

Index

A

- access checks, 127
- access control list entries
 - (ACEs), 24, 174
 - components, 174
 - deny, 184–186
 - Documents and Settings with, 184–185
 - icalcls tool and find all, 195
 - SIDs and, 174
- access control lists (ACLs), 114–117, 171–201. *See also* ACL UI; discretionary access control lists; mandatory access control lists; system access control lists
 - default, 183
 - significant changes in, 183
- definition, 171
- earlier versions, 178–179
- editor, 177
- forms of, 173
- major changes in, 178–179
- management, 171–201
 - best practices, 201
 - permissions, 24, 171
 - modification, 156
 - registry, 199–200
 - representations, 174
 - resetting, 195
 - icacls and, 195
 - restoring, 192–193
 - icacls and, 192–193
 - saving, 191, 192
 - editing and, 192
 - icacls tool and, 191, 192
 - subinacl tool and, 199, 201
 - terminology, 172–175
 - tools for managing, 190–199
 - using, 175–178
 - verification of, 177
 - Windows XP, 178–179
 - default, 179
 - problems in, 178–179
- access control permissions, IIS, 326–332
- “Access Credential Manager as a trusted caller,” 141
- Access data sources
 - across domains (setting), 270, 279
- access masks, 174
- access points (APs), 462. *See also* Wi-Fi
- access tokens, 114, 125. *See also* security tokens
- account lockout, 47, 539–546
 - facts, 540–541
 - parameters/settings, 539–540
 - password strength and, 541–545
- account rights, 140
- privileges *v.*, 140
- accounts. *See specific accounts*
- ACEs. *See* access control list entries
- ACL editor, 177. *See also* access control lists
- ACL UI, 177, 197–199. *See also* access control lists
 - changes to, 197–199
 - Windows XP, 197
- ACLs. *See* access control lists
- Active Directory, 112. *See also* Security Accounts Manager
 - SAM *v.*, 112
 - Schema, 514
- Active Scripting (setting), 275, 281
- ActiveX controls, 33, 222, 223, 257

562 Index ■ A

- ActiveX controls and
 - plug-ins (settings), 265–268, 278–279. *See also specific settings*
 - summary of, 278–279
- ActiveX Installer service, 136, 137, 218–220, 222
- Adobe Flash Player
 - and, 219
 - configuration, 218–220
 - documentation on, 219
 - usage, 219
- Add-on management, 256–257
- Address Space Layout Randomization (ASLR), 5
- Ad-Hoc mode, 462–463
- admin-approval mode, 133, 136, 168
 - consent prompt settings for, 150
- administrative templates, 492–493
 - settings, 504
 - new, 504–510
 - reboot/logon required, 510
- Administrator account,
 - built-in, 146–147, 180
 - disabled by default, 180
 - security importance of, 528, 529
 - filtered token for, 150
 - setting, 150
 - RID 500, 124, 146, 180
 - in safe mode, 146, 147
 - special treatment of, 146–147, 180
- Administrator Lists, 317
- administrators
 - (admins), 128
 - non-, 129
 - UAC and, 129–130
 - power of, 129
- ADMX files, 39, 492–493, 514, 515
 - migration tool, 493
 - template embedding, 493
- Adobe Flash Player, 219
 - ActiveX Installer and, 219
- Advanced Group Policy Management toolkit, Microsoft, 222
- advfirewall, 424
- adware, 64–65
 - browser cookies, 237
- AES. *See* Asymmetric Encryption Standard
- Airsnort, 465
- All Users profile, 91
- Allow META REFRESH (setting), 270, 279
- Allow previously unused ActiveX controls to run without prompting (setting), 265, 278
- Allow programmatic clipboard access (setting), 275–276, 281
- Allow scripting of Internet Explorer web browser control (setting), 270–271, 279
- Allow script-initiated Windows without size or position constraints (setting), 271, 279
- Allow scriptlets (setting), 266, 278
- Allow status bar updates via script (setting), 276, 281
- Allow web pages to use restricted protocols for active content (setting), 271, 280
- Allow websites to open Windows without address or status bars (setting), 271, 280
- Allow websites to prompt for information using scripted window (setting), 276, 281
- Anonymous authentication, 320, 323
- anti-hammering defense, 47
- anti-malware. *See* malware, automated
- anti-phishing filter. *See* phishing filter
- anti-virus programs. *See* viruses
- API. *See* Application Programming Interfaces
- application(s)
 - malware location in, 66
 - manifests, 165
 - misconfiguration, 56–57
 - security, 203–223
 - best practices, 222–223
 - UAC leveraging in, 164–167
 - UIAccess and, 152
 - vulnerabilities, 54–56
 - web server, 294–295
- application pools, 309–311
 - identities, 311–314
- Application Programming Interfaces (API), 424
 - Windows Firewall, 424–425
- APs. *See* access points
- Aronoff, Andrew, 70
- ASLR. *See* Address Space Layout Randomization
- ASP.NET Impersonation, 320–321
 - other authentication methods *v.*, 325
- Asymmetric Encryption Standard (AES), 26, 466
- at.exe, 216
- Attachment Manager, 506
- attachments, malicious. *See* malicious file attachments
- attacks. *See specific attacks*
- auditing, 162, 533
 - elevation, 162–164
 - Process Tracking, 538
 - security tweak, 533
- Auditpol.exe, 30

- authentication exemption rules, 428
 - authentication methods, 14–16, 109. *See also* logon authentication; *specific authentication methods*
 - IIS, 318–325
 - support for, 14–16
 - authentication protocols, 110–112. *See also* Kerberos; LAN Manager; NT LAN Manager
 - challenge-response, 111
 - Authenticode, 265
 - reliant components-Run signed/not signed with, 265, 278
 - AuthIP, 451–452
 - multiple credentials and, 451–452
 - SDI and, 451–452
 - automated malware. *See* malware, automated
 - Automatic prompting for ActiveX controls (setting), 266, 278
 - Automatic prompting for file downloads (setting), 268–269, 279
 - Automatic Updates, 230
 - autorun programs, 99–100
 - locations for, 99–100
 - Autoruns utility, 70, 100, 235
 - example, 100
 - Web site location, 100
- B**
- back-end databases, 295
 - issues, 295
 - backup application, improvements to, 31
 - Backup, Windows, 31
 - Basic authentication, 322, 324
 - other authentication methods *v.*, 325
 - BCD store. *See* Boot Configuration Data store
 - BCD00000000, 102
 - Bcdedit.exe, 9, 10
 - BCD.log, 9
 - beacon packets, 462
 - Biba model, 146, 158
 - binaries
 - signed, 134
 - Microsoft, 134
 - un-signed, 134, 135
 - Binary and script behaviors (setting), 266, 278
 - binary behaviors, 266
 - biometrics, support for, 14, 15, 16
 - BitLocker Drive Encryption, 11–12, 76–79, 534, 535. *See also* Trusted Platform Module
 - applet, 83
 - enabling steps for TPM and, 80–87
 - Group Policy settings, 82, 83, 514
 - recovery key, 84
 - saving, 84, 85
 - storage options, 84, 85
 - startup options, 84
 - system check, 86
 - BitLocker Drive Preparation Tool, 78
 - black screen, 133, 158
 - Blaster worm, 448, 508, 526
 - blue screens, 19
 - device drivers and, 19
 - Bluetooth, 461
 - boot code, Vista, 74, 75
 - Boot Configuration Data (BCD) store, 8–10, 74, 75
 - boot files, new, 9
 - Boot Loader, Vista, 75, 76
 - Boot Manager EFI, 74, 75
 - Windows, 9, 74, 75, 76
 - boot sequence
 - improvements, 8–12
 - process, 74–76
 - summary, 75
 - boot time filtering, Windows Firewall and, 409–410
 - boot viruses, 76
 - Bootmgr, 9, 74, 75, 76
 - Bootmgr.efi, 74, 75
 - Boot-up key, 79
 - options, 79
 - bot(s), 63, 64, 226
 - phoning home, 64
 - botnets, 63, 546
 - Bradley, Susan, 128
 - Brown, Keith, 128
 - browser(s). *See also* Internet Explorer 7.0; *specific browsers*
 - IE *v.* other, 245–247
 - browser cookies, unwanted, 237. *See also* Windows Defender
 - Browsing (settings)
 - Disable script debugging (Internet Explorer or other), 282, 287
 - Display a notification about every script error, 282, 287
 - Enable third-party browser extensions, 282, 287
 - Use inline AutoComplete, 282, 287
 - brute force attacks, 46
 - buffer overflows, 51–54
 - attack programs, 52
 - defense against, 54, 92
 - e-mails and, 384
 - exploitation, 51–54
 - web server software, 296
 - built-in Administrator account. *See* Administrator account, built-in
 - built-in groups. *See* groups, built-in

