

# Index

**Note to the Reader:** Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

## Symbols & Numbers

\$ (dollar sign), in hidden share names, 194  
802.11b protocol, 31

## A

- access control, **17–19**
  - encryption-based, **18–19**
  - permissions-based, **17–18**
- Access Control Entries (ACE), 179
  - creating new, 182
- access control lists, **215–216**
- access token, 176, 177
- accountability, 17
- Active Directory, **184, 185**
- Active IDS, 308
- ActiveX, 72
  - security proxies check for, 94–95
- Address Book, virus access to, 136
- adduser command (Unix), 210
- .ade file extension, 294
- Adelman, Leonard, 9
- ADMIN\$ share, 194
- administrative accounts, 7–8
- administrative shares, 194
- .adp file extension, 294
- adult hackers, underemployed, **26–27**
- advertising. *See* spam
- AH (Authenticated Headers), 108, 195
- AIX, 203
- alarm systems for security, 166
- algorithm, 46
  - asymmetric, 49
  - one-way functions, **47–49**
- AMaVIS, **289**
- America Online (AOL), 10, 295
- anonymous access, for Internet Information Server, 276
- anonymous FTP, 238
- anti-virus software, 134
- Apache web server, 3, 242, 253
  - configuration, 269
  - directory security, 270
  - encrypted passwords, 261
  - scripting security, 270–271
  - security of, 255
  - user-based security, 269–270
- Apple, 13
- AppleTalk, 110, 111
- application-layer proxy, 93–94
- applications
  - computer policies to control, 189
  - security, best practices, **70**
- appropriate use policy, **65–66**
- architecture probes, **34–35**
- archive marking, 155
- archiving, **164**
  - laptop files, **126**
  - policy, 148
- Asynchronous Transfer Mode (ATM), 112
- AT&T Bell Labs, 202, 203
- Athena project (MIT), 225
- attachments to e-mail, 65–66, 71, 136, **290–295**
  - allowing only specific, 291–292
  - quarantine, 138
  - stripping, 290
  - stripping dangerous, 292–295
- attacks, techniques, **35–41**
- audit trail, 308, 309
- auditing, 163
- auditors, **311–312**
- audits in Windows, 313–314
- Authenticated Headers (AH), 108, 195
- authentication, **15–16, 46, 51–57**. *See also* passwords
  - biometric, 16, **57, 166**
  - certificate-based, **55–57**
  - challenge/response, **52–53**
  - cryptographic, **106**
  - by firewall, 96
  - Kerberos, **185–188**

- public key, 55
- session, **54–55**
- auto-changers, 157
- automated security policy, **74–75**
- avalanche attack, 37
- asymmetric algorithms, 49

## B

- Back Orifice, 39
- backdoors, 15, 39
- background radiation, 308
- backups, **155–160**
  - vs. archiving, 164
  - best practices, **158–160**
  - of laptop files, **126**
  - methods, **155–156**
- bandwidth, 84
- .bas file extension, 294
- Basic authentication, for Internet Information Server, 276
- Basic Input/Output System (BIOS), 162
- .bat file extension, 38, 72, 292
- batteries in UPS, 160–161
- BBS (bulletin-board systems), 10
- benign viruses, 133
- best practices
  - backups, **158–160**
  - in security policy, **66–73**
    - application security, **70**
    - e-mail, **71–72**
    - office documents, **71**
    - for passwords, **67–70**
    - web browsing, **72–73**
  - virtual private network (VPN), **113–115**
- Bind (Unix), 32
- biometric authentication, 16, **57**, 166
- BIOS (Basic Input/Output System), 162
- black listing services, 300–302
- block devices, 208, 209
- blocking list of spammers, 301–302
- BO2K, 39
- booby traps, 247
- boot sector, 135
  - locking, 138
- boot sector viruses, **135**
- border gateways, 83. *See also* firewall
- border security, **84–85**
- bottlenecks, firewall as, 87
- brute-force attack, 51
  - challenge/response authentication to prevent, 53

- BSD (Berkeley Software Distribution) Unix, 13, 203, 204
- buffer overrun, 34, **39**
- bugs, 257
- bulletin-board systems (BBS), 10

## C

- C programming language, 202
- cable-DSL routers, 124
- cable modem networks, worms, 114
- caching options for share, 192
- call-back security, 9
- CardFlash, 125
- Carnegie-Mellon University, 5, 203
- cat command (Unix), 209
- catalogs, disk-based vs. media-based, 158
- CD-ROM drives, in Unix, 207
- CERT (Computer Emergency Response Team), 5
- certificate systems, 16, **55–57**
  - free personal, 284
  - in IPSec, 196
- CGI (Common Gateway Interface), **266–267**
- chain of authority, **16**
- challenge/response authentication, **52–53**
- Change share permission, 195
- character devices, 208
- Check Point Firewall-1, 85
- .chm file extension, 294
- chmod command, 215
- CIFS (Common Internet File System), 237
- ciphers, 5–7, 47
- circuit, 150
  - data loss from failure, 150
  - redundancy, 165
- circuit-layer switch, 89
  - SOCKS as, 95
- CIX (commercial Internet exchange), 107
- clear-channel tunneling, 105
- clients, virus protection, **141–142**
- clustered servers, **166–169**
- .cmd file extension, 38, 72, 292
- Code Red worm, 5, 123, 137
- coded messages. *See* encryption
- codes, 5–7
- .com file extension, 292
- combination, 166
- command files, restrictions on downloading, 292
- command shell (Unix), 134
- commercial Internet exchange (CIX), 107
- Common Gateway Interface (CGI), **266–267**
- Common Internet File System (CIFS), 237

