - add-ons to, 265
 - administrative template, 304
 - Configurations, 266
 - group policy settings, 302
 - RMS in, 78–79
 - and Windows Defender, 261–263
 - Internet Explorer (IE) 7
 - and ActiveX, 241–243
 - address bar, 257
 - binary behavior, 246
 - Binary Behaviors, 246
 - and cross-domain scripting attacks, 243–244, 244
 - defined, 336
 - discussed, 15, 237, 256–257
 - MIME, 249–250
 - and MMC, 320
 - network protocols, 250–253
 - object caching, 253–156
 - Parental Controls in, 16
 - permissions in, 15
 - phishing protection in, 16, 244–246
 - Protected Mode, 237–241, 320
 - security features in, 15–16
 - SSL improvements in, 257
 - Zones, 247–249
 - Internet Options (WSC), 47–48
 - Internet Protected Mode, 15, 237–241, 257, 336
 - Internet Protocol security. *See* IPsec
 - Internet Protocol version 6 (IPv6)
 - defined, 336
 - and static IP addresses, 229
 - Internet Security Settings, 48
 - Internet service provider (ISP)
 - broadband, 313
 - discussed, 313–314
 - Internet Zone
 - ActiveX in, 250
 - assigning local file to, 249
 - discussed, 247
 - HTML, 248
 - and HTML, 248
 - intranet, 248
 - inventory, 29–30, 31
 - IP address, static, 229, 234
 - IP Security Policies, 301
 - IPsec (Internet Protocol security)
 - and Authenticate Communications, 211
 - defined, 336
 - and roaming profiles, 170
 - and Windows Firewall, 18
 - IPv6 (Internet Protocol version 6)
 - defined, 336
 - and static IP addresses, 229
 - IRM. *See* Information Rights Management
 - ISP (Internet service provider)
 - broadband, 313
 - discussed, 313–314
 - ISV (Independent Software Vendor), 43, 215
 - IUSR (account), 85, 86
- **I** •
- Jetico BCWipe, 333
- **K** •
- key(s)
 - backing up, 170
 - encryption, 170
 - password-protecting, 170
 - public, 160–161
 - Registry, 117
 - secret, 160
 - startup, 179, 182
 - support for, 161
 - Windows Defender, 124
 - key (token), 96, 130
 - key objects, 117
 - key pair, 161

• L •

LAN (local area network), 207
 last-accessed date, 256
 Latest Security and Virus Information, 49
 Least Privilege, 238
 least privilege, 15
 legislation
 data breach, 171
 on PII, 169, 171
 regulatory mandates, 169
 Linux/Unix, 300
 local area network (LAN), 207
 Local Intranet Zone, 247, 248
 Local Machine Zone, 248
 Local Security Authority Key, 123
 Local Security Policy, 296–305
 account-lockout policy, 297–298
 Admin Approval mode, 59–63
 administrative templates, 302–304
 audit policy, 298
 and BitLocker, 178
 configuration policy, 301
 discussed, 59, 296, 300–301
 and encryption, 164, 165
 event log, 300
 Group Policy Object Editor for, 296
 password-policy, 296–297
 security options, 299–300
 user rights, 298
 user-configuration, 302
 and Windows Firewall, 205
 LOCAL SERVICE (identity), 86
 lockout policies, 297–298
 Log Access, 129
 log file
 connections in, 210
 size of, 300
 Log File Path, 127
 logging. *See also* Auditing
 access management with, 124–132
 defined, 125
 Low alert, 271

• M •

MAC (Media Access Control) address
 filtering, 235
 Malicious Mobile Vode (MMC), 319–320