564 Index ■ B-D

- built-in users. *See* users, built-in
- Bypass Traverse
 - Checking, 186
- C**
- C++ security, 4–5
- CA. *See* Collision Avoidance
- cached credentials, 113–114
- cacls.exe tool, 191.
 - See also* icacls.exe
 - command-line tool
 - replacement of, 191
 - updates, 191
- Cain & Abel program, 48, 49, 57
 - network sniffing with, 50, 51
- cards, 33
- CardSpace, 33–34, 259–260
 - Web discussion on, 259
- cellular wireless technologies, 461
- Certificate
 - authentication, 324
- change owner tool, 194.
 - See also* icacls.exe
 - command-line tool
- “Change the time zone,” 141
- channels, 463
- Chopchop, 465
- class identifier. *See* CLSID
- Client Certificates, other authentication methods *v.*, 325
- client protection, 225–241.
 - See also* Forefront Client Security, Microsoft; information security; Malicious Software Removal Tool; Windows Defender; Windows Live OneCare
 - subscription service
 - best practices, 241
- client security, 203–216. *See also* information security hacks, 526–530
- Client Side Mapping, SSL/TSL, 323
- client-side attacks, 58–59, 526–530. *See also* social engineering
 - popularity of, 225–226
 - types, 58–59
- client-to-DC IPsec, 451
- Clipboard application, 275–276
- CLSID (class identifier), 105
- Collision Avoidance (CA), 463
- COM. *See* Component Object Model
- COM Elevation Monikers, 143–144, 197
- Common Internet File System (CIFS), 97–98
 - SMB and, 97–98
- CompletePC backup feature, 31
- Component Object Model (COM), 143
- Components key, 102
- computer accounts, 109
- Computer Browser service, 98, 99
- computer viruses.
 - See* viruses
- connection security rules, 427–428
- consec, 424
- Coordinated Universal Time. *See* UTC
- CORE IMPACT, 57
- “Create symbolic links,” 143
- Creator Owner, 24
- credential hacking, 44. *See also* logon credential guessing/cracking
- credential manager
 - privilege for, 141
- Credential Providers API, 15, 16
- crimeware, 70. *See also* malware, automated
- criminal hacking, 70, 71.
 - See also* hacker(s)
- cross-site scripting (XSS) attacks, 55
- cryptographic hash, 110
 - properties, 110
- Cryptographic Operators, 24
- D**
- dark screen, 133, 158
- data, 101
- Data Execution Protection (DEP), 6
 - security tweak, 536
- data malformation, 55–56
- DDoS attack. *See* distributed DoS attack
- debug.exe, 216
- Default Icon subkey, 106
- Default User, 92
- “defense in depth,” 520, 523. *See also* information security
- delayed start services, 18
- delegation, 115, 116, 127, 249
 - feature, 316–318, 342
 - impersonation *v.*, 115, 116, 127
- deletion, Windows Explorer elevation and, 154–156
- denial of service (DoS) attack, 57–58, 298–299
- distributed, 63
 - web servers and, 298–299
- wireless networks and, 475
- deny ACEs, 184–186.
 - See also* access control list entries
 - Documents and Settings with, 184–185
- deny operations, icacls and, 195
- DEP. *See* Data Execution Protection

- desktops, 132. *See also*
 - secure desktop
 - definition, 211
 - device driver(s), 18–19
 - blue screens and, 19
 - improvements, 18–19
 - Device Driver
 - Experience, 19
 - device installation
 - settings, 506–508
 - DHTML. *See*
 - Dynamic HTML
 - Diagnostics and Recovery
 - Toolset, Microsoft, 222
 - DIALUP, 181, 182
 - Digest authentication, 322, 324
 - other authentication
 - methods *v.*, 325
 - digital certificates, 257–258
 - encryption and, 257–258
 - direct action Trojan, 63
 - directional rules, 427
 - directories, as securable
 - objects, 172
 - directory traversal attacks, 296–297
 - representative
 - example, 297
 - discretionary access
 - control lists (DACLS), 173. *See also* access control lists
 - definition, 173
 - empty, 177
 - NULL *v.*, 177
 - NULL, 177, 178
 - Display mixed content
 - (setting), 271–272, 280
 - Display video and
 - animation on a Web page that does not use external media player (setting), 267, 278
 - distributed DoS (DDos)
 - attack, 63
 - Distributed John
 - program, 48
 - DNS. *See* Domain Name System
 - Documents and Settings, 184–185
 - deny ACEs on, 184–185
 - domain blocking,
 - Windows Mail, 387–390
 - Domain Isolation, 36–37, 446–447
 - Domain Name System (DNS), 89
 - query order, 89, 90
 - Domain profile, 35
 - domain-joined situations,
 - FUS and, 159
 - Don't prompt for client
 - certificate selection
 - when no certificates or only one certificate exists (setting), 272, 280
 - DoS attack. *See* denial of service attack
 - Download
 - signed/unsigned
 - ActiveX controls (setting), 267, 278
 - Downloads (security zone
 - setting), 268–270, 279
 - Automatic prompting
 - for file downloads, 268–269, 279
 - File download, 269, 279
 - Font download, 270, 279
 - Drag and drop or copy
 - and paste files (setting), 272–273, 280
 - Dsniff, 57
 - DVD player
 - components, 215
 - Dynamic HTML (DHTML), 266
 - Dynamic WEP, 480–481
- E**
- EAP. *See* Extensible Authentication Protocol
 - eavesdropping, 57.
 - See also* man-in-the-middle attacks
 - wireless networks and, 472–474
 - ECC. *See* Elliptical Curve Cryptography
 - edit.exe, 216
 - edlin.exe, 216
 - Effective Permissions
 - tab, 172
 - EFI (Extended Firmware Interface), 9, 10, 74
 - Boot Manager, 74, 75
 - firmware, 74, 75
 - 64-bit platform and, 74
 - EFS. *See* Encryption File System
 - 802.11 Legacy
 - wireless security
 - recommendations, 477–480
 - changing AP's default Administrator Password, 480
 - changing AP's default SSID, 478
 - disabling DHCP on AP, 478–479
 - disabling SSID
 - broadcasting, 479–480
 - enabling MAC filtering, 478
 - requiring user authentication
 - passwords, 479
 - 802.11 Wi-Fi standards, 463–464
 - 802.11 wireless networks, 461. *See also* wireless networks
 - elevate tool, 166
 - elevated processes, 134
 - elevate.exe application, 166, 167
 - elevation, 130–140
 - auditing, 162–164
 - command prompt, 166–167
 - installers and, 166
 - non-admin, 137–139
 - prompts, 133

566 Index ■ E-F

- scripts and, 166
- special topics, 139–140
- of standard users, 150–151, 168
- of unsigned executables, 151
- Windows Explorer and attempted, 154–156
- Elliptical Curve Cryptography (ECC), 26
- e-mail. *See also* Windows Mail
- defenses, 390–398
 - anti-malware software, 398
 - disable automatic download of HTML content, 394–395
 - file attachment blocking, 395–398
 - HTML content in Restricted zone, 393–394
 - plain-text conversion, 391–393, 535
 - plain-text passwords disabled, 398
- protection, 351–399
 - best practices, 399
- as spam, 226
- threats, 351–384
 - buffer overflow, 384
 - embedded content, 381–382
 - embedded links, 382
 - file attachments, 58, 351–381
 - leaked passwords, 383
 - miscellaneous, 383–384
- embedded content, 381–382. *See also* malicious file attachments
- embedded links, 382
- empty DACLs. *See* discretionary access control lists
- Enable .NET Framework setup (setting), 270, 279
- encryption
 - digital certificates and, 257–258
 - enhancements/support, 26–27, 257–258
 - hard disk, 534–535
- Encryption File System (EFS), 27, 77. *See also* BitLocker Drive Encryption
- enhancements, 27
- escalation, of privileges, 54–55
- Ettercap, 57
- event forwarding, 29, 30
- Event Log interface, 29, 30
- Event Log Readers, 24
- event logs, 28
 - Group Policy and, 497–498
 - improvements, 28–29
 - as securable objects, 173
 - subscriptions, 30
- event numbers, 162
 - new, 162
- event triggers, 29
- events, as securable processes, 173
- exploitation techniques, malicious, 43–60
- Extended Firmware Interface. *See* EFI
- Extensible Application Markup Language. *See* XAML
- Extensible Authentication Protocol (EAP), 468
- versions, 468
- F**
- fast user switching (FUS), 139
 - domain-joined situations and, 159
- feature delegation, 316–318, 342
- Federal Information Processing Standard (FIPS) 140-2, 26
- file associations, 104
 - HKCR and, 103, 104
 - HKCU and, 104
 - HKLM and, 104
- file attachments, malicious. *See* malicious file attachments
- File download (setting), 269, 279
- files. *See also specific files*
 - IE file types (by file extension), 269
 - malware location in, 66
 - protection, 23
 - as securable objects, 172
 - UAC and access of, 153–154
 - virtualization, 25, 145
- filtered tokens, 132
 - built-in Administrator account and, 150
- filtering platform. *See* Windows Filtering Program
- finger.exe, 216
- fingerprint scanners, 14, 15
- FIPS 140-2. *See* Federal Information Processing Standard 140-2
- Firefox. *See* Mozilla Firefox
- firewall context, 424
- Firewall, Windows, 230, 403–444
 - with Advanced Security MMC snap-in, 422, 443
 - API, 424–425
 - best practices, 444
 - boot time filtering, 409–410
 - control panel, 419–421
 - Group Policy and, 422–423
 - IPsec and, 407, 424

