



Index

A

- acceptance of risk, 15–16
- AcceptSecurityContext, 331
- access checks
 - AccessChecksLevelAttribute, 282–283
 - adding explicit, 285–286
 - auditing, 251
 - in Authorization Manager, 241–245, 243–244
 - authorization scripts and, 249–251
 - COM/COM+, 281–284
 - delegation and, 317
 - disabling, 285–286
 - order in, 198
 - overloading, 244–245
 - role-based, 281–286
 - tokens in, 75–76
- AccessChecksLevelAttribute, 282–283
- access control. *See also* ACLs
 - ColnitializeSecurity and, 266–267
 - discretionary, 87, 183–186
- access mask, 201, 202, 207
- account names, 113
- ACEs (access control entries), 195, 197–198
 - audits, 201–202
 - auto-propagation of, 216–219, 217
 - denials, 201–202
 - direct *vs.* inherited, 215–217, 219–220
 - evaluation of, 198
 - inheritance of, 211–214
 - managing, 215–219
 - negative, 197, 199, 220–221
 - order of, 220–221
 - permission grants, 201–202
 - positive, 197, 199, 220–221
 - removing, 215–216
- ACLs (access control lists), 197–203
 - auto-propagation in, 217–219
 - divergent access policies and, 221–223
 - inheritance of, 196, 211–223
 - order in, 198–200
 - permissions in, 199–200, 206–207
 - persisting, 233–234
 - programming, 229–231
 - security based on, 182, 183–184
 - SIDs in, 61, 63
 - structure of, 197–198
 - window stations and, 82
- Active Directory
 - auditing, 53
 - authorization stores in, 245–246
 - delegation and, 316–320
 - delegation via, 325–326
 - domain authorities in, 59
 - Global Catalog, 92–93
 - group policy in, 369–370
 - SSPI and, 333
- Active Directory Users and Computers, 59–60
- AdjustTokenPrivileges, 106–109
- administrator logon, non-admin code
 - development and, 35–46
- adminShell.cmd, 39–40
- adminShellInit.cmd, 39–40
- admin window
 - customization of, 38–39
 - skinning, 38–39
- All Users, 88
- ANONYMOUS LOGON, 175

382 ■ INDEX

- anonymous users
 - in COM, 257–258
 - dealing with, 175–178
 - guest logon, 173–174
 - null session and, 79, 169–171
 - AppIDs, 264–265
 - ApplicationAccessControlAttribute, 281–282
 - Application class, 44
 - application groups, 247–248
 - apps, code usable by non-admins and, 42–44
 - Art of Deception, The* (Mitnick), 16
 - As Activator Activation, 289–290
 - ASP.NET
 - authentication in, 277–279
 - impersonation and, 154–155, 157–161, 277–279
 - secrets in configuration files, 356–357
 - security context and, 71
 - Thread.CurrentPrincipal in, 165–166
 - aspnet_setreg, 356–357
 - ASPNET_WPEXE, 277
 - attack trees, 14–15
 - audits
 - ACLs in, 197–203
 - Authorization Manager, 243–245
 - enabling, 47–49
 - finding settings for, 48–49
 - impersonation and, 151
 - Authenticated Users, 171
 - granting permissions with, 175
 - authentication, 25–26, 293–298. *See also* CIA
 - ApplicationAccessControlAttribute and, 281–282
 - ASP.NET, 277–279
 - audit logs of, 47–49
 - in Authorization Manager, 241–244
 - CoInitializeSecurity and, 255–258, 271–273
 - COM, 255–258, 271–273, 275–276
 - configuring COM, 275–276
 - cross-domain, 303–305
 - daemon identity and, 137–138
 - forcing, 158
 - group membership in, 94–96
 - impersonation and, 151
 - importance of, 293–294
 - IPSEC, 342
 - in logon sessions, 77
 - multifactor, 25–26
 - mutual, 26, 301–302
 - name and password, 126–129
 - .NET remoting, 339–340
 - NTLM, 59
 - null session, 169–171
 - protocol transition and, 321–324
 - in role-based security, 181–182
 - security context and, 71–72
 - security principals and, 57–60
 - service principal names and, 309–310, 312–313
 - sharing secrets in, 297–298
 - SSPI and, 327–328, 331
 - user-to-user, 307–308
 - Authentication Header (AH), 343, 344, 347
 - AuthenticationType, 118, 123
 - authenticators, 300–302
 - authorities, security principals and, 58–59
 - authorization
 - IPSEC, 341–342
 - in role-based security, 181–182
 - scripts, 249–251
 - security context and, 71–72
 - storing, 245–246
 - Thread.CurrentPrincipal and, 163–164
 - Authorization Manager, 182, 235–252. *See also* role-based security
 - administrator mode, 239
 - application groups, 247–248
 - applications, 246
 - auditing in, 251
 - authorization store, 240–241
 - deployment of, 237–238
 - developer mode, 239
 - interop assembly, 242
 - nesting roles in, 240–241
 - runtime interface, 241–245, 244
 - runtime *vs.* administration, 236
 - sample app for, 238–239
 - scopes, 246
 - scripts, 248–251
 - stores, 245–246
 - task/role creation in, 236–238
 - auto-refresh, 373
 - AzMan. *See* Authorization Manager
 - AZMAN.MSC, 236
 - AZROLES.DLL, 236
- ## B
- BackBitmap, 38–39
 - batch logons, 129, 139
 - BeginInvoke, 164
 - biometric data, 26
 - block ciphers, 295–296
 - buffer overflow vulnerabilities, 4–5
 - Bypass Traverse Checking, 104