- Communications Act of 1957, 202
  - Compaq Tru64, 203
  - CompuServe, 10
  - computer accounts, 175
  - Computer Emergency Response Team (CERT), 5
  - Computer Management snap-in, Shared Folders extension, 193
  - computer policy, in group policy object, 189
  - computer-related crime, 24
  - computers
    - appropriate use policy, **65–66**
    - boot sector, 135
    - first, 7
    - impact of virus scanning, 142
    - information storage, 132
    - security weaknesses, **2–4**
  - condensation, data loss from water damage, 153
  - confidential information, storing, 263
  - conflicting requirements, 63–64
  - connections for VPN, **123–125**
  - Contacts folder, virus access to, 136
  - content blocking, by firewall, 97–98
  - content signing, 72
  - copy backup, 156
  - copying files, and permissions, 257
  - Cornell University, “sidecar” project, 234
  - corporate spies, **28**
  - cost of downtime, 168
  - .cpl file extension, 294
  - crackz, 26
  - credentials, 231
  - crime, data loss from, **151–152**
  - criminal hackers, **27–28**
  - .crt file extension, 294
  - cryptographic authentication, **106**
  - cryptography, 50
  - cryptosystem, 46
  - Ctrl+Alt+Del keystroke, for logon, 178
  - customers, views on security, 3
- D**
- D-Link, 124
  - DACL (Discretionary Access Control List), 179, 181
  - daemons, **218–219**, 227
    - execute permission, 216
  - DARPA (Defense Advanced Research Projects Agency), 8
  - data, 132
    - loss by laptop theft, 121
    - protection and reliability, **125**
  - Data Encryption Standard (DES), 9
  - data gathering, 34. *See also* information gathering
  - data loss causes, **148–154**
    - crime, **151–152**
    - data circuit failure, 150
    - environmental events, **153–154**
    - hardware, **149**
    - human error, **148**
    - power failure, 150
    - software, 150
  - data payload encryption, **106**
  - DCE (Distributed Computing Environment), 234
  - decoys, **310–311**
  - dedicated leased lines, 106
  - dedicated web servers, 257–258
  - default settings for firewalls, 85–86
  - default shares, 194
  - Defense Advanced Research Projects Agency (DARPA), 8
  - delegation of authentication, 188
  - deleting groups in Unix, 212
  - Demarc PureSecure, 316
  - demilitarized zone, 85
    - snort sensor, 315
    - web server on, 262
  - Denial-of-service (DoS) attack, 27, **36**
  - deny ACE, 180
  - deployment testing, 150, 165
  - DES (Data Encryption Standard), 9
  - Desktop shortcuts, for directories, 193
  - /dev/cdrom directory (Unix), 207
  - dial-back security, 9
  - dial-up hacking, 30
  - dial-up modem bank, outsourcing, 110
  - differential backup, 156
  - Diffie, Whitfield, 9, 50
  - Digital Equipment, 8
  - digital signatures, 13, 55–57
    - for ActiveX controls, 72
  - Digital UNIX, 203
  - direct intrusion by hacker, **29–30**
  - directories
    - for Apache server, 270
    - share security, **191–195**
    - in Unix, 206, 207, 208
    - virtual, 274–275
  - directory security, in Apache web server, 270
  - directory service lookups, 35
  - Directory Services Agent (DSA), 178
  - Discretionary Access Control List (DACL), 179, 181

- disgruntled employees, **28**, 152
- disk packs, 162
- distributed logon, in Unix, **231–236**
- distributions of Linux, 205
- DNS (Domain Name Service), 32
- DNS lookup, 32
- dollar sign (\$), in hidden share names, 194
- domain controller, 174
- Domain Name Service (DNS), 32
- domains
  - group policies, 190
  - restrictions for web servers, 260–261
  - trust relationships between, 187
- DoS (Denial-of-service) attack, 27, **36**
- downloading scripts, 267
- downtime, cost of, 168
- DSA (Directory Services Agent), 178
- DSL networks, worms, 114
- due diligence, 123

## E

### e-mail

- attachments, 65–66, 71, 136, **290–295**
  - allowing only specific, 291–292
  - policy development, 65–66, 71
  - quarantine, 138
  - stripping, 290
  - stripping dangerous, 292–295
- best practices, **71–72**
- development, 11
- encryption and authentication, **282–285**
  - PGP, **284–285**
  - S/MIME, **283–284**
- foreign servers, **295**
- forged, 13, **37–38**, 71, **286**
- Postfix daemon, 247
- spam, **296–303**
  - SMTP authentication, **297–300**
  - systemic prevention, **300–303**
- unsigned, 38
- viruses, **287–289**. *See also* viruses

e-mail gateway, virus protection, **143**

earthquake, 154

EEPROM (Electrically Erasable Programmable Read-Only Memory), 125

eEye security, 266, 277

EFS (Encrypting File Service), **183**

EGRP (Exterior Gateway Routing Protocol), 164

electrical power failure, 150

emergency power generators, 160

employees, disgruntled, **28**, 152

- Encapsulating Security Payload (ESP), 108, 195
- encapsulation, IP, **104–105**, 105
- encrypted tunnels, 96. *See also* virtual private network (VPN)
- Encrypting File Service (EFS), **183**
- encryption, 13, **46–50**
  - data payload, **106**
  - of e-mail, **282–285**
  - early efforts, 9
  - file compression before, 114
  - hybrid cryptosystems, **50**
  - one-way functions, **47–49**
  - to protect stolen data, 125
  - public key, **49–50**
  - secret key vs. public key, **47**
  - X.509 certificate-based, 13
- encryption-based access control, **18–19**
- end user license agreement (EULA), 289
- enforceability of security policy, 64–65, 76
- enterprise
  - backup software, 159–160
  - firewall, 85
  - virus protection, **144**
- Entrust, 56
- environmental events, data loss from, **153–154**
- ESP (Encapsulating Security Payload), 108, 195
- /etc/exports file, 240
- /etc/ftpshosts file, 238
- /etc/group file, 212
- /etc/hosts.allow file, 247
- /etc/hosts.deny file, 247–248
- /etc/httpd.conf file, 242
- /etc/pam.d directory, 230
- /etc/passwd file, 209–220
- /etc/rhosts file, 226
- /etc/shadow file, 213
- /etc/smb.conf file, 243
- /etc/sysconfig/network file, 234
- EULA (end user license agreement), 289
- Everyone permission, 212, 214
  - Full Control, 182
- Excel documents, macro viruses, 2
- .exe file extension, 38, 72, 292
- executable code, 132
  - removing from web servers, 264
  - restrictions on downloading, 292
- executable files, user security context, 216
- executable viruses, 136
- Execute permission, 214
- execution environment, 70, 132
- Explorer (Windows), 134
- export for NFS, 240