malicious programs
 application installations by, 65
 best practices for, 278–279
 protection against, 278–279
 and Secure Desktop, 68
 third-party software for, 279
 malware
 and backing up, 136
 defined, 260, 337
 and privilege settings, 10
 in removable media, 285–286
 spyware, 11
 Windows Defender for, 261
 Malware Protection (WSC)
 discussed, 17, 46
 monitoring, 46
 remediation functionality of, 46
 virus-protection options in, 47
 Windows Defender options in, 47
 in WSC, 46–47
 managed file extension, 77
 Mandatory Integrity Control (MIC), 238
 Mark of the Web (MOTW), 249
 Maximum Log Size, 129
 MBSA (Microsoft Security Baseline Analyzer), 330–331
 Media Access Control (MAC) address
 filtering, 235
 Media Player (Windows), 241
 Medium alert, 270
 Meeting Space (Microsoft), 320
 Meeting Space (Windows), 340
 MHTML, 249–250
 Microsoft, e-mail newsletter from, 329–330
 Microsoft Genuine Advantage Validation Tool, 255
 Microsoft Management Console (MMC)
 group creation in, 94
 and User Management, 91
 and Windows Firewall, 18, 43, 44, 205
 Microsoft Meeting Space, 320
 Microsoft Office suite, 76
 Microsoft Office Update Engine, 255
 Microsoft Outlook, 76–78
 Microsoft Security Baseline Analyzer (MBSA), 330–331
 Microsoft Security Central Web site, 49
 Microsoft SpyNet, 262, 277

- Microsoft Visual Web Developer 2005 Express, 241
 - Microsoft Windows NT, 161
 - Microsoft Windows Vista TechCenter, 213
 - Microsoft Windows XP. *See* Windows XP
 - MIME (Multipurpose Internet Mail Extension)
 - and HTTP, 249
 - and IE7, 249–250
 - mitigation, of risk, 38
 - MK protocol, 249–250
 - MMC. *See* Microsoft Management Console
 - mobile code, 319–320
 - mobile device
 - defined, 337
 - encryption for, 322
 - firewalls for, 322
 - MMC attacks via, 319
 - security risks with, 322–323
 - Modify Binary Data, 119
 - monitoring
 - Automatic Updating, 45
 - Malware Protection, 46
 - by Parental Controls, 13
 - Windows Firewall, 43
 - Monitoring section (Getting Started), 213
 - MSG files, 77
 - Multipurpose Internet Mail Extension (MIME)
 - and HTTP, 249
 - and IE7, 249–250
- N •
- Name Not Found, 92, 93
 - name section (File Sharing Wizard), 99
 - National Institute of Standards and Technology (NIST)
 - and security risks, 27
 - on threats, 31–32
 - natural threat-sources (acts of God), 32
 - Need to Know, 238
 - netsh command line, 220
 - network. *See also* wireless network (Wi-Fi)
 - access to, 299
 - administrative template, 304
 - backing up to, 152
 - nonbroadcasting, 14
 - private, 219
 - protection for, 328–329
 - public, 219
 - unsecure, 219
 - NETWORK (identity), 86
 - Network and Sharing Center
 - discussed, 97
 - File Sharing, 98
 - functionality, 220
 - interface, 225
 - Password Protected Sharing, 101
 - for wireless networks, 225–226
 - Network Configuration Operators, 86
 - Network connection not selected, 205
 - Network connection selected, 204–205
 - Network connections view, 225
 - network location, 219
 - Network map, 225
 - network profile, 221
 - network protocols
 - in IE7, 250–253
 - and XRML, 250
 - NETWORK SERVICE (identity), 86
 - Network-Connected Programs, 277
 - NewsBites (SANS), 329
 - newsletters, 329–330
 - NIST (National Institute of Standards and Technology)
 - and security risks, 27
 - on threats, 31–32
 - nonbroadcast mode, 219
 - nonbroadcasting network, 14
 - Not Yet Classified, 271
 - Notepad, 241
 - NTFS (NT File System)
 - access management with, 111–116
 - backup operators in, 84
 - and BitLocker, 173–174
 - defined, 111, 337
 - drive partitions, 173–174
 - file encryption, 162
 - with File Sharing Wizard, 98–101
 - permissions, 166
 - NTFS object
 - auditing and logging of, 130–131
 - key objects versus, 117

• 0 •

object(s)
 auditing and logging of, 130–132
 child, 109, 111
 creation of, 104
 defined, 103–104
 discussed, 130
 effective permissions, 105–108
 and inheritance, 108–111
 key, 117
 NTFS, 130–131
 owner of, 104
 Registry, 131
 service, 131
object caching
 ActiveX, 253
 in IE7, 253–156
object-level security
 discussed, 96–97, 103–116
 NTFS permissions, 111–116
Office suite (Microsoft), 76
Office Update Engine(Microsoft), 255
Offline Files cache, 161
off-site backup, 140
on-demand scanning
 defined, 337
 with Windows Defender, 266–269
128-bit encryption, 173, 188
Open Files Based on Content, 250
operating system (OS). *See specific types,*
 e.g.: Windows XP
Oracle call interface, 300
OS (operating system). *See specific types,*
 e.g.: Windows XP
OS volume, 174, 181
Other Security Settings, 17, 47
OTS (Over-the-Shoulder) credentials
 defined, 337
 in Standard User mode, 57–58
Ouch! (newsletter), 329
outbound connections, 207, 209
Outlook (Microsoft), 76–78
Outlook Web-Access (OWA), 79
Over-the-Shoulder (OTS) credentials
 defined, 337
 in Standard User mode, 57–58