C

cacls.exe, 217–219
 CATID_MARSHALER, 267
 CBC-MAC technique, 295–296
 certificates
 authentication of, 26
 stores of, 87
 X.509, 344
 challenge-response, 59
 CheckTokenMembership, 122
 CIA (confidentiality, integrity, authentication), 293–298, 327–328
 in .NET remoting, 335–340
 in socket-based apps, 329–334
 using SSPI, 329–340
 Cipher Block Chaining (CBC) mode, 295–296
 clearance levels, 185
 ClientAuthenticate, 331
 client context object, 250
 cloaking, 267–268
 CLR, luring attacks and, 28
 CoInitializeSecurity, 263–269
 calling, 271–273
 IIS 6 and, 278
 passing values to, 278–279
 COM/COM+
 access checks in, 281–284
 AppIDs and, 264–265
 ASP.NET and, 277–279
 authentication levels, 255–258, 275–276
 client security configuration, 271–273
 CoInitializeSecurity and, 263–269
 configuring authentication/impersonation in, 275–276
 daemons, 134
 impersonation levels, 259–261, 275–276
 IPSEC and, 342–343
 logon rights, 139
 null sessions and, 171
 process identity configuration, 287–290
 role-based security in, 182, 235, 281–286
 user interface display from daemons and, 142–143
 Windows XP service pack 2 and, 268–269
 command prompt
 code development and, 37–39
 CommonAppDataPath, 44
 ComponentAccessControlAttribute, 284
 Component Services, 264–265

Computer Configuration, 369–370, 373. *See also* group policy
 Software Settings, 375–376
 concurrency issues, 246
 confidentiality, 293, 327–328. *See also* CIA
 console, locking, 365
 CONTAINER_INHERIT_ACE, 214
 ContainerObjectSecurity, 195–196
 ContextUtil.IsCallerInRole, 285–286
 ContextUtil.IsSecurityEnabled, 286
 control+alt+delete, 359
 control flags, 193, 195
 countermeasures
 categorization of, 7–9
 determining appropriate, 11–12
 CreateMutex, 74
 CreateProcessAsUser, 153
 CreateProcessWithLogonW, 37, 147–149
 credentials. *See also* authentication
 daemon logons and, 137–138
 delegating, 316–320
 Kerberos, 302–303
 network, 39
 prompting for, 359–363
 protocol transition and, 321–324
 CredUIOptions.DoNotPersist, 363
 CredUIPromptForCredentials,)))361–363
 cross-domain authentication, 303–305
 cross-site scripting, 4–5
 cryptographic keys, 299
 cryptography, 8. *See also* encryption
 false security from, 9
 CryptoStream, 330–331
 csrss.exe, 143
 custom marshalers, 267

D

DACLs (discretionary access control lists), 185–186
 control of, 183–184
 default, 208–209
 gating access with, 197
 grants/denials in, 201–202
 inheritance and, 220–221
 order of, 220–221
 ownership and, 187–191
 permissions, 208–209
 in security descriptors, 193, 195
 taking object ownership and, 226–227
 user profiles and, 87
 viewing, 200–201