- IPv6 and, 36, 406–407, 412
 - management, 417–443
 - mixed/down-level environment, 438–442
 - management interfaces, 419–429
 - Netsh and, 423–424
 - new features/improvements, 36, 405–417
 - OneCare and, 238
 - outbound filtering and, 412–417, 525
 - security of, 413–417
 - profiles, 417–419
 - per-interface, 444
 - RPC and, 442–443
 - rules, 426–429
 - authentication exemption, 428
 - connection security, 427–428
 - directional, 427
 - precedence order, 428–429
 - server to server, 428
 - tunnel, 428
 - types, 426–429
 - when to use, 428
 - scenarios, 429–438
 - allowing management traffic via VPN, 437–438
 - blocking outbound SMB in public profile, 436–437
 - restricting access based on end-point, 429–436
 - Security Center and, 421
 - service hardening and, 411
 - stealth feature, 408
 - strict source mapping and, 410–411
 - firewalls, 404
 - need for, 404
 - policies, 207
 - restricting services with, 207
 - profiles, 417–419
 - Windows XP, 403, 404
 - folder(s). *See also specific folders*
 - low integrity, 250–251
 - malware locations in, 67
 - protection, 23
 - Font download (setting), 270, 279
 - Forefront Client Security, Microsoft, 239
 - FORMS authentication, 322, 324
 - other authentication methods *v.*, 325
 - forwarded events, 29, 30
 - Full Volume Encryption Key (FVEK), 77
 - FUS. *See fast user switching*
 - fuzzers, 4
 - FVEK. *See Full Volume Encryption Key*
- G**
- Gaobot, 226
 - GINA. *See Graphical Interface for Network Authentication*
 - Globally Unique Identifier. *See GUID*
 - GPEdit.msc (Local Security Policy), 88, 486
 - application order, 88
 - GPMC. *See Group Policy Management Console v 2.0*
 - gpmmc.msc, 495
 - GPOs. *See Group Policy objects*
 - gpresult.exe, 489, 491
 - GPT. *See GUID partition table*
 - grant operations, *icacls* and, 195
 - Graphical Interface for Network Authentication (GINA), 15, 16. *See also Credential Providers API*
 - graphical user interface (GUI), 197. *See also ACL UI*
 - Grimes, Roger, 113
 - Group Policy, 485–518. *See also specific settings*
 - Active Directory Schema and, 514
 - administration tools, 221
 - administrative templates, 492–493
 - new settings, 504–510
 - settings that require reboot/logon, 510
 - application intervals, 494
 - best practices, 518
 - Client service, 496–497
 - Editor, 486
 - IE management and, 495–496
 - Management Console, 38, 494–495
 - in mixed environment, 514–515
 - MLGPOs, 486–491
 - in domain environment, 491
 - precedence, 489–491
 - NAP environment and, 516–517
 - new features, 38–39, 486–494
 - OS upgrade/rollout strategy and, 515–516
 - settings, 38–39, 498–510
 - BitLocker, 82, 83, 514
 - new/updated, 498–510
 - reboot/logon required, 510
 - TPM, 82, 83, 514
 - UAC configuration and, 150–152

568 Index ■ G-I

- system event log and, 497–498
 - updated features, 494–498
 - Web information on, 485, 518
 - Windows Firewall and, 422–423
 - Winlogon and, 496–497
 - Group Policy
 - Management Console (GPMC) v 2.0, 38, 494–495
 - Group Policy: Management, Troubleshooting and Security* (Moskowitz), 485
 - Group Policy objects (GPOs), 88. *See also*
 - multiple local Group Policy objects
 - application order, 88
 - domain, 491
 - local, 486, 491
 - domain *v.*, 491
 - types of, 486
 - groups, built-in
 - modifications of, 179
 - new changes, 24–25, 179
 - guessing. *See*
 - password guessing
 - GUI. *See* graphical user interface
 - GUID (Globally Unique Identifier), 105, 136
 - GUID partition table (GPT), 74, 75
- H**
- hacker(s). *See also*
 - information security;
 - malware, automated
 - client security and, 526–530
 - criminal, 70, 71
 - dedicated, 60–61
 - exploitation techniques, 43–60
 - IE and, 253–254, 289
 - intentions, 70–71
 - malware types and, 62–70
 - methodology, 60–61
 - PM’s impact on, 253–254
 - popular software and, 246, 289
 - hard disk encryption, 534–535
 - hardening, 547. *See also*
 - Internet Information Services 7.0; named pipes; service(s)
 - people, 547
 - Hardware key, 102
 - harmonics, 463
 - hash tables,
 - pre-computed, 49
 - hashes. *See specific hashes*
 - HelpAssistant
 - account, 181
 - removal of Support and, 181
 - hives, 101. *See also*
 - registry; *specific hives*
 - abbreviations, 101
 - levels under, 102–103
 - types, 101
- HKCC (HK_Current Config) hive, 107–108
- HKCR (HKey_Classes_Root) hive, 103–107
- file associations and, 103, 104
 - sections, 104–105
 - Trojans and, 106, 107
 - use of, 103
- HKCU (HKey_Current_Users) hive, 107
- file associations and, 104
 - spyware and, 107
- HK_Current Config hive. *See* HKCC hive
- HKey_Classes_Root hive. *See* HKCR hive
- HKey_Local_Machine hive. *See* HKLM hive
- HKey_Users hive. *See* HKU hive
- HKLM (HKey_Local_Machine) hive, 102–103
- file associations and, 104
 - keys in, 102–103
 - Software, 103
 - System, 103
- HKU (HKey_Users) hive, 107
- Howard, Michael, 4, 128
- Http.sys kernel mode driver, 308
- hybrid mode, 90
- Hydra program, 45. *See also* password guessing
- Hyperterminal, 215. *See also* telnet client

- I**
- IAS. *See* Internet Authentication Service
 - icacls.exe command-line tool, 177, 201. *See also* subinacl tool
 - ACLs and, 191
 - resetting, 195
 - restoring, 192–193
 - saving, 191, 192
 - change owner with, 194
 - deny operations and, 195
 - find all ACEs granted to particular user and, 195
 - functionality, 191–197
 - grant operations and, 195
 - notes on, 188
 - remove operations and, 195–196
 - set integrity levels with, 196–197
 - shortcomings of, 199
 - substitute SIDs with, 193–194

