

Index

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

A

- ABA (American Bankers Association), 334
- Acceptable Use policies, 395, 428
- access attacks, 53–54
- access control, 14–15, 254–255, 285
 - Bell La-Padula model, 286, 286
 - Biba model, 287, 287
 - biometric systems, 261–262
 - Clark-Wilson model, 287–288, 288
 - in cryptographic systems, 319–320
 - Information Flow model, 288–289, 288
 - in ISO 17799 standard, 280
 - Noninterference model, 289, 289
 - physical barriers, 255–256, 255–256
 - partitioning, 259–260, 260
 - perimeter security, 256–257, 257
 - security zones, 257–259, 259
 - practical applications, 459
 - privilege management, 407–408
- Access Control Lists (ACLs), 15, 231, 233
- accountability
 - as design goal, 26–27
 - in policies, 276
 - practical applications, 459
- accounting, proxy firewalls for, 113
- ACK attacks, 72–73, 72
- ACLs (Access Control Lists), 15, 231, 233
- acquiring evidence, 421–422
- Active Directory (AD), 222, 239, 403–404, 404
- active interception, 54
- active responses, 180–182, 181–183
- active sniffing, 73–74, 74
- ActiveX technology, 137
- activities
 - in IDSs, 175
 - logging in Linux, 224
- AD (Active Directory), 222, 239, 403–404, 404
- AD-IDSs (anomaly-detection IDSs), 176–178, 178
- Adams, Carlisle, 313
- AdAware program, 77
- add-ins, web, 136–139
- Address Resolution Protocol (ARP), 65
- adjusting procedures as incident response, 190–191
- Adleman, Leonard, 314, 336
- administrative policies, 10
- administrative requirements in standards, 278
- administrators in IDSs, 175
- adware, 77
- AES (Advanced Encryption Standard), 313
- AFS (Apple File Sharing), 227–228
- ALE (annual loss expectancy) values, 274–275
- alerts in IDSs, 175
- algorithms
 - in code breaking, 310
 - cryptographic systems
 - asymmetric, 313–315, 314
 - attacks on, 330
 - hashing, 310–311
 - symmetric, 312–313, 312
- allocating resources, 431
- alternate sites, 388–390
- American Bankers Association (ABA), 334
- analyzers in IDSs, 175
- analyzing evidence, 422
- ankle biters, 458
- annual loss expectancy (ALE) values, 274–275
- annualized rate of occurrence (ARO), 274–275
- anomalies, 187
- anomaly-detection IDSs (AD-IDSs), 176–178, 178
- anonymous authentication, 127
- anonymous FTP, 139–140
- antivirus software, 14, 87, 467–468
- APIPA (Automatic Private IP Addressing) addresses, 237
- APIs (Application Program Interfaces), 69
- Apple File Sharing (AFS), 227–228

Apple Macintosh, hardening, 225
 AppleTalk protocol, 173, 227
 applets, 136–137
 appliances, 109, 231
 Application layer, 64
 application-level proxies, 112
 Application Program Interfaces (APIs), 69
 applications

- backing up, 383
- exploitation of, 76–77
- updating, 436

 apropos utility, 174
 archiving keys, 352–354, 352
 armored viruses, 82
 ARO (annualized rate of occurrence), 274–275
 ARP (Address Resolution Protocol), 65
 assets

- identifying, 34–35
- in ISO 17799 standard, 279
- valuing, 36

 asymmetric cryptographic algorithms, 313–315, 314
 ATT Wireless NOCs, 108
 attacks

- on cryptographic systems, 330–332
- practical application, 464–466
- recognizing, 57
 - back door, 57–58, 58
 - man-in-the-middle, 59–60, 60
 - password-guessing, 61
 - replay, 60, 61
 - response in, 62
 - spoofing, 58–59, 59
- strategies, 52–57
 - access, 53–54
 - DoS, 55–57, 56
 - modification, 55
- on TCP/IP, 70–74, 72–74

 auditing

- IDSs for, 180
- practical application, 470–471
- in privilege management, 405–407
- processes and files, 90–91
- proxy firewalls for, 113

 auditors, 285
 authentication, 16, 127

- biometric devices, 21

certificates, 17–18, 18
 CHAP, 17
 in cryptographic systems, 318–319
 of evidence, 422
 factors, 460–461
 issues in, 21–22
 Kerberos, 18–19, 20
 multi-factor, 19, 20, 22
 mutual, 460–461
 PAP, 17
 practical application, 460
 protection, 462
 RADIUS, 130–131, 131
 security tokens, 18, 19
 smart cards, 19, 21, 21, 154
 usernames and passwords, 16
 Authenticode method, 137
 Automatic Private IP Addressing (APIPA)

- addresses, 237

 availability

- as design goal, 25
- fault tolerance in, 375
- RAID for, 375–378, 376
- redundancy in, 373–375, 374

 awareness and education, 433–435, 457

B

back door attacks, 57–58, 58, 466
 Back Orifice tool, 58
 background investigations, 396–397
 backup operators, 15
 backup power, 268
 Backup Server method, 385–387, 386
 backup sites, 388–390
 backups

- in disaster recovery, 378–387, 382
- policies for, 428
- practical application, 488–489

 bait messages, 195
 barriers, 255–256, 255–256

- partitioning, 259–260, 260
- perimeter security, 256–257, 257
- security zones, 257–259, 259

 baseband signaling, 143, 144
 baselines

- for IDSs, 176

- in network security, 215–217
- practical application, 482–483
- .bat extension, 196
- BCM (Business Continuity Management), 280
- BCP. *See* Business Continuity Planning (BCP)
- Bell La-Padula model, 286, 286
- best practices, 426
 - allocating resources, 431
 - defining responsibilities, 431
 - enforcing policies and procedures, 432
 - minimizing mistakes, 431–432
 - policies and procedures for, 426–430
- beta tests, 282
- BGP (Border Gateway Protocol), 116
- BIA (Business Impact Analysis), 272–273
- Biba model, 287, 287
- binding, network, 218, 219
- biometric devices, 21, 261–262
- birthday attacks, 331
- Black Viper, 463
- blind FTP, 139–140
- block ciphers, 312
- Blowfish encryption, 313
- bombs, 85–86, 86
- bootable operating systems, 487
- Border Gateway Protocol (BGP), 116
- border routers, 114
- Boyce, Christopher, 263
- bribery, 263
- bridge trust models, 327–328, 328
- broadband signaling, 143, 144
- broadcasts
 - in IGMP, 142
 - in IM, 195
- brute force attacks
 - on codes, 310
 - on encryption, 487
 - on passwords, 61, 468
- budget issues, 431
- buffer overflows, 56, 137–138
- Business Continuity Management (BCM), 280
- Business Continuity Planning (BCP), 271–272, 371
 - Business Impact Analysis, 272–273
 - disaster recovery in. *See* disaster recovery
 - high availability in, 372–377
 - risk assessment in, 273–275
 - utilities in, 371–372