384 ■ INDEX

- daemons
 - characteristics of, 133
 - definition of, 133–135
 - dialog boxes and, 83, 134, 287–289
 - displaying user interfaces from, 141–144
 - identity selection for, 137–140
 - least privilege and, 18
 - logon sessions and, 78–79
 - machine stores with, 135
 - message boxes and, 143–144
 - passwords and, 99, 138–139
 - security context and, 70–71
 - service principal names and, 309–310
 - starting, 133–134
 - user profiles and, 88–89, 134–135
 - window stations and, 81–83
 - in WinSta0, 141–142
 - data files, recommended locations for, 42–44
 - data flow diagrams, 12
 - DataProtection class, 357–368
 - DCOM calls, 153–154
 - DCOM Config, 264–265, 271
 - debugging
 - interactive logon in, 287–289, 290
 - privileges for, 40–41
 - Default Domain Policy, 371
 - Default User, 85
 - defense in depth, 21–23
 - delegation, 315–320
 - configuring, 325–326
 - protocol transition and, 322–323
 - DELETE permission, 206–207
 - denial of service (DOS), 13, 14
 - deployment, 375–377
 - Authorization Manager, 237–238
 - no-touch, 46
 - xcopy, 46
 - 3DES, 346–347
 - desktop applications
 - ACL-based security in, 184
 - least privilege and, 18
 - security context and, 70
 - user profiles in, 87–88
 - detection, 7–9
 - developers
 - debugging privileges and, 40–41
 - installation tips for, 46
 - isolated storage and, 44–46
 - non-admin code development by, 35–46
 - as nonprivileged users, 31–33
 - writing code that is usable by non-admins, 42–44
 - dialog boxes, 83
 - daemons and, 83, 134, 287–289
 - message boxes and, 143–144
 - Diffie-Hellman key exchange, 347
 - discretionary access control lists. *See* DACLs
 - DLLHOST.EXE, 263
 - domain authorities
 - security principals and, 59
 - domain controllers, 8
 - domain credentials, 39, 309. *See also* authentication; service principal names (SPNs)
 - domain local groups, 92, 94
 - expanding, 96
 - domains, group expansion and, 95–98
 - domain trusts, 303–305
 - DPAPI (Data Protection API), 135, 352–355
 - DataProtection class and, 357–368
 - password persisting, 363
 - DuplicateTokenEx, 122
- ## E
- EditSD, 229–230, 233–234
 - Electronic Codebook mode (ECB), 295–296
 - elevation of privilege, 13, 14
 - elevation-of-privilege attacks, 27–29
 - employees, as security risks, 23
 - Encapsulating Security Payload (ESP), 343, 344
 - encryption, 293–294. *See also* Kerberos
 - ASP.NET configuration file, 356–357
 - block ciphers, 295–296
 - DPAPI, 135, 352–355
 - IPSEC and, 346–347
 - MACs and, 294–298
 - .NET remoting and, 340
 - password, 351
 - secret storage and, 351
 - sharing secrets and, 297–298
 - EnterpriseServices, 281–286
 - EOAC_APPID, 266
 - EOAC_DISABLE_AAA, 268
 - erasability, 355–356
 - ESP (Encapsulating Security Payload), 343, 344
 - Everyone, 171
 - guest logon and, 174
 - SID for, 62
 - Excel, 289–290
 - ExitWindowsEx, 367–368
 - Explorer
 - administrative tasks in, 38–39

isolated storage and, 45–46
 running programs as another user in,
 145–146
 SACL editing in, 51
 secondary logon service and, 37
 user profiles in, 85–86
 explorer.exe, 38

F

factoring out high-privileged code,
 139–140
 Ferguson, Niels, 343
 files
 auditing access to, 51–53
 recommended locations for, 42–44
 firewalls, 22–23
 Forms Authentication
 security context and, 71
 Thread.CurrentPrincipal and, 167

G

Generate Audits privilege, 251
 GetTokenInformation, 116, 123
 ghosting, SIDs and, 62
 Global Catalog (GC), 92–93, 324
 global groups, 91–93
 expanding, 95, 97
 gpedit.msc, 369
 gpupdate, 373
 group membership lists, 324
 group policy, 369–373
 adding objects to, 371–372
 audit settings in, 49
 privileges and, 111–112
 software deployment via, 375–377
 viewing, 370–371
 groups, 91–99
 application, 247–248
 definition of, 91
 domain local, 92, 94
 expanding, 94–98
 global, 91–93
 latency/authenticity and, 98–99
 local, 92, 93–94
 looking up, 118
 membership rules for, 96–97
 nesting, 93
 NTLM and, 98
 scoping, 97–98
 universal, 91–93
 Guest account, 173–174
 guest logon, 173–174