- ICF. *See* Internet Connection Firewall
- ICMP. *See* Internet Control Message Protocol
- identity, 108–109. *See also* logon authentication
- IE. *See* Internet Explorer
- IEAK. *See* Internet Explorer Administration Kit
- IFRAME, 273, 280
- IIS. *See* Internet Information Services
- IIS_IUSRS, 24, 314–315
- IIS_WPG, 25
- impersonation, 115, 127, 219
 - delegation *v.*, 115, 116, 127
- Include local directory path when uploading files to a server (setting), 273, 280
- “Increase a process working set,” 141
- Independent Software Vendors (ISV), 128
- information disclosure, 55
- information security, 519–547. *See also* security tweaks
 - best practices, 547
 - complementary approach, 523–524
 - “defense in depth” and, 520, 523
 - different views on, 526
 - account lockout, 539–546
 - anti-malware, 530–532
 - client security hacks, 526–530
 - security tweaking, 532–538
 - external factors, 519
 - risk management, 520–523, 547
 - enterprise, 521–523
 - security awareness programs, 546, 547
 - social engineering and, 50, 59–60, 546
 - examples, 59
 - SRP and, 524–525
 - strategies *v.* new tools, 519, 547
 - three-step approach, 523–525
 - keep attacks off box, 524
 - keep malicious code from communicating, 525
 - stop malicious code from running, 524
 - user education and, 524, 532
 - wetware, 546
- infrared wireless technologies, 461
- Infrastructure mode, 462–463
- infrastructure, Windows, 73–117
- inheritance
 - dangers, 175
 - definition, 174
- Initialize and script ActiveX controls not marked as safe for scripting (setting), 267, 279
- installers
 - elevating, 166
 - heuristic detection of, 151
- integrity controls, 22–23, 116–117
 - mandatory, 22–23, 116, 146
- integrity labels
 - low, 146
 - privilege for, 141
- integrity levels, 116, 117, 190
 - setting, 196
 - icacls and, 196–197
- integrity model, 158
- integrity SIDs, 22–23
- Interactive Service Detection Service, 17
- International - Send UTF-8 URLs, 283, 287
- INTERNET, 181, 182
- Internet Authentication Service (IAS), 467, 469
- Internet Connection Firewall (ICF), 403. *See also* Firewall, Windows shortcomings of, 403, 404, 409
- Internet Control Message Protocol (ICMP), 493. *See also* Network Location Awareness service
- ECHO, 493, 494
- Internet Explorer (IE) 7.0
 - ActiveX control handling, 33, 222, 223, 257
 - Add-on management, 256–257
 - advanced settings, 282–288
 - Browsing, 282, 287
 - International, 283, 287
 - Java (or Java-Sun), 283, 287
 - Security, 283–286, 287–288
 - summary of, 287–288
 - best practices, 290–291
 - browsers *v.*, 245–247
 - defenses/recommendations, 288–289
 - digital certificate handling, 257–258
 - encryption improvements, 26–27, 257–258
 - file types by file extension, 269
 - Group Policy and, 495–496

570 Index ■ I

- IEAK and, 495–496
- malware and, 253–254, 289
- as optional component, 247
- phishing filter, 32, 254–256
- Protected Mode, 32, 146, 248–254, 277
 - malware/hackers impacted by, 253–254, 289
- recommendations/defenses, 288–289
- securing, 245–291
- security
 - improvements/new features, 32–34, 248–260
- Security Options, 230
- security zone settings, 264–281
 - ActiveX controls and plug-ins, 265–268, 278–279
 - Downloads, 268–270, 279
 - Java VM-Java Permissions, 270, 279
 - Miscellaneous, 270–275, 279–281
 - .NET Framework, 264–265, 277–278
 - recommendations, 277–281
 - Scripting, 275–277, 281
 - summary of, 277–281
 - User Authentication, 277, 281
- security zones, 260–264
 - Internet site, 261–262
 - Local Computer, 260–261
 - Local intranet, 262–263
 - Restricted sites, 263–264
 - Trusted Sites, 263
- shim compatibility architecture, 251–252
- URL handling protections, 258–259
- vulnerabilities *v.* market share, 247
- Internet Explorer
 - Administration Kit (IEAK), 495
 - IE management without, 495–496
- Internet Information Services (IIS) 7.0, 293–350
 - access control permissions, 326–332
 - administration, 315–318
 - authentication methods, 318–325
 - comparison of, 325
 - summary of, 323–324
 - components, 302–307
 - default, 305–306
 - individual descriptions, 302–305
 - configuration/tightening of, 339–344
 - defending, 332–348
 - summary of steps for, 333
 - Handler Permissions, 326–331
 - summary/usage of, 331
 - hardening procedures, 332–348
 - application installation/securing, 347
 - cleaning/testing, 347
 - deploying to production, 347–348
 - host firewall configuration, 335
 - log file/firewall monitoring, 348
 - minimal configuration on IIS, 336
 - network/perimeter security configuration, 333–334
 - OS hardening, 337–339
 - OS installation, 334–335
 - patch installations, 336–337
 - penetration tests, 347
 - physical security, 334
 - remote administration configuration, 335–336
 - summary of, 348–350
 - updated hardware drivers, 334
 - Web site securing, 344–346
 - web-server specific, 39–344
 - installation of, 301
 - additional features, 340
 - introduction, 299–300
 - modules, 340–341
 - list/description of, 340
 - new features/improvements, 34, 57, 300–301
 - NTFS permissions and, 332
 - strengthening, 342–343
 - protocol listeners, 307–309
 - versions, 300
 - web component minimization, 342
 - web server threats, 293–299
- Internet site security zone, 261–262. *See also* security zone settings
- Interprocess Communications mechanism. *See* IPC mechanism

- Interprocess
 - Communications
 - Share. *See* IPCS
- IP version 6 (IPv6), 36, 412
 - Windows Firewall and, 36, 406–407, 412
- IPC (Interprocess Communications)
 - mechanism, 207. *See also* named pipes
- IPCS (Interprocess Communication Share), 97
- IPsec, 407
 - client-to-DC, 451
 - definition, 407
 - Windows Firewall and, 407, 424
- IPv6. *See* IP version 6
- isolation. *See also*
 - information security; Server and Domain
 - Isolation
 - Domain, 36–37, 446–447
 - Domain and Server, 445–459, 524, 526, 530, 531
 - Server, 447–448
 - Session 0, 210–213
 - sessions, 16–17, 211–212
 - UAC and process, 158, 169
- ISV. *See* Independent Software Vendors
- IUSR_*computername*, 314–315
- J**
- Java (or Java-Sun) - Use
 - JRE x.x for [applet], 283, 287
- Java applets, 277
 - scripting of, 277, 281
- Java Virtual Machine (JVM) component, 270
- Java VM-Java
 - Permissions, 270, 279
- Johansson, Jesper, 174
- John the Ripper program, 48, 61
- junction points, 23, 143, 184, 185, 186
- junk mail detection, Windows Mail, 386–387
- JVM component. *See* Java Virtual Machine component
- K**
- Keeping Your Business Safe From Attack: Passwords and Permissions* (Grimes), 113
- Kerberos, 109, 111, 112, 431, 433, 435
- kernel objects, 173
- Kernel Patch
 - Protection, 39
- keylogging, 50
- keys, 101. *See also specific keys*
- Kismet, 57
- Konqueror, 246
- L**
- LAN Manager (LM), 14, 110, 112
 - disabled, 14
 - hash, 110
- LAND attacks, 58
- Launching applications
 - and unsafe files (setting), 273, 280
- Launching programs and files in an IFRAME
 - (setting), 273, 280
- least privilege, 128, 179, 525, 526, 528, 530, 531. *See also* information security; User Account Control
- LeBlanc, David, 4, 449
- leinstal.exe, 252
- leuser.exe, 252
- Link-Layer Topology
 - Discovery, 35
- Link-Layer Topology
 - Discovery Responder, 35
- LM. *See* LAN Manager
- LMCompatibilityLevel
 - setting, 534
- Local Computer
 - Policy, 486
- Local Computer security
 - zone, 260–261. *See also* security zone settings
- Local intranet security
 - zone, 262–263. *See also* security zone settings
- Local Security Policy (GPEdit.msc), 88, 486
 - application order, 88
- Local Service account, 92, 205
- Local System account, 92, 205
- logon architecture
 - improvements, 14–17
 - process, 16
 - session isolation, 16–17
- logon authentication, 108–114
- logon credential
 - guessing/cracking, 44–51
- logon scripts, 516
 - UAC and failure of, 516
- LogonUI, 15, 16
- logs, 29
- Longhorn server, 514
 - future improvements, 40
- Loose XAML (setting), 264, 277
- LophtCrack, 57, 112
- low integrity folders, 250–251
- Lynx, 246