- Business Impact Analysis (BIA), 272–273
- business policies, 397–398
- businesses
 - topologies for, 34–39
 - VLANs for, 35

C

- cabling, 142
 - coaxial, 142–145, 143–145
 - UTP and STP, 146–147, 146–147
- cache poisoning, 234
- CALEA (Communications Assistance for Law Enforcement Act), 479
- Canonical Names (CNs), 239
- CAs (certificate authorities), 17
 - for Certificate policies, 398–400, 400
 - in hierarchical trust models, 326–327, 328–329
 - for non-repudiation, 319
 - in PKI, 321, 322
- CAST encryption, 313
- Categories, cable, 146–147
- CBFs (critical business functions), 271
- CC (Common Criteria) standard, 215, 345
- CCITT (Comite Consultatif International Telephonique et Telegraphique), 335
- CD Recordable (CD-R) technology, 152–153
- CEH (Certified Ethical Hacker), 464
- cell networks, 149–150, 150
- cell phones, 264–265
- Center for Education and Research in Information Assurance and Security (CERIAS), 437
- Central Office (CO), 120
- centralized key generation, 346–347, 347
- CERT/CC Current Activity web page, 84
- CERT Coordination Center (CERT/CC), 213–215, 437
- CertCities magazine, 438
- certificate authorities (CAs), 17
 - for Certificate policies, 398–400, 400
 - in hierarchical trust models, 326–327, 328–329
 - for non-repudiation, 319
 - in PKI, 321, 322

536 Certificate Management Protocols (CMP) – continuity

- Certificate Management Protocols (CMP), 339
- Certificate Practice Statements (CPSs), 17, 325, 400
- Certificate Revocation Lists (CRLs), 17, 325–326
- certificates, 321
 - in authentication, 17–18, 18
 - in PKI, 324–326
 - policies for, 398–400, 400
 - practical application, 484–485
 - revoking, 325–326
- Certified Ethical Hacker (CEH), 464
- CESA (Cyberspace Electronic Security Act), 442
- CGI (Common Gateway Interface), 138
- chain of custody, 187, 423–424
- Challenge Handshake Authentication Protocol (CHAP), 17, 17, 128
- change documentation, 430
- checksums
 - in hashing, 307
 - in IDSs, 183
 - in integrity, 316
- chip creep, 267
- CIO magazine, 438
- ciphers
 - block and stream, 312
 - substitution, 304
 - transposition, 304–305, 305
- circuit-level proxies, 113
- Clark-Wilson model, 287–288, 288
- classification, information. *See* information security
- client/server authentication, 127
- Clipper system, 351
- clustering, 374–375, 374
- CMP (Certificate Management Protocols), 339
- CNs (Canonical Names), 239
- CO (Central Office), 120
- coaxial cable, 142–145, 143–145
- code escrow, 392–393
- cold sites, 389
- collecting evidence, 425
- collusion, 397
- .com extension, 196
- Comite Consultatif International Telephonique et Telegraphique (CCITT), 335
- Common Criteria (CC) standard, 215, 345
- Common Gateway Interface (CGI), 138
- communication security, 471–472
 - dial-up, 472–473
 - directory services, 476–477
 - e-mail, 474–475
 - file sharing, 477–478
 - Internet, 475–476
 - remote control, 473–474
 - VPNs, 473
 - wireless, 478–479
- communications
 - in ISO 17799 standard, 280
 - media in. *See* transmission media
 - for security awareness, 433–435
- Communications Assistance for Law Enforcement Act (CALEA), 479
- companion viruses, 83
- compartmentalization, 396
- compliance in ISO 17799 standard, 280
- compromising DNS record integrity, 235
- computer forensics, evidence in, 420
 - acquiring, 421–422
 - analyzing, 422
 - authenticating, 422
 - chain of custody in, 423–424
 - collecting, 425
 - preserving, 424
- Computer Fraud and Abuse Act, 441
- Computer Professionals for Social Responsibilities (CPSR), 395
- Computer Security Act, 442
- Computer Security Institute (CSI), 437
- computers, selling, 355, 428
- confidential information, 11, 283
- confidentiality
 - in cryptographic systems, 315
 - as design goal, 25
- configuration
 - changes to, 181, 182
 - network protocols, 218–220
 - policies for, 429
 - routers and firewalls, 230–231
- connection-oriented protocols, 69
- connectivity. *See* infrastructure and connectivity
- connectors, 142–143, 143–145
- continuity. *See* Business Continuity Planning (BCP)

cookies, 138
 core dumps, 350
 CPSR (Computer Professionals for Social Responsibilities), 395
 CPSs (Certificate Practice Statements), 17, 325, 400
 credit card information, 341
 criteria in standards, 277
 critical business functions (CBFs), 271
 critical functions in BIA, 272
 critical information losses, recovering from, 6
 CRLs (Certificate Revocation Lists), 17, 325–326
 cross certification, 325
 cryptanalysts, 303
 cryptographers, 303
 cryptography, 303, 483–484
 algorithms, 310
 asymmetric, 313–315, 314
 attacks on, 330
 hashing, 310–311
 symmetric, 312–313, 312
 certificates, 484–485
 exam essentials, 358–360
 hands-on labs, 361–362
 mathematical, 306–307, 306
 myth of unbreakable codes, 309–310
 physical, 304
 quantum, 308–309, 309
 review questions, 363–368
 standards and protocols, 332
 CC, 345
 CMP, 339
 FIPS, 344
 government agencies in, 333
 HTTPS, 343–344
 industry associations in, 334–336
 IPSec, 344
 ISO 17799, 345
 key management. *See* keys
 PGP, 343, 343
 PKIX/PKCS, 336–337
 Public Domain Cryptography, 336
 S-HTTP, 344
 S/MIME, 340
 SET, 340
 SSH, 340–342, 342
 SSL and TLS, 338–339
 WEP, 345

WTLS, 345
 X.509 standard, 337–338
 steganography, 305–306
 substitution ciphers, 304
 summary, 356–358
 systems
 access control in, 319–320
 attacks on, 330–332
 authentication in, 318–319
 confidentiality in, 315
 digital signatures in, 316–318, 317
 hybrid, 306
 integrity of, 315–316, 316–317
 non-repudiation in, 319
 PKI. *See* PKI (Public Key Infrastructure)
 transposition ciphers, 304–305, 305
 CSI (Computer Security Institute), 437
 CSO Magazine, 438
 current keys, 353
 custodians of information, 284–285
 Cyber Security Enhancement Act, 442
 Cyberspace Electronic Security Act (CESA), 442