Overview section, 207
overwrite, 139–140
owner, 100, 104
ownership, 40

• p •

pagefile encryption, 161
pagefile.sys, 178
parent object, 109, 111
Parental Controls
 capabilities of, 12–13
 defined, 337
 discussed, 12–13, 13
 and IE7, 16
partitioning
 hard disk, 174–176
 security risks with, 196
 space for, 178
 unprotected, 196
passive action, 130, 131
passive auditing, 131
passive discovery broadcasting, 220
password(s)
 for accounts, 286
 and Active Directory, 296–297
 and BitLocker, 180
 for keys, 170
 and MBSA, 330
 in mobile devices, 323
 nonsecure, 294
 and PWSafe, 331
 recovery, 180
 for router, 232
 for screen saver, 286
 security risks with, 196, 294
 tips for, 315–316
 for user account, 88–90
 weak, 315, 330
 for wireless networking hardware,
 232–233
 in wireless networks, 315–316
Password Protected Sharing Center, 85
password-policy, 296–297
password-protected sharing, 101
password-protection statement, 98
PDF (Portable Document Format), 73

- PEAP, 228
- peer-to-peer (ad hoc) wireless network
 - defined, 335
 - discussed, 230–232
 - security risks with, 320
- People Near Me, 337
- Performance Log Users, 87
- Performance Monitor Users, 87
- Performance Options, 138
- permissions
 - Change, 78
 - Contributor, 100
 - Co-Owner, 100
 - effective, 105–108
 - from e-mail, 79
 - explicit security, 111
 - FAT32, 112
 - file, 112
 - folder, 112
 - Full Control, 78, 106
 - and IE7, 15
 - including, 115
 - inheritable, 115
 - inheritability, 109
 - least privilege, 15
 - Read, 78, 79, 166
 - replace, 115
 - RMS, 79, 80
 - for services, 15
 - Take Ownership, 106
 - verifying, 79
- Permission Level column, 100
- Permissions area, 115
- persistent protection, 74
- personal data
 - backing up, 141
 - and IE7, 16
 - protection of, 16, 22
- personal firewall, 314
- personal identification number. *See* PIN
- Personally Identifiable Information (PII)
 - defined, 20, 337
 - encryption of, 169
 - legislation on, 169, 171
 - protection of, 20–21
 - regulatory mandates, 169
 - security risks with, 171
- pervious version, 139
- phishing
 - defined, 337
 - and IE7, 16, 244–246
 - in IE7, 257
 - and Internet Protected Mode, 244
 - protection against, 257
- Phishing Filter
 - defined, 337
 - discussed, 244–245
 - key, 124
 - on/off toggle, 245
 - options, 245–246
 - settings, 246
- physical security, 21
- PII. *See* Personally Identifiable Information
- PIN (personal identification number)
 - and BitLocker, 183–186
 - boot protection, 172
 - defined, 182
 - and TPM, 179
 - and TPM chips, 183–186
- PKI (Public Key Infrastructure), 338
- PKI signature checks, 66
- point-in-time copy, 139
- policy(-ies)
 - auditing and logging of, 124–129
 - AutoPlay and AutoRun, 304
 - defined, 293
- policy settings
 - account-lockout policy, 297–298
 - audit policy, 298
 - configuration policy, 301
 - discussed, 293
 - with Group Policy Object Editor, 295–296
 - implementing, 294
 - Local Security Policy, 296–305
 - managing, 296
 - password-policy, 296–297
 - reasons for use of, 294–295
 - security templates for, 305–309
 - user rights, 298
 - user-configuration, 302
- port
 - defined, 203
 - opening, 202
- port number, 203
- Portable Document Format (PDF), 73
- Posix subsystem, 300
- Prevent Memory Overwrite, 189–191