572 Index ■ M

M

- MAC. *See* Media
 - Access Control
- MACLs. *See* mandatory
 - access control lists
- Mail. *See* e-mail;
 - Windows Mail
- malicious code, 524.
 - See also*
 - information security
 - three-step approach for
 - management of, 524–525
- malicious exploitation
 - techniques, 43–60
- malicious file attachments,
 - 58, 351–384. *See also*
 - e-mail
 - file extension tricks, 380–381
 - number of, 352
 - table list
 - details of file type, 352–379
 - file extension, 352–379
 - file type, 352–379
 - risk level, 352–379
- Malicious Software
 - Removal Tool (MSRT), 13–14, 225–229
 - command-line
 - switches, 228
 - download, 227
- malware, automated, 4,
 - 62–71, 225. *See also*
 - adware; bot(s); client protection; hacker(s); information security; spyware; Trojans; viruses; Windows Defender; worms
 - anti-, 524, 531–532
 - Microsoft and, 239–240
 - bootable, 76
 - business *v.* home
 - computer attacks, 520
 - criminal gain through, 64, 70, 71
 - defense, 241, 520
 - e-mail defense
 - against, 398
 - hybrid, 63
 - IE and, 253–254, 289
 - intentions of, 64, 70, 71, 520
 - locations modified by, 65–70
 - application areas, 66
 - file areas, 66
 - folder areas, 67
 - other, 67
 - registry keys, 67–70
 - PM's impact on, 253–254
 - removal procedures, 71
 - as side-effect install, 240
 - types, 62–70
 - UAC and, 122, 123, 158, 169
 - wireless networks and, 474–475
 - mandatory access control
 - lists (MACLs), 173. *See also*
 - access control lists
 - definition, 173
 - mandatory integrity
 - controls (MICs), 22–23, 116, 146. *See also*
 - integrity controls
 - man-in-the-middle (MitM) attacks, 27,
 - 50, 57
 - Margosis, Aaron, 128
 - Master Boot Record (MBR), 74, 75
 - MBR. *See* Master Boot Record
 - Media Access Control (MAC) addresses, 478
 - media devices, controlled,
 - 19, 525
 - Message Integrity Code (MIC), 466
 - Metasploit Framework (MSF), 53, 57
 - web interface, 53
 - MIC. *See* Message Integrity Code
 - Microsoft, anti-malware
 - and, 239–240
 - Microsoft Desktop
 - Optimization Pack (MSDOP), 221–222
 - technologies, 221–222
 - Web information on, 222
 - Microsoft Management Console (MMC), 486
 - Microsoft Security Web Site, 230
 - Quick Link, 230
 - Microsoft Windows Internals, Fourth Edition* (Russeinovich, Solomon), 73
 - MICs. *See* mandatory
 - integrity controls
 - Milw0rm Web site, 52
 - MIME type identifier, 105
 - MIMO. *See* Multimedia In Multimedia Out
 - Miscellaneous (security zone setting), 270–275, 279–281. *See also*
 - specific settings*
 - misconfiguration, 56
 - application, 56–57
 - OS, 56–57
 - MitM attacks. *See* man-in-the-middle attacks
 - mixed/down-level
 - environment, Windows Firewall and, 438–442
 - MLGPOs. *See* multiple
 - local Group
 - Policy objects
 - Mlink.exe utility, 23
 - MMC. *See* Microsoft Management Console
 - “Modify an object label,” 141

- Moskowitz, Jeremy, 485, 518
- Mozilla Firefox, 245, 246
security of, 246
vulnerabilities *v.* market share, 247
- Msascui.exe, 233
- MSDOP. *See* Microsoft Desktop Optimization Pack
- MSF. *See* Metasploit Framework
- Msmpeg.exe, 233
- MSN Explorer, 214
- MSRT. *See* Malicious Software Removal Tool
- Multimedia In
Multimedia Out (MIMO), 464
- multiple local Group Policy objects (MLGPOs), 486–491.
See also Group Policy in domain environment, 491 precedence, 489–491 Web information on, 491
- N**
- name resolution, 89–90
NetBIOS, 90
- named pipes, 97
definition, 207
hardening, 207–208
as securable objects, 173
- NAP. *See* Network Access Protection (NAP), 37, 471
Group Policy and, 516–517
- network domains, 35. *See also specific domains*
isolation, 36–37
- Network Location Awareness (NLA)
service, 35, 87, 493–494
- network location SIDs, 181–182
new, 181–182
- network mapping tool, 35.
See also Link-Layer Topology Discovery Responder
- Network Policy Server (NPS), 467, 469, 471
- network ports
as securable objects, 173
- reliant components-
Run components signed/not signed with Authenticode, 265, 278
- XAML browser applications, 264, 277
- XPS documents, 264–265, 278
- NetBios
name resolution, 90
- NetMeeting, 214–215.
See also Windows Meeting Space
- Net.MSMQ protocol
listener, 309
- Net.P2P protocol
listener, 308
- Net.Pipe protocol
listener, 308
- Netsh, 423
Windows Firewall and, 423–424
- Net.Tcp protocol
listener, 308
- NETWORK, 182
- Network Access Protection (NAP), 37, 471
Group Policy and, 516–517
- network domains, 35. *See also specific domains*
isolation, 36–37
- Network Location Awareness (NLA)
service, 35, 87, 493–494
- network location SIDs, 181–182
new, 181–182
- network mapping tool, 35.
See also Link-Layer Topology Discovery Responder
- Network Policy Server (NPS), 467, 469, 471
- network ports
as securable objects, 173
- network profiles, 91
- Network Service account, 92, 205
- network sniffing. *See* sniffing, network
- network threat modeling, 450, 451
- Nigerian scams, 383
- NLA. *See* Network Location Awareness
- Nmap, 60, 61
- No eXecute (NX)
mechanism, 6
- nodes, 462. *See also* Wi-Fi
- NPS. *See* Network Policy Server
- NT hashes, 110
- NT LAN Manager (NTLM), 110, 112
- NT ServiceTrusted Installer, 181. *See also* Trusted Installer service
- NTFS (Windows NT file system)
changes/improvements, 23–24
permissions, 115
Share *v.*, 115
- NTFS permissions, 332
IIS and, 332
share permissions *v.*, 115
strengthen, 342–343
- Ntfsdos, 77
- NTLM. *See* NT LAN Manager
- Ntoskrnl.exe, 75, 76
- NULL DACLs. *See* discretionary access control lists
- NX mechanism. *See* No eXecute mechanism
- O**
- OAR. *See* Owner Access Restriction objects, 171. *See also* securable objects; *specific objects*

574 Index ■ O–P

- Office Live
Communicator, 214
- OneCare. *See* Windows Live OneCare
subscription service
- Open files based on
content, not file
extension (setting),
274, 280
- Opera, 246
vulnerabilities *v.* market
share, 247
- operating system (OS)
files, 184
Trusted Installer
and, 184
Group Policy and
upgrade/rollout
strategy, 515–516
- IIS
hardening, 337–339
web server services,
337–339
misconfiguration, 56–57
vulnerabilities, 54–56
web server, 295
- OS. *See* operating system
- OS kernel, Vista, 7, 75
- outbound filtering,
Windows Firewall and,
412–417, 525
- Outlook Express, 31. *See*
also Windows Mail
- Owner Access Restriction
(OAR), 24
- OWNER RIGHTS,
182–183, 201
SID, 182–183
- P**
- P2P networking. *See* peer-
to-peer networking
- package point and print
functionality, 506
- Passport services, 34, 259.
See also CardSpace;
Windows Live ID
- password authentication,
14, 16
- password cracking, 14, 44,
48–50. *See also* logon
credential
guessing/cracking
benefits of, 48, 50
methodology, 48
programs, 48
speed of, 48, 49
tools, 112, 113
ebook for, 113
- password dictionaries, 47
attacks, 46
- password guessing, 44–47
attacks, 299
web servers and, 299
automated, 44–46
problems with, 47
types of, 46
- password hacking
methods, 50–51
- password hashes, 48
LM, 110
NT, 110
- password hybrid
attacks, 46
- password storage, 110
- password strength,
533, 535
account lockout and,
541–545
- passwords, leaked, 383.
See also malicious
file attachments
- PatchGuard, 39
- patching
hot, 28
management, 28
- PC / AT BIOS, 74, 75. *See*
also EFI
- Peer Name Resolution
Protocol (PNRP), 37
- peer-to-peer (P2P)
networking, 37
- people, hardening, 547
- perimeters, SDI and,
448–449
- permissions. *See also* NTFS;
Share permissions
ACLs and, 24, 171
default, 186–189, 201
changes to, 186–189
modification of,
188–189, 201
- phishing attacks, 383
- phishing detection,
Windows Mail, 385–386
- phishing filter, 32, 254
anti-, 254–256
security zone setting,
274–275, 281
- Piaget, Chris, 212
- plain-text conversion,
e-mail, 391–393. *See*
also e-mail
- Platform Software
Developers Kit, 174
- PM. *See* Protected Mode
- PNRP. *See* Peer Name
Resolution Protocol
- Ponemon Institute, 77
- Pop-up Blocker
security zone setting,
275, 281
- portscanning, 409
- POSIX subsystem
optional, 214
- POST. *See* Power-on-
Self Test
- post-boot startup, 87
- Power Users, 25, 180, 199
end of, 147, 180
- Power-on-Self Test
(POST), 74, 75
- preferred networks, 463
- Pre-Shared Key (PSK), 466
- printer deployment, 506
- Private network
domain, 35
- privilege(s). *See also*
specific privileges
account rights *v.*, 140
common task
delegations and,
140–143