D

DAC (Discretionary Access Control) model, 15, 408, 459
 Daemen, Joan, 313
 Data Encryption Standard (DES), 312
 data repositories, hardening, 238–241, 238
 data sources in IDSs, 175
 databases
 backing up, 381–382, 382
 exploitations, 76
 hardening, 240–241
 DDoS (distributed DoS) attacks, 56–57, 56
 decentralized key generation, 348, 348
 deception in active responses, 182, 183
 decision making in privilege management, 404–405
 demilitarized zones (DMZs), 30–31, 30
 denial of service (DoS) attacks, 55–57
 on DNS servers, 235
 flaw-exploitation, 466
 TCP SYN floods, 72–73, 72

538 DES (Data Encryption Standard) – EDGAR site

- DES (Data Encryption Standard), 312
 - desensitizing process, 268–269
 - design
 - requirements, 10
 - security zones, 31
 - topologies, 25–27
 - destroying
 - information, 427
 - keys, 355
 - policies for, 398
 - detection, 6, 13
 - DHCP (Dynamic Host Configuration Protocol) services, 237
 - diaries in computer forensics, 422
 - dictionary attacks, 61, 468
 - differential backups, 383–384
 - Diffie-Hellman encryption, 314
 - Digital Signature Algorithm (DSA), 315
 - digital signatures
 - in applets, 137
 - in cryptographic systems, 313–318, 317
 - Direct-Sequence Spread Spectrum (DSSS) technology, 192
 - directory services
 - hardening, 238–239, 238
 - practical application, 476–477
 - directory sharing, 236–237, 236
 - disabling services and protocols, 231
 - disaster recovery, 378
 - backups for, 378–381
 - DRPs for, 10, 381
 - alternate sites in, 388–390
 - auditing, 407
 - backup plans in, 381–387, 382
 - system recovery in, 387–388, 387
 - planning, 489
 - Discretionary Access Control (DAC) model, 15, 408, 459
 - disk duplexing, 375
 - disk mirroring, 375
 - disk striping, 375
 - disk striping with parity, 376
 - disk wiping, 427
 - diskettes, 153
 - Distinguished Names (DNs), 239
 - distributed DoS (DDoS) attacks, 56–57, 56
 - distributing keys, 348–350, 349
 - DMZs (demilitarized zones), 30–31, 30
 - DNs (Distinguished Names), 239
 - DNS (Domain Name Service), 23, 64
 - DNS (Domain Name Service) servers,
 - hardening, 234–235
 - DNS spoofing, 58
 - Document Disposal and Destruction policies, 398
 - documentation
 - incident responses, 190
 - practical application, 532
 - Domain Name Service (DNS), 23, 64
 - Domain Name Service (DNS) servers,
 - hardening, 234–235
 - DoS (denial of service) attacks, 55–57
 - on DNS servers, 235
 - flaw-exploitation, 508
 - TCP SYN floods, 72–73, 72
 - DRPs (disaster recovery plans), 10, 381
 - alternate sites in, 388–390
 - auditing, 407
 - backup plans in, 381–387, 382
 - system recovery in, 387–388, 387
 - DSA (Digital Signature Algorithm), 315
 - DSSS (Direct-Sequence Spread Spectrum) technology, 192
 - dual-homed firewalls, 112–113, 112
 - Due Care policies, 397–398
 - dumpster diving, 53
 - duplexing, 375
 - Dynamic Host Configuration Protocol (DHCP) services, 237
-
- E**
- e-mail, 22–23, 133–134, 133
 - encapsulation in, 66–67, 66–67
 - exploitation of, 77
 - incidents with, 189
 - practical application, 474–475
 - viruses in, 80, 81
 - e-mail servers, hardening, 233, 233
 - EALs (Evaluation Assurance Levels), 215–217
 - eavesdropping, 53
 - eBay, non-repudiation in, 320
 - ECC (Elliptic Curve Cryptography), 265, 314–315
 - EDGAR site, 197

- eDirectory, 169, 224, 239
 - education, 433–435
 - EICAR (European Institute for Computer Anti-Virus Research), 438
 - 8.3 file format, 195–196
 - 802.1X protocols, 117, 130, 192
 - El Gamel encryption, 315
 - electromagnetic interference (EMI), 268–269, 269
 - electronic wallets, 340, 341
 - electronic watermarking, 306
 - Elliptic Curve Cryptography (ECC), 265, 314–315
 - EMI (electromagnetic interference), 268–269, 269
 - enabling services and protocols, 231
 - encapsulation
 - in TCP/IP, 66–67, 66–67
 - in tunneling, 34
 - encryption. *See* cryptography
 - end-entity certificates, 337
 - End User License Agreements (EULAs), 281
 - enforcing policies and procedures, 432
 - Enigma machine, 306
 - enticement, 185
 - entrapment, 185
 - environment
 - fire suppression, 270–271, 271
 - in ISO 17799 standard, 280
 - location, 265–268
 - shielding, 268–269, 269
 - wireless cells, 264–265, 264
 - escalation
 - auditing, 407
 - in incident response, 187
 - privilege, 403
 - escrow systems
 - code, 392–393
 - key management, 350–351
 - ethical hacking, 464
 - ethics policies, 394–395
 - EU (European Union) laws, 443–444
 - EULAs (End User License Agreements), 281
 - European Institute for Computer Anti-Virus Research (EICAR), 438
 - European Union (EU) laws, 443–444
 - evaluating security, 261
 - Evaluation Assurance Levels (EALs), 215–217
 - Event Viewer, 221, 221
 - events in IDSs, 175–176
 - evidence, 186–187
 - acquiring, 421–422
 - analyzing, 422
 - authenticating, 422
 - chain of custody, 423–424
 - collecting, 425
 - preserving, 424
 - exam essentials
 - cryptography, 358–360
 - hardening, 243
 - infrastructure and connectivity, 156
 - monitoring, 199–200
 - network and environment security, 291–292
 - policies and procedures, 409–410
 - risk identification, 92–94
 - security concepts, 40–42
 - security management, 445–446
 - exception statements in policies, 276
 - .exe extension, 196
 - executable scripts, 232
 - expiration dates, key management, 351
 - Extensible Markup Language (XML), 135
 - extension types
 - in software exploitation, 78
 - working with, 195–196
 - external threats, 37, 38
 - extranets, 29–30, 30
 - extrusion, 29
-
- F**
- faillog file, 184
 - failover in high availability, 373
 - Family Educational Rights and Privacy Act (FERPA), 441
 - Faraday Cages, 268
 - FAT (File Allocation Table), 225
 - fault tolerance, 375
 - Federal Information Processing Standard (FIPS), 344
 - FERPA (Family Educational Rights and Privacy Act), 441
 - FHSS (Frequently-Hopping Spread Spectrum) technology, 192
 - fiber optic technology, 147–148, 148