GUIDs, 61
 GUIs, code development and, 37–39

H

Hacking Exposed (McClure), 170
 hidden files in user profiles, 85–86
 HKEY_CURRENT_USER, 86–87
 daemons and, 134–135
 HKEY_USERS, 63, 85–86
 HMAC-SHA1, 347
 home directories, 85

I

IAzClientContext.AccessCheck, 237
 identification tokens, 323–324
 identifier authority, 62
 IDisposable, 106, 109
 iexplore.exe, 38
 IHttpAsyncHandler, 154
 IIdentity, 71–72, 115–118
 IIS 6
 CoInitializeSecurity, 278
 logon rights, 139
 null sessions and, 171
 registry settings and, 278
 worker processes, 134
 IIS, hosting in, 337–339
 IKE (Internet Key Exchange), 343
 ImpersonateAnonymousToken, 169–170,
 175–177
 impersonation
 of anonymous users, 177
 ApplicationAccessControlAttribute and,
 281–282
 ASP.NET, 154–155, 157–161, 277–279
 CoInitializeSecurity and, 255–258,
 271–273
 COM, 259–261, 271–273, 275–276
 configuring COM, 275–276
 dangers of, 152–155
 definition of, 151–155
 delegation and, 315–320
 of fixed identities, 160
 HKEY_CURRENT_USER and, 86
 implementation of, 153–155
 kernel handle closure and, 155
 least privilege and, 18–19
 nested, 159
 .NET remoting and, 340
 null session and, 169
 SSPI and, 331
 temporarily stopping, 160–161

386 ■ INDEX

impersonation (*continued*)
 thread switches and, 164
 token, 122
 undoing, 158–159
 with a user token, 157–161
 information disclosure, 13, 14
 inheritance
 ACL, 196, 211–223
 options, 212–214
 INHERIT_ONLY_ACE, 214
 InitializeClientContextFromStringSid, 245
 InitializeCOMSecurity, 272–273
 InitializeSecurityContext, 331
 input
 malformed, 23
 validating, 23
 installation, 46
 integrity, 293. *See also* CIA
 MACs and, 294–298
 .NET remoting and, 340
 SSPI and, 327–328
 integrity management systems, 8
 IntelliMirror, 375–377
 interactive logons, 129
 debugging and, 287–289
 interactive security editor, 225–228
 interactive services, dangers of, 141–142
 interactive window stations, 81–83
 Internet Key Exchange (IKE), 343
 Internet Security Association Key
 Management Protocol (ISAKMP), 343
 interop assembly, 242
 intrusion detection systems (IDSs), 8
 IPPrincipal, 71–72, 115–118
 IPSEC, 341–344
 connection options, 346–347
 enabling, 345–346
 using, 345–348
 IRemoteDispatch, 284
 ISAKMP (Internet Security Association Key
 Management Protocol), 343
 IsAuthenticated, 120
 IsInRole, 116–117
 in role-based security, 181–182
 Thread.CurrentPrincipal and, 167
 WindowsPrincipal creation and, 119–123
 Isolated Storage, 18
 IsSystem, 120
 IUSR_MACHINE, 160

J

JScript, 248–249

K

Kerberos, 299–308, 359
 cross-domain authentication, 94–96,
 303–305
 default authentication in, 26
 delegation and, 315–320
 groups in, 98–99
 IIS and, 338–339
 Internet and, 303
 key distribution in, 299–303
 key exchange, 297–298, 344
 mutual authentication in, 301–302
 .NET Remoting and, 339–340
 passwords in, 99
 protocol transition and, 321–324
 in role-based security, 181–182
 service principal names and, 311–313
 SSPI and, 331
 TGTs, 302–303
 tokens and, 75
 user-to-user authentication, 307–308
 kernel handles, closing, 155
 Key Distribution Center (KDC), 299–303
 keys
 auditing registry, 52, 53
 Diffie-Hellman protocol for, 347
 exchange protocols, 343–344
 in Kerberos, 297–303, 344
 master, 59, 60
 registry, 52, 53, 205, 206
 session, 299
 knowledge base article 322906, 39–40

L

latency
 groups and, 98–99
 in Kerberos tickets, 306
 privileges and, 112
 tickets and, 98–99
 LDAP query groups, 248
 least privilege, 17–19
 database connections, 4
 debugging and, 40–41
 developers and, 31–33
 stages of security compromise and, 17–18
 tradeoffs in, 11
 library applications, 275–276
 LoadUserProfile, 89
 local authorities, 59
 local groups, 92, 93–94
 expanding, 96
 NTLM and, 98