- escalation, 54–55
 - new, 140–143
 - services with less, 205–207
- Process Tracking
 - auditing, 538
- processes, 173. *See also*
 - specific processes*
 - as securable objects, 173
- profiles, firewall, 417–419.
 - See also* Firewall, Windows;
 - specific profiles*
- per-interface, 444
- Protect Your PC
 - marketing campaign, 128, 526
- Protect Your Windows Network: From Perimeter to Data* (Johansson, Riley), 174
- Protected Mode (PM), 32, 146, 248–254, 277.
 - See also* Internet Explorer 7.0
- low integrity folders, 250
- malware/hackers
 - impacted by, 253–254, 289
- shim compatibility
 - architecture, 251–252
- turn off, 251
- protected processes, 7
 - Task Manager and, 7
- protocol listeners, 307–309. *See also* *specific protocol listeners*
- protocols, 295
 - vulnerabilities, 295–296
- PSK. *See* Pre-Shared Key
- Public network
 - domain, 35
- Pwdump, 112
- R**
- rainbow tables, 49–50
- RATs. *See* remote access Trojans
- Rbot, 226
- RDP. *See* Remote Desktop Protocol
- ReadyBoost
 - technology, 19
 - USB flash memory drives and, 19
- Recovery key, 79. *See also*
 - Boot-up key
- REG_DWORD, 101
- Regedit.exe, 101
- registry, 101
 - ACLs, 199–200
 - protection, 23
 - replacement, 108
 - structure, 101–108
 - virtualization, 25
- registry keys, 173
 - list, 67–70
 - malware in, 67–70
 - low integrity, 250
 - as securable objects, 173
- REG_MULTI_SZ, 102
- REG_SZ, 102
- relative identifier (RID), 124, 125. *See also*
 - Administrator account, built-in 500, 124, 146, 180
- reliant components-Run
 - components signed/not signed with Authenticode (setting), 265, 278
- remote access
 - UAC and, 148, 160
- remote access Trojans (RATs), 63
- Remote Assistance (RA), 148–149
 - UAC and, 149
- Remote Desktop, 148–149
- Remote Desktop Protocol (RDP), 26, 27
- Remote Procedure Call. *See* RPC
- remove operations, icaccls and, 195–196
- Request Filtering, 343–344
 - configuration, 343–344
- Restart Manager, 28, 216–218, 222
 - Web information on, 218
- RESTRICTED SID, 199, 200
- Restricted sites security
 - zone, 263–264. *See also* security zone settings
- restricted token, 199, 200
- Resultant Set of Policy (RSOP) tools, 450, 489
- RID. *See* relative identifier
- rights, 140. *See also*
 - account rights
- Rights Management
 - Service (RMS), 27
- Riley, Steve, 174, 448
- risk management, 520–523, 547. *See also*
 - information security enterprise, 521–523
- RMS. *See* Rights Management Service
- roaming profiles, 91
- robot code, 63. *See also* bot(s)
- rogue Internet links, 58
- rootkits, 65, 129, 226
- routing
 - compartmentalization, 36
- RPC (Remote Procedure Call), 95–96
 - disabling, 96
 - Endpoint Mapper service, 205, 206
 - Windows XP, 205
- importance, 96
- settings, 508
- Windows Firewall and, 442–443
- Rpc-dump.exe, 97
- RSOP. *See* Resultant Set of Policy tools
- rsop.msc, 489, 491
- rules. *See* *specific rules*

576 Index ■ R-S

- rules, Windows Firewall, 426–429
 - authentication exemption, 428
 - connection security, 427–428
 - directional, 427
 - precedence order, 428–429
 - server to server, 428
 - tunnel, 428
 - types, 426–429
 - when to use, 428
- Run ActiveX controls and plug-ins (setting), 268, 279
- Russinovich, Mark, 19, 73
- S**
- SA customers. *See* Software Assurance customers
- SACLs. *See* System ACLs
- Safari, 246
 - vulnerabilities *v.* market share, 247
- Safe Exception Handling switch (/SafeSEH), 5
- safe mode
 - built-in Administrator account in, 146, 147
- SAL. *See* Standard Annotation Language
- SAM. *See* Security Accounts Manager
- SAMjuicer, 112
- SCM. *See* Service Control Manager
- Script ActiveX controls marked safe for scripting (setting), 268, 279
- Scripting (security zone setting), 275–277, 281
 - Active Scripting, 275, 281
 - Allow programmatic clipboard access, 275–276, 281
 - Allow status bar updates via script, 276, 281
 - Allow websites to prompt for information using scripted window, 276, 281
 - Scripting of Java applets, 277, 281
 - Scripting of Java applets (setting), 277, 281
 - scriptlets, 266, 278
 - scripts
 - elevating in, 166
 - Sdbot, 226
 - SDDL. *See* Security Descriptor Definition Language
 - SDI. *See* Server and Domain Isolation
 - SDL. *See* Security Development Lifecycle
 - SDs. *See* security descriptors
 - SeChangeNotifyPrivilege, 186
 - SeCreateSymbolicLinkPrivilege, 143
 - securable objects, 172. *See also* objects
 - examples of, 172–173
 - SDs and, 173–174
- secure desktop, 21, 132–133
 - switch to, 133, 134
 - disabling, 133, 152
- UAC dialog boxes and, 21
- Secure Windows Initiative Attack Team (SWIAT), 4
- Security (IE advanced settings), 283–286, 287–288
- Security Accounts Manager (SAM), 77
 - Active Directory *v.*, 112
 - key, 102–103
 - security awareness programs, 546, 547. *See also* information security
 - Security Center, 230–231
 - features, 230
 - view/configure, 230–231
 - Windows Firewall and, 421
 - Security Descriptor Definition Language (SDDL), 174
 - discussion of, 174
 - learn, 201
 - security descriptors (SDs), 173–174
 - securable objects and, 173–174
 - Security Development Lifecycle (SDL), 3–4
 - security features, Vista
 - essential, 128
 - new, 3–42
 - future, 40
 - Group Policy settings, 38–39
 - host-based, 8–31
 - IE 7, 32–34, 248–260
 - IIS 7, 34
 - networking, 34–38
 - 64-bit platform, 39–40
 - Windows Mail, 31
 - Security Guide, Vista, 510–513, 547. *See also* Group Policy
 - benefits of, 511
 - importance of, 513
 - limitations, 511–513
 - need for, 511
 - security identifiers (SIDs), 18, 124–125. *See also specific security identifiers*
 - ACEs and, 174
 - components of, 124–125
 - definition, 124