540 File Allocation Table (FAT) – GUIDs (globally unique identifiers)

File Allocation Table (FAT), 225
 File Transfer Protocol (FTP), 23–24, 64, 139–140
 File Transfer Protocol (FTP) servers, hardening, 234
 files
 hardening, 236–237, 236
 naming, 195–196
 sharing, 140, 236–237, 236, 477–478
 transferring, 140
 filesystems, hardening, 225–228, 227
 filters for web servers, 232
 Financial Modernization Act, 440–441
 FIPS (Federal Information Processing Standard), 344
 fire corridors, 260
 fire extinguishers, 270
 fire suppression, 266, 270–271, 271
 fireproof storage, 380
 firewalls, 109–110, 110
 configuring, 230–231
 for IDSs, 178–179, 179
 packet filter, 110
 proxy, 110–114, 112
 stateful inspection, 113–114
 five nines availability, 373
 fixed fire suppression systems, 270–271, 271
 Flash cards, 153
 flaw-exploitation attacks, 466
 flood damage, 266
 floods
 SYN, 72–73, 72
 UDP, 74
 flushed disk data, 421
 footprinting
 DNS servers, 235
 in signal intelligence, 197–198
 forensics, evidence in, 420
 acquiring, 421–422
 analyzing, 422
 authenticating, 422
 chain of custody in, 423–424
 collecting, 425
 preserving, 424
 frequency analysis in code breaking, 309
 Frequently-Hopping Spread Spectrum (FHSS) technology, 192

FTP (File Transfer Protocol), 23–24, 64, 139–140
 FTP (File Transfer Protocol) servers, hardening, 234
 FTP ports with firewalls, 111
 Full Archival backup method, 385, 386
 full backups, 383
 full distributions, 282

G

G8 nations, laws by, 443–444
 gaps in the WAP, 193, 479
 gas-based fire suppression systems, 271
 General Security Concepts, 458
 access control, 459
 accountability, 459
 auditing, 470–471
 authentication, 460–462
 malicious events, 464–470
 system hardening, 462–464
 GFS (Grandfather-Father-Son) rotation system, 152, 384–385, 385
 Global Information Assurance Certification (GIAC), 464
 Global System for Mobile Communications (GSM), 265
 globally unique identifiers (GUIDs), 403
 goals
 design, 25–27
 information security, 13–14
 Good Time virus, 84
 government classifications, 283–284
 governmental agency encryption standards, 333
 Gramm-Leach-Bliley Act, 440–441
 Grandfather-Father-Son (GFS) rotation system, 152, 384–385, 385
 granularity in PKI trust models, 326
 greed, 263
 group management, 401–402, 402
 GroupWise tool, 169
 GSM (Global System for Mobile Communications), 265
 guidelines, 278
 GUIDs (globally unique identifiers), 403

H

- H-IDS (host-based IDS), 183, 184
- hallways, 260
- Halon gas, 271
- hands-on labs
 - cryptography, 361–362
 - hardening, 244–245
 - infrastructure and connectivity, 157
 - monitoring, 201–203
 - network and environment security, 293
 - policies and procedures, 411–412
 - risk identification and assessment, 95–96
 - security concepts and process, 43
 - security management, 447
- handshakes, 69, 69
- hard drives, 153
- hardening, 213, 217
 - Apple Macintosh, 225
 - data repositories, 238–241, 238
 - DHCP services, 237
 - DNS servers, 234–235
 - e-mail servers, 233, 233
 - exam essentials, 243
 - file and print servers and services, 236–237, 236
 - filesystems, 225–228, 227
 - FTP servers, 234
 - hands-on labs, 244–245
 - Microsoft Windows 2000, 220–222, 221
 - Microsoft Windows XP, 222
 - network devices, 229–231
 - NNTP servers, 235–236
 - Novell NetWare, 224–225
 - operating system updating, 228–229
 - practical application, 462–464
 - protocol configuration in, 218–220
 - review questions, 246–251
 - servers, 125–126
 - summary, 241–242
 - Unix/Linux, 223–224
 - web servers, 232
 - Windows Server 2003, 222–223
- hardware-based keystroke loggers, 487
- hardware components, 106–107, 106
- hash values, 306
- hashing
 - cryptographic algorithms for, 310–311
 - overview, 306–307, 306
 - reverse hash matching, 468
- Health Insurance Portability and Accountability Act (HIPAA), 440
- Heisenberg Uncertainty Principle, 308
- Hellman, M. E., 314
- hierarchical trust models, 326–327, 327
 - bridge, 327–328, 328
 - hybrid, 329, 329
 - mesh, 328–329, 328
- high availability
 - as design goal, 25
 - fault tolerance in, 375
 - RAID for, 375–378, 376
 - redundancy in, 373–375, 374
- hijacking attacks, 73–74, 74, 466
- HIPAA (Health Insurance Portability and Accountability Act), 440
- hiring policies, 393–394
- hoaxes, 84
- honey pots
 - in deception, 182, 183
 - practical application, 482
 - using, 184–185
- Honeynet Project, 185
- host-based IDS (H-IDS), 183, 184
- Host-to-Host layer, 64–65
- hosts in TCP/IP, 63
- hot sites, 10, 388
- hotfixes, 228
- HTML (Hypertext Markup Language), 64, 134
- HTTP (Hypertext Transfer Protocol), 64
- HTTP ports with firewalls, 111
- HTTP/S (HTTP Secure) protocol, 136
- HTTPS ports with firewalls, 111
- hubs
 - for IDSs, 179, 179
 - security for, 114
- human errors in code breaking, 310
- human resources
 - in ISO 17799 standard, 280
 - policies for, 393–397
- humidity control, 266
- hybrid attacks, 468