Locally Unique Identifiers (LUIDs), 106
 Local Security Authority (LSA), 59
 granting/revoking privileges via, 111–113
 Local Service logon session, 78, 79
 daemon identity and, 137–138, 140
 LocalUserAppDataPath, 44
 LockWorkstation, 365
 logging off, 367–368
 Logo Program for Windows
 code usable by non-admins and, 42–44
 least privilege and, 18
 logons, 77–80
 audit logs of, 47–49
 batch, 129
 built-in, 77–79
 for daemons, 137–140
 destruction of, 77
 guest, 173–174
 interactive, 129, 287–289
 LogonUser and, 126–129
 multiple, 35–46
 network, 129
 null, 79, 169–171
 privileges and, 105
 secondary logon service, 36–37
 service, 129
 service principal names and, 313
 Terminal Services and, 35–36
 types of, 128–129
 window stations and, 28, 81–83
 LogonUser, 126–129
 SSPI workaround with, 129–131
 logs, audit, 47–49
 LsaLogonUser, 126–127
 LUIDs (Locally Unique Identifiers), 106
 luring attacks, 27–29
 window stations and, 82–83

M

MAC, *see* message authentication codes
 machine.config, 263, 277, 337
 machine principals, 57–58, 60
 malicious user input
 logon sessions and, 79–80
 secure code and, 3–5
 mandatory access controls, 185–186
 marshalers, 284–285
 custom, 267
 master keys
 machine principals and, 60
 security principals and, 59

message authentication codes (MACs),
 294–298
 sharing secrets and, 297–298
 message boxes, 143–144
 MessageBoxOptions.DefaultDesktopOnly,
 143
 MessageBoxOptions.ServiceNotification,
 143
 Microsoft Next Generation Secure
 Computing Base (NGSCB), 8
 Microsoft Transaction Server (MTS), 235,
 317
 mitigation of risk, 15, 16
 MMC snap-ins
 Active Directory Users and Computers,
 59–60
 Component Services, 264–265
 security principal listing with, 59–60
 MSI files, 375–377
 multifactor authentication, 25–26
 multitier systems, 316–319
 mutual authentication, 26
 in Kerberos, 301–302
 service principal names and, 309–310,
 312–313
 SSPI and, 331

N

NegotiateStream, 130, 332–333
 SSPI and, 329–333
 nesting
 groups, 93
 impersonation, 159
 roles, 240–241
 NETBIOS names, 312
 .NET Framework
 code usable by non-admins and, 42–44
 COM security configuration and,
 263–264
 DataProtection class, 357–368
 DPAPI and, 353–355
 impersonation in, 159
 IPSEC and, 342–343
 Isolated Storage in, 18, 44–46
 least privilege and, 18–19
 persisting security descriptors in,
 233–234
 remoting with, 335–340
 role management in, 167
 security context and, 71–72
 security descriptors, 195–196
 SIDs in, 63

388 ■ INDEX

.NET Framework (*continued*)
 SSPI and, 335–340
 taking object ownership in, 227–228
 Thread.CurrentPrincipal in, 163–164
 tokens in, 73–74
 netmon.exe, 348
 .NET Remoting, 142, 335–340
 network logons, 129
 SSPI for, 129–131
 networks
 authentication in, 26
 credentials in, 39
 Network Service logon session, 78–79
 daemon identity and, 137–138, 140
 Next Generation Secure Computing Base (NGSCB), 8
 nonprivileged users, 31–33
 NO_PROPAGATE_INHERIT_ACE, 214
 no-touch deployment, 46
 NT Authority, 62
 NTLM protocol, 59
 delegation and, 315–316
 groups and, 98
 NTUSER.DAT, 85–86
 null session, 79, 169–171
 in COM, 257–258
 dangers of, 170
 limitations on, 170–171
 tokens, getting, 175–177

O

OBJECT_INHERIT_ACE, 214
 objects
 access control and, 185–186
 ownership of, 183–184, 187–191
 taking ownership of, 225–228
 OLE automation interfaces, 289–290
 ownership, 183–184, 187–191
 ACL, 202
 taking, 225–228
 transferring, 189–190

