

Index

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

Symbols and Numbers

\$ (dollar sign), for hidden shares, lab, 519
3DES (Triple-DES), 324
8.3 file naming, 204–205
802.11 protocol, 135
802.16 standard, 135
2600: *The Hacker Quarterly*, 452

A

ABA (American Bankers Association), 345
acceptable use policy, 409, 433, 439, 465, 466
access control, 262–270, 379, 415
 common methods, 445–446
 in cryptographic systems, 330–331
 implementation, 14–15
 for information, 295–299
 location of computers, 274–277
 partitioning, 267–268, 269
 perimeter security, 265, 265–266
 physical barriers, 263–268
 security zones, 266–267
 three-layer security model, 263
 troubleshooting, 471
access control list (ACL), 14, 240, 259, 445, 466
 changing on all files in Linux directory, lab, 515
 to control spam, 242
access control models
 Bell La-Padula model, 296, 296
 Biba model, 297, 297
 Clark-Wilson model, 297–298, 298
 Information Flow model, 298, 298–299
 Noninterference model, 299, 299
account database in Windows XP, encryption, lab, 535–536
accountability, 49
 as topology design goal, 24–25
 accountability statement, in policy, 285–286
accounts
 changing default names, 129
 expiration, 445
ACL. *See* access control list (ACL)
active/active model, 402
active backup model, 402
Active Directory (AD), 231, 248, 417, 417
active sniffing, 76
ActiveX, vulnerabilities of, 141
activity, 181
AD. *See* Active Directory (AD)
Adams, Carlisle, 324
AdAware, 80
Address Resolution Protocol (ARP), 67, 72
Adleman, Leonard, 325
administrative auditing, 420–421
administrative policies, 9
administrative requirements, in standards, 287
administrative shares, in Windows systems, 236
administrator, 181
 user accounts with access as, lab, 512–513
Adobe Reader, 547
Advanced Encryption Standard (AES), 324
adware, 80
AES (Advanced Encryption Standard), 324
AES256, 324
AFS (Apple File Sharing), 236
AH (Authentication Header), 356
alarm systems, 5
ALE (annual loss expectancy), 283
alert, 181
algorithms
 attacking, 342
 errors, for code breaking, 320
American Bankers Association (ABA), 345
analyzer, 181
annual loss expectancy (ALE), 283
annualized rate of occurrence (ARO), 283
anomaly-detection IDS, 183–184, 184

- anonymity, on Internet, 26
- anonymous authentication, in WAP, 130
- anonymous logon, to FTP site, 145, 243
- anti-antiviruses, 104
- antiquated protocols, 67
- antivirus software, 13–14, 83, 89–90, 196, 490
 - definition database files for, 90
 - log files, 421–422
 - retrovirus attack of, 85
 - troubleshooting, 492–493
- APIPA (Automatic Private IP Addressing), 247
- AppArmor
 - configuring in openSUSE, lab, 525–526
 - viewing reports, lab, 526
- Apple File Sharing (AFS), 236
- Apple Macintosh, hardening, 233–234
- Apple protocol, 178
- AppleTalk, 178, 236
- appliances, 113
 - firewalls as, 239
- Application layer, 66–67
- application-level proxy functions, 117
- Application Programming Interface (API), 72
- applications
 - backup plan for, 396
 - design requirements, 10–11
 - exploitation, 78–80
 - hardening, 240–250
 - DHCP services, 246
 - DNS servers, 243–244
 - e-mail servers, 241–242
 - file and print servers, 245–246
 - FTP servers, 242–243
 - NNTP servers, 244–245
 - web servers, 240–241
 - removing unneeded, 501–502
 - types, 546
 - updates, 450
 - upgrades to new versions, timing of, 493
 - users installing unauthorized, 130
- apropos utility, 180
- archive, 440
- archive bit, 397
- archiving
 - keys, 365, 365–366
 - media for, 170
- armored virus, 83, 104
- ARO (annualized rate of occurrence), 283
- Art of Deception: Controlling the Human Element of Security* (Mitnick), 271
- assets identification, 34, 49
- asymmetric algorithms, 324–326, 325, 379
- at service, 295
- AT&T Wireless, Network Operations Center (NOC), 112
- attachments to e-mail, 484
 - common file extensions, 80–81
- attack strategies, 53–58
 - access attacks, 54–55
 - exam essentials, 95–97
 - modification attacks, 55–56
 - recognizing, 58–63
 - backdoor attacks, 59, 59, 63, 104, 491
 - man-in-the-middle attacks, 60–62, 61, 104, 202, 491
 - password-guessing attacks, 62–63, 105
 - privilege escalation, 63, 416
 - replay attacks, 62, 62, 104, 491
 - spoofing attacks, 60, 61, 491
 - repudiation attacks, 56
 - responding to, 64
 - review questions, 100–105
- attacks, 470
 - frequency of, 222
 - through NetBIOS services, 245
- attributes, for Unix file or directory, 235
- audit, 287, 434
- audit files, 93
 - for database transactions, 395, 395
- audit logs, 473
- auditing, 414, 418–422
 - administrative auditing, 420–421
 - escalation auditing, 420
 - and log files, 421–422
 - privilege auditing, 419
 - processes, 93–94
 - reporting to management, 422
 - usage auditing, 419
- auditors, 295
- authentication, 15–20, 48
 - biometrics, 15, 48, 270, 308, 474
 - certificates, 16, 16. *See also* certificates
 - Challenge Handshake Authentication Protocol (CHAP), 16, 17, 132

- in cryptographic systems, 329–330
- issues, 21–22
- Kerberos, 17, 18, 48
 - SSO and, 417
 - time synchronization for, 361
- multi-factor, 17, 18, 22, 48, 415
- mutual, 19
- Password Authentication Protocol (PAP), 19
 - for remote user, 132
 - security tokens, 19, 19
 - smart cards, 20, 20, 159, 170, 474
 - individuals forgetting, 367
 - for keys, 362
 - username/password, 20, 21
 - in WAP, 130
- authentication factors, 473–474
- Authentication Header (AH), 356
- authentication protection, 475–476
- Automated System Recovery, in Windows Server 2003, lab, 427
- Automatic Private IP Addressing (APIPA), 247
- availability, as topology design goal, 24

B

- Back Orifice, 59
- backdoor attacks, 59, 59, 63, 104, 491
- background investigations, 410
- BackTrack, 207
- backup plan, 394–396
 - developing, 397–400
- backup policy, 465
 - drafting and documentation, 440
- backup power, 276
- Backup Server method, 399, 400
- backups
 - for disaster recovery, 391–394
 - media, 170
 - recovery, 400–401, 401
 - security for, 55, 392
 - in SuSE Linux, lab, 428
 - troubleshooting management, 476
 - types, 396–397
- baseband signaling
 - vs. broadband, 150
 - coaxial cable support for, 149

- baselines, 259
 - for Internet access, lab, 511
 - for security, 222–224
 - troubleshooting, 476–477
 - standards, 287
- basic input/output (BIOS) chip, 438
- .bat file extension, 80, 204
- BCP. *See* Business Continuity Planning (BCP)
- behavior-based baseline for IDS, 183
- Bell La-Padula model of information access, 296, 296, 309
- benchmarking, 287
- best practices, 411, 465
 - defining responsibility, 443
 - drafting and documentation, 436–443
 - backup policy, 440
 - change documentation, 441–442
 - configuration management policies, 440
 - information classification policies, 437
 - information destruction policies, 438–439
 - information retention and storage policies, 437
 - logs and inventories, 440
 - notification policies, 437
 - security policies, 439
 - system architecture, 441
 - use policies, 439–440
 - user management, 442
 - minimizing mistakes, 443
 - policy and procedure enforcement, 443
 - resource allocation, 442–443
- beta test software, 291
- BIA (Business Impact Analysis), 281–282
- Biba model of information access, 297, 297
- bindery services, in NetWare, 175
- binding, 225–226, 226, 259
- biometrics, 15, 48, 270, 308, 474
- BIOS (basic input/output) chip, 438
- birthday attack, 342–343, 380
- Bitlocker, 228, 259
- black lists, 491
- blind/anonymous FTP, 145
- block cipher, 323
- Blowfish encryption system, 324
- blue jacking, 202
- bluesnarfing, 202
- Bluetooth, 202

BNC connectors, 149

bootable CD, 506

bootable portable operating system, 496

booting to good Windows configuration, lab, 537

botnet, 57

bounced e-mails, log report of, 195

bridge trust models for PKI, 339–340, 340

bridges, 73

broadband signaling
vs. baseband, 150
coaxial cable support for, 149

broadcasts, 118, 147
in IM systems, 203

brute-force attack, 63, 493
for code breaking, 320–321

budget, for security, 442

buffer overflow, 57, 204
vulnerabilities of, 141

Business Continuity Planning (BCP), 281–284, 383–403
disaster recovery plans (DRPs), 9, 391–403, 433
backups, 391–394
creating, 394–403
planning for alternate sites, 401–403
testing, 420
troubleshooting, 482

high availability, 385–386
fault tolerance, 387–388
formulating, 385
RAID, 388–391
redundancy, 386
testing, 420
troubleshooting, 482
utilities, 384
vendor support reinforcement, 404–406
code escrow agreements, 406
service-level agreement (SLA), 404–405

Business Impact Analysis (BIA), 281–282

business partner, creating corporate connection to, 34

business policies, 410–412
document disposal and destruction policies, 411–412
due care policies, 411
physical access control policies, 411
separation of duties, 410–411

C

CA. *See* certificate authorities (CA)

cabling
coaxial, 148, 148–150
fiber-optic technology, 152–153
unshielded (UTP) and shielded twisted pair (STP), 150–152, 151

cache in web browser, clearing, lab, 530–531

CALEA (Communications Assistance for Law Enforcement Act of 1994), 503

callback security, 480

caller ID verification, 480

Canonical Name (CN), 248

carrier, victim system as, 86

CAST algorithm, 324

Category 5 cable standard, 152

CC (Common Criteria), 222–224, 357

CCITT (Comité Consultatif International Téléphonique et Télégraphique), 347

CD-R/DVD-R, 157

CD-RW, 157

CEH (Certified Ethical Hacker), 489

cell phones, 155, 156, 272–274, 273
acceptable use policies on, 439–440

Center for Education and Research in Information Assurance and Security (CERIAS), 451

centralization, of network monitoring, 112

centralized key generation, 359, 360

CERIAS (Center for Education and Research in Information Assurance and Security), 451

CERT/CC Current Activity web page, 87

CERT Coordination Center (CERT/CC), 221–222, 451

CERT organization, 87

CertCities, 452

certificate authorities (CA), 16, 330, 379
designing, 340
in hierarchical trust model, 337, 338