542 hybrid cryptography systems – infrastructure and connectivity

- hybrid cryptography systems, 306
 - hybrid trust models, 329, 329
 - Hypertext Markup Language (HTML), 64, 134
 - Hypertext Transfer Protocol (HTTP), 64
 - Hypertext Transport Protocol Secure (HTTPS), 343–344
-
- I**
- I&A (Identification and Authentication)
 - process, 16
 - IANA (Internet Assigned Numbers Authority), 67
 - ICMP (Internet Control Message Protocol), 23
 - alerts for, 175
 - attacks in, 74–75
 - in Internet layer, 65
 - for ping of death attacks, 56
 - for Smurf Attacks, 75, 141
 - stateful inspection firewalls for, 113
 - tunneling in, 75
 - IDEA (International Data Encryption Algorithm), 313
 - identification
 - asset, 34–35
 - in incident responses, 187
 - risk. *See* risk identification and assessment
 - threat, 36–38, 37
 - Identification and Authentication (I&A)
 - process, 16
 - IDSs (intrusion detection systems), 124, 124, 174–175
 - host-based, 183, 184
 - incident responses in, 186–191
 - network-based, 178–182, 179, 181–183
 - practical application, 482
 - terms for, 175–178, 177
 - IEEE (Institute of Electrical and Electronics Engineers), 335–336
 - IEEE 802.1X protocols, 117, 130, 192
 - IETF (Internet Engineering Task Force), 334
 - IGMP (Internet Group Management Protocol), 65, 142
 - ignoring attacks, 180
 - IM (Instant Messaging), 23, 194–195, 194
 - IMAP (Internet Message Access Protocol), 134
 - IMAP ports with firewalls, 111
 - impact analysis in BIA, 272–273
 - Incident Response Plans (IRPs), 186, 190
 - incident responses, 186–187
 - adjusting procedures, 190–191
 - documenting, 190
 - identifying incidents, 187
 - policies for, 400–401
 - practical application, 490
 - repairing damage, 188–189
 - incidents, 13, 400. *See also* evidence
 - incremental backups, 383
 - industry association encryption standards, 334–336
 - info utility, 174
 - Info World magazine, 439
 - Information Flow model, 288–289, 288
 - information security, 3–4, 4
 - classification in, 280, 281
 - access control in, 285–289, 286–289
 - full distribution, 282
 - government and military, 283–284
 - internal information, 283
 - limited distribution, 281–282
 - policies for, 426
 - private information, 282–283
 - public information, 281
 - restricted information, 283
 - roles in, 284–285
 - destruction in, 427
 - operational security, 7–9, 8
 - physical security, 5–7
 - policies for, 11, 426–427
 - retention and storage in, 427
 - Information Security Magazine, 439
 - Information Week magazine, 439
 - infrared (IR) communications, 148
 - infrastructure and connectivity, 105–106
 - exam essentials, 156
 - firewalls, 109–114, 110, 112
 - hands-on labs, 157
 - hardware components, 106–107, 106
 - hubs, 114
 - IDSs, 124, 124
 - Internet, 132
 - e-mail, 133–134, 133
 - ports and sockets, 132–133, 132

- Web, 134–135, 135
- Web add-Ins, 136–139
- mobile devices, 127, 127
- modems, 119
- network monitors, 123–124
- RAS 110, 120
- remote access, 128–131, 128, 131
- removable media, 151–154
- review questions, 158–163
- routers, 114–116, 115
- software components, 108
- summary, 154–155
- switches, 116, 116
- TCP/IP protocols, 141–142
- telecom/PBX systems, 120–122, 121
- transmission media. *See* transmission media
- VPNs, 122–123, 122
- WAPs, 117–118, 117
- workstations and servers, 125–126
- infrastructure security, 479–481
 - baselines, 482–483
 - IDSs and honey pots, 482
 - security zones, 481–482
- Initial Sequence Numbers (ISNs), 69
- Instant Messaging (IM), 23, 194–195, 194
- Institute of Electrical and Electronics Engineers (IEEE), 335–336
- intangible impact analysis in BIA, 273
- Integrated Services Digital Network (ISDN), 128, 128
- integrity
 - cryptographic systems, 315–316, 316–317
 - as design goal, 25
- interactive users in Unix, 342
- interception, 53–54, 331
- interference, 268–269, 269
- intermediate CAs, 327, 327
- internal information, 11, 283
- internal threats, 37–38, 37
- International Data Encryption Algorithm (IDEA), 313
- international efforts, 443–444
- International Telecommunications Union (ITU), 335
- Internet, 28–29, 28, 132
 - e-mail, 133–134, 133
 - ports and sockets, 132–133, 132
 - practical application, 475–476
 - Web, 134–135, 135
 - Web add-Ins, 136–139
- Internet Assigned Numbers Authority (IANA), 67
- Internet Control Message Protocol. *See* ICMP (Internet Control Message Protocol)
- Internet Engineering Task Force (IETF), 334
- Internet Group Management Protocol (IGMP), 65, 142
- Internet layer, 65
- Internet Message Access Protocol (IMAP), 134
- Internet Protocol (IP), 65
- Internet Protocol Security (IPSec), 122, 130, 344, 473
- Internet Society (ISOC), 334–335
- Internetwork Packet Exchange (IPX) protocol, 169
- intranets, 29, 29
- intrusion detection systems (IDSs), 124, 124, 174–175
 - host-based, 183, 184
 - incident responses in, 186–191
 - network-based, 178–182, 179, 181–183
 - practical application, 482
 - terms for, 175–178, 177
- inventory policies, 429
- investigating incidents, 187–188. *See also* evidence
- IP (Internet Protocol), 65
- IP addresses, invalid, 237
- IP spoofing, 58
- IPCONFIG program, 123
- IPSec (IP Security), 122, 130, 344, 473
- IPX (Internetwork Packet Exchange) protocol, 169
- IPX/SPX protocol, hardening, 220
- IR (infrared) communications, 148
- Irina virus, 84
- IRPs (Incident Response Plans), 186, 190
- ISDN (Integrated Services Digital Network), 128, 128
- ISNs (Initial Sequence Numbers), 69
- ISO 17799 standard, 279–280, 345
- ISOC (Internet Society), 334–335
- ITU (International Telecommunications Union), 335
- IUSR_ accounts, 234

J

jamming in IM, 195
 Java applets, 136–137
 JavaScript language, 136
 .js extension, 196

K

KDCs (Key Distribution Centers), 19,
 348–349, 349
 KEA (Key Exchange Algorithm), 348–349,
 349
 Kerberos authentication, 18–19, 20
 Key Distribution Centers (KDCs), 19,
 348–349, 349
 Key Exchange Algorithm (KEA), 348–349,
 349
 key rollover, 354
 keys, 320, 346
 in asymmetric cryptographic algorithms,
 313
 attacks on, 330
 centralized generation, 346–347, 347
 decentralized generation, 348, 348
 destroying, 355
 escrow systems for, 350–351
 expiration dates, 351
 practical application, 485–486
 private key protection, 350
 recovering and archiving, 352–354, 352
 renewing, 354
 revoking, 351–352
 storing and distributing, 348–350, 349
 suspending, 352
 in symmetric cryptographic algorithms, 312
 usage, 355
 keystroke loggers, 487
 Klez32 virus, 87