- icacls and substitute, 193–194
- integrity, 22–23
- network location, 181–182
 - new, 181–182
- NT ServiceTrusted Installer, 181
- OWNER RIGHTS, 182–183
- Security key, 103
- security options, Vista, 498–504
 - with modified defaults, 498, 500–503
 - new, 499–500
 - removed, 504
- security policies
 - application of, 88
- security principals, 171
- security settings, default, 12–13
- security strategies. *See* information security
- security tokens
 - changes to, 189–190
 - contents, 125–127
 - Whoami command and, 125
- security tweaks, 532–538. *See also* information security
 - auditing, 533
 - bad, 536–538
 - ACL changes, 536–537
 - disabling MSV1_0, 537
 - disabling Process Tracking auditing, 538
 - too many user rights/privileges, 537
 - UAC disabling, 538
- don't use public, shared computers, 536
- e-mail conversion to plain text, 391–393, 535
- hard disk encryption, 534–535
- LMCompatibilityLevel setting, 534
- password strength, 533, 535
- remove logon privileges from service accounts, 534
- run services on non-default ports, 535–536
- SDI, 534
- turn on DEP, 536
- security zone settings, 264–281. *See also* specific settings
 - ActiveX controls and plug-ins, 265–268, 278–279
 - Downloads, 268–270, 279
 - Java VM-Java Permissions, 270, 279
 - Miscellaneous, 270–275, 279–281
 - .NET Framework, 264–265, 277–278
 - recommendations, 277–281
 - Scripting, 275–277, 281
 - summary of, 277–281
 - User Authentication, 277, 281
- security zones, 260–264
 - Internet site, 261–262
 - Local Computer, 260–261
 - Local intranet, 262–263
 - Restricted sites, 263–264
 - Trusted Sites, 263
- SeIncreaseWorkingSet-Privilege, 141
- sender white/black lists, Windows Mail, 387
- SeRelabelPrivilege, 141
- Server and Domain Isolation (SDI), 445–459, 530, 531, 534, 536. *See also* information security
 - AuthIP and, 451–452
 - best practices, 459
 - configuration user interface, 453–458
 - documentation, 446
 - Domain Isolation and, 36–37, 446–447
 - negotiation flow and, 452–453
 - network threat modeling and, 450, 451
 - overview, 445–448
 - perimeters and, 448–449
 - rules, 454–458
 - domain, 454–457
 - server, 457–458
 - security tweak, 534
 - Server Isolation and, 447–448
 - value of, 458–459
- Server Core, 40
- Server Message Block (SMB) 2.0, 38, 97–98
 - access, 148
 - UAC and, 148
- CIFs and, 97–98
- disabling, 98
- Server service, 98, 99
 - disabling, 99
- server to server rules, 428
- service(s), 92–94. *See also* specific services
 - accounts, 92, 93
 - complete list, 17
 - delayed start, 18
 - desktop interaction with, 93, 94
 - essential, 94–100
 - failure, 94
 - hardening, 17–18, 92, 181, 204, 222
 - features, 204–207
 - Windows Firewall and, 411, 525
 - less privileged, 205
 - number of, 92
 - privilege reduction in, 205–207

578 Index ■ S

- restriction, 93
 - firewall policies
 - and, 207
 - security, 17–18
 - SIDs, 204–205
 - write-restricted tokens
 - and, 207
- Service Control Manager (SCM), 18, 92
- Service Host Process. *See* Svchost
- Service Set Identifier (SSID), 462
 - broadcasting, 479–480
 - disabling, 479–480
- Session 0 isolation, 210–213, 222
 - mechanics of, 212–213
- sessions, 210–211
 - isolation, 16–17
 - need for, 211–212
 - security, 16–17
- SeTimeZonePrivilege, 141–142
- SeTrustedCredManAccessPrivilege, 141
- share permissions, 115
 - default, 189
 - NTFS permissions *v.*, 115
- Sharing tab, 190
- shatter attacks, 212. *See also* Session 0 isolation
- ShellOpenCommand subkey, 106
- shoulder-surfing, 50
- SIDs. *See* security identifiers
- Silentranner.vbs script, 70
- simplicita.com, 63
- 64-bit platform
 - EFI on, 74
 - improvements to, 39–40
- smart cards
 - support, 15, 16
- SMB. *See* Server Message Block
- sniffing attacks, web servers and, 297–298
- sniffing, network, 48, 50, 111
 - Cain & Abel and, 50, 51
 - Kismet and, 57
- social engineering, 50, 59–60, 546. *See also* information security examples, 59
- sockets, permissions, 24
- SoftGrid, Microsoft, 221
- Software Assurance (SA) customers, 221, 223
- Software channel
 - permissions (setting), 274, 281
- Software Explorer, 235
 - Windows Defender and, 235, 236
- Software Restriction Policies (SRP), 524–525, 529. *See also* information security
- software, unintended consequences of, 56
- Solomon, David, 73
- spam, 226
- Spectorsoft, 64
- SpyNet, 12, 231, 233. *See also* Windows Defender online community, 13
- spyware, 64
 - browser cookies, 237
 - HKCU and, 107
- SQL Slammer, 62, 448
- SRP. *See* Software Restriction Policies
- SRT. *See* Startup Recovery Tool
- SSID. *See* Service Set Identifier
- SSL VPNs, 448
- SSL/TSL Client Side Mapping, 323
- Standard Annotation Language (SAL), 4
 - coding and, 4
 - website information, 4
- standard users
 - elevation of, 150–151, 168
- Startup Recovery Tool (SRT), 10, 11
- stealth feature, Windows Firewall, 408
- Storage Root Key, 78
- strict source mapping, Windows Firewall and, 410–411
- SUA. *See* Subsystem for Unix-Based Applications
- subinacl tool, 199, 201. *See also* icaccls.exe
 - command-line tool
 - ACLs management and, 199, 201
- subjects, 171. *See also* security principals
- subkeys, 101. *See also specific subkeys*
- Submit non-encrypted form data (setting), 274, 281
- Subsystem for Unix-Based Applications (SUA), 28
- subtrees, 101. *See also* hives
- sudo, 160–162
 - UAC *v.*, 160–162
- Sullivan, Kevin, 221
- Support account, 181
 - removal of
 - HelpAssistant and, 181
- Svchost (Service Host Process), 94–95. *See also* RPC processes, 95
- SWIAT. *See* Secure Windows Initiative Attack Team
- symbolic links, 23, 143
 - creation, 143
 - privilege for, 143
 - user profile, 91

- SYN-ACK packet, 404
 Sysinternals, 70, 235
 system access control lists (SACLs), 173. *See also* access control lists definition, 173 modification of, 199
 System ACLs (SACLs), 24
 system recovery tools, improvements on, 10–11
 System Restore Points, 24
- T**
- Tablet PC Optional Components, 215
 Task Manager
 protected processes and, 7
 security improvements, 30–31
 Tasklist /svc, 95
 TCP/IP stack
 with IPv6, 36
 rebuilt, 34, 35, 36
 telnet client, 215
 optional, 214
 telnet server, optional, 214
 template embedding, 493
 ADMX files and, 493
 Temporal Key Integrity Protocol (TKIP), 466
 Terminal Services, 508
 Group Policy settings, 508–510
 TFTP client, optional, 214
 thinking about
 security. *See* information security
 Threat Code
 (threatcode.com), 169, 206
 threat modeling, 3–4, 56
 network, 450, 451
 time
 UTC, 142
 Zulu, 142
 time zone modification
 privilege, 141–142
 TKIP. *See* Temporal Key Integrity Protocol
 tokens. *See* security tokens; *specific tokens*
 TPM. *See* Trusted Platform Module
 Tpm.msc, 12, 80
 Trojans, 62–63, 225
 direct action, 63
 HKCR and, 106, 107
 RATs, 63
Trusted for Delegation, 116
 Trusted Installer service, 26, 181
 new feature, 181
 NT SERVICE, 181
 SID of, 181
 OS files and, 184
 Trusted Platform Module (TPM), 78. *See also* BitLocker Drive Encryption
 chip, 11, 12, 78
 initialization, 80, 81, 82
 Web site
 information, 78
 enabling steps for
 BitLocker and, 80–87
 Group Policy settings, 82, 83, 514
 password creation, 81, 82
 recovery keys, 514
 Trusted Sites security
 zone, 263. *See also* security zone settings
 tunnel rules, 428
- U**
- UAC. *See* User Account Control
 UIAccess. *See* User Interface access
 UMDF. *See* User-Mode Driver Framework
 unintended software
 consequences, 56
 Unix, on Windows, 28.
 See also Subsystem for Unix-Based Applications
 URL Filtering, 343. *See also* Request Filtering
 URL handling protections, 258–259
 USB flash memory drives, 10, 19
 boot disk, 549
 WinPE and building, 549–554
 ReadyBoost and, 19
 Use phishing filter
 (setting), 274–275, 281.
 See also phishing filter
 Use Pop-up Blocker
 (setting), 275, 281
 User Access Control
 Status, 230
 User Account Control (UAC), 20–21, 121–169
 applications and leveraging, 164–167
 basics, 123–124
 best practices, 168–169
 disabling, 152, 156–157, 159
 consequences of, 157
 facts about, 122–123
 file access and, 153–154
 frequently asked questions, 153–164
 goals/purpose of, 129–130, 168
 Group Policy
 configuration, 150–152
 importance of, 168
 introduction, 121–123
 least privilege and, 128, 179, 525, 526, 528, 530, 531
 logon script failure and, 516
 malware and, 122, 123, 158, 169