Certificate Management Protocol (CMP), 351

certificate policies, 412–413, 433

Certificate Practice Statement (CPS), 16, 413

Certificate Revocation List (CRL), 16, 336–337

certificates, 16, 16
implementing, 335–336
management, troubleshooting, 477–478

- certification programs, 448
- Certified Ethical Hacker (CEH), 489
- CGI (Common Gateway Interface), 241
 - vulnerabilities of, 141–142
- chain of custody, 37, 193
- Challenge Handshake Authentication Protocol (CHAP), 16, 17, 48, 132
- change documentation, 465
 - drafting and documentation, 441–442
- change management, 421
- checksums, 190, 317
- chgrp command, 518
- chip creep, 276
- chmod utility, lab, 515–516
- CIO, 452
- cipher, 314
- cipher command, lab, 528
- cipherng, 314
- circuit-level proxy, 117
- Cisco
 - IP Telephony Security in Dept white paper, 39
 - Switched Port Analyzer (SPAN), 185
- Cisco Certified Internetwork Expert (CCIE) certification, 239
- Clark-Wilson model of information access, 297–298, 298
- classified information model, 296
- classifying information
 - classifying, 290, 290–299
 - full distribution information, 292
 - government and military, 293–294
 - internal information, 292
 - limited distribution information, 291–292
 - private information, 292
 - public information, 290–291
 - restricted information, 292
- client, 71
- Clipper, 363
- clustering, for fail-over capabilities, 386, 387
- CMOS (complimentary metal oxide semiconductor), 438
- CMP (Certificate Management Protocol), 351
- CN (Canonical Name), 248
- code escrow agreements, 406, 433
- Code Red attack, 57
- code words, 330
- cold site, 402–403
- collusion, 410
- .com file extension, 80, 204
- Comité Consultatif International Téléphonique et Télégraphique (CCITT), 347
- Common Criteria (CC) standards, 222–224, 357
- Common Gateway Interface (CGI), 241
 - vulnerabilities of, 141–142
- communications
 - of security issues, 447
 - troubleshooting security, 478–481
- Communications Assistance for Law Enforcement Act of 1994 (CALEA), 503
- companion CD, 546–548
 - system requirements, 547
 - troubleshooting, 548
 - using, 547
- companion virus, 84
- compartmentalization, 409
- complimentary metal oxide semiconductor (CMOS), 438
- CompTIA Security+ certification, 468
- computer battery, 465
- computer crime, state laws on, 454
- Computer Fraud and Abuse Act, 455
- Computer Management console, 513
- Computer Professionals for Social Responsibility (CPSR), 408
- Computer Security Act of 1987, 456
- Computer Security Incident Response Team (CSIRT), 414
- Computer Security Institute, 451
- computer startup in Windows XP
 - adding legal notice, lab, 532–533
 - configuration, lab, 533, 534
- confidential data classification, 10
- confidentiality
 - in cryptographic systems, 326–327
 - of information, 293, 411
 - as topology design goal, 23
- configuration settings
 - group policies to lock, 129
 - management policies, 465
 - drafting and documentation, 440
- connection
 - filtering for remote access, 479
 - Initial Sequence Number (ISN) for, 71

contingency plan, 434. *See also* Business Continuity Planning (BCP)

Control Panel (Vista), Security applet, 228

cookies

- limiting to first party, lab, 531–532
- vulnerabilities of, 142
- in web browser, clearing, lab, 530–531

core dump, to obtain key, 362

Counterpane Systems, 324

counters, in System Monitor, 229

CPS (Certificate Practice Statement), 413

CPSR (Computer Professionals for Social Responsibility), 408

cracking systems, 37

credit card numbers

- encryption for, 351–352, 352
- transmission of information, 353

criminal investigation, 486

critical business functions (CBF), 281, 308

- identifying and prioritizing, 281–282

CRL (Certificate Revocation List), 16, 336–337

cross certification, 336, 338

cross-site scripting (XSS), vulnerabilities of, 142

cryptanalysts, 313

cryptographers, 313

cryptographic algorithms, 321–326

cryptographic systems

- access control, 330–331
- attacks, 341–343
- authentication, 329–330
- confidentiality, 326–327
- digital signature, 328, 328–329
- integrity, 327, 327
- nonrepudiation, 330

cryptography, 313–321

- exam essentials, 370–372
- mathematical, 316–317
- myth of unbreakable codes, 319–321
- physical, 314–316
 - hybrid systems, 316
 - steganography, 316
 - substitution ciphers, 314
 - transposition ciphers, 315, 316
- public domain, 347
- quantum, 318–319, 320
- review questions, 374–380

- SSL (Secure Sockets Layer), 349–350, 350
- standards, 343–358
 - origins, 344–347
- CSIRT (Computer Security Incident Response Team), 414
- CSO Magazine*, 453
- current keys, in archiving system, 365
- custodian of data, 294
- customer care from Wiley, 548
- Cyber Security Enhancement Act, 456
- Cybercrime Treaty, 457
- Cyberspace Electronic Security Act (CESA), 456

D

DAC (Discretionary Access Control) method, 14–15, 423, 434

Daemen, Joan, 324

data assets, assigning value to, 35

data breaches, chronology of, 443

data classification matrix, 10

data depositories, 246–249

data emanation, radio frequency signals for, 201

Data Encryption Standard (DES), 323–324

data source, 181

data storage. *See* removable media

database transactions, audit files for, 395, 395

databases, 249–250

- exploitation, 78–79

date-stamp, and user file backup, 395

DDoS (distributed denial-of-service) attacks, 57, 58

decentralized key generation, 360, 360

default account names, changing, 129

default password, changing, 113

default permissions, for new files in Linux, lab, 516

definition database files, for antivirus software, 90

degaussing, 438

deleting files, 438

demilitarized zones (DMZ), 28, 29, 49

demo versions of software, 546

- denial-of-service (DoS) attacks, 56–57, 104, 146, 203, 243, 491
 - and NetWare, 233
 - DES (Data Encryption Standard), 323–324
 - desensitizing, 277
 - destination port, 137
 - destroying keys, 367
 - detection, as information security goal, 13
 - DHCP (Dynamic Host Configuration Protocol), 246
 - troubleshooting, 247
 - dial-up, troubleshooting security, 480
 - dictionary attack, 63, 493
 - differential backup, 397, 433
 - Diffie-Hellman key exchange, 325–326
 - digital signature, 412
 - in cryptographic systems, 328, 328–329
 - direct-sequence spread spectrum (DSSS), 199–200
 - directory services, 246–248, 247
 - troubleshooting, 481–482
 - disaster recovery plans (DRPs), 9, 391–403, 433
 - backups, 391–394
 - creating, 394–403
 - planning for alternate sites, 401–403
 - testing, 420
 - troubleshooting, 482
 - Discretionary Access Control (DAC) model, 14–15, 423, 434
 - disk duplexing, 388
 - disk mirroring, 388
 - disk striping, 388, 389
 - disk striping with parity, 389, 389
 - disk striping with parity disk, 388
 - disk wiping, 438, 465
 - diskettes, 157
 - Distinguished Name (DN), 248
 - distributed denial-of-service (DDoS) attacks, 57, 58
 - distributing keys, 361–362
 - DMZ (demilitarized zones), 28, 29, 49
 - DN (Distinguished Name), 248
 - DNA scanners, 15
 - DNS (Domain Name Service), 66, 259, 421
 - hardening servers, 243–244
 - DNS poisoning, 60
 - DNS spoofing, 60
 - .doc file extension, 80
 - documentation. *See also* best practices, drafting and documentation
 - for alternative sites, 403
 - disposal and destruction policies, 411–412
 - troubleshooting, 483
 - dollar sign (\$), for hidden shares, lab, 519
 - Domain Name Kiting, 60
 - Domain Name Service (DNS). *See* DNS (Domain Name Service)
 - domain password policy, 446, 466
 - DoS (denial-of-service) attacks, 56–57, 104, 146, 203, 243, 491
 - and NetWare, 233
 - draft documents, 345
 - DSSS (direct-sequence spread spectrum), 199–200
 - dual-homed firewall, 116, 116, 117
 - dual sided certificates, 336
 - due care policies, 411, 433
 - due diligence, 420
 - dumpster diving, 54
 - duplexing, 388
 - DVD-R, 157
 - Dynamic Host Configuration Protocol (DHCP), 246
 - troubleshooting, 247
-
- E**
- e-mail incident, 195
 - e-mail servers, hardening, 241–242
 - e-mails
 - attachments, 484
 - common extensions for, 80–81
 - encrypting, 351
 - exploitation, 79
 - troubleshooting, 483–484
 - and virus spread, 83, 84
 - viruses in, 38
 - EALs (Evaluation Assurance Levels), 223
 - EAP (Extensible Authentication Protocol), 357
 - eavesdropping, 54
 - eBay, nonrepudiation and, 331
 - EC Council, 489

- ECC (Elliptic Curve Cryptography), 274, 326
 - EDGAR (business research website), 206
 - eDirectory, 176, 233, 249
 - education
 - to prevent virus spread, 90
 - on security issues, 447–448
 - against social engineering, 92, 272
 - El Gamal algorithm, 326
 - electromagnetic interference (EMI), 277, 278, 308
 - electronic flashcards, 547
 - electronic wallet, 351
 - electronic watermarking, 316
 - Elliptic Curve Cryptography (ECC), 274, 326
 - EMI (electromagnetic interference), 277, 278, 308
 - employees. *See also* users
 - knowledge of security policies, 8–9
 - and privacy expectations, 409
 - transfers and access rights, 11
 - Encapsulating Security Payload (ESP), 356
 - encapsulation, 68, 69
 - encryption, 93. *See also* cryptography
 - asymmetric algorithms, 324–326, 325
 - authentication, 475
 - of folders with cipher, lab, 528
 - in Linux, lab, 373–374
 - origins of standards, 344–347
 - symmetric algorithms, 323–324
 - weakest link, 322
 - of Windows account database, lab, 535–536
 - of Windows file, lab, 519
 - end-entity certificate, 348
 - End User License Agreements (EULAs), 291
 - and selling old computers, 438
 - enticement, 192
 - entrapment, 192, 217
 - environment, scanning, 272–280
 - erasing files, on computer system, 438
 - escalation, 194
 - escalation auditing, 420
 - ESP (Encapsulating Security Payload), 356
 - ethical hacking, 489
 - ethics policies, 408
 - EULAs (End User License Agreements), 291
 - and selling old computers, 438
 - European Institute for Computer Anti-Virus Research, 451
 - European Union (EU), cyber laws, 457
 - Evaluation Assurance Levels (EALs), 223
 - evaluation versions of software, 546
 - Event Viewer, 231, 231
 - Security Log object, 421
 - events, 181
 - as incident, 193
 - locating in Windows XP, lab, 512
 - exam essentials
 - attack strategies, 95–97
 - cryptography, 370–372
 - hardening, 252
 - information security, 40–42
 - infrastructure, 162–163
 - intrusion detection systems (IDSs), 208–209
 - physical security, 301–302
 - policies and procedures, 425–426
 - security management, 458
 - exception statement, in policy, 286
 - .exe file extension, 80, 204
 - expiration of key, 363–364
 - extended warranty agreement, 405
 - Extensible Authentication Protocol (EAP), 357
 - Extensible Markup Language (XML), 81, 140
 - external security threats, 36, 36, 37
 - extranets, 28, 28
 - extrusion, 26
-
- F**
- fail-over, 386, 433
 - failed login attempts, viewing in Linux, lab, 518
 - faillog utility, 191, 518
 - false positives, 194, 497
 - from IDSs, 194
 - Family Education Rights and Privacy Act, 455–456
 - Faraday cage, 277
 - FAT (File Allocation Table), 234, 259
 - fault tolerance, 387–388
 - Federal Information Processing Standard (FIPS), 357
 - Fedora, SELinux configuration in, lab, 531
 - FHSS (frequency-hopping spread spectrum), 199, 200