Exterior Gateway Routing Protocol (EGRP), 164  
extranet server, IP address and domain  
restrictions for, 260

## F

fail-over clustering, 166–167  
FAT file system, 181  
  share creation, 192  
  share security, 195  
fault tolerance, **147–169**  
  causes for data loss, **148–154**  
    crime, **151–152**  
    data circuit failure, 150  
    environmental events, **153–154**  
    hardware, **149**  
    human error, **148**  
    power failure, 150  
    software, 150  
  measures, **155–170**  
    archiving, **164**  
    auditing, 163  
    backups, **155–160**. *see also* backups  
    circuit redundancy, 165  
    clustered servers, **166–169**  
    deployment testing, 165  
    offsite storage, 163–164  
    permissions, 163  
    physical security, **165–166**  
    power generators, 160–161  
    RAID (Redundant Array of Independent  
      Disks), **161–163**  
    uninterruptible power supplies, 160–161  
  file contents, in Unix, 208  
  file extensions, restrictions on downloading  
    files, 291–292  
  file service, load balancing, 169  
  file shares, 239  
  file sharing  
    protocols, 237  
    in Unix, **237–244**  
    in Windows, 191–192  
  file system object, in Unix, 206  
  File Transfer Protocol (FTP), **237–239**  
    packet-scrubbing proxy for, 248  
  files, 17  
    backups and archiving, **126**  
    compression before encryption, 114  
    corruption by virus, 139  
    synchronization, 164  
  filters to block spam, 302–303  
  find command (Unix), 218

Finder (Macintosh), 134  
Finger, 35  
fingerprint scanners, 57  
fire, data loss from, 153  
firewall, 4, 11, 13, 64, 83, **87–98**  
  border security principles, **84–85**  
  consistency in using, 85  
  content blocking, 97–98  
  default settings, 85–86  
  fundamental functions, **88–95**  
    network address translation (NAT), **90–93**  
    packet filtering, **88–90**, 89  
    proxy server, **93–95**, 94  
  importance for laptops, 123  
  and load balancing, 168  
  privacy services, **95–96**  
  selecting, **99**  
  in Unix, **245–249**  
  virus scanning, 97, 144  
  for VPN, 113  
Firewall Toolkit (FWTK), **248–249**  
flash memory, 125  
floods [data], **36–37**  
floods [water], data loss from, **153–154**  
floppy disks  
  for root access, 217  
  virus spread by, 133, 135  
foreign servers, **295**  
forged e-mail, 13, **37–38**, 71, **286**  
frame relay, 107  
FreeBSD, 203  
Friday the 13th virus, 133  
FTP (File Transfer Protocol), 11, **237–239**  
  application-layer proxy for, 93  
  disabling unused, 264  
  packet-scrubbing proxy for, 248  
  proxy software for, 95  
  security risks, **238–239**  
full backup, 156, 159  
Full Control share permission, 195  
FWTK (Firewall Toolkit), **248–249**

## G

Gates, Bill, on Internet, 12  
gateway virus scanners, **288**  
Gauntlet Firewall, 248  
General Electric, 202  
GNU foundation, 204  
Gopher, 11, 257  
grass-rooted trust system, 285

Group in Security Descriptor, 179  
group policies, 64, **188–191**  
groupadd command (Unix), 212  
groups in Unix, **212**

## H

habit, security as, 76  
hackers, 4, 23, 24  
    bulletin-board use, 10  
    home computers for network access, 120  
    network access, 29, **29–31**  
    restricting international, 260  
    types, **25–28**  
hacking, 4, 9  
    common occurrences, 5  
    data loss from, 151  
    techniques, **32–41**  
        attacks, **35–41**  
        information gathering, **34–35**  
        target selection, **32–34**  
    what it is, **24**  
hard disk drives, failure, 149  
hard links (Unix), 207  
hardware  
    data loss from, **149**  
    tape devices, **157**  
        problems, **157–158**  
hardware interrupt, Ctrl+Alt+Del keystroke as, 178  
hashes, **47–49**  
    for passwords, **52**  
hate groups, blocking access to sites, 97  
Hellman, Martin, 9, 50  
hijacking session, **40–41**  
history of security, **5–14**, 6  
    to 1945, 5–7  
    1945 to 1955, 7  
    1955 to 1965, 7  
    1965 to 1975, 7–8  
    1975 to 1985, 8–10  
    1985 to 1995, 10–11  
    1995 to 2005, 11–13  
    2005 to future, 13–14  
history of viruses, **133–134**  
HKEY\_Current\_User registry component, 190  
HKEY\_Local\_Machine registry component, 189–190  
.hlp file extension, 294  
home computers  
    as corporate network weakness, 114–115  
    firewall devices for, **124–125**

    hackers' use of, 120  
    VPN software client, 123–124  
/home directory (Unix), 207  
honey pots, 247, **310–311**  
HP-UX, 203  
.hta file extension, 293  
HTML application, restrictions on downloading, 293  
HTTP (HyperText Transfer Protocol), **241–244**  
    application-layer proxy for, 93  
    packet-scrubbing proxy for, 248  
    proxy software for, 95  
HTTP WebDAV (Web Distributed Authoring and Versioning), 242  
HTTPS, 258. *See also* SSL (Secure Socket Layer)  
hubs, UPSs for, 160  
human error, data loss from, **148**  
human security, **75–77**  
hybrid cryptosystems, **50**  
HyperText, 11  
HyperText Transfer Protocol (HTTP). *See* HTTP (HyperText Transfer Protocol)

## I

I/O port, 208  
ICMP  
    filter to check for redirection, 88  
    invalid packets, 36  
identity, proof of, 51  
ideological hackers, **27**  
IGRP (Interior Gateway Routing Protocol), 164  
IIS. *See* Internet Information Server (IIS)  
IKE (Internet Key Exchange), 109  
image backup, 156  
IMAP (Internet Mail Access Protocol), 295  
immunity of Windows NT to viruses, **139**  
incremental backup, 156, 158  
.inf file extension, 294  
information gathering, techniques, **34–35**  
information hiding, 86  
inherit, 182  
inheriting permissions, 182  
inoculators, 140  
    on clients, 142  
inodes, 207, **208–209**  
inspectors, **308–310**  
Intel, 9  
Intel microcomputers, Xenix for, 203  
intellectual property, 27  
Interior Gateway Routing Protocol (IGRP), 164  
internal DNS servers, 32