580 Index ■ U–W

- non-admins and, 129–130
 - process isolation and, 158, 169
 - purpose/goals of, 129–130, 168
 - RA and, 149
 - remote access and, 148
 - Secure Desktop and, 21
 - SMB access and, 148
 - sudo *v.*, 160–162
 - system-wide setting of, 159
 - User Account Control:
 - AdminApproval Mode for the Built-in Administrator Account, 150
 - User Account Control: Behavior of the Elevation Prompt for Administrators in Admin Approval Mode, 150
 - User Account Control: Behavior of the Elevation Prompt for Standard Users, 150–151
 - User Account Control: Detect Application Installations and Prompt for Elevation, 151
 - User Account Control: Only Elevate Executables that Are Signed and Validated, 151
 - User Account Control: Only Elevate UIAccess Applications that Are Installed in Secure Locations, 152
 - User Account Control: Run All Administrators in Admin Approval Mode, 152
 - User Account Control: Switch to the Secure Desktop when Prompting for Elevation, 152
 - User Account Control: Virtualize File and Registry Write Failures to Per-User Locations, 152
 - User Authentication, 277
 - security zone settings, 277, 281
 - User data persistence (setting), 275, 281
 - User Experience (UX), Vista, 7–8
 - User Interface access (UIAccess), 152, 157
 - user profiles, 90–92
 - symbolic links and, 92
 - User-Mode Driver Framework (UMDF), 19
 - users, built-in
 - modifications of, 179
 - new changes, 24–25, 179
 - UTC (Coordinated Universal Time), 142
 - UX. *See* User Experience
- V**
- values, 101
 - virtualization, 145
 - disabling, 152
 - file, 25, 145
 - registry, 25
 - removal of, 145
 - viruses, 62, 524. *See also*
 - Windows Live OneCare subscription service anti-virus programs, 220–221, 524
 - limitations of, 221
 - boot, 76
 - OneCare and scanning, 238
 - Vista. *See* Windows Vista
 - VMK. *See* Volume Master Key
 - Volume Master Key (VMK), 77, 78
 - Volume Shadow Copy service, 24
 - VPN protocols, 481
 - vulnerabilities. *See also*
 - data malformation;
 - information disclosure;
 - privilege(s);
 - unintended software consequences
 - application, 54–56
 - defense, 57
 - OS, 54–56
 - testing tools, 53, 57
- W**
- WAIK. *See* Windows Automated Installation Kit
 - web servers, 293–294
 - buffer overflows, 296
 - DoS attacks, 298–299
 - OS vulnerabilities, 295
 - password guessing attacks, 299
 - sniffing attacks, 297–298
 - threats, 293–299
 - list of, 294
 - Web sites in less privileged web content zone can navigate into this zone (setting), 275, 281
 - Wecsvc service. *See* Windows Event Collector service
 - WEP. *See* Wired Equivalent Privacy
 - wetware, 546. *See also* information security
 - wf.msc, 422
 - WFP. *See* Windows File Protection; Windows Filtering Program

- Whoami /all
 - command, 114
 - security token and, 125
- Wi-Fi, 461–471. *See also* wireless networks
 - Ad-Hoc mode, 462–463
 - Alliance, 462
 - best practices, 482
 - 802.11 network
 - technologies, 461
 - 802.11 standards, 463–464
 - comparison of, 464
 - types, 463
 - Infrastructure mode, 462–463
 - security standards, 464–471
 - setup diagram, 462
 - terminology/technologies, 461–471
- Wi-Fi Protected Access. *See* WPA
- Wi-Fi Protected Setup (WPS), 466, 467
- Windows Stations (winsta), 211
- Windows authentication, 322–323, 324
 - other authentication methods *v.*, 325
- Windows Automated Installation Kit (WAIK), 549, 550. *See also* Windows Pre-Installation Environment
- Windows Backup. *See* Backup, Windows
- Windows CardSpace. *See* CardSpace
- Windows Defender, 13, 14, 230, 231–238. *See also* Windows Live OneCare subscription service
 - accuracy, 236–237
 - heuristic scanning, 235
 - OneCare and, 238, 239
 - real-time scanning, 232
 - areas of, 232–233
 - Software Explorer
 - feature, 235, 236
 - startup program
 - information by, 236
- Windows Event Collector (Wecsvc) service, 30
- Windows Explorer, 154
 - elevation motions for, 154–156
 - deletion and, 154–156
- Windows Fax and Scan service, 215
- Windows File Protection (WFP), 25, 26, 209. *See also* Windows Resource Protection
 - WRP *v.*, 209
- Windows Filtering Program (WFP), 405–407
 - architecture diagram of, 406
- Windows Firewall. *See* Firewall, Windows
- Windows infrastructure, 73–117
- Windows Installer 4.0, 28
- Windows Live ID, 34
- Windows Live Mail, 352
- Windows Live Messenger, 214
- Windows Live OneCare subscription service, 238–239
 - anti-virus scanning, 238
 - firewall, 238
- Windows Defender and, 238
- Windows Mail, 31. *See also* e-mail
 - domain blocking, 387–390
 - e-mail storage in, 390
 - introduction, 384–390
 - junk mail detection, 386–387
 - phishing detection, 385–386
 - security features, 384–390
- Windows Meeting Space, 214, 215
- Windows Messenger, 214. *See also* Office Live Communicator
- Windows Modules Installer, 181. *See also* Trusted Installer service
- Windows Name Service (WINS), 90
- Windows NT file system. *See* NTFS
- Windows Pre-Installation Environment (WinPE), 10–11, 549
 - bootable USB flash drive, 549
 - building, 549–554
 - features, 10–11
 - packages in, 551
- Windows Presentation Foundation (WPF) platform, 264
- Windows Protected Media Path (WMPM), 7
- Windows Recovery Environment (WinRE), 10
- Windows Remote Management (WinRM) service, 30
- Windows Resource Protection (WRP), 26, 209–210
 - Web information on, 210
 - WFP *v.*, 209
- Windows Shared View, 37
- Windows Sidebar, 215
- Windows Terminal Services, 148. *See also* Remote Desktop

582 Index ■ W–Z

- Windows Vista. *See also*
 access control lists;
 Group Policy;
 information security;
 security features, Vista;
 wireless networks
 ACLs, 114–117, 171–201
 client protection,
 225–241
 components
 new, 215
 optional, 213–214, 214
 reduction of, 213–214
 removed, 214–215
 undesirable, 215–216
 information security,
 519–547
 security features, 3–42
 Security Guide, 510–513
 security options, 498–504
 wireless improvements
 in, 476–477
- Windows XP, 178. *See also*
 access control lists
 ACL UI, 197
 ACLs, 178–179
 default, 179
 problems in, 178–179
 firewall, 403, 404
- WindowsSystem32 files
 protection of, 23
- Winload.exe, 9, 75, 76
- Winlogon, 496. *See also*
 Group Policy
 Group Policy and,
 496–497
- WinPE. *See* Windows
 Pre-Installation
 Environment
- WinRE. *See* Windows
 Recovery Environment
- Winresume.exe, 10
- WinRM service. *See*
 Windows Remote
 Management service
- WINS. *See* Windows
 Name Service
- winsta. *See* Window
 Stations
- Wired AutoConfig, 467
- Wired Equivalent Privacy
 (WEP), 465–466,
 480–481
 Dynamic, 480–481
- Wireless Fidelity, 462. *See
 also* Wi-Fi
- wireless networks, 482.
See also Wi-Fi
 best practices, 482
 securing, 37, 477–481
 threats, 471–475
 DoS attacks, 475
 eavesdropping,
 472–474
 malware, 474–475
 unauthorized
 access, 474
 Vista improvements for,
 476–477
- Wireshark, 57
- WMF worm, 228, 229
- WMI filters, 440–441
 version specification, 441
- Work network
 domain, 35
- worker processes, 309
- working set, privilege
 for, 141
- Workstation service, 98,
 99, 205
 disabling, 98–99
- worms, 62. *See also*
specific worms
- WPA (Wi-Fi Protected
 Access), 466, 481
 Enterprise Mode, 467–471
 Personal Mode, 466–477
 using, 481
- WPA2 Enterprise Mode,
 467–471
- WPA2/802.11i, 466,
 481, 482
- WPF platform. *See*
 Windows Presentation
 Foundation platform
- WPS. *See* Wi-Fi
 Protected Setup
- write-restricted
 tokens, 207
 services with, 207
- WRP. *See* Windows
 Resource Protection
- X**
- XAML (Extensible
 Application Markup
 Language), 264
- XAML browser
 applications (setting),
 264, 277
- XML Paper Specification.
See XPS
- XP. *See* Windows XP
- Xprobe2, 60
- XPS (XML Paper
 Specification), 264–265
 documents (setting),
 264–265, 278
- XSS attacks. *See* cross-site
 scripting attacks
- Z**
- ZoneAlarm, 240
- zones. *See* security zones;
 time zone
- Zulu time, 142