- fiber-optic technology, 152–153
 - networks, 170
 - fiber splitter, 153
 - File Allocation Table (FAT), 234, 259
 - file exchange systems, 483
 - file extensions, 204
 - and attacks, 80
 - hiding, 205
 - making visible in Windows XP, lab, 211
 - file names, 8.3 convention, 204–205
 - file servers, hardening, 245–246
 - file sharing
 - in FTP, 145
 - troubleshooting, 484–485
 - file structure, in Unix, 232
 - File Transfer Protocol (FTP), 66, 144–146, 230
 - hardening servers, 242–243
 - ports, 115
 - security risks, 354
 - files, disappearance of, 82
 - files in Linux
 - changing access control list, lab, 515
 - changing group, lab, 517–518
 - changing permissions, lab, 515–516
 - default permissions for new, lab, 516
 - hiding, lab, 518–519
 - files in Windows
 - displaying Security tab for, lab, 520
 - encryption, lab, 519
 - viewing effective permissions, lab, 521
 - filesystems, hardening, 234–236
 - filters, to limit web traffic, 241
 - Financial Modernization Act, 454
 - fingerprint reader, 270, 474
 - FIPS (Federal Information Processing Standard), 357
 - fire corridors, 268
 - fire detectors, 275
 - fire extinguishers, 279, 308
 - fire-rated storage, 393–394
 - fire suppression, 279–280
 - Firefox, 225
 - clearing private data, lab, 531
 - firewalls, 93, 113–117, 114, 180
 - configuring, 239–240
 - for DMZ, 28
 - and IDS, 128, 128
 - IDS location based on, 184
 - log files, 421
 - NAT as, 32
 - packet filter, 114–115
 - proxy, 116, 116–117
 - stateful inspection, 117–118
 - in Windows XP, lab, 509–511, 510, 511
 - firmware, 113
 - first-party cookies, lab, 531–532
 - first responders, 194
 - FISK program, 438
 - five nines availability, 385
 - fixed systems for fire suppression, 279–280
 - Flash, 140
 - flash cards, 158
 - flaw-exploitation DoS attacks, 491
 - flood attack, IDS active response to, 187, 187
 - flooding channel, 203
 - floppy disks, 157
 - Folder Options dialog box (Windows), View tab, 520, 520
 - folders
 - encryption with cipher, lab, 528
 - preventing sharing, lab, 523
 - footprinting, 206, 217, 243–244
 - forensics, 192
 - fraud, 412
 - freeware, 546
 - frequencies, 272
 - frequency analysis, for code breaking, 320
 - frequency-hopping spread spectrum (FHSS), 199, 200
 - FTP (File Transfer Protocol), 66, 144–146, 230
 - hardening servers, 242–243
 - ports, 115
 - security risks, 354
 - Full Archival backup method, 398–399, 399
 - full backup, 396
 - full distribution information, 292
-
- G**
- gap in the WAP, 198, 200, 503
 - gas-based fire-suppression systems, 280, 308
 - GET command (FTP), 145

- Global Information Assurance Certification (GIAC), 489
 - Global System for Mobile Communications (GSM), 274, 308
 - GNU software, 546
 - goals, of information security, 12–13
 - Good Time virus, 87
 - Googlebot, 57
 - government
 - agencies role in cryptography standards, 344–345
 - archival requirements, 400
 - classification of information, 293–294
 - Gramm-Leach-Bliley Act of 1999, 454–455
 - Grandfather-Father-Son backup method, 397–398, 398, 433
 - grep, 191
 - group policies, 229, 446, 466
 - to lock configuration settings, 129
 - groups, 444–445
 - changing association for file, lab, 517–518
 - GroupWise, 176
 - GSM (Global System for Mobile Communications), 274, 308
 - Guest account, turning off in Windows XP, lab, 521, 521–522
 - guidelines, 287–288, 309
-
- H**
- Hacken9*, 453
 - hacking, international laws in, 457
 - hand scanners, 15
 - hard drives, 158
 - hardening, 221, 259
 - Apple Macintosh, 233–234
 - applications, 240–250
 - DHCP services, 246
 - DNS servers, 243–244
 - e-mail servers, 241–242
 - file and print servers, 245–246
 - FTP servers, 242–243
 - NNTP servers, 244–245
 - web servers, 240–241
 - exam essentials, 252
 - filesystems, 234–236
 - network devices, 238–240
 - Novell NetWare, 232–233
 - operating systems, 224–238
 - review questions, 255–260
 - troubleshooting, 500–502
 - Unix/Linux, 231–232
 - Windows 2000, 230–231
 - Windows Server 2003, 229–230
 - Windows Vista, 227–228
 - Windows XP, 228–229
 - hardware-based keystroke loggers, 496
 - hash total, 321
 - hash value, 316–317, 321
 - creating rule, lab, 373
 - hashing, 316–317, 317
 - science of, 321–323
 - hashing algorithm, 379
 - Health Insurance Portability and Accountability Act (HIPAA), 454
 - Heisenberg, Werner, 319
 - Heisenberg Uncertainty Principle, 319
 - hiding
 - files in Linux, lab, 518–519
 - IP addresses, 116
 - Windows shares, lab, 519
 - hierarchical trust models for PKI, 337–338, 338
 - high availability, 385–386
 - fault tolerance, 387–388
 - formulating, 385
 - RAID, 388–391
 - redundancy, 386
 - HIPAA (Health Insurance Portability and Accountability Act), 454
 - hiring policies, 407
 - .hlp file extension, 80
 - hoaxes, identifying, 87–88
 - Homeland Security Act of 2002, Section 225, 456
 - honeyd, 191
 - Honeynet Project, 191–192
 - honeypot, 188, 191–192, 217
 - troubleshooting, 485–486
 - host, 65
 - host-based intrusion detection systems (HIDSs), 189–190, 190, 217
 - Host-to-Host (Transport) layer, 67
 - hostnames, resolving to IP addresses, 243

- hot site, 9, 402
 - hotfixes, 237, 259
 - HTML (Hypertext Markup Language), 139
 - HTTP (Hypertext Transfer Protocol), 66
 - port, 115
 - HTTPS (Hypertext Transport Protocol Secure), 140, 354
 - port, 115
 - hubs, 118
 - attaching N-IDS to network, 185, 185
 - human error, and encryption vulnerabilities, 321, 322
 - human resource policies, 406–410
 - acceptable use policy, 409
 - background investigations, 410
 - ethics policies, 408
 - hiring policies, 407
 - need-to-know policies, 409–410
 - privacy policies, 409
 - termination policies, 407
 - human vulnerabilities, 3
 - humidity control, 274–275
 - hushmail.com, 483
 - hybrid attacks, 494
 - hybrid physical cryptography systems, 316
 - hybrid trust models for PKI, 340–341, 341
 - Hypertext Markup Language (HTML), 139
 - Hypertext Transfer Protocol (HTTP), 66
 - port, 115
 - Hypertext Transport Protocol Secure (HTTPS), 354
 - port, 115
-
- I**
 - IANA (Internet Assigned Numbers Authority), 70
 - ICMP (Internet Control Message Protocol), 68, 72, 117, 146, 169
 - disabling traffic, 147
 - packets, 57
 - tunneling, 78
 - IDEA (International Data Encryption Algorithm), 324
 - identification and authentication (I & A), 15
 - identity proofing, 21
 - identity theft, 475
 - IDPS, 190
 - IDSs (intrusion detection systems), 127, 128, 128, 169, 179–198
 - active response, 187–189
 - components, 182
 - exam essentials, 208–209
 - host-based, 189–190, 190
 - network-based, 184–189, 185
 - passive response, 186
 - review questions, 213–218
 - troubleshooting, 485–486
 - IEEE (Institute of Electrical and Electronics Engineers), 347
 - 802.1x protocols, 135
 - 802.11x wireless protocols, 199–200
 - IETF (Internet Engineering Task Force), 345–346
 - IGMP (Internet Group Management Protocol), 67, 147, 169
 - IIS. *See* Internet Information Services (IIS)
 - IIS (Internet Information Services), 230, 240
 - default mail system in early versions, 130
 - security patches, 73–74
 - IM (instant messaging), 202–204, 203, 217
 - attacks by, 91
 - privacy, 204
 - vulnerabilities, 203
 - IMAP (Internet Message Access Protocol), 138, 169
 - port, 115
 - impersonation, 475
 - to gain access, 271
 - implicit denies, 295
 - incident response, 192–198, 217
 - adjusting procedures, 198
 - cycle, 193
 - damage repair, 196
 - documenting and reporting, 196–197
 - identification, 193–194
 - investigation, 194
 - plan functioning, 197
 - troubleshooting, 486
 - incident response plan (IRP), 192
 - incident response policies, 413–414
 - incidents, 12
 - detection, 13

- incremental backup, 396–397, 433
- inductive pickup, 150
- industry associations, 345–347
- info utility, 180
- information
 - access control, 295–299
 - classifying, 290, 290–299
 - full distribution information, 292
 - government and military, 293–294
 - internal information, 292
 - limited distribution information, 291–292
 - private information, 292
 - public information, 290–291
 - restricted information, 292
 - social engineering to obtain, 91
- information classification policies, 465
 - drafting and documentation, 437
- information destruction policies, drafting and documentation, 438–439
- Information Flow model of information access, 298, 298–299
- information integrity, 23
 - Biba model and, 297
- information policies, 10
- information retention and storage policies, 465
 - drafting and documentation, 437
- information security, 3–12
 - exam essentials, 40–42
 - goals of, 12–13
 - review questions, 44–49
- Information Security Magazine*, 453
- InformationWeek*, 453
- InfoWorld*, 453
- infrared (IR), 154
- infrastructure
 - compiling list, 111
 - exam essentials, 162–163
 - network devices, 113–127
 - firewalls, 113–117, 114. *See also* firewalls
 - hubs, 118, 185, 185
 - modems, 118–119, 480
 - Remote Access Services (RAS), 119–120
 - routers, 120, 120–121. *See also* routers
 - switches, 73, 122, 122, 169
 - telecom/PBX systems, 122–124, 123
 - virtual private networks (VPNs), 124, 124–125. *See also* virtual private networks (VPNs)
 - wireless access points, 125, 126, 127
 - review questions, 165–170
- infrastructure security, 109–112
 - hardware components, 110, 110–111
 - software components, 112
 - troubleshooting, 497–499
- Initial Sequence Number (ISN), for connection, 71
- inline BNC connector, 149
- input validation, vulnerabilities of, 142
- installing
 - biometric devices, 270
 - software, preventing, 130
- instant messaging (IM), 202–204, 203, 217
 - attacks by, 91
 - privacy, 204
 - vulnerabilities, 203
- Institute of Electrical and Electronics Engineers (IEEE), 347
 - 802.1x protocols, 135
 - 802.11x wireless protocols, 199–200
- integrity
 - in cryptographic systems, 327, 327
 - as topology design goal, 23
- interception, 54
- intermediate CA, 337
- internal data classification, 10
- internal information, 292
- internal security threats, 36, 36–37
- International Data Encryption Algorithm (IDEA), 324
- international efforts, in privacy regulation, 457
- International Organization for Standardization (ISO), Code of Practice for Information Security Management, 288–289
- International Telecommunications Union (ITU), 346
 - X.500 standard, 248
 - X.509 certificate structure, 335
- Internet, 26, 27
- Internet Assigned Numbers Authority (IANA), 70
- Internet Connection Sharing, 32

- Internet connections, 111
 - baselines for, lab, 511
 - common sense, troubleshooting and, 486–487
 - security, 136–146
 - for e-mail, 137–138, 138
 - port and sockets, 136–137
 - for Web, 139, 139–140
 - Internet content filter, 228
 - Internet Control Message Protocol (ICMP), 68, 72, 117, 146, 169
 - disabling traffic, 147
 - packets, 57
 - tunneling, 78
 - Internet Engineering Task Force (IETF), 345–346
 - Internet Explorer
 - clearing private data, lab, 530–531
 - limiting cookies to first party, lab, 531–532
 - phishing filter configuration, lab, 532
 - popup blocker settings, lab, 522, 523
 - susceptibility to exploitation, 225
 - viewing security settings, lab, 522
 - Internet Group Management Protocol (IGMP), 68, 147, 169
 - Internet Information Services (IIS), 230, 240
 - default mail system in early versions, 130
 - security patches, 73–74
 - Internet layer, 67–68
 - Internet Message Access Protocol (IMAP), 138, 169
 - port, 115
 - Internet Packet Exchange/Sequence Packet Exchange (IPX/SPX), 225
 - vulnerability, 227
 - Internet Protocol (IP), 67, 72
 - Internet Protocol Security (IPSec), 134, 169, 355–356, 481
 - errors in performance statistics, lab, 374
 - Internet Protocol v6 (IPv6), turning off in openSUSE, lab, 527–528
 - Internet service provider (ISP), 26
 - Internet Storm Center, 222
 - Internetwork Packet Exchange (IPX), 175
 - intranets, 27, 27
 - intrusion, 180. *See also* social engineering
 - immediate response to current, 195
 - intrusion detection systems (IDSs), 127, 128, 128, 169, 179–198
 - active response, 187–189
 - components, 182
 - exam essentials, 208–209
 - host-based, 189–190, 190
 - network-based, 184–189, 185
 - passive response, 186
 - review questions, 213–218
 - troubleshooting, 485–486
 - inventories, drafting and documentation, 440–441
 - involuntary termination, 407
 - IP (Internet Protocol), 137
 - IP addresses
 - hiding, 116
 - origination, 247
 - resolving hostnames to, 243
 - IP forwarding, 117
 - IP spoofing, 60
 - IP Telephony Security in Dept white paper (Cisco), 39
 - IPSec (Internet Protocol Security), 134, 169, 355–356, 481
 - errors in performance statistics, lab, 374
 - IPX (Internetwork Packet Exchange), 175
 - IPX/SPX (Internet Packet Exchange/Sequence Packet Exchange), 225
 - vulnerability, 227
 - Irina virus, 87
 - IRP (incident response plan), 192
 - ISN (Initial Sequence Number), for connection, 71
 - ISO 17799 security standard, 288–289, 358
 - ISOC (Internet Society), 346
 - ISP (Internet service provider), 26
 - ITU (International Telecommunications Union), 346
 - X.500 standard, 248
 - X.509 certificate structure, 335
 - IUSR_*computername* account, 241, 243
-
- J**
- jamming, 203, 218
 - Java, 140
 - applet vulnerabilities, 143

JavaScript, vulnerabilities, 143
 journaled file system (JFS), 393
 journaling, 393
 .js file extension, 204

K

KDC (Key Distribution Center), 361, 361
 KEA (Key Exchange Algorithm), 361, 362
 Kerberos, 17, 18, 48
 openSUSE as client, lab, 526–527
 SSO and, 417
 time synchronization for, 361
 key attacks, 341
 Key Distribution Center (KDC), 17, 48,
 361, 361
 key escrow, 363, 379
 Key Exchange Algorithm (KEA), 361, 362
 key life cycle, 358
 key management, 358–367. *See also* private
 key; public key infrastructure (PKI)
 centralized vs. decentralized generation,
 358–361
 destruction, 367
 expiration, 363–364
 key escrow, 363
 recovery and archiving, 365–366
 renewal, 366
 revocation, 364
 storage and distribution, 361–362
 suspension, 364
 troubleshooting, 488–489
 usage, 367
 keystroke loggers, hardware-based, 496
 Klez32 virus, 90

L

L2F (Layer 2 Forwarding), 134, 355, 356
 L2TP (Layer 2 Tunneling Protocol), 33, 134,
 355, 356, 481
 LANMAN protocol, 322
 passwords, 494
 last command, 191
 last known good configuration, booting to,
 lab, 537
 lastlog utility, 191
 lab, 517
 latency, 337
 law enforcement
 key escrow for, 363
 rules of evidence, 193
 Layer 2 Forwarding (L2F), 134, 355, 356
 Layer 2 Tunneling Protocol (L2TP), 33, 134,
 355, 356, 481
 LCP (Link Control Protocol), 133
 LDAP (Lightweight Directory Access Protocol),
 248, 259
 openSUSE as client, lab, 527
 port, 115
 leaf CA, 338
 leaf objects in NetWare, 175
 least privilege, 295
 legal notice, adding to computer startup, lab,
 532–533
 license server, 396
 Lightweight Directory Access Protocol (LDAP),
 248, 259
 openSUSE as client, lab, 527
 port, 115
 limited distribution information, 291–292, 309
 Link Control Protocol (LCP), 133
 Linux. *See also* Unix/Linux
 changing ACL on all files in directory,
 lab, 515
 changing password, lab, 514
 changing permissions on all files in
 directory, lab, 515–516
 counting number of running processes,
 lab, 520
 default permissions for new files, lab, 516
 encryption in, lab, 373–374
 help for utilities, 180
 hiding file, lab, 518–519
 identifying running processes, lab, 98–99
 installing snort, lab, 211
 log files in, 191
 network traffic monitoring, lab, 211–212
 Novell product conversion to, 176
 rescue disk in, lab, 427
 resources in, 180
 routing table, lab, 164
 setup for lab exercises, 506
 updating system, lab, 43

- viewing failed login attempts, lab, 518
- viewing logins, lab, 516–517
- LinuxSecurity, 452
- Local Area Connection Properties dialog box,
 - General tab, 226
- local policies, 230
- local registration authority (LRA), 333–334, 334, 379
- locking down desktop, 130
- locks, 496
- logged warnings, viewing in openSUSE, lab, 525
- logging
 - in IDS, 186
 - in Linux, 232
- logic bombs, 88–89, 89, 94, 104
- logical tokens, 446, 466
- login prompt, message display prior to
 - accessing, lab, 532–533
- logins
 - viewing failed attempts in Linux, lab, 518
 - viewing in Linux, lab, 516–517
- logon process, 20, 21
 - spoofing attacks as part of, 60
- logon spoofing, 475
- logs
 - and auditing, 421–422
 - drafting and documentation, 440
 - Event Viewer for reviewing, 231, 231
 - in Linux, 191
 - reviewing, 421
- low-level format, 438, 465
- LRA (local registration authority), 333–334, 334, 379

M

- M of N Control method of access, 366
- MAC, various meanings of acronym, 68
- MAC (Mandatory Access Control) model, 14, 48, 423
- MAC (Media Access Control) address, 67
- MAC (message authentication code), 379
 - for verifying integrity, 327, 328
- macro virus, 79, 84
- Magic Lantern, 363
- maintenance contracts, 404
- maintenance requirements, in standards, 287
- malicious code, surviving, 81–90
- malicious events, preventing, 489–494
- malware, 483
 - training users to avoid, 492–493
- man-in-the-middle attacks, 60–62, 61, 104, 202, 491
- man tool, 180
- Managed Security Service Provider (MSSP), 112
- management, 7–11
 - education on security issues, 448
- manager, 181, 217
- Mandatory Access Control (MAC) model, 14, 48, 423
- mandatory vacations, 408
- mantrap, 264, 264–265
- masquerading, 475
- mathematical attacks, 343
- mathematical cryptography, 316–317
- McAfee Corporation, 452
- MD (Message Digest Algorithm), 322
- mean time between failure (MTBF), 405
- mean time to repair (MTTR), 405
- media, 109
- Media Access Control (MAC) address, 67
- Media Access layer, 14
- Melissa virus, 81, 89
- memory dump, to obtain key, 362
- memory sticks, 158
- mesh trust models for PKI, 339, 340
- message authentication code (MAC), 379
 - for verifying integrity, 327, 328
- Message Digest Algorithm (MD), 322
- metal oxide varistors (MOVs), 276
- Microsoft
 - AntiSpyware, 80
 - Baseline Security Analyzer, lab, 459–460
 - Internet Information Services (IIS), 230, 240
 - default mail system in early versions, 130
 - security patches, 73–74
 - Office, susceptibility to exploitation, 225
 - protocols, 176–178
 - SQL Server, 249
 - Systems Management Server (SMS)
 - package, 73
 - TechNet website, 230

website on security, 450
 Windows Group Policy FAQ, 230
 microwave systems, 154–155, 170
 middle-tier server, 250
 military classification of information, 293–294
 MIME, 351
 minimum age of passwords, changing in
 Windows XP, lab, 528–529
 misuse-detection IDS, 183
 Mitnick, Kevin, *Art of Deception: Controlling
 the Human Element of Security*, 271
 mobile devices, 130–132, 131
 modems, 118–119, 480
 MOVs (metal oxide varistors), 276
 msconfig command, lab, 533
 MSSP (Managed Security Service
 Provider), 112
 MTBF (mean time between failure), 405
 MTTR (mean time to repair), 405
 multi-factor authentication, 17, 18, 22, 48, 415
 multicasting, 118, 147
 multihomed system, 117
 multipartite virus, 85, 85
 multiple barrier system, 263
 mutation of virus, 85
 mutual authentication, 19, 475
 myth of unbreakable codes, 319–321

N

NAC (network access control), 5
 NAT (Network Address Translation), 30–32,
 32, 48
 National Institute of Standards and Technology
 (NIST), 344–345, 379, 452
 National Security Agency/Central Security
 Service (NSA/CSS), 344
 National Security Agency (NSA), 232, 344
 National Security Institute (NSI), 452
 natural disaster, impact on utilities, 384
 NCP (Network Control Protocol), 133
 NDS (NetWare Directory Services), 175
 tree structure, 175
 NDS (Novell Directory Services), 175, 233
 need-to-know policies, 292, 409–410
 Nessus, 94, 222
 NetBIOS (Network Basic Input Output
 System), 176, 259
 attacks through services, 245
 NetBIOS Extended User Interface
 (NetBEUI), 225
 vulnerability, 227
 NetBIOS Session service, port, 115
 NetBus, 59
 NetMeeting, 139
 Netscape, 349
 susceptibility to exploitation, 225
 NetWare, 174
 hardening, 232–233
 NetWare Directory Services (NDS), 175
 tree structure, 175
 NetWare File System (NFS), 235, 259
 NetWare Loadable Modules (NLMs), 233
 network access control (NAC), 5
 Network Address Translation (NAT), 30–32,
 32, 48
 network attached storage, 158
 network audit files, 186
 network-based IDS, 184–189, 185
 Network Basic Input Output System
 (NetBIOS), 176, 259
 attacks through services, 245
 Network Control Protocol (NCP), 133
 network devices
 hardening, 238–240
 updates, 450
 updating, 238–239
 Network File System (NFS), 236
 Network File System Protocol (NFS), 178, 178
 network interface cards (NICs)
 Media Access Control (MAC) address
 for, 67
 promiscuous mode for, 73
 for proxy firewall, 116
 Network Interface layer, 68
 Network Intrusion Prevention Systems
 (NIPSs), 190
 network mapping, 74, 207
 Network Monitor, lab, 210–211
 network monitoring, 127–128, 173–179
 Network News Transfer Protocol (NNTP)
 hardening servers, 244–245
 port, 115

- network operating systems, hardening, 224–238
 - Network Operations Center (NOC), 112
 - network protocols. *See* protocols
 - network security zone, 267, 268
 - network share, connection, 245
 - network sniffer, 73, 217
 - T-connector attached to, 149
 - network threats, overview, 221–222
 - network traffic
 - monitoring in Linux, lab, 211–212
 - recognizing types, 174–178
 - Apple protocol, 178
 - Microsoft protocols, 176–178
 - Network File System Protocol (NFS), 178, 178
 - Novell protocols, 174–176
 - TCP/IP, 174
 - networks, virus transmission in, 86
 - New Technology File System (NTFS), 234–235
 - NFS (NetWare File System), 235, 259
 - NFS (Network File System), 178, 178, 236
 - NICs (network interface cards)
 - Media Access Control (MAC) address for, 67
 - promiscuous mode for, 73
 - for proxy firewall, 116
 - NIDS, 217
 - NIPSs (Network Intrusion Prevention Systems), 190
 - NIST (National Institute of Standards and Technology), 344–345, 379, 452
 - NLMs (NetWare Loadable Modules), 233
 - nmap, 74, 207
 - NMAP port scanner, 222
 - NNTP (Network News Transfer Protocol)
 - hardening servers, 244–245
 - port, 115
 - nondisclosure agreement (NDA), 291
 - Noninterference model of information access, 299, 299
 - nonrepudiation, 56, 379
 - in cryptographic systems, 330
 - and eBay, 331
 - notification, 182
 - in IDS, 186
 - notification policies, drafting and documentation, 437
 - Novell. *See also* Netware
 - product conversion to Linux, 176
 - protocols, 174–176
 - Novell Directory Services (NDS), 175, 233
 - Novell NetWare Storage Services, 235
 - NSA/CSS (National Security Agency/Central Security Service), 344
 - NSA (National Security Agency), 232, 344
 - NSI (National Security Institute), 452
 - NT LAN Manager (NTLM), 322
 - NTFS (New Technology File System), 234–235
 - null session attack, 57
-
- O**
- OCSP (Online Certificate Status Protocol), 336–337, 380
 - OES (Open Enterprise Server), 176
 - OFDM (orthogonal frequency division multiplexing), 199, 200
 - Office, susceptibility to exploitation, 225
 - offsite storage, 394
 - old computers, selling, 368
 - and operating systems, 438
 - one-tier model for database, 250
 - one-time pad, 329, 329
 - one-way hash, 321
 - one-way process, 317
 - Online Certificate Status Protocol (OCSP), 336–337, 380
 - onsite storage, 393
 - for backups, 393
 - Open Enterprise Server (OES), 176
 - open relay, 144
 - open-source movement, 259
 - open-systems philosophy, 231
 - Open Vulnerability and Assessment Language (OVAL), 81
 - OpenLDAP, installing on SuSE server, lab, 253
 - openSUSE, 506
 - AppArmor configuration, lab, 525–526
 - AppArmor reports, lab, 526
 - configuring local security, lab, 524
 - defaults for new users, lab, 524–525
 - firewalls, lab, 523–524
 - as Kerberos client, lab, 526–527
 - as LDAP client, lab, 527

- screensaver password for, lab, 513
- turning off IPv6, lab, 527–528
- view logged warnings, lab, 525
- operating systems
 - bootable portable, 496
 - hardening, 129
 - security limitations, 470, 477
 - updates, 237–238, 449–450
- operational considerations, in guidelines document, 288
- operational environment, survey of, 8
- operational security, 5–7
 - issues, 7
- operator, 182
- orphanware, 406
- orthogonal frequency division multiplexing (OFDM), 199, 200
- OS X, 234, 236
- out-of-band method to send key, 323
- Outlook, and virus spread, 90, 195
- Outlook Express, and virus spread, 90, 195
- OVAL (Open Vulnerability and Assessment Language), 81
- overload, from manual network monitoring, 194
- overview statement, in policy, 285
- owner of data, 294

P

- packet-capture device, 133, 356
- packet filter firewalls, 114–115, 169
- packet sniffing, 205
- parental controls, applying to accounts, 228
- parity information, 388
- partitioning network, 267–268, 269, 308
- Password Authentication Protocol (PAP), 19
- password crackers, 62
- password expiration policy, 6–7
- password-guessing attacks, 62–63, 105
- password utility, 416
- passwords, 93, 318, 474. *See also*
 - username/password access to, 55
 - BIOS-based, 439
 - changing default, 113

- changing minimum age in Windows XP, lab, 528–529
- encryption for Macintosh, 233
- external requirements for, 91
 - for FTP, 145
 - in Linux, lab, 514
 - policies, 446
 - for smart cards, 159
 - on sticky notes, 94
 - troubleshooting, 493–494
 - U.S. Air Force security audit on, 343
 - for Windows XP screensaver, lab, 512
- PAT (Port Address Translation), 32
- patches, 238, 259
 - to close backdoors, 59
 - for Linux, lab, 43
 - in Unix/Linux, 232
- PATRIOT act, 457
- PBX (Private Branch Exchange) system, 169
 - attack, 39
- .pdf file extension, 80
- PDF file of book, 546
- peer-to-peer connection, 145
- penetration
 - detection, 5
 - testing, 222
- performance
 - criteria in standards statement, 287
 - virus impact, 82
- performance baseline, 222
- Performance Monitor, 231
 - lab, 253–254
- perimeter security, 173, 265, 265–266, 308
- permissions
 - changing on all files in Linux directory, lab, 515–516
 - viewing effective in Windows XP, lab, 521
- personal development, 450–451
- personal lab environment, 469
- Personally Identifiable Information (PII), 421
- personnel management, 495
- PGP (Pretty Good Privacy), 324, 347, 354, 355
- phage virus, 85
- phishing, 92, 475
 - configuring filter in Internet Explorer, lab, 532
- physical access control policies, 411

- physical barriers, 263–268
- physical cryptography
 - hybrid systems, 316
 - steganography, 316
 - substitution ciphers, 314
 - transposition ciphers, 315, 316
- physical environment, survey of, 6
- physical security, 4–5, 48, 262–280
 - access control, 262–270
 - location of computers, 274–277
 - partitioning, 267–268, 269
 - perimeter security, 265, 265–266
 - physical barriers, 263–268
 - security zones, 266–267
 - three-layer security model, 263
 - biometrics, 15, 48, 270, 309, 474
 - exam essentials, 301–302
 - review questions, 304–309
 - troubleshooting, 495–497
- physical token, for access, 264
- .pif file extension, 81
- PII (Personally Identifiable Information), 421
- PIN, for smart cards, 159
- ping, 146, 206
- ping of death, 57
- PKC (Public Key Cryptography), 325
- PKCS (Public-Key Cryptography Standards), 348
- PKI. *See* Public Key Infrastructure (PKI)
- Plain Old Telephone Service (POTS), 119
- platform hardening, 129
- plumbing, 148
- Point-to-Point Protocol (PPP), 169
 - remote access with, 132–133, 133
- Point-to-Point Tunneling Protocol (PPTP), 133, 356, 481
- policies and procedures, 7–11, 406–414. *See also* best practices; security policies
 - administrative, 9
 - assembling and examining, 11–12
 - business policies, 410–412
 - document disposal and destruction policies, 411–412
 - due care policies, 411
 - physical access control policies, 411
 - separation of duties, 410–411
 - certificate policies, 412–413
 - enforcement, 443
 - exam essentials, 425–426
 - human resource policies, 406–410
 - acceptable use policy, 409
 - background investigations, 410
 - ethics policies, 408
 - hiring policies, 407
 - need-to-know policies, 409–410
 - privacy policies, 409
 - termination policies, 407
 - implementing, 285–286
 - incident response policies, 413–414
 - information, 10
 - review questions, 429–434
 - updates, 450
 - usage, 11
 - user management, 11
- polymorphic virus, 85, 86
- POP (Post Office Protocol), 66, 138
 - port, 115
- popunders, 143
- popup blocker, Internet Explorer settings, lab, 522, 523
- popup blockers, 143
- popups, vulnerabilities of, 143
- Port Address Translation (PAT), 32
- port mirroring, 185
- port scan, 73–74, 185, 206
 - to reveal Trojan horse, 88
- ports, 136–137
 - checking available on system, 74
 - packet filtering based on, 114
 - security with hubs, 118
 - viewing active, lab, 210
 - and vulnerability, 139
 - well-known, 69–71
- Post Office Protocol (POP), 66, 138
 - port, 115
- postmortem, 198
- POTS (Plain Old Telephone Service), 119
- power conditioners, 276
- power generators, 277
- power systems, 275–277
- PPP (Point-to-Point Protocol), 169
 - remote access with, 132–133, 133
- PPTP (Point-to-Point Tunneling Protocol), 133, 356, 481

- preauthentication systems, for remote access, 479
- Pretty Good Privacy (PGP), 324, 347, 354, 355
- prevention, as information security goal, 12–13
- previous keys, 365–366
- prime numbers, and key generation, 359
- principle, for Key Distribution Center, 17
- print servers, hardening, 245–246
- privacy
 - for IM systems, 204
 - information obtained through monitoring, 444
 - policies, 409
- privacy regulation, 454–457
 - Computer Fraud and Abuse Act, 455
 - Computer Security Act of 1987, 456
 - Cyber Security Enhancement Act, 456
 - Cyberspace Electronic Security Act (CESA), 456
 - Family Education Rights and Privacy Act, 455–456
 - Gramm-Leach-Bliley Act of 1999, 454–455
 - Health Insurance Portability and Accountability Act (HIPAA), 454
 - international efforts, 457
 - PATRIOT act, 457
- Private Branch Exchange (PBX) system, 169
 - attack, 39
- private information, 292
 - clearing from Firefox, lab, 531
 - clearing from Internet Explorer, lab, 530–531
 - data classification, 10
- private IP addresses, 48
 - NAT assignment to internal hosts, 32
- private key, 324–325
 - protection, 362
- privilege auditing, 419
- privilege creep, 11, 419
- privilege management, 414–424
 - access control, 422–424
 - auditing, 418–422
 - administrative auditing, 420–421
 - escalation auditing, 420
 - and log files, 421–422
 - privilege auditing, 419
 - reporting to management, 422
 - usage auditing, 419
 - decision making, 418
 - privilege escalation, 63, 416
 - user and group role management, 415–416
- procedures. *See* best practices; policies and procedures
- processes
 - counting number running in Linux, lab, 520
 - identifying running, lab, 98–99
 - terminating, 187
- programs. *See* applications
- promiscuous mode, for NIC, 73
- protocol analyzers, 205
- protocols, 146–147
 - antiquated, 67
 - checking available on system, 74
 - configuring, 225–227
 - enabling and disabling, 240
 - well-known ports, 69–71
 - working with, 69–72
- proxy, NAT as, 32
- proxy firewalls, 116, 116–117
- ps utility (Linux), lab, 99
- public data classification, 10
- public domain cryptography, 347
- public information, 290–291
- public key, 324, 380
 - distribution procedure, 348
- Public Key Cryptography (PKC), 325
- Public-Key Cryptography Standards (PKCS), 348
- Public Key Infrastructure (PKI), 10, 331–341
 - certificate authorities (CA), 332, 333
 - certificate implementation, 335–336
 - certificate policies, 336
 - certificate revocation, 336–337
 - trust models, 337–341
 - bridge, 339–340, 340
 - hierarchical, 337–338, 338
 - hybrid, 340–341, 341
 - mesh, 339, 340
 - X.509 standard, 348
- purpose statement
 - in guidelines document, 287
 - in standards statement, 286
- PUT command (FTP), 145
- PuTTY, 354

Q

quantum cryptography, 318–319, 320
queries in SQL, 249

R

radio frequency interference (RFI), 277, 278
radio frequency (RF) communications,
154, 155
RADIUS (Remote Authentication Dial-In User Service), 135, 135–136, 479
RAID (Redundant Array of Independent Disks), 388–391, 433
rainbow tables, 63, 494
RDN (Relative Distinguished Name), 248
real time detection, 218
reciprocal agreement, 402, 403, 433
reconstitution, 477
recovering keys, 365, 365–366
recovery, 5. *See also* disaster recovery plans (DRPs)
from backups, 400–401, 401
Red Hat, website on security, 450
redundancy, 386
Redundant Array of Independent Disks (RAID), 388–389, 433
reference documents, for standards, 286
registrar, 243
registration authority (RA), 332, 333
Registry
editing to display message at login, 532–533
virus change to, 84
relational database, 249
Relative Distinguished Name (RDN), 248
releases, to repair multiple problems, 238
relying party, in transaction, 413
remote access, 132–136
network connections for, 134
with Point-to-Point Protocol, 132–133, 133
troubleshooting, 478–479
with tunneling protocols, 133–134
with wireless protocols, 135
Remote Access Services (RAS), 119–120
remote authentication, 132
Remote Authentication Dial-In User Service (RADIUS), 135, 135–136, 479
remote clients, compromise of, 479
remote control/remote shell, troubleshooting security, 480
remote desktop, running, lab, 534–535
Remote Procedure Call (RPC), 245
removable media, 156–161
CD-R/DVD-R, 157
diskettes, 157
flash cards, 158
hard drives, 158
network attached storage, 158
smart cards, 159
tape, 159–160
USB drives, 161, 439, 465
and virus spread, 82, 83
renewing keys, 366
replay attacks, 62, 62, 104, 491
reporting audit to management, 422
repudiation attacks, 56
Requests for Comments (RFCs), 345, 379
1466 on subnetting, 32
1918 on subnetting, 32
rescue disk, in Linux, lab, 427
resources, in Linux, 180
response, as information security goal, 13
responsibilities
accountability and, 471
defining, 443
in guidelines document, 287
in standards statement, 286
restore point in Windows XP, lab, 536–537
restricted information, 292
retinal scanners, 15
retrovirus, 85
reverse hash matching, 493
reverse lookups, 491
review questions
attack strategies, 100–105
cryptography, 374–380
hardening, 255–260
information security, 44–49
infrastructure, 165–170
intrusion detection systems (IDSs), 213–218
physical security, 304–309

- policies and procedures, 429–434
 - security management, 461–466
- revoking keys, 364
- RF collar, 150
- RF (radio frequency) communications, 154, 155
- RFCs. *See* Requests for Comments (RFCs)
- RFI (radio frequency interference), 277, 278
- Rijmen, Vincent, 324
- Rijndael algorithm, 324
- RIP (Routing Information Protocol), 66
- risk analysis, 282
- risk assessment, 35, 281, 282–284
 - computations, 284
 - conducting, 283
- Rivest, Ron, 325
- Rivest, Shamir, and Adleman (RSA) algorithm, 325, 347
- Rivest’s Cipher, 324
- rogue access points, 202
- rogue servers, 247
- Role-Based Access Control (RBAC) model, 15, 48, 423
- roles
 - in guidelines document, 287
 - in security process, 294–295
 - in standards statement, 286
- root CA, 337
- root directories, 236
- rootkits, 80
- rot13 encoding algorithm, 315
- rotation schemes for tape, 160
- routers, 120, 120–121, 169
 - and block for external attacks, 72
 - configuring, 239–240
 - as defense against external attacks, 238–239
 - and security zones, 26
- Routing and Remote Access Services (RRAS), 119
- Routing Information Protocol (RIP), 66
- routing table, lab, 164
- RPC (Remote Procedure Call), 245
- RSA (Rivest, Shamir, and Adleman) algorithm, 325, 347
- rubber hose attack, 500
- Rule-Based Access Control (RBAC), 423–424

S

- S-HTTP (Secure HTTP), 140, 355
- S/MIME (Secure Multipurpose Internet Mail Extensions), 351
- salt, 494
- sandbox, for Java applets, 143
- SANS Institute, 452
 - policy website, 477
- scanner, 73
- scanning, 206–207, 217
 - environment, 272–280
- scanning ports, 73–74
- schemes, 383
- Schneier, Bruce, 324
- scope statement
 - in guidelines document, 287
 - in policy, 285
 - in standards statement, 286
- .scr file extension, 80, 81
- screensaver password
 - for openSUSE, lab, 513
 - for Windows XP, lab, 512
- scripts
 - Common Gateway Interface (CGI), 241
 - disabling, 142
 - to turn off unneeded Unix service, 232
- secret handshake, 330
- secret information, 293
- Secure Electronic Transaction (SET), 351–352, 352
- Secure File Transfer Protocol (SFTP), 145, 243, 483
- Secure Hash Algorithm (SHA), 321
- Secure HTTP (S-HTTP), 140, 355
- Secure Multipurpose Internet Mail Extensions (S/MIME), 351
- Secure Shell (SSH), 134, 145, 352, 353, 480
- Secure Sockets Layer (SSL), 140, 349–350, 350
 - in Windows Server 2003, lab, 373
- SecureLogix, voice firewall, 39
- SecurID, 264
- security, 2
 - analogy, 92–93
 - baselines for, 222–224
 - troubleshooting, 476–477
 - circumventing, 266

- evaluating, 269
- standards, 288–289
- from Windows Server 2003 administrator's view, 224
- of wireless connection, 202
- Security Center dialog box, 511
- Security+ certificate, 2
- Security Enhanced Linux (SELinux), 232
 - configuring in Fedora, lab, 531
- security events, locating in Windows XP, lab, 512
- Security Focus, 452
- security groups, 415–416, 416, 434
- security guard, 266
- security logs, 93
- security management, 436, 465. *See also*
 - best practices
 - exam essentials, 458
 - privacy regulation, 454–457
 - Computer Fraud and Abuse Act, 455
 - Computer Security Act of 1987, 456
 - Cyber Security Enhancement Act, 456
 - Cyberspace Electronic Security Act (CESA), 456
 - Family Education Rights and Privacy Act, 455–456
 - Gramm-Leach-Bliley Act of 1999, 454–455
 - Health Insurance Portability and Accountability Act (HIPAA), 454
 - international efforts, 457
 - PATRIOT act, 457
 - review questions, 461–466
 - security awareness and education program, 446–448
 - simplifying, 444–446
 - staying current, 449–453
 - trade publications, 452–453
 - websites tracking issues, 451–452
- security policies, 10
 - drafting and documentation, 439
 - personnel knowledge of, 8–9
- security process, 13–20
 - access control implementation, 14–15
 - antivirus software, 13–14
 - authentication, 15–20, 48
 - biometrics, 15, 48, 270, 308, 474
 - certificates, 16, 16. *See also* certificates
 - Challenge Handshake Authentication Protocol (CHAP), 16, 17, 132
 - in cryptographic systems, 329–330
 - issues, 21–22
 - Kerberos, 17, 18, 48, 361, 417
 - multi-factor, 17, 18, 22, 48, 415
 - mutual, 19
 - Password Authentication Protocol (PAP), 19
 - for remote user, 132
 - security tokens, 19, 19
 - smart cards, 20, 20, 159, 170, 362, 367, 474
 - username/password, 20, 21
 - in WAP, 130
 - security professional, 294–295
 - security templates, 229
 - comparing system to, lab, 529–530
 - security tokens, 19, 19
 - security topologies, 22–39
 - business concerns, 33–38
 - assets identification, 34
 - risk assessment, 35
 - threat identification, 35–37
 - design goals, 23–25
 - security zones, 26–29
 - demilitarized zones (DMZ), 28, 29
 - extranets, 28, 28
 - Internet, 26, 27
 - intranets, 27, 27
 - technologies, 29–33
 - Network Address Translation (NAT), 30–32, 32
 - tunneling, 33
 - virtual local area networks (VLAN), 30, 31
 - virtualization, 29–30
 - telephony issues, 38–39
 - vulnerabilities, 38
- security triad, 4
- security zones, 266–267, 308
 - troubleshooting, 499–500
- SEI (Software Engineering Institute), 221
- SELinux (Security Enhanced Linux), 232
 - configuring in Fedora, lab, 531
- selling old computers, 368
 - and operating systems, 438
- sender, authenticating, 329

- sensitive but unclassified information, 293
- sensor, 182
- separation of duties, 297, **410–411**
- Sequenced Packet Exchange (SPX), 175
- Serial Line Internet Protocol (SLIP), 132
- servers
 - authentication, 475
 - in WAP, 130
 - as e-mail relay, 144
 - hardening, 131
 - implementing secure environment, 223
 - security for, **129–130**
- service-level agreement (SLA), **404–405**, 433
- service packs (Microsoft), 233, **237**, 259
- services
 - enabling and disabling, 240
 - removing unneeded, 501
- session hijacking attacks, 491
- sessions in web browser, clearing, lab, 530–531
- sessions, terminating, 187
- SET (Secure Electronic Transaction), **351–352**, 352
- SFTP (Secure File Transfer Protocol), 145, 243, 483
- SGID files, finding in Linux, lab, 514–515
- SHA (Secure Hash Algorithm), 321
- shadow copies, 393
- Shamir, Adi, 325
- shared folders, preventing, lab, 523
- shared resources, and security risk, 36
- shareware software, 546
- sheep-dip system, 493
- shielded twisted pair (STP), **150–152**, 151
 - common cable specifications, 152
- shielding, **277–278**, 308
- shoulder surfing, 271–272
- SHTTP (Secure HTTP), 140, 355
- shunning, in IDS, 186
- signal analysis, 205–207
- signal intelligence, **205–207**
- signature-based-detection IDS, 183, 183
- signed applets, vulnerabilities of, **143–144**
- SIM (Subscriber Identification Module), 274
- Simple Mail Transfer Protocol (SMTP), 66, 138, 259
 - port, 115
 - relay vulnerabilities, **144**
 - virus, 195
- Simple Network Management Protocol (SNMP), 66, 72, 146
- single loss expectancy (SLE), 283
- single sided certificates, 336
- single sign-on (SSO), 415, **416–418**
- single-tier environment, 250
- site surveys, 201, 217
- SLA (service-level agreement), **404–405**, 433
- Slammer attack, 57
- Slapper attack, 57
- SLE (single loss expectancy), 283
- SLIP (Serial Line Internet Protocol), 132
- smart cards, 20, **20**, 159, 170, 474
 - individuals forgetting, 367
 - for keys, 362
- SMTP (Simple Mail Transfer Protocol), 66, 138, 259
 - port, 115
 - virus, 195
 - vulnerabilities of relay, **144**
- smurf attack, 104, 147
- sniffers, 127–128, 169, 205
 - 10Base-T network with, 153
- SNMP (Simple Network Management Protocol), 66, 72, 146
- snooping, 54
- snort, 205
 - lab, 211
- social engineering, **91–93**, 104, **270–272**, 308
 - testing, lab, 303
 - troubleshooting, **500**
- sockets, **136–137**, 169
- software. *See* applications
- Software Engineering Institute (SEI), 221
- software exploitation attack, 105
- Sophos Anti-Virus, 421–422, 422
- source code, conditions of release, 406
- source port, 137
- spam, 87–88
 - ACL to control, 242
- spare parts, 387
- sPing, 57
- split generation system, 359
- split-system key generation, 361
- spoofing attacks, **60**, 61, 491
- SPX (Sequenced Packet Exchange), 175
- Spybot, 80
- spyware, 79–80, 88

Spyware Doctor, 80
 SQL (Structured Query Language), 249, 259
 SQL Server (Microsoft), 249
 SSH (Secure Shell), 134, 145, 352, 353, 480
 SSID broadcast, 201
 SSL (Secure Sockets Layer), 140, 349–350, 350
 in Windows Server 2003, lab, 373
 SSO (single sign-on), 415, 416–418
 standards, 286–287
 state laws on computer crime, 454
 stateful inspection firewalls, 117–118
 stateful packet filtering, 117
 static electricity, 497
 preventing, 275
 stealth virus, 86, 86, 104
 steganography, 314, 316
 storage. *See* removable media
 storing keys, 361–362
 STP (shielded twisted pair), 150–152, 151
 common cable specifications, 152
 stream cipher, 323
 Structured Query Language (SQL), 249, 259
 Subscriber Identification Module (SIM), 274
 subscriber, in transaction, 413
 substitution ciphers, 314
 SUID files, finding in Linux, lab, 514–515
 support packs (Novell), 233, 237
 surge protectors, 276
 surveillance systems, 5
 survey
 of operational environment, 8
 of physical environment, 6
 of surroundings, 55
 SuSE Linux
 backups in, lab, 428
 installing OpenLDAP, lab, 253
 suspending keys, 364, 379
 switches, 73, 122, 122, 169
 Sybex test engine, 546
 Symantec Corporation, 87, 452
 symmetric algorithms, 323–324
 symmetric key, 323
 SysAdmin, Audit, Network, Security (SANS)
 certification, 489
 system architecture, drafting and
 documentation, 441

System Configuration Utility (Windows),
 lab, 534
 system files, clearing infection from, 196
 system logs, 49, 440
 reviewing, 173
 system vulnerabilities, 3
 Systems Monitor, 228–229

T

T-connector (BNC), 149, 150, 151
 TACACS (Terminal Access Controller Access
 Control System), 136, 479
 port, 115
 TACACS/+, 136
 tailgating, 271
 tap, 179, 179
 tape, 159–160
 for backups, 393
 tar pit, 192
 Tavares, Stafford, 324
 TCP (Transmission Control Protocol), 67, 72
 attacks, 74–76
 three-way handshake, 71–72
 well-known ports, 70
 TCP ACK flood attack, 74–75, 104
 TCP/IP (Transmission Control Protocol/
 Internet Protocol), 174, 225
 NetBIOS binding to, 226
 vulnerability, 227
 TCP/IP hijacking, 62, 76, 76, 104, 105
 TCP/IP (Transmission Control Protocol/
 Internet Protocol), 38
 architectural layers, 65, 65–68
 Application layer, 66–67
 encapsulation, 68, 69
 Host-to-Host (Transport) layer, 67
 Internet layer, 67–68
 Network Interface layer, 68
 common ports, 115
 recognizing attacks, 72–78
 security concerns, 64–78
 susceptibility to attacks, 79
 TCP packet, 137
 TCP ports, viewing active, lab, 210
 TCP sequence number attack, 75–76, 76

- TCP SYN flood attack, 74–75, 75
- TCP wrappers, 232
- technical staff, education on security issues, 448
- technology standards, 287
- telecom/PBX systems, 122–124, 123
- telephony issues, 38–39
- Telnet, 66, 480
 - for attacks, 74
 - port, 115
 - security risks, 354
- temperature, 274–275
- TEMPEST project, 278, 308
- Temporal Key Integrity Protocol (TKIP), 357
- temporary files in web browser, clearing, lab, 530–531
- “Ten Commandments of Computer Ethics”, 408
- Terminal Access Controller Access Control System (TACACS), 136, 479
- terminated employees, as threat, 11
- terminating processes or sessions, 187
- termination policies, 407
- termination process, in coax network, 149
- testing environment, 501–502
 - setup for lab exercises, 506
- TFTP (Trivial File Transfer Protocol), 145
- theft, detection, 5
- thin clients, 159
- third party, 433
 - in transaction, 413
- third-party cookies, lab, 531–532
- thp, 191
- threat
 - assessment, 49
 - identification, 35–37
 - terminated employees as, 11
- three-layer security model, 263
- three-tier model for database, 250, 259
- thumb drives, 161
- tickets, for Kerberos, 17
- time-of-day restrictions, 446
- time synchronization, for Kerberos, 361
- TKIP (Temporal Key Integrity Protocol), 357
- TLS (Transport Layer Security), 140, 350, 350, 379
- tokens, 49
- Top Secret information, 293
- TPM (Trusted Platform Module), 317
- Traceroute, 146, 206
- trade publications, on security, 452–453
- traffic generation DoS attacks, 491
- training, importance of, 25
- Transmission Control Protocol. *See* TCP (Transmission Control Protocol)
- Transmission Control Protocol/Internet Protocol (TCP/IP). *See* TCP/IP (Transmission Control Protocol/Internet Protocol)
- transmission in network, intercepting, 342
- Transport Layer Security (TLS), 140, 350, 350, 379
- transposition ciphers, 315, 316
- trash, access to, 55
- tree structure, in hierarchical trust model, 337
- trial versions of software, 546
- Triple-DES (3DES), 324
- Trivial File Transfer Protocol (TFTP), 145
- Trojan horse, 59, 88, 104, 491
- troubleshooting, companion CD, 548
- troubleshooting guide, 468–503
 - access control issues, 471
 - accountability concerns, 471–472
 - antivirus software, 492–493
 - auditing, 472–473
 - authentication schemes, 473–476
 - backup management, 476
 - baselining security, 476–477
 - certificate management, 477–478
 - communications security, 478–481
 - directory services, 481–482
 - disaster planning, 482
 - documentation, 483
 - e-mail issues, 483–484
 - file sharing, 484–485
 - getting started, 469–471
 - hardening, 500–502
 - honeypot, 485–486
 - incident response, 486
 - infrastructure security, 497–499
 - Internet common sense and, 486–487
 - intrusion detection systems (IDSs), 485–486
 - key management, 488–489
 - passwords, 493–494

- personnel management, 495
 - physical security, 495–497
 - preventing malicious events, 489–494
 - security zones, 499–500
 - social engineering, 500
 - wireless network security, 502–503
 - trust, and e-commerce, 412
 - trust models for PKI, 337–341
 - bridge, 339–340, 340
 - hierarchical, 337–338, 338
 - hybrid, 340–341, 341
 - mesh, 339, 340
 - Trusted Computer System Evaluation Criteria (TCSEC), 223
 - Trusted Computing Group, 317
 - Trusted Platform Module (TPM), 317
 - trusted transaction, 412–413
 - tunneling, 33, 48
 - tunneling protocols, 133–134, 356
 - two-factor authentication system, 17, 18
 - two-tier model for database, 250
 - two-way (client and server) authentication, in WAP, 130
 - two-way hash, 321
 - Twofish, 324
 - .txt file extension, 80
-
- ## U
- Ubuntu, website on security, 450
 - UDP ports, viewing active, lab, 210
 - umask utility, lab, 516
 - unclassified information, 293
 - undeliverable e-mails, log report of, 195
 - unicasts, 118, 147
 - uninterruptible power supply (UPS), 276, 387–388
 - United States
 - automatic declassification system, 437
 - federal laws on privacy and security, 454–457
 - Computer Fraud and Abuse Act, 455
 - Computer Security Act of 1987, 456
 - Cyber Security Enhancement Act, 456
 - Cyberspace Electronic Security Act (CESA), 456
 - Family Education Rights and Privacy Act, 455–456
 - Gramm-Leach-Bliley Act of 1999, 454–455
 - Health Insurance Portability and Accountability Act (HIPAA), 454
 - PATRIOT act, 457
 - U. S. Air Force, security audit on
 - password, 343
 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, 457
 - University of Maryland, A. James School of Engineering, 74
 - Unix Filesystem, 235, 235
 - Unix/Linux. *See also* Linux
 - file structure in, 232
 - hardening, 231–232
 - Network File System (NFS), 236
 - as default file-sharing protocol, 178
 - networking, lab, 254
 - securing for interactive users, 354
 - unshielded twisted pair (UTP), 150–152, 151, 170
 - common cable specifications, 152
 - updates
 - network devices, 238–239
 - operating systems, 237–238
 - in Unix/Linux, 232
 - upgrades, policies on, 9
 - UPN (User Principal Name), 248
 - UPS (uninterruptible power supply), 276, 387–388
 - uptime, 24
 - usage auditing, 419
 - usage policies, 11
 - USB flash drives, 161
 - policies on use, 439, 465
 - use policies, drafting and documentation, 439–440
 - user access and rights review, 418
 - user accounts, identifying those with
 - administrator access in Windows XP, lab, 512–513
 - user behavior modification, 484
 - User Datagram Protocol (UDP), 67, 72, 117
 - well-known ports, 71

user files, 395–396

user management policies, 11

- drafting and documentation, 442

user of data, 294

User Principal Name (UPN), 248

username/password

- authentication, 20, 21
- policies, 446

users

- defaults for new, in open SUSE, lab, 524–525
- education
 - to prevent virus spread, 90
 - on security issues, 447–448
 - against social engineering, 92, 272

utilities

- for Linux, help for, 180
- natural disaster impact, 384

UTP (unshielded twisted pair), 150–152, 151, 170

- common cable specifications, 152

V

vacations, mandatory, 408

validation of input, vulnerabilities of, 142

vampire tap, 149–150, 151

/var/log/faillog file, 191, 518

/var/log/lastlog file, 191

/var/log/messages file, 191

/var/log/wtmp file, 191

.vbs file extension, 204

vendor support reinforcement, 404–406

- code escrow agreements, 406
- service-level agreement (SLA), 404–405

VeriSign, 350

VeriSign/InterNic, 206

virtual local area networks (VLAN), 30, 31

Virtual Network Computing (VNC), 119

virtual private networks (VPNs), 48, 124, 124–125, 354

- IPSec for, 355
- troubleshooting security, 480–481
- tunnels as, 33

virtualization, 29–30

virus scanner, on e-mail servers, 241, 242

viruses, 13, 81–86

- with CD-R, 157
- how they work, 82–83, 83
- losses due to, 82
- present activity, 87
- in removable media, 156
- symptoms of infection, 82
- transmission in network, 86
- types, 83–86

VLAN (virtual local area networks), 30, 31

VMware Player, 469

VNC (Virtual Network Computing), 119

Voice over IP (VoIP), 39

VPN. *See* virtual private networks (VPNs)

vulnerabilities, 3, 38

- scans, 74, 94, 207
- testing, 222

W

W3C (World Wide Web Consortium), 346

W32/Klez.mm virus, 90

WAP (Wireless Application Protocol), 198, 200, 217

- security levels, 130

war driving, 201–202

warm site, 402, 433

warranties, 405

warscan, 207

water, 276

- damage from, 275
- in fire-suppression system, 280

watermarking, electronic, 316

WDP (Wireless Datagram Protocol), 132

weak key attack, 343

Web connections

- security, 139, 139–140
- vulnerabilities of add-ins, 141–144
 - ActiveX, 141
 - buffer overflow, 141
 - Common Gateway Interface (CGI), 141–142
 - cookies, 142
 - cross-site scripting (XSS), 142
 - input validation, 142
 - Java applets, 143

- JavaScript, 143
 - popups, 143
 - signed applets, 143–144
 - SMTP relay, 144
- web request, TCP connection process for, 71
- web servers, hardening, 240–241
- web structure, 339
- websites, 139
 - for tracking security issues, 451–452
- well-known ports, 69–71
- WEP (Wired Equivalent Privacy), 61, 127, 200–201, 201, 342, 357, 502
- wetware, 270
- whatis utility, 180
- whereis utility, 180
- white lists, 491
- whole disk encryption, 228
- Wi-Fi, 199
- Wi-Fi Alliance, 127
- Wi-Fi Protected Access (WPA), 127, 201, 357
 - changing to, lab, 508–509
- Wi-Fi Protected Access 2 (WPA2), 201, 217, 357
- Wiley Tech Support, 548
- Windows
 - file encryption, lab, 519
 - identifying running processes, lab, 98
 - password cracking, 494
 - preventing shared folders, lab, 523
 - routing table, lab, 164
- Windows 2000, hardening, 230–231
- Windows Media Center, 228
- Windows Registry, lab, 532–533
- Windows Server 2003
 - Automated System Recovery, lab, 427
 - hardening, 229–230
 - hash rules, lab, 373
 - security from administrator's view, 224
 - SSL in, lab, 373
 - updating system, lab, 43
- Windows Server 2008, updating system, lab, 43
- Windows shares, hiding and accessing, lab, 519
- Windows Socket (WinSock), 72, 72
- Windows Vista, hardening, 227–228
- Windows XP
 - account database encryption, lab, 535–536
 - adding legal notice to computer startup, lab, 532–533
 - Automatic Updates, lab, 459
 - booting to good configuration, lab, 537
 - changing password minimum age, lab, 528–529
 - changing to Wi-Fi-Protected Access (WPA), lab, 508–509
 - displaying Security tab for files and folders, lab, 520
 - firewall in, lab, 509–511, 510, 511
 - firewall log, 421
 - folder encryption with cipher, lab, 528
 - hardening, 228–229
 - identifying user accounts with administrator access, lab, 512–513
 - locating security events, lab, 512
 - making file extensions visible, lab, 211
 - network binding in, 226
 - restore point, lab, 536–537
 - screensaver password, lab, 512
 - startup configuration, lab, 533, 534
 - turning off Guest account, lab, 521, 521–522
 - viewing effective permissions, lab, 521
- Windows XP Home edition, 228
- Windows XP Professional, 228
- WinSock (Windows Socket), 72, 72
- Wired Equivalent Privacy (WEP), 61, 127, 200–201, 201, 342, 357, 502
- wireless access points, 125, 126, 127
- Wireless Application Protocol (WAP), 198, 200, 217
 - security levels, 130
- wireless cells, 272–274, 273, 308
 - security for, 274
- Wireless Datagram Protocol (WDP), 132
- Wireless Markup Language (WML), 200
- wireless networks, 155, 198–202
 - troubleshooting security, 502–503
 - vulnerabilities, 201–202
- wireless protocols, 135
- Wireless Session Protocol (WSP), 132
- Wireless Transaction Protocol (WTP), 132

Wireless Transport Layer Security (WTLS),
132, 198, 199, 274, 357

Wireshark, 73

wiring

- coaxial, 148, 148–150
- fiber-optic technology, 152–153
- unshielded twisted pair (UTP) and shielded twisted pair (STP), 150–152, 151

WML (Wireless Markup Language), 200

WMLScript, 200

work factor, of cryptography algorithm, 326

working copy backups, 393, 433

working documents, 292

workstations, security for, 129–130

World Wide Web Consortium (W3C), 346

WORM (write once, read many) device,
472–473

worms, 89, 104, 196

WPA (Wi-Fi Protected Access), 127, 201, 357

WPA2 (Wi-Fi Protected Access 2), 201, 217, 357

write down, preventing, 296

write-protected tape, and backup, 25

WSP (Wireless Session Protocol), 132

WTLS (Wireless Transport Layer Security),
132, 198, 199, 274, 357

WTP (Wireless Transaction Protocol), 132

X

X.509 standard, 348–349, 412

- certificate structure, 335, 335–336

XKMS (XML Key Management Specification),
351, 380

.xls file extension, 80

XML (Extensible Markup Language),
81, 140

XML Key Management Specification (XKMS),
351, 380

Y

YaST, 506

yousendit.com, 483

Z

ZENworks, 176

Zimmerman, Phil, 347

.zip file extension, 81

zombies, 57