- internal hosts, NAT to hide, 91–92
  - international keyboards, 70
  - Internet Connector License, 271–272
  - Internet Explorer
    - encrypted passwords, 261
    - and Gopher, 257
    - transmission of account name and password hash, 53, 73
  - Internet, hacker use, **30–31**
  - Internet Information Server (IIS), 3, 253
    - vs. Apache server, 268
    - avoiding user authentication, 275–276
    - buffer overrun, 277
    - buffer-overrun attacks, 39
    - configuration, 272–274, 273
    - encrypted passwords, 261
    - NTFS permissions, 277
    - security of, 255
    - security proxy, 277
    - virtual directories, 274–275
    - worm propagation, 114
  - Internet Key Exchange (IKE), 109
  - Internet Mail Access Protocol (IMAP), 295
  - Internet Security and Acceleration Server (Microsoft), 277
  - Internet service providers, 11
    - SMTP port blocking by, 303
    - for VPN, 113
  - internetwork, 11
  - Internetwork Packet Exchange (IPX), 110, 111
  - InterNIC, 91
  - interpreters, 132, 133
  - intranet servers, virtual private network (VPN) for, 259–260
  - intrusion detection system, **308–312**
    - auditors, **311–312**
    - available systems, **313–316**
      - Demarc PureSecure, 316
      - NFR Network Intrusion Detector, 317
      - Snort, 314–316
      - Tripwire, 314
      - Windows reports, **313–314**
    - decoys, **310–311**
    - inspectors, **308–310**
  - IP address
    - restrictions for web servers, 260
    - single for network, 90
  - IP encapsulation, **104–105**, 105
  - IP spoofing, filter to check for, 88
  - IPC\$ share, 194
  - IPChains, **245–246**
  - IPSec, **108–110**, 115, **195–197**
  - IPTables, **245–246**
  - IPX (Internetwork Packet Exchange), 110, 111
    - .isp file extension, 294
    - IUSR\_COMPUTERNAME user account, 275
- ## J
- Java, 70, 72
    - security proxies check for, 94–95
  - JavaScript, restrictions on downloading, 293
    - .js file extension, 72, 293
    - .jse file extension, 293
- ## K
- kerberized service, 235
  - Kerberos
    - authentication, **185–188**
      - and IPSec, 196
      - development, 225
      - and Unix, **233–236**
  - Key Distribution Center (KDC), 185, 234
  - key ring, 284
  - keyboards, international, 70
  - keys, 16
  - kinit program (Unix), 234–235
  - Konquerer, 261
- ## L
- L2TP (Layer 2 Tunneling Protocol), **110**
  - LAN (local area networks), 106, 226
    - vs. VPN, 107
  - laptops, **120–121**
    - theft, 121
  - Layer 2 Tunneling Protocol (L2TP), **110**
  - LDAP (Lightweight Directory Access Protocol), 35, 229
  - leased lines, dedicated, 106
  - lessons learned, 76–77
  - licensing, for Internet Information Server, 271–272
  - Lightweight Directory Access Protocol (LDAP), 35, 229
  - links to documents, in e-mail, 71
  - Linksys, 124
  - Linux, 13
    - access control list support, 216
    - history, 204
  - .lnk file extension, 293
  - load balancing, **167–168**

- local administrator account, 175
- local area networks (LAN), 106, 226
  - vs. VPN, 107
- local group policy, 190
- Local Security Authority (LSA), 175, 176
- local security in Windows, **174–183**
  - Encrypting File Service, **183**
  - logging in, **176–177**, 177
  - NTFS file system permissions, **181–182**
  - objects and permissions, **179–181**
  - resource access, **177–178**
  - security identifiers, **175–176**
- Locally Unique Identifier (LUID), 176
- LocalSystem account (Windows), 211
- lockdown tools, 265
- lockout, after incorrect password, 69
- locks on doors, 165–166
- logging in, **176–177**, 177
  - forcing for sensitive data on website, 261–262
- mandatory, **178**
  - as root, 211
  - in Unix, 206
    - distributed, **231–236**
    - remote, **226–227**
- logon prompt, 174
- ls command (Unix), 208–209
- LSA (Local Security Authority), 175
- LUID (Locally Unique Identifier), 176

## M

- Mac OS X, 13
  - BSD Unix and, 204
- Mach micro-kernel, 203
- Macintosh
  - Finder, 134
  - as web server, 255
- macro viruses, 2, 71, **136**, 138
- macros, 70, 132
- Mail Abuse Prevention System (MAPS), **300–302**
- Mail Exchange (MX) records, 291
- mail forgery, **286**
- mainframe, 7
- malignant viruses, 133
- man-in-the-middle attacks, **41**
- mandatory logons, **178**
- Mandrake, 205
- manual secret keys, in IPSec, 196
- mapping drive to share, 193
- MAPS (Mail Abuse Prevention System), **300–302**
- Massachusetts Institute of Technology (MIT), 185, 202
  - Athena project, 225
- McCool, Rob, 271
- .mda file extension, 294
- .mdb file extension, 294
- .mde file extension, 294
- .mdz file extension, 294
- Mean Time Between Failures (MTBF), 149
- member servers, local administrator account on, 175
- Memory Stick, 125
- message routing, 9
- Microsoft. *See also* Internet Explorer; Internet Information Server (IIS)
  - Internet Security and Acceleration Server, 277
  - .NET Passport, 14
  - Office applications, and virus spread, 71, 136, 288
  - patches to web server, 254
  - rush to market, 12
  - and security risks, 2–3
  - Syskey utility, 125
  - Xenix, 203
- Microsoft Outlook
  - danger of, 71
  - scripting language, 2
  - viruses, 136, **287–288**
- MIME (Multipurpose Internet Mail Extensions), 290
- minicomputers, 8
- mirroring, **161**
- MIT (Massachusetts Institute of Technology), 185, 202
  - Athena project, 225
- modem banks, 11
  - dial-up, outsourcing, 110
- modems, 8, 30
- modulus, 48
- Moore's law, 3
- mount command (Unix), 207, 240
- mounting partition in Unix, **206–207**
- moving files, and permissions, 257
- Mozilla, and encrypted passwords, 261
- .msc file extension, 294
- .msi file extension, 293
- .msp file extension, 293
- .mst file extension, 293, 294
- MTBF (Mean Time Between Failures), 149
- Multics, 8, 201, 202
- MultiMedia card, 125

Multipurpose Internet Mail Extensions (MIME), 290  
MX (Mail Exchange) records, 291  
My Network Places, 193  
MySQL, 219

## N

NAI Gauntlet Firewall, 99  
name, of root account, 211  
NAT (network address translation), **90–93**  
    routers, 124  
National Center for Supercomputing Applications, 268  
.NET service, 13  
NetBEUI, 110, 111  
NetBIOS, 38  
    session port, 264  
NetBSD, 203  
NetBus, 39  
netcat, 39  
NETGEAR, 124  
Netscape Navigator, 73  
    and encrypted passwords, 261  
network access  
    by hackers, 29, **29–31**  
    with stolen laptop, 121  
network address scanning, 32–33  
network address translation (NAT), **90–93**  
    and IPSec Authenticated Headers, 109  
network-based authentication of e-mail, 298  
Network File System (NFS), 38, 224, **239–241**  
network file systems, 237  
Network Information Service (NIS), **231–233**  
Network Neighborhood, 193  
network security in Windows, **184–197**  
    Active Directory, **184, 185**  
    group policies, **188–191**  
    IPSec, **195–197**  
    Kerberos authentication, **185–188**  
    share security, **191–195**  
networked PCs, 10  
networks, eliminating virus infection, 140  
New Technology LAN Manager (NTLM), 176  
newgrp command (Unix), 212  
NFR Network Intrusion Detector, 317  
NFS (Network File System), 38, 224, **239–241**  
Nimda worm, 5, 120, 137, 265  
NIS+, 232  
NIS (Network Information Service), 224, **231–233**  
    master server setup, 233  
NNTP, disabling unused, 264  
No Access permission, 181  
Norton AntiVirus for Enterprises (Symantec), 144  
Norton Personal Firewall and ZoneAlarm (Symantec), 123  
Novell  
    patches to web server, 254  
    Unix, 203  
NTBACKUP.EXE (Windows), 155  
NTFS file system  
    permissions, **181–182**  
        for web security, 277  
    share creation, 192  
    and viruses, 139  
NTFS permissions, in Internet Information Server (IIS), 277  
NTLM (New Technology LAN Manager), 176

## O

objects, 178  
    and permissions, **179–181**  
Office documents  
    best practices, 71  
    macro viruses, 136  
offline, 151  
offline caching, 192  
offsite storage, 163–164  
one-time passwords, 227  
one-way functions, **47–49**  
    for passwords, 52  
online, 162  
Open Relay Blocking System (ORBS), 302  
open relay servers, 296  
open source, 112  
Open Source community, 13  
OpenBSD, 4, 203  
Opera, and encrypted passwords, 261  
operating systems. *See also* Unix; Windows operating system  
    absence of diversity, 3  
    archive marking support, 155  
    computer policies to control, 189  
    early connections, 111  
    hacker determination of, 34  
    Linux, 13, 204, 216  
    OpenBSD, 4  
    research, 8  
    and security policy implementation, 74  
    for VPN, 113  
ORBS (Open Relay Blocking System), 302  
organizational unit, group policies, 191

- outline of policy requirements, **63–66**
- Outlook Web Access, 299
- outsourcing
  - dial-up modem bank, 110
  - offsite storage, 163–164
- owner
  - of process, 206
  - of Unix file object, permissions, 214
- Owner in Security Descriptor, 179

## P

- packet-based networks, 8, 54
- packet filtering, **88–90, 89**
  - IPChains and IPTables for, **245–246**
  - for VPN, 113–114
- packets
  - collecting, 35
  - IP encapsulation, **104–105**
- Pakistani Brain virus, 133
- PAM (pluggable authentication modules), **229–230**
- PAMed, 236
- parent process, 182
- partitions, mounting in Unix, **206–207**
- pass phrase, 57
- passive IDS, 308
- passwd command (Unix), 210
- passwd file, distributed, 231
- passwords, **51–53**
  - automated guessing, **38**
  - best practices, **67–70**
  - for FTP, 239
  - hackers' cracking of, 67–68
  - hashing, 49, 52
  - Internet Explorer sharing of, 53
  - management, **69–70**
  - for new accounts, 68
  - one-time, 227
  - as security weakness, 2
  - shadow in Unix, **213**
- patches, 4
  - maintaining, 265–266
- PC computers, growth, 10
- pcAnywhere, 39
- .pcd file extension, 294
- PCMCIA card, 125
- Peer Web Services, 272
- periodic backup, 156
- Perl, 267, 294
- permissions, 64, 163, 178, 179
  - NTFS file system, **181–182**
  - rights vs., 181
  - for share, 195
  - in Unix, 212
    - changing, 215
- permissions-based access control, **17–18**
- personal firewall applications, 123
- PGP (Pretty Good Privacy), 283, **284–285**
- phone numbers, war-dialing, 9
- PHP, 267
- physical security, 30, **165–166**
- pi, and pseudorandom numbers, 54–55
- .pif file extension, 72, 292
- Ping of Death, 36
- pipes, 208, 209
- PKI (Public Key Infrastructure) systems, 18–19
- pluggable authentication modules (PAM), **229–230**
- Point-to-Point Protocol (PPP), 110, **111**
  - securing, 112
- Point-to-Point Tunneling Protocol (PPTP), **110–111**
- policy, 62
  - on laptop backups, 126
- political purpose of hacking, 27
- POP before SMTP authentication, **299–300**
- POP3 (Post Office Protocol, version 3), 295
- pornography, blocking, 97
- port scanning, to monitor remote computers, 122
- portmap, for NFS, 240
- ports, 33
  - blocking, 67
  - scanning, 33
- Post Office Protocol, version 3 (POP3), 295
- Postfix daemon, 297
- Postfix e-mail daemon, 247
- power failure, data loss from, 150
- power generators, 160–161
- PPP (Point-to-Point Protocol), 110, **111**
  - securing, 112
- PPP/SSH, **111–112**
- PPP/SSL, **111–112**
- PPTP (Point-to-Point Tunneling Protocol), **110–111**
- Pretty Good Privacy (PGP), 283
- PRINT\$ share, 194
- privacy services, by firewall, **95–96**
- private key, 18
- PRNG (pseudorandom number generator), 54
- probe, 34
- process, 174
- program information files, restrictions on
  - downloading, 292
- program links, restrictions on downloading, 293

programmers, 3  
 programming. *See* ActiveX; Java; Visual Basic  
 propagation engine, 133  
 propagation of virus, 133, **134–135**, 135  
 proprietary secrets, loss by laptop theft, 121  
 protocols, 4  
     for file sharing, 237  
     FTP (File Transfer Protocol), **237–239**  
     HTTP (HyperText Transfer Protocol), **241–244**  
     Internet Key Exchange (IKE), 109–110  
     L2TP support for interior, 110  
     network address translation (NAT) and, 92  
     proxies for, 95  
     Samba, **243–244**  
     stateless, 167  
 proxy server, 88, **93–95**, 94  
 pseudorandom number generator (PRNG), 54  
 public key authentication, 55  
 public key encryption, 47, **49–50**, 282  
     for VPN, 114  
 Public Key Infrastructure (PKI) systems, 18–19  
 Python, 267

## Q

qmail, 297

## R

RAID (Redundant Array of Independent Disks),  
     **161–163**  
 RAIT (Redundant Arrays of Independent Tapes),  
     157  
 Read share permission, 195, 214  
 realms in Kerberos, 187, 234  
 red flag, 312  
 Red Hat distribution, 205  
     NIS server on, 234  
     .reg file extension, 293  
 registry, 175  
     HKEY\_Current\_User component, 190  
     HKEY\_Local\_Machine component, 189–190  
     restrictions on downloading files, 293  
 relay server, 291  
 remote access, 227  
     protecting remote machines, 122, **122–126**.  
         *See also* virtual private network (VPN)  
         backups and archiving, **125**  
         data protection and reliability, **125**  
         VPN connections, **123–125**

        protection against, **127**  
         security, 114  
             laptops, **120–121**  
             virtual private holes, **120**  
         in Unix, **228–230**  
 Remote Access Server, 30  
 remote login, in Unix, **226–227**  
 removable media, 149  
 replay attack, 51  
     challenge/response authentication to  
         prevent, 52  
 resource access, **177–178**  
 restoration of backup files, 156  
 reverse proxies, for web services, 258–259  
 Ritchie, Dennis, 202  
 Rivest, Ron, 9  
 rlogin service, 226  
     packet-scrubbing proxy for, 248  
 root account in Unix, **210–211**  
     daemons requiring, 219  
     permissions, 214  
 Root Certifying Authority (Root CA), 56  
 root of Unix file system, 206  
 routers, UPSs for, 160  
 RPC Portmapper service, 247  
 rpc.mountd daemon, 240  
 rpc.nfsd daemon, 240  
 RSA encryption algorithm, 9  
 rsh, 226  
 rule base, 99

## S

S/MIME (Secure Multipurpose Internet Mail  
     Extensions), 283  
 SA (Security Associations), 109  
 sabotage, 152  
 SACL (System Access Control List), 179, 181  
 SAM (Security Accounts Manager), 175  
 Samba, **243–244**  
 sandbox environment, 72  
 Santa Cruz Operation (SCO), 203  
 scan, 32  
     of ports, 33  
     of services, 33–34  
     .scr file extension, 72, 292  
 ScramDisk, 125  
 screen saver, restrictions on downloading, 292  
 script kiddie, **25–26**  
 scripting hosts, 132, 133  
 scripting language, for Microsoft Outlook, 2  
 scripting security, in Apache web server, 270–271

- scripts, **266–267**
  - location on web server, 262
- .sct file extension, 294
- secret key, 46
- secret key encryption, **47**
- Secure Digital card, 125
- Secure Multipurpose Internet Mail Extensions (S/MIME), 283
- Secure Shell (SSH), 111, **112**, 127, 226
- Secure Socket Layer (SSL), 104, 111, **112**
  - for web services, 258
- secure space, 166
- SecureIIS, 266, 277
- security, 1
  - concepts, **15–19**
    - access control, 17–19
    - accountability, 17
    - authentication, **15–16**
    - chain of authority, **16**
    - trust, **15**
  - history, **5–14**, 6
    - to 1945, 5–7
    - 1945 to 1955, 7
    - 1955 to 1965, 7
    - 1965 to 1975, 7–8
    - 1975 to 1985, 8–10
    - 1985 to 1995, 10–11
    - 1995 to 2005, 11–13
    - 2005 to future, 13–14
- Security Accounts Manager (SAM), 175
- Security Associations (SA), 109
- Security Descriptor of object, 179
- security domain, 234
- security experts as hackers, **25**
- Security Group, 174
- security identifiers, **175–176**
- Security Identifiers (SIDs), **175–176**
- security policy, 61
  - development, **62–73**
    - appropriate use policy, **65–66**
    - best practices, **66–73**
    - requirements outline, **63–66**
  - implementation, **74–77**
    - automated policy application, **74–75**
    - human security, **75–77**
  - updates, **78–79**
- security proxy, in Internet Information Server (IIS), 277
- seduction servers, 247
- seed number, 54
- selecting firewall, **99**
- self-replication, 131, 132
- Sendmail, 282
- sensors for Snort, 315
- sequence number for packets, 54
- Server Message Block (SMB) protocol, 237, 243
- server replication, 166
- Server service (Windows), 263
- server-side scripting, 266–267
- ServerRoot directory for Apache server, 270
- servers
  - clustered, **166–169**
    - fail-over clustering, 166–167
    - load balancing, **167–168**
    - protection against worms, 137
    - as proxies, 94
    - redundancy, **168–169**
    - virus protection, **142–143**
    - web-based managers, **267–268**
- services
  - execute permission, 216
  - scanning, 33–34
- session authentication, **54–55**
- session hijacking, **40–41**
- session ticket in Kerberos, 186
- setgid flag, 216–217
  - monitoring system for programs, 218
- setuid flag, 216–217
  - monitoring system for programs, 218
  - security problems, 217
  - shell scripts, **217–218**
- shadow passwords
  - and NIS, 233
  - in Unix, **213**
- Shamir, Adi, 9
- share security, **191–195**
  - vs. file security, 194–195
- shares, 243
- Sharing Properties dialog box, 192
- shell, 136, 210, 227
  - setting to load as root, 217
- shell scripts, as SetUID programs, **217–218**
- .shs file extension, 294
- shutdown script, computer policies to control, 189
- SIDs (Security Identifiers), **175–176**
- signatures of viruses, 139
- Simple Mail Transfer Protocol (SMTP), 227
  - application-layer proxy for, 93
  - packet-scrubbing proxy for, 248
  - port blocking by ISP, 303
- Simple Network Management Protocol (SNMP), data gathering, 34
- single signon, 231

site, group policies, 190  
 smart cards, 15, 228, 229  
 Smart Media, 125  
 SMB over TCP/IP  
   for password checking, 67  
   port, 264  
 SMB (Server Message Block) protocol, 237, 243  
 SMTP (Simple Mail Transfer Protocol), 227, 282  
   application-layer proxy for, 93  
   authentication, **297–300**  
   disabling unused, 264  
   packet-scrubbing proxy for, 248  
   port blocking by ISP, 303  
 sniffing, 35, 52  
 SNMP (Simple Network Management Protocol),  
   data gathering, 34  
 Snort, 314–316  
 sockets, 208, 209  
 SOCKS, 95  
 software  
   data loss from, 150  
   firewall applications, **123–124**  
   open source, 112  
   security features, 2  
 Solaris, 203  
   access control list support, 216  
 SonicWall Firewalls, 99, 124  
 Sony, 159  
 source routing, **40, 88**  
   NAT and, 92  
 spam, 227, **296–303**  
   SMTP authentication, **297–300**  
   systemic prevention, **300–303**  
 Spam Prevention Early Warning System  
   (SPEWS), 302  
 spies, corporate, **28**  
 Squirrel Mail, 299  
 SSH (Secure Shell), 111, **112**, 127, 226  
 SSL (Secure Socket Layer), 104, 111, **112**  
   for web services, 258  
 Stampede, 205  
 startup scripts, computer policies to control, 189  
 stateful inspection, IPTables for, 245  
 stateful inspection packet filters, 89  
 stateless packet filters, 89  
   IPChains for, 245  
 stateless protocols, 167  
 steganography, 7  
 Stoned virus, 133  
 Storm, 205  
 striping, **161**  
 striping with mirroring, **162–163**

striping with parity, **162**  
 su (set user) command (Unix), 211  
 Sun Microsystems, 203  
 SuSe, 205  
 Symantec  
   AntiVirus, 288  
   Norton AntiVirus for Enterprises, 144  
   Norton Personal Firewall and ZoneAlarm, 123  
   VelociRaptor Security Device, 99  
 symmetrical algorithm, 46  
 SYN flood, 36–37  
 synchronization of files, 164  
 system, 64  
 System Access Control List (SACL), 179, 181  
 system initialization, computer policies applied  
   at, 189  
 SYSVOL\$ share, 194  
 SysVol share, group policy objects in, 189

## T

T1 leased lines, 107  
 taint (Perl), 270–271  
 tape hardware, **157**  
   problems, **157–158**  
 TapeRAID, 157  
 tar tool (Unix), 155  
 target selection, techniques, **32–34**  
 TCP connection, initiating, 89  
 TCP/IP, 84  
   NAT implementation, 91–92  
   source routing, **40**  
 TCP Wrappers, 240, **245–248**  
 tcpd daemon, 247  
 teaching security principles, **77**  
 Telnet, 226  
   packet-scrubbing proxy for, 248  
   proxy software for, 95  
   SSH and, 112  
 Terminal Services (Windows), 127  
 terminals, 226  
 terrorism, 152  
 TGT (Ticket-Granting-Ticket), 186, 235  
 Thawte, 56, 284  
 theft, 151–152  
   of laptops, 121  
 Thompson, Ken, 202  
 Ticket-Granting-Ticket (TGT), 186–187, 235  
 ticket in Kerberos, 186  
 time synchronization, and Kerberos, 235  
 TIS (Trusted Information Systems), 248  
 TiVo, 204

- TLDs (Top Level Domain Names), 260–261
- Top Level Domain Names (TLDs), 260–261
- Torvalds, Linus, 204, 205
- transmitting messages, 6
- transparent proxies, 94
- transport mode for IPsec, 109
- Trend Micro, 143
- Tripwire, 314
- Trojan horse, 37, **38–39**, 72, 290
- trust, **15**, 224
- trust provider, 16
- trust relationships between domains, 187
- Trusted Information Systems (TIS), 248
- tunnel mode for IPsec, 109
- tunneling, 84
  - clear-channel, 105
  - encrypted, 96. *See also* virtual private network (VPN)
- TurboLinux, 205

## U

- UID (User Identifier), 210
  - for root account, 211
- underemployed adult hackers, **26–27**
- uninterruptible power supplies (UPS), 160–161
- Unix, 3, 8, 201
  - Bind, 32
  - command shell, 134
  - disabling unused web services, 264
  - file system security, **214–219**
    - access control lists, **215–216**
    - execution permissions, **216–219**
  - hackers' concentration on, 12
  - history, **202–205**
  - inodes, 207, **208–209**
  - network security
    - basics, **224–225**
    - distributed logon, **231–236**
    - file sharing, **237–244**
    - firewall, **245–249**
    - remote access, **228–230**
    - remote login, **226–227**
  - PPTP implementation, 111
  - security basics, **206–213**
    - file systems, **206–209**
    - user accounts, **209–213**
  - tar tool, 155
  - vs. UNIX, 202
- unsigned e-mail, 38
- UPS (uninterruptible power supplies), 160–161
- .url file extension, 294

- URLs, decoding, 259
- USB Flash memory, 125, 126
- use requirements, 62
- user accounts, 7–8, 15, 174
  - Internet Explorer sharing of, 53
  - in Kerberos, 236
  - passwords, 51
    - for new accounts, 68
  - in Unix, **209–213**
- user authentication, avoiding in Internet Information Server (IIS), 275–276
- user-based security, in Apache web server, 269–270
- user context, 227
- User directive for Apache server, 269
- User Identifier (UID), 210
  - for root account, 211
- user policy, 190
  - in group policy object, 189
- user rights, 181
- userdel command (Unix), 210
- users
  - policies on website access, 97–98
  - security policy for, 65–66
  - as security weakness, **75–77**

## V

- VA Linux, 205
- /var directory (Unix), 207
- /var/yp/securenets file, 234
- .vb file extension, 72, 293
- .vbe file extension, 293
- .vbs file extension, 293
- vendor, problem hiding by, 3
- Venema, Wietse, 247
- VeriSign, 56, 284
- video surveillance, 165
- virtual directories, in Internet Information Server (IIS), 274–275
- virtual host, 269
- virtual intrusion detection host system, 311
- virtual private network (VPN), 34, 96, **103–115**
  - basics, **104–106**
    - cryptographic authentication, **106**
    - data payload encryption, **106**
    - IP encapsulation, **104–105**, 105
  - best practices, **113–115**
  - characteristics, **107**
  - connections, **123–125**
  - determining need for, 127
  - implementations, **108–112**

- IPSec, **108–110**
- L2TP, **110**
- PPP/SSL or PPP/SSH, **111–112**
- PPTP, **110–111**
- for intranet servers, **259–260**
- security holes, **120**
- software client, **123–124**
- virus hoaxes, **287**
- virus scanners, **139–140**
  - on clients, **142**
  - firewall and, **97**
  - subscription services, **141**
- viruses, **2, 5, 287–289**
  - AMaViS, **289**
  - basics, **132–137**
  - benign, **133**
  - damage from, **131**
  - gateway virus scanners, **288**
  - history, **133–134**
  - laptop infection by, **120**
  - malignant, **133**
  - operation, **133**
  - for Outlook, **287–288**
  - propagation, **133, 134–135, 135**
  - protection against, **138–140**
    - implementation, **141–144**
  - types, **135–137**
- Visual Basic, **71**
- Visual Basic script, restrictions on downloading, **293**
- VMS, **8**
- VMware, **311**
- VNC, **39**
- voiceprint recognition, **57**
- volumes, share security, **191–195**
- VPN (virtual private network). *See* virtual private network (VPN)

## W

- WAN (wide area networks), **106**
  - vs. VPN, **107**
- WAPs (Wireless Access Points), **31**
- war-dialing, **9**
- WatchGuard, **99, 124**
- water damage, data loss from, **153–154**
- web browsing
  - best practices, **72–73**
  - and encrypted passwords, **261**
- web e-mail interface, **298–299**
- web enabled applications, **258**
- web of trust, **285**

- web server security, **253**
  - Apache web server, **268–271**
    - directory security, **270**
    - scripting security, **270–271**
    - user-based security, **269–270**
  - implementations, **255–271**
    - bugs, **257**
    - centralizing risky content, **262**
    - CGI and scripts, **266–267**
    - connections to private network, **262**
    - data sensitivity, **262–263**
    - dedicated servers, **257–258**
    - demilitarized zone, **262**
    - domain restrictions, **260–261**
    - extranet server, **260**
    - installing minimum, **254, 263–264**
    - lockdown tools, **265**
    - patches, **265–266**
    - reverse proxies, **258–259**
    - SSL (Secure Socket Layer), **258**
    - user logon, **261–262**
    - VPN for intranet, **259–260**
      - Web-based server managers, **267–268**
  - Internet Information Server (IIS), **271–277**
    - avoiding user authentication, **275–276**
    - NTFS permissions, **277**
    - security proxy, **277**
    - virtual directories, **274–275**
  - problems, **254**
- web servers, **3**
  - configuring in Unix, **242**
  - redundancy, **168**
  - stateless clustering, **168**
- WebObjects (Apple server), **255**
- websites
  - for ASCII table, **259**
  - on Kerberos, **233**
  - for open-source web e-mail interfaces, **299**
  - for SSH (Secure Shell), **227**
- WEP (Wired Equivalent Privacy), **31**
- wheel group, **213**
- Whois, **35**
- wide area networks (WAN), **106**
  - vs. VPN, **107**
- Windows Active Directory, **32**
- Windows authentication, for Internet Information Server, **276**
- Windows operating system, **2, 3**
  - 2000
    - Encrypting File Service, **125**
    - group policy manager, **75**
    - ports opened, **264**

- administrative accounts, 69
- disabling unused web services, 264
- domain model vs. NIS, 232
- Explorer, 134
- hackers' concentration on, 12
- local security, **174–183**
  - Encrypting File Service, **183**
  - logging in, **176–177**, 177
  - NTFS file system permissions, **181–182**
  - objects and permissions, **179–181**
  - resource access, **177–178**
  - security identifiers, **175–176**
- network security, **184–197**
  - Active Directory, **184**, 185
  - group policies, **188–191**
  - IPSec, **195–197**
  - Kerberos authentication, **185–188**
  - share security, **191–195**
- NT-based, immunity to viruses, **139**
- NTBACKUP.EXE, 155
- security, 173
- security problems, 214
- servers on Internet, ports to block, 67
- version 95/98/ME, 174
- Windows Terminal Services, 127
- WinLogon process, 175, 176
  - and access token, 177–178
- Wired Equivalent Privacy (WEP), 31
- Wireless Access Points (WAPs), 31
- wireless hacking, 31
- wiretapping, sniffing as, 35
- Word documents, macro viruses, 2, 132
- word processing, and virus spread, 71
- workstations, 8
  - and backups, 159
  - local administrator account on, 175
- world, 215
- World Wide Web, 11
- World Wide Web consortium, web server recommendations, 255
- worms, 5, 33, 114, 135, **137**
- write access, to anonymous FTP server, 239
- Write permission, 214
- .wsc file extension, 294
- .wsf file extension, 294
- .wsh file extension, 294
- WU-FTP, 254
  - security flaw, 238

## X

- X.509 certificate-based encryption, 13
- Xenix, 203

## Y

- Yellow Dog, 205
- yellow pages, 231
- ypserv, 233