P

packet sniffing, 348
 paging, 355–356
 PasswordChar, 359
 Password Minder, 99, 307
 passwords, 25. *See also* authentication
 changing service account, 302–303
 collecting from console applications, 360–362
 daemons and, 99, 138–139
 echoing, 359–360

finding, 359–360
 getting user, 126–129
 groups and, 99
 guest logon, 173
 prompting for, 359–363
 for user-to-user authentication, 307
 peer-to-peer authentication, 307–308
 permissions, 205–209
 ACL, 199–200, 206–207
 auditing, 51–53
 CoInitializeSecurity and, 267
 ownership and, 189–190
 Take Ownership, 189–190
 taking object ownership and, 226–227
 for unauthenticated clients, 175–178
 Windows XP service pack 2 and, 269
 persistence
 ACL, 233–234
 password, 363
 security descriptor, 233–234
 pipes, service principal names and, 313
 Power Users, 46
 PrincipalPermissionAttribute, 167–168, 334
 prioritization
 damage and likelihood in, 15
 of threats, 14–15
 PrivilegePolicy, 113
 privileges, 101–104
 dangerous, 106
 enabling/disabling, 103–104, 106, 107–109
 granting/revoking via security policy, 111–113
 impersonation and, 152–155
 listing, 102–103
 in tokens, 74
 using, 103–104, 105–109
 when they take effect, 112
 processes
 displaying user interfaces from daemons, 141–144
 logon sessions and, 79–80
 security context and, 69–72
 Program Files, 42, 87
 programs, running as another user, 145–149
 protection, 7–9
 ProtectionLevel.EncryptAndSign, 332
 ProtectionLevel.Sign, 332
 protocol transition, 118, 321–324
 configuring, 323

R

reaction, 7–9
 READ_CONTROL permission, 189, 206–207
 read-only permission, 18
 rebooting, 367–368
 redundant security measures, 21–22
 refreshing settings, 373
 regedit, 38–39
 registry hives, 85–87
 registry keys
 auditing, 52, 53
 permissions for, 205, 206
 regsvcs.exe, 284–285
 remoting, .NET, 142, 335–340
 repudiation, 13
 ResetPrivileges, 106, 109
 resource domains, 95–96
 resource leaks, 155
 Revelation, 360
 RevertToSelf, 152
 RIDs (Relative IDs), 63
 risk management, 12. *See also* threat modeling
 acceptance in, 15–16
 mitigation in, 15, 16
 removing risk in, 15, 16
 response choices in, 15–16
 transferring risk in, 15, 16
 role-based security, 181–182
 Authorization Manager in, 235–252
 implementing for COM+, 281–286
 local groups in, 92, 93–94
 Thread.CurrentPrincipal and, 164, 165–168
 RSA, 11
 runas, 37
 checking installation with, 46
 running programs as another user with, 146

S

SACLs (system access control lists), 202–203
 audits and, 49, 51–53, 197
 editing, 51
 order in, 202–203
 in security descriptors, 193, 195, 201–202
 viewing, 203
 Saltzer, 17
 SAM (Security Accounts Manager), 59
 sandboxes, 28
 interactive services and, 141–142
 Schneier, Bruce, 7, 11, 26, 343
 scope, groups and, 97–98
 scripts
 Authorization Manager, 248–251
 SDDL (Security Descriptor Description Language), 229–230, 233–234
 SeAssignPrimaryTokenPrivilege, 137
 SeAuditPrivilege, 137
 SeBackupPrivilege, 371–372
 secedit/refreshpolicy machine_policy, 373
 SeChangeNotifyPrivilege, 104
 Secondary Logon Service, 36–37
 impersonation and, 153
 privileges and, 112
 secpol.msc, 48–49, 111
 secrets
 ASP.NET configuration file, 356–357
 DPAPI, 135, 352–355
 sharing in authentication, 297–298
 storing on machines, 351–358
Secrets and Lies (Schneier), 7, 16
 secure attention sequence, 359
 SecureMethodAttribute, 284
 SecureRoleAttribute, 284–285
 Secure Server policy, 345–346
 security
 audits in, 47–49
 developer understanding of, 31–33
 as process, 32–33
 protection, detection, reaction in, 7–9
 protocols, 341–344
 redundance in, 21–23
 secure code in, 3–5
 tradeoffs in, 11
 usability balance with, 8–9, 12, 29
 security account databases, 61
 Security Association (SA), 343–344
 security contexts, 69–72
 definition of, 69
 getting fresh, 70
 impersonation and, 158–159
 software deployment and, 376–377
 Security Descriptor Description Language (SDDL), 229–230, 233–234
 security descriptors, 187–189, 193–196
 access to, 200–201
 ACLs and, 211
 CoInitializeSecurity and, 266–267
 persisting, 233–234
 SecurityIdentifier, 113, 122
 security identifiers. *See* SIDs (security identifiers)