L

L2F (Layer 2 Forwarding) protocol, 129
 L2TP (Layer 2 Tunneling Protocol), 122, 129,
 473

labels in MAC, 15
 labs, 457
 LAN framing, translating to WAN framing,
 114
 laptops, SLAs for, 392
 lastlog file, 184
 latency in CRLs, 326
 law enforcement, 186, 425
 Layer 2 Forwarding (L2F) protocol, 129
 Layer 2 Tunneling Protocol (L2TP), 122, 129,
 473
 LCP (Link Control Protocol), 129
 LDAP (Lightweight Directory Access
 Protocols), 239
 LDAP ports with firewalls, 111
 leaf CAs, 327, 327
 Lee, Daulton, 263
 limited distribution information, 281–282
 Link Control Protocol (LCP), 129
 Linux
 hardening, 223–224
 log files in, 184
 security information, 174
 local registration authorities (LRAs),
 322–323, 323
 location
 environment, 265–268
 power systems, 267–268
 locking down desktops, 125
 logic bombs, 85–86, 86
 logon process, 16, 16
 logs
 attacks on, 90–91
 audit, 470–471
 Event Viewer, 221, 221
 with IDSs, 179–180
 in Linux, 184, 224
 policies for, 429
 LRAs (local registration authorities),
 322–323, 323

M

M of N Control method, 353
 MAC (Mandatory Access Control), 15,
 407–408, 459
 MAC (Media Access Control) addresses, 65

- MAC (message authentication code), 316, 317
 - Macintosh, hardening, 225
 - macro viruses, 83
 - magnetic tape, 151–152
 - mail services. *See* e-mail
 - maintenance contracts, 391
 - maintenance requirements in standards, 278, 280
 - malicious code, 78
 - antivirus software for, 87, 467–468
 - in IM, 195
 - logic bombs, 85–86, 86
 - practical application, 464–470
 - Trojan horses, 85
 - viruses, 78–85, 80–83
 - worms, 86
 - man-in-the-middle attacks, 59–60, 60, 466
 - man tool, 174
 - Managed Security Service Providers (MSSPs), 108
 - managers
 - in IDSs, 176
 - and policies, 9–13
 - training, 434
 - Mandatory Access Control (MAC), 15, 407–408, 459
 - mantraps, 256, 256
 - mathematics in cryptographic systems, 306–307, 306, 332
 - McAfee Corporation, 438
 - MD-IDSs (misuse-detection IDSs), 176, 177
 - MD5 algorithm, 311
 - MDA (Message Digest Algorithm), 311
 - Mean Time Between Failure (MTBF), 391
 - Mean Time To Repair (MTTR), 392
 - media
 - network, 105
 - transmission. *See* transmission media
 - Media Access Control (MAC) addresses, 65
 - memory dumps, 350
 - memory sticks, 153
 - mesh trust model, 328–329, 328
 - message authentication code (MAC), 316, 317
 - Message Digest Algorithm (MDA), 311
 - message digests, 318
 - messages file, 184
 - Metal Oxide Varistors (MOV), 267
 - Microsoft FAT, 225
 - Microsoft NTFS, 226
 - Microsoft protocols, network traffic with, 170–172, 171
 - Microsoft systems, hardening
 - Windows 2000, 220–222, 221
 - Windows XP, 222
 - Microsoft TechNet website, 221
 - microwave systems, 117, 149–150, 150
 - military classifications, 283–284
 - mistakes, minimizing, 431–432
 - misuse-detection IDSs (MD-IDSs), 176, 177
 - Mitnick, Kevin, 263, 470
 - mobile devices, 127, 127
 - modems, 119, 472
 - modification attacks, 55
 - monitoring, 167–168, 432
 - 8.3 file naming, 195–196
 - exam essentials, 199–200
 - hands-on labs, 201–203
 - IDSs for. *See* IDSs (intrusion detection systems)
 - instant messaging, 194–195, 194
 - mechanisms, 173, 173
 - network traffic types, 168–173
 - packet sniffing, 196–197
 - review questions, 204–209
 - signal analysis and intelligence, 197–198
 - summary, 198–199
 - wireless systems, 191–194, 191, 193
 - monitors, 123–124
 - MOV (Metal Oxide Varistors), 267
 - MSSPs (Managed Security Service Providers), 108
 - MTBF (Mean Time Between Failure), 391
 - MTTR (Mean Time To Repair), 392
 - multi-factor authentication, 19, 20, 22
 - multicasts, 142
 - multihomed systems, 112
 - multipartite viruses, 82, 83
 - multiple barrier systems, 255
 - mutations, virus, 80
 - mutual authentication, 460–461
 - myth of unbreakable codes, 309–310
-
- N**
- N-IDSs (network-based IDSs), 178–182, 179, 181–183

546 NAT (Network Address Translation) – nonessential protocols and services

- NAT (Network Address Translation), 32–33, 33
- National Institute of Standards and Technology (NIST), 333, 438
- National Security Agency (NSA), 333
- National Security Agency/Central Security Service (NSA/CSS), 333
- National Security Institute (NSI), 438
- NCP (Network Control Protocol), 129
- NDAs (nondisclosure agreements), 282
- NDS (NetWare Directory Services), 169, 170, 224
- need-to-know information, 283
- Need to Know policies, 396
- NetBEUI (NetBIOS Extended User Interface) protocol, 171, 171, 219–220
- NetBIOS (Network Basic Input Output System) protocol, 171, 218–220, 219
 - firewall ports, 111
 - services, 24
- NetBus tool, 58
- NetMeeting program, 24, 134
- NetWare, hardening, 224–225
- NetWare Directory Services (NDS), 169, 170, 224
- NetWare File System, 226
- NetWare Loadable Modules (NLMs), 224
- Network Address Translation (NAT), 32–33, 33
- network and environment security
 - baselines in, 215–217
 - Business Continuity Planning, 271–275
 - exam essentials, 291–292
 - guidelines, 278
 - hands-on labs, 293
 - hardening in. *See* hardening
 - information classification. *See* information security
 - information security
 - physical, 5–7, 254
 - access control, 254–261
 - environment, 264–271, 264
 - in ISO 17799 standard, 280
 - social engineering, 261–263
 - policies, 275–277
 - review questions, 294–299
 - standards, 277–279
 - summary, 289–291
 - threats, 213–215
- network audit files, 180
- network-based IDSs (N-IDSs), 178–182, 179, 181–183
- Network Basic Input Output System (NetBIOS) protocol, 171, 218–220, 219
 - firewall ports, 111
 - services, 24
- Network Control Protocol (NCP), 129
- network devices
 - hardening, 229–231
 - updating, 436
- Network File System (NFS), 24, 172, 172, 226
- Network Interface layer, 66
- network monitors, 123–124
- Network News Transfer Protocol (NNTP), 23
- Network News Transfer Protocol (NNTP) servers, hardening, 235–236
- network operating systems, hardening. *See* hardening
- Network Operations Centers (NOCs), 108
- network protocols, configuring, 218–220
- network sniffers, 70–71, 123–124, 145, 196–197
- network traffic types, 168
 - Microsoft protocols, 170–172, 171
 - Network Files System, 172, 172
 - Novell protocols, 169, 170
 - TCP/IP, 168
- networks
 - binding, 218, 219
 - configuration changes, 181, 182
 - Internet. *See* Internet
 - virus transmission on, 84
- New Technology File System (NTFS), 226
- newsgroup servers, hardening, 235–236
- newsgroups, 23
- NFS (Network File System), 24, 172, 172, 226
- NIST (National Institute of Standards and Technology), 333, 438
- NLMs (NetWare Loadable Modules), 224
- NNTP (Network News Transfer Protocol), 23
- NNTP (Network News Transfer Protocol) servers, hardening, 235–236
- NNTP ports with firewalls, 111
- NOCs (Network Operations Centers), 108
- non-repudiation, 55, 319
- nondisclosure agreements (NDAs), 282
- nonessential protocols and services, 23–24

Noninterference model, 289, 289
 NOSs, hardening. *See* hardening
 notifications
 in IDSs, 176, 180
 policies for, 426
 Novell Directory Services, 169
 Novell NetWare, hardening, 224–225
 Novell NetWare File System, 226
 Novell protocols, network traffic with, 169, 170
 NSA (National Security Agency), 333
 NSA/CSS (National Security Agency/Central Security Service), 333
 NSI (National Security Institute), 438
 NTFS (New Technology File System), 226

O

OCSP (Online Certificate Status Protocol), 326
 OFDM (Orthogonal Frequency Division Multiplexing), 192
 offsite storage, 381
 old computers, selling, 355, 428
 one-tier database models, 241
 one-time pads, 318, 318
 one-way processes, 307
 Online Certificate Status Protocol (OCSP), 326
 onsite storage, 380
 open relays, 139
 Open Shortest Path First (OSPF) protocol, 116
 open source programs, 224
 operating systems
 hardening. *See* hardening
 updating, 228–229, 436
 operation/organizational security, 7–9, 8, 487
 backups, 488–489
 disaster planning, 489
 documentation, 490
 incident handling, 490
 personnel management, 489–490
 physical, 487–488
 operational considerations in guidelines, 278
 operations management in ISO 17799 standard, 280
 operators in IDSs, 176
 organization in ISO 17799 standard, 279
 organizational security policies, 426

Orthogonal Frequency Division Multiplexing (OFDM), 192
 OS hardening. *See* hardening
 OSPF (Open Shortest Path First) protocol, 116
 out-of-band method for keys, 312
 overflows, buffer, 56, 137–138
 overview statements in policies, 276
 owners of information, 284

P

packet-capture devices, 129
 packet filter firewalls, 110
 packet sniffing, 196–197
 packets, TCP, 132, 133
 Panda Software site, 83
 PAP (Password Authentication Protocol), 17
 partitioning, 259–260, 260
 PASS method, 270
 passive interception, 53
 passive responses, 179–180
 Password Authentication Protocol (PAP), 17
 password-generation systems, 307–308
 passwords, 16
 attacks on, 61, 330, 468–469
 for FTP, 140
 and social engineering, 88
 strong, 468–469
 patches, 229
 Patriot Act, 442–443
 PDAs (Personal Digital Assistants), 127
 penetrations, detecting, 6
 performance criteria in standards, 277
 Performance Monitor, 221
 perimeter security, 167, 256–257, 257
 personal development, 436–437
 Personal Digital Assistants (PDAs), 127
 personnel security
 in ISO 17799 standard, 279
 policies for, 393–397
 practical application, 487–488
 PGP (Pretty Good Privacy), 336, 343, 343
 phage viruses, 83
 phishing, 89
 photons in quantum cryptography, 308
 phreakers, 122
 Physical Access Control policies, 398

548 physical cryptography – practical application

- physical cryptography, 304
- physical security, 5–7, 254
 - access control, 254–261
 - barriers, 255–256, 255–256
 - partitioning, 259–260, 260
 - perimeter security, 256–257, 257
 - security zones, 257–259, 259
 - environment, 264–271, 264
 - in ISO 17799 standard, 280
 - practical application, 529–530
 - social engineering, 261–263
- ping of death attacks, 56, 74
- PKC (Public Key Cryptography), 314
- PKCS (Public Key Cryptography Standards), 336–337
- PKI (Public Key Infrastructure), 320–321
 - CAs in, 321, 322
 - certificate policies in, 325
 - certificate revocation in, 325–326
 - certificates in, 323
 - CPSs in, 325
 - RAs in, 322–323, 323
 - trust models in, 326–329
 - X.509 version, 324–325, 324
- PKI Policy Document, 321
- PKIX (Public Key Infrastructure X.509), 336
- Plain Old Telephone Service (POTS), 119, 120
- platform hardening, 125–126
- plug and play technology, 153
- plumbing, 143
- Point-to-Point Protocol (PPP), 128–129, 128
- Point-to-Point Tunneling Protocol (PPTP), 122, 129, 473
- policies and procedures, 9–13, 275–277, 371
 - in best practices, 426–430
 - business continuity. *See* Business Continuity Planning (BCP)
 - business policies, 397–398
 - Certificate policies, 398–400, 400
 - exam essentials, 409–410
 - hands-on labs, 411–412
 - human resource policies, 393–397
 - incident response policies, 400–401
 - in incident responses, 191
 - in ISO 17799 standard, 279
 - privilege management. *See* privilege management
 - review questions, 413–418
 - summary, 408–409
 - updating, 436
 - vendor support, 390–392
- polymorphic viruses, 80, 81
- POP (Post Office Protocol), 64, 134
- POP3 ports with firewalls, 111
- ports
 - with firewalls, 111
 - hubs for, 114
 - Internet, 132–133, 132
 - scanning, 71–72
 - TCP/IP, 67–69, 168
 - UDP, 168
- Post Office Protocol (POP), 64, 134
- POTS (Plain Old Telephone Service), 119, 120
- power conditioners, 267
- power systems, 267–268
- PPP (Point-to-Point Protocol), 128–129, 128
- PPTP (Point-to-Point Tunneling Protocol), 122, 129, 473
- practical application, 456
 - communication security, 471–472
 - dial-up, 472–473
 - directory services, 476–477
 - e-mail, 474–475
 - file sharing, 477–478
 - Internet, 475–476
 - remote control, 473–474
 - VPNs, 473
 - wireless, 478–479
 - cryptography, 483–484
 - certificates, 484–485
 - key management, 485–486
 - General Security Concepts, 458
 - access control, 459
 - accountability, 459
 - auditing, 470–471
 - authentication, 460–462
 - malicious events, 464–470
 - system hardening, 462–464
 - infrastructure security, 479–481
 - baselines, 482–483
 - IDSs and honey pots, 482
 - security zones, 481–482
 - operation/organizational security, 487
 - backups, 488–489
 - disaster planning, 489
 - documentation, 490

- incident handling, 490
- personnel management, 489–490
- physical, 487–488
- preparation for, 456–490
- preauthentication systems, 472
- preserving evidence, 424
- Pretty Good Privacy (PGP), 336, 343, 343
- prevention as goal, 13
- previous keys, 353
- principles in KDCs, 19
- print servers and services, hardening, 236–237, 236
- prioritizing in BIA, 272–274
- privacy
 - in IM, 195
 - policies for, 396
 - regulating, 440–444
- Private Branch Exchange (PBX) systems, 120–122, 121
- private information, 11, 282–283
- private keys
 - in asymmetric cryptographic algorithms, 313
 - protecting, 350
 - in symmetric cryptographic algorithms, 312
- privilege creep, 12, 406
- privilege management, 401
 - for access control, 407–408
 - auditing in, 405–407
 - decision making in, 404–405
 - privilege escalation, 403
 - single sign-on, 403–404
 - user, group, and role management, 401–402, 402
- procedures. *See* policies and procedures
- processes, terminating, 181, 181
- professionals, security, 285
- promiscuous mode, 70
- protocols, 22–24
 - configuring, 218–220
 - cryptography. *See* cryptography
 - enabling and disabling, 231
 - Microsoft, 170–172, 171
 - Novell, 169, 170
 - TCP/IP, 67–69, 69–70, 141–142
- proxy firewalls, 110–114, 112
- Public Domain Cryptography, 336
- public information, 11, 281
- Public Key Cryptography (PKC), 314

- Public Key Cryptography Standards (PKCS), 336–337
- Public Key Infrastructure. *See* PKI (Public Key Infrastructure)
- Public Key Infrastructure X.509 (PKIX), 336
- public keys
 - in asymmetric cryptographic algorithms, 313
 - CAs for, 319

Q

- quantum cryptography, 303, 308–309, 309

R

- "R" services, 24
- radio frequency (RF) communication, 148–149, 149
- radio frequency (RF) spectrum, 117
- radio frequency interference (RFI), 268–269
- RADIUS (Remote Authentication Dial-In User Service), 130–131, 131
- RAID (Redundant Arrays of Independent Disks), 375–378, 376
- rainbow tables, 469
- RAs (registration authorities), 322–323, 323
- RAS (Remote Access Services), 119, 120
- RBAC (Role-Based Access Control) models, 15, 408, 459
- RC encryption, 313
- RDNs (Relative Distinguished Names), 239
- read up process, 286–287
- real time detection, 167
- reciprocal agreements, 389
- recovery
 - disaster. *See* disaster recovery
 - keys, 352–354, 352
 - from theft and critical information losses, 6
- redundancy, 373–375, 374
- Redundant Arrays of Independent Disks (RAID), 375–378, 376
- reference checks, 396–397
- reference documents in standards, 277
- registration authorities (RAs), 322–323, 323
- Relative Distinguished Names (RDNs), 239

550 relying parties in trusted transactions – routing tables

- relying parties in trusted transactions, 399, 400
- remote access, 128
 - 802.1X wireless protocols, 130
 - PPP, 128–129, 128
 - practical application, 473–474
 - RADIUS, 130–131, 131
 - SLIP, 128
 - TACACS, 131
 - tunneling protocols, 129–130
- Remote Access Services (RAS), 119, 120
- Remote Authentication Dial-In User Service (RADIUS), 130–131, 131
- remote file transfers, 140
- Remote Procedure Call (RPC), 24
- Remote Procedure Call (RPC) port, 236
- Remote Shell (RSH) utility, 341
- removable media, 151
 - CD Recordable technology, 152–153
 - diskettes, 153
 - Flash cards, 153
 - hard drives, 153
 - smart cards, 154
 - tape, 151–152
- renewing keys, 354
- repairing damage, 188–189
- replay attacks, 60, 61, 466
- reports, audit, 407
- repudiation attacks, 55
- Requests for Comments (RFCs), 334
- research, 457
- resource allocation, 431
- responses, 13
 - with IDSs, 179–182, 181–183
 - incident. *See* incident responses
- responsibility, defining, 431
- restricted information, 283
- retention policies, 427
- retroviruses, 82
- reverse hash matching, 468
- reverse lookups, 466
- review questions
 - cryptography, 363–368
 - hardening, 246–251
 - infrastructure and connectivity, 158–163
 - monitoring, 204–209
 - network and environment security, 294–299
 - policies and procedures, 413–418
 - risk identification, 97–102
 - security concepts, 44–49
 - security management, 449–453
- revoking
 - certificates, 325–326
 - keys, 351–352
- RF (radio frequency) communication, 148–149, 149
- RF (radio frequency) spectrum, 117
- RFCs (Requests for Comments), 334
- RFI (radio frequency interference), 268–269
- Rijmen, Vincent, 313
- RIP (Routing Information Protocol), 64, 116
- risk identification and assessment, 35–36, 52
 - attack recognition, 57–61, 58–61
 - attack strategies, 52–57, 56
 - auditing for, 90–91
 - in Business Continuity Planning, 273–275
 - exam essentials, 92–94
 - hands-on labs, 95–96
 - malicious code. *See* malicious code
 - review questions, 97–102
 - social engineering, 88–89
 - software exploitation, 76–78
 - summary, 91–92
 - TCP/IP. *See* TCP/IP (Transmission Control Protocol/Internet Protocol)
- Rivest, Ron, 314, 336
- robots, 235
- rogue servers, 237
- Role-Based Access Control (RBAC) models, 15, 408, 459
- roles and responsibilities
 - in guidelines, 278
 - managing, 401–402, 402
 - in security process, 284–285
 - in standards, 277
- root CAs, 327, 327
- root-cause analysis, 420
- rootkits, 77
- rot13 encoding, 305
- Round Robin rotation system, 152
- routers
 - configuring, 230–231
 - security for, 114–116, 115
 - updating, 230
- Routing and Remote Access Services (RRAS), 119
- Routing Information Protocol (RIP), 64, 116
- routing tables, 116

RPC (Remote Procedure Call