- configuring, 190–191
 - Disabled, 190
 - Enabled, 190
 - Not Configured, 189
 - Principle of Least Privilege, 238, 337
 - Print Content, 79
 - printer(s)
 - administrative template, 304
 - sharing, 101–102
 - private key
 - backing up, 170
 - discussed, 160–161
 - loss of, 165
 - private network, 219
 - Private Profile, 207
 - privilege levels
 - discussed, 58
 - elevated, 336
 - and malware, 10
 - profile
 - Domain Profile, 207
 - network profile, 221
 - Private Profile, 207
 - Public Profile, 207
 - roaming, 170
 - roaming profile, 170
 - and System Restore, 138
 - program menu, 205
 - Prompt for Consent, 61, 63
 - Prompt for Credentials
 - in Administrator mode, 62
 - in Standard User mode, 63
 - Prompt User, 250
 - protection
 - of business information, 21
 - discussed, 19
 - of hardware, 19–20
 - from phishing, 16
 - of PII, 20–21
 - of sensitive information, 21, 22
 - of software, 19–20
 - protocol support, 220
 - Public folder, 101
 - public key, 160–161
 - Public Key Infrastructure (PKI), 338
 - Public Key Policies, 301
 - public network, 219
 - Public Profile, 207
 - PWSafe, 331
- Q •**
- quarantined item(s), 273–274
 - quick scan, 11, 266–267
- R •**
- Read (permission)
 - discussed, 78, 79
 - at NTFS level, 166
 - for user, 166
 - Reader (permission), 100
 - real-time protection, 263–266
 - real-time scanning, 12, 338
 - recovery
 - 48-bit option, 192
 - 256-bit option, 192
 - options for, 192–193
 - System Restore for, 138
 - Recovery Agent, 163
 - recovery console, 299
 - reformatting, of removable media, 286
 - Regedit, 118–123
 - Registry
 - access management to, 116–124
 - and administrative templates, 302
 - defined, 116
 - direct editing, 248
 - discussed, 116–117
 - editing, 248, 302
 - hives, 117
 - keys, 117
 - modifying, 118–123
 - settings, 116
 - values, 117
 - viewing, 118–123
 - Registry keys, 123–124
 - Registry object, 131
 - regulatory mandates, 169
 - remediation, 46
 - remote Virtual Private Network (VPN), 328
 - removable media
 - attaching, 284
 - and BitLocker, 196
 - data protection on, 287–288
 - and data removal, 286–287
 - defined, 283, 338
 - detaching, 284

- removable media (*continued*)
 - Device Control for, 286, 287, 288–292
 - discussed, 283
 - encryption for, 287–288
 - malware in, 285–286
 - physical security for, 287, 288
 - protection for, 285–288
 - reformatting, 286
 - scanning, 285
 - security risks of, 196, 283–284
 - viruses in, 285–286
 - Remove (threat), 271
 - Remove button (ACEs), 114
 - Replace All Existing Inheritable Permissions, 115
 - Replace Permissions, 115
 - Report This Web Site, 246
 - Resources pane, 213–214
 - Restore Defaults, 205
 - Restricted Sites, 247
 - restrictions, 13
 - Retain Old Events, 129
 - Revocation Lists, 76
 - Rights Management Service (RMS)
 - defined, 338
 - discussed, 73–74
 - DRM versus, 80
 - encryption with, 74
 - in IE, 78–79
 - integration of, 74–75
 - and IRM, 76–79
 - management features, 75–76
 - use of, 74
 - weaknesses of, 80
 - Rights Policy Templates, 75
 - risk(s)
 - of ActiveX, 236
 - of ActiveX Opt-In, 243
 - assessing, 26–29
 - with connectivity, 313–314
 - DDoS, 317–318
 - defined, 26, 338
 - determining, 28–29, 37–38
 - discussed, 25, 313
 - with e-mail, 318–319
 - human element of, 39–40
 - with IM, 321
 - impact of, 36–37
 - introduction of, 39–40
 - mitigation, 38
 - with mobile code, 319–320
 - with mobile devices, 322–323
 - with peer-to-peer networking, 320
 - reducing, 29, 38–39
 - of removable media, 196, 283–284
 - safeguards against, 34–35, 38–39
 - security breach, 28
 - of system, 26–29
 - threat identification, 27
 - toolbox for, 28
 - understanding, 26
 - user education for, 168
 - vulnerable systems, 27–28
 - with Windows File Sharing, 224
 - @RISK: The Consensus Security Alert (newsletter), 329
 - risk management, 35
 - RMS. *See* Rights Management Service
 - roaming profile, 170
 - router. *See also* wireless router
 - broadband, 314
 - username and password for, 232
 - as wireless access point, 218
 - Rule Merging, 210
 - Run, 123
 - Run as Administrator, 82
 - RunOnce, 123
 - Russinovich, Mark, 332
- S ●
- SACL (System Access Control List), 105, 130
 - safeguards (security controls)
 - current, 34–35
 - defined, 338
 - against security risks, 34–35, 38–39
 - sales information, 21
 - SAM account, 299
 - SANS (SysAdmin, Audit, Network, Security), 329
 - saved from url, 249
 - scans and scanning
 - automatic, 269, 270
 - custom, 268
 - discussed, 11–12, 326
 - full, 267, 268
 - on-demand, 266–269, 337

- quick, 266–267
- real-time, 338
- removable media, 285
- scheduled, 269, 270
- with Windows Defender, 266–270
- scheduled (automatic) scan, 269, 270
- SDDL (Security Descriptor Definition Language), 129
- SDL (Security Development Lifecycle), 9–10
- Search Results, 93
- secpol.msc, 296
- secret key, 160
- Secure by Default, 9, 10
- Secure by Design, 9, 10
- Secure Desktop
 - defined, 338
 - disabled, 70
 - discussed, 69
 - and elevation prompts, 70–71
 - enabled, 70
 - and malicious programs, 68
- Secure in Communications, 9, 10
- Secure in Deployment, 9, 10
- secure protocol, 328
- security
 - bypassing, 316
 - and common sense, 24
 - cross-domain, 15–16, 243–244, 257
 - defined, 1
 - explicit, 108–111
 - in IE7, 15–16
 - inherited, 108–111
 - new features in, 9–19
 - object-level, 111–116
 - physical, 21
 - shortcuts with, 314–316
 - software patches for, 316–317
 - and tolerance, 23
- Security Admins groups, 106
- security breach
 - assessment of, 28
 - discussed, 28
 - impact of, 36–37
- Security Center key, 124
- Security Central Web site (Microsoft), 49
- security controls. *See* safeguards
- security descriptor, 97, 104
- Security Descriptor Definition Language (SDDL), 129
- Security Development Lifecycle (SDL), 9–10
- Security Essentials, 338
- Security Essentials Notification pane, 42, 48, 49
- Security Event log, 128–129
- Security Guide (Vista), 307–308
- security guide templates
 - applying, 308–309
 - creating, 305–307
 - custom, 305–307
 - defined, 295
 - discussed, 305
 - for policy settings, 305–309
 - Windows Vista Security Guide, 307–308
- security plan
 - discussed, 25
 - establishing, 33–40
- security risk(s). *See* risk(s)
- Security status bar, 16
- security toolbox
 - discussed, 22
 - requirements for, 22–23
 - for risks, 28
 - technical tools in, 23–24
- Security Utilities, 332
- Security Zones. *See* Zones
- Select Objects, 90–93
- Select This Object Type, 92, 93
- sensitive information (data)
 - defined, 338
 - encryption of, 168–169
 - protection of, 21, 22
- Server Parameters key, 124
- SERVICE (identity), 87
- Service Hardening (Windows)
 - defined, 340
 - discussed, 14–15
- Service Isolation, 15, 338
- service object, 131
- service set identifier (SSID)
 - and AP, 235
 - changing, 233
 - disabling broadcasts, 235
 - discussed, 219
 - and nonbroadcasting networks, 14
 - and WAP, 235
 - and wireless networking hardware, 233, 235
- Severe alert, 270

- shadow copy
 - backing up with, 139–140, 157
 - and CompletePC Backup, 156–157
 - description, 146
 - and system restore point, 157
- Share button, 100
- sharing
 - access to, 299
 - and Administrator, 98
 - defined, 81
 - discussed, 97–102
 - encrypted files, 166
 - files, 98–102, 166
 - and firewalls, 101–102
 - folders, 101
 - management of, 81
 - password-protected, 101
 - printers, 101–102
 - public folders, 101
- Sharing and Discovery, 225
- shatter attacks, 238
- Shield icon, 55
- Shockwave Flash Object, 255
- Sidebar, 331
- sidebar gadget, 331
- signature checks
 - for elevation prompts, 66–67
 - PKI, 66
- smart card, 161
- software
 - antivirus, 325–326
 - for backing up, 327–328
 - discussed, 30
 - protection of, 19–20
 - for spyware, 279
 - third-party, 279, 327–328
 - unsanctioned, 259–260
- Software Explorer, 262, 275–277
- software patches, 316–317
- Software Restriction Policies, 301
- special identity (built-in group), 83–87
- SpyNet (Microsoft), 262, 277
- spyware
 - best practices for, 278–279
 - classifying, 277
 - defined, 259, 260, 338
 - detection of, 261
 - discussed, 11, 259
 - protection against, 278–279
 - removal tools, 261, 326–327
 - third-party software for, 279
 - and Windows Defender, 261
 - Windows Defender for, 261
- SSID. *See* service set identifier
- Standard User mode
 - and Admin Approval mode, 55–57
 - Administrators versus, 55
 - common tasks of, 55
 - defined, 339
 - discussed, 54
 - effective permissions of, 106
 - elevation prompt for, 63–65
 - OTS credentials, 57–58
 - Shield icon in, 55
 - and UAC, 54–58, 63–65
 - in Windows XP, 54
- Start Menu, 304
- Startup, System Restore for, 138
- startup key
 - and BitLocker, 186–187
 - defined, 182
 - and TPM, 179
 - TPM chips with, 186–187
- Startup Programs, 276
- static IP address
 - and DHCP disabling, 234
 - discussed, 229
 - in wireless networks, 228–229
- storage media, 142
- students, controls for, 12
- subkey
 - creating, 118–119
 - defined, 117
 - inheritance, 130
- surfing, Internet, 315
- symmetric encryption
 - AES, 188
 - and asymmetric encryption, 163
 - defined, 339
 - discussed, 160
- system(s)
 - backing up, 141
 - BitLocker on, preparing fir, 174–178
 - hardware of, 30
 - information on, 31
 - interface of, 31
 - inventory, 29–30
 - multiple-user, 29

- security risks in, 26–29
 - software of, 30
 - threats to, 27, 31–33
 - types of, 29
 - understanding, 27, 29–30
 - usage of, 31
 - vulnerability of, 27–28, 33–34
 - SYSTEM (identity), 87
 - System Access Control List (SACL), 105, 130
 - System administrative template, 304
 - System Configuration (Settings), 265
 - system image. *See* CompletePC Backup
 - System Restore
 - backing up with, 137–138, 147–149
 - for hardware, 138
 - options, 138
 - for preserving data, 147–149
 - to previous restore points, 149–150
 - for recovery, 138
 - for Startup, 138
 - User Profile Settings for, 138
 - system restore point
 - description, 146
 - discussed, 138, 149–150
 - and shadow copy, 157
 - weaknesses of, 138
 - system volume, 174
 - Systinternals, 332
- T •**
- Take Ownership (permission), 106
 - Taskbar, 304
 - TCP (Transmission Control Protocol), 102
 - technical tools, 23–24
 - temporary network name, 220
 - third-party software
 - for backing up, 327–328
 - for malicious programs, 279
 - for spyware, 279
 - for viruses, 279
 - threat(s)
 - of ActiveX, 243
 - defined, 31–32
 - identification of, 27
 - identifying, 27, 31–33
 - levels, 270–271
 - likelihood of occurrence, 35–36
 - potential, 32–33
 - setting levels, 271
 - to system configuration, 27, 31–33
 - Windows Defender for, 269–272
 - time restrictions, 13
 - TPM (Trusted Platform Module)
 - and BitLocker, 173, 179, 182–187
 - with PIN, 179, 183–186
 - with startup key, 179, 186–187
 - trade secrets, 21
 - traffic, filtering, 18
 - Transmission Control Protocol (TCP), 102
 - Trojan (Trojan horse), 260, 339
 - Trusted Platform Module. *See* TPM
 - Trusted Sites Zone, 247
 - Turn Off Automatic Web Site Checking, 245
 - 256-bit encryption, 173, 188
 - 256-bit recovery option, 192
- U •**
- UAC. *See* User Account Control
 - UDP (User Datagram Protocol), 102
 - UIAccess
 - disabled, 68
 - elevation prompt, 67–68
 - enabled, 68
 - UIPI (User Interface Privilege Isolation), 238
 - unencrypted file, 162
 - Unicast Response, 210
 - Uniform Resource Locator (URL)
 - defined, 339
 - saved from, 249
 - unsanctioned software, 259–260
 - insecure wireless network
 - automatic connection to, 221
 - defined, 219
 - discussed, 234
 - update
 - automatic, 316
 - Check for Updates, 45
 - Microsoft Office Update Engine, 255
 - of spyware removal tools, 327
 - View Update History, 46
 - URL (Uniform Resource Locator)
 - defined, 339
 - display, 16
 - saved from, 249
 - USB device, 180
 - Users (group), 63, 82, 87, 106

- user account
 - creating, 88–90
 - disabling, 90
 - discussed, 88
 - password for, 88–90
 - re-enabling, 90
 - User Account Control (UAC)
 - admin approval mode, 300
 - and Admin Approval mode, 69–70
 - administering, 53
 - defined, 339
 - discussed, 10–11, 53
 - elevation prompt, 61–68
 - and IE7 Protected Mode, 238
 - Local Security Policy settings, 59–72
 - and MMC, 320
 - privilege levels, 58
 - for removable media, 285
 - Standard User mode, 54–58, 63–65
 - and user context, 82
 - virtualization settings, 71–72
 - and WSC, 49
 - user context, 82
 - User Datagram Protocol (UDP), 102
 - user education
 - for EFS, 168
 - for security programs, 40
 - user error, 136
 - User Interface Privilege Isolation (UIPI), 238
 - User Management, 91
 - User Profile Settings, 138
 - user rights
 - assignment of, 96
 - policy, 298
 - user session, 82
 - user-configuration policy, 302
- U •
- vendor information, 21
 - vendor resources, 18
 - View and Create Firewall Rules section (Getting Started), 211–213
 - View Update History, 46
 - Virtual Private Network (VPN), 328
 - virtualization settings, 71–72
 - virus(es)
 - best practices for, 278–279
 - defined, 260, 339
 - discussed, 260
 - protection against, 278–279
 - in removable media, 285–286
 - third-party software for, 279
 - virus-protection options, 47
 - Vista (Microsoft)
 - and BitLocker, 173
 - code, 10
 - discussed, 1, 9
 - previous OSs versus, 9
 - versions of, 341–344
 - Vista Backup, 135
 - Vista Business, 293, 342
 - Vista Default Security, 307
 - Vista Enterprise, 176, 343
 - Vista Firewall, 319
 - Vista Home Basic
 - discussed, 341
 - and policies, 293
 - User Management in, 91
 - Vista Home Premium
 - discussed, 342
 - and policies, 293
 - User Management in, 91
 - Vista identity model, 81–82
 - Vista Security Guide (Windows), 307–308
 - Vista Security Guide Enterprise Client (VSG EC), 307
 - Vista Security Guide Specialized Security (VSG SSLF), 307
 - Vista Starter
 - and policies, 293
 - User Management in, 91
 - Vista Ultimate, 293, 342
 - Vista Web Filter, 339
 - Visual Web Developer 2005 Express (Microsoft), 241
 - VoIP (Voice over IP), 246
 - VPN (Virtual Private Network), 328
 - VSG EC (Vista Security Guide Enterprise Client), 307
 - VSG SSLF (Vista Security Guide Specialized Security), 307

vulnerability
defined, 33, 339
identifying, 27–28, 33–34
potential, 34
of system, 27–28
of systems, 27–28, 33–34

• W •

WAP. *See* wireless access point
war-driving (war-flying), 222, 234
Web Filter, 13
Web pages
and ActiveX controls, 241
IE7 security for, 244
Voice over IP, 246
WebDAV, 162
WEP (Wired Equivalent Privacy)
defined, 340
discussed, 233
Wi-Fi. *See* wireless network
Wi-Fi Protected Access (WPA)
defined, 339
discussed, 219
Wi-Fi Protected Access 2 (WPA2)
defined, 339
discussed, 219
Windows Components, 304
Windows Defender
administrative template, 304
alerts in, 270–271
Allowed Items, 274–275
and antivirus software, 279
automatic scan with, 269, 270
custom scan with, 268
definition files, 262–263
discussed, 11–12, 262
features of, 11–12
full scan with, 267, 268
and IE, 261–263
interface of, 11, 262
key, 124
for malware, 261
and Malware Protection, 47
new features of, 261–262
on-demand scan with, 266–269
options, 47
quarantined items in, 273–274

quick scan with, 266–267
real-time protection, 263–266
scheduled scan with, 269, 270
setting threat levels in, 271–272
Software Explorer, 275–277
and spyware, 261
for spyware, 261
and threats, response to, 269–272
tools, 272–277
updating, 262–263
use of, 261
Web site for, 277
Windows Explorer, 304
Windows File Sharing, 224
Windows Firewall
with Advanced Security applet, 205–214,
213, 301
Advanced tab, 204–205
configuring, 199–205
defined, 339
discussed, 18, 199
enhancements, 18–19
Exceptions tab, 202–203
and firewalls, other, 201
General tab, 201
Getting Started section of, 211–213
guidelines for, 214–215
interface, 199
interface of, 18
and IPsec, 18
monitoring, 43
profiles, 18–19
properties, 208
rules, 207
for services, 15
settings, 43–44, 199–205
and Windows Security Center, 43–44
and WSC, 18
Windows Firewall applet, 199–201
Windows Media Player, 241
Windows Meeting Space, 340
Windows NT (Microsoft), 161
Windows Pre-installation Environment
(WinPE), 178
Windows Security Center (WSC)
accessing, 42
alerts, 50
Automatic Updating, 44–46

- Windows Security Center (*continued*)
 - defined, 340
 - discussed, 17, 41
 - enhancements, 17–18
 - features of, 41–42
 - interface, 42
 - Internet Options, 47–48
 - Latest Security and Virus Information, 49
 - Malware Protection, 46–47
 - notification options, 50
 - Options pane of, 43, 44, 49–50
 - Other Security Settings, 47
 - Protected Modes Elevation policy, 241
 - UAC, 49
 - and Windows Firewall, 18, 43–44
 - Windows Firewall settings, 43–44
 - and Windows XP SP2, 42
 - Windows Service Hardening
 - defined, 340
 - discussed, 14–15
 - Windows services, 14–15
 - Windows Vista Security Guide, 307–308
 - Windows Vista TechCenter (Microsoft), 213
 - Windows XP
 - Power Users Group, 54
 - Service Pack (SP) 2, 14, 42
 - Standard User mode in, 54
 - WinPE (Windows Pre-installation Environment), 178
 - Winsock Service Providers, 277
 - WinZip, 287–288
 - Wipe – Secure File Deletion, 333
 - Wired Equivalent Privacy (WEP)
 - defined, 340
 - discussed, 233
 - wired networking, 218
 - wireless access point (WAP)
 - administrative username, 232–233
 - configuring, 232–236
 - and DHCP, 234
 - MAC address filtering, 235
 - password, 232–233
 - range of, 236
 - as router, 218
 - router as, 218
 - secure communication over, 233–234
 - SSID, 233, 235
 - and SSID values, 235
 - Wireless Encryption Protocol (WEP), 233
 - wireless network (Wi-Fi)
 - ad hoc, 219, 230–232, 320, 335
 - configuration of, 221–232
 - connecting to, 221–224
 - discussed, 217–219
 - hardware configuration for, 230–232
 - hotspots, 223–224
 - modifying connection to, 226–228
 - Network and Sharing Center, 225–226
 - range of, 236
 - restricting use to, 224–225
 - security enhancements for, 13–14
 - static IP addresses, 228–229
 - unprotected, 221
 - unprotected/unsecure, 234
 - unsecure, 219, 221–224, 234
 - Vista-specific features, 220–221
 - wireless router
 - administrative username, 232–233
 - configuring, 232–236
 - and DHCP, 234
 - discussed, 232–236
 - MAC address filtering, 235
 - password, 232–233
 - secure communication over, 233–234
 - SSID, 233, 235
 - wireless services, 322
 - working pane, 206
 - WPA (Wi-Fi Protected Access)
 - defined, 339
 - discussed, 228
 - WPA2 (Wi-Fi Protected Access 2)
 - for ad hoc wireless networks, 230
 - defined, 339
 - WPA2-Enterprise
 - discussed, 228
 - WPA2-Personal ad hoc networking, 221
 - WSC. *See* Windows Security Center
-
- X •
 - XRML (eXtensible Rights Markup Language), 74, 250
 - Z •
 - Zones (IE7), 247–249, 256, 257
 - zone hopping, 247
 - zone spoofing, 247