390 ■ INDEX

- security policy
 - auditing in, 52–53
 - delegation via, 325–326
 - granting/revoking privileges via, 111–113
 - IPSEC and, 345–346
- security principals, 57–60
 - authorities and, 58–59
 - listing, 59–60
 - machine, 57–58
 - service, 57–58
 - Thread.CurrentPrincipal and, 163–164
 - user, 57–58
- Security Support Provider Interface.
 - See* SSPI (Security Support Provider Interface)
- SE_DACL_PROTECTED, 195
- SeDebugPrivilege, 106
- SeImpersonatePrivilege, 101, 104
- server applications
 - ACL-based security in, 184
 - security context and, 70–71
- ServerAuthenticate, 331
- server process identities, 287–290
- server-to-server communication, 23
- Service Control Manager (SCM)
 - daemons and, 133–134
 - security context and, 70
- ServicedComponent, 281–286
- service logons, 129
- service principal names (SPNs), 131, 309–310
 - configuring, 311
 - .NET remoting and, 339–340
 - SSPI and, 331
 - structure of, 311–312
 - user-to-user authentication and, 308
 - using, 311–313
- service principals, 57–58
- SE_SACL_PROTECTED, 195
- SeSecurityPrivilege, 203
- SeShutdownPrivilege, 102, 368
- session keys, 299
- SeSystemtimePrivilege, 101
- SeTakeOwnershipPrivilege, 191
- SeTcbPrivilege, 323
- setspn.exe, 311, 333
- SetTokenInformation, 74
- SHA1, 346–347
- SHA-256, 296
- shatter attack, 142
- SIDs (security identifiers), 61–63
 - account names and, 113
 - ANONYMOUS LOGON, 169–170
 - Authenticated Users, 120, 170, 175
 - checking for in tokens, 122
 - group, 193, 194–195
 - guest logon, 174
 - owner, 187–189, 193, 194
 - programming with, 65–67
 - security context and, 69–72
 - in security descriptors, 193, 194–195
 - in tickets, 306
 - in tokens, 73
- sledgehammer checkbox, 223
- smartcards, 25–26. *See also* authentication
- SMB signing, 256
- Snort, 8
- SOAP formatter, 337
- social engineering, 16
- software deployment, 375–377
- Software Settings, 375–376
- SPNEGO protocol, 331
- spoofing, 13
- SQL Server
 - role-based security in, 182
 - service principal names and, 312
- SQL statements
 - injection vulnerability, 3–5
 - secure coding for, 3–5
- SSL, 293
 - mutual authentication in, 26
- SSPI (Security Support Provider Interface), 297–298, 327–328
 - LogonUser and, 129–131
 - socket-based apps and, 329–334
- STARTUPINFO, 82
- storage
 - authorization settings, 245–246
 - isolated, 44–46
 - of secrets on a machine, 351–358
- storeadm/list, 45–46
- STRIDE, 13–14
- SYNCHRONIZE permission, 206–207
- SYN-flood attacks, 8–9
- system access control lists. *See* SACLs (system access control lists)
- System.Diagnostics.Process, 79–80, 134
- System.EnterpriseServices, 281–286
- SYSTEM logon session, 78, 79
 - daemon identity and, 137–140
- System.Security.AccessControl, 230–231
- System.Threading.Timer, 164

T

Take Ownership, 189–190
 tampering, 13
 TCP channel, 339
 TCP stack, 8–9
 Terminal Services
 second logon via, 35–36
 TextMode=Password, 359
 Thread.CurrentPrincipal, 163–164, 334
 in role-based security, 181–182
 testing, 166–167
 tracking client identity with, 165–168
 WindowsIdentity and, 178
 ThreadPool.QueueUserWorkItem, 164
 threads
 attaching tokens to, 157–160
 impersonation and, 151
 permissions for, 205–206
 security context and, 69
 Thread.CurrentPrincipal and, 163–164
 threat modeling, 11–16
 attack trees in, 14–15
 data flow diagrams in, 12
 STRIDE acronym in, 13–14
Threat Modeling (Swiderski, Snyder), 16
 ticket-granting tickets (TGTs), 302–303, 304
 tickets
 group membership in, 95, 98–99
 Kerberos, 303–306
 latency / authenticity and, 98–99
 timestamps, 301
 tokens, 73–76
 checking for groups in, 122
 creating WindowsPrincipals from, 119–123
 default DACLs in, 208–209
 definition of, 73
 duplicating, 123
 expiration of, 74–75
 getting for users, 125–131
 identification, 323–324
 impersonation and, 153–155, 157–161
 logon sessions and, 77
 null session, 175–177
 passing between machines, 75–76
 primary, 122
 privileges and, 105–109
 propagating manually, 154–155
 protocol transition and, 323–324
 security context and, 69–70
 SIDs in, 61

WindowsIdentity and, 115–118
 WindowsPrincipal and, 119–123
 wrapping, 118, 119–123
 wrapping null session, 175–177
 transference of risk, 15, 16
 Tripwire, 8
 trust
 in Kerberos, 303–305
 transitive, 304–305
 trusted code, luring attacks and, 27–29
 trusted computing base (TCB), 137

U

Underwriters Laboratories, 8
 universal groups, 91–93
 expanding, 95, 96
 UNIX, access control in, 186
 untrusted code, luring attacks and, 27–29
 UPNs. *See* user principal names (UPNs)
 UserAppDataPath, 44
 User Configuration, 369–370. *See also* group policy
 Software Settings, 375–376
 user interfaces
 daemons and, 83
 displaying from daemons, 141–144
 user principal names (UPNs), 125–126
 protocol transition and, 321–324
 user principals, 57–58
 USERPROFILE, 87–88
 user profiles, 85–89
 All Users, 88
 daemons and, 88–89, 134–135
 users, nonprivileged, 31–33
 USS *Halibut*, 21
 UUIDs, 61

V

VBScript, 248–249
 Visual Studio.NET
 admin command prompt in, 39–40
 debugging in, 41
 programming SIDs in, 65, 66
 SSPI and, 329–333
 Web project creation in, 42
 VS Developers group, 42

W

web.config, 158, 335–337
 WellKnownSidType, 63, 122
 whoami, privilege listing with, 102–103

392 ■ INDEX

- Windows
 - access control in, 186
 - group types in, 91–92
 - Logo, 18
 - nonprivileged users in, 31–33
 - NT, 31–32
 - WindowsAccountType, 117
 - WindowsBuiltInRole, 117
 - Windows Forms
 - code usable by non-admins in, 43–44
 - COM security in, 273
 - WindowsIdentity, 72, 115–118
 - getting tokens for users in, 125–126
 - null session tokens and, 175–178
 - tokens in, 73–74
 - token wrapping and, 119
 - WindowsIdentity.GetAnonymous, 118
 - null session tokens and, 177–178
 - WindowsIdentity.GetCurrent, 118, 122
 - token propagation with, 154–155
 - WindowsIdentity.Impersonate, 154–155, 158
 - WindowsIdentity.Token, 116
 - WindowsImpersonationContext, 158–159
 - WindowsImpersonationContext.Undo, 161
 - WindowsPrincipal, 72, 115–118
 - creating, 119–123
 - in role-based security, 181–182
 - tokens in, 73–74
 - window stations, 28, 81–83
 - interactive, 81–83
 - Windows XP service pack 2, 268–269
 - Win32 functions
 - AdjustTokenPrivileges, 106–109
 - CheckTokenMembership, 122
 - CoInitializeSecurity, 263–269, 278–279
 - CreateProcessWithLogonW, 147–149
 - enabling/disabling privileges with, 104, 106, 107–109, 112–113
 - ExitWindowsEx, 367–368
 - ImpersonateAnonymousToken, 169–170
 - impersonation and, 152
 - LoadUserProfile, 89
 - LockWorkstation, 365
 - LogonUser, 126–129
 - programming ACLs with, 229–231
 - RevertToSelf, 152
 - running programs as another user with, 147–149
 - SetProcessWindowStation, 82
 - SetTokenInformation, 74
 - winnt.h, 208, 214
 - SIDs in, 63
 - WinSta0, 81–83
 - daemons in, 141–142
 - WMI (Windows Management Instrumentation), 9
 - World Authority, 62
 - WRITE_DAC, 189, 206–207
 - WRITE_OWNER, 189–190, 206–207
 - Writing Secure Code* (Howard, LeBlanc), 16
- X**
- xcaccls.exe, 217
 - X.509 certificates, 344
 - xcopy deployment, 46
 - XML files, authorization stores as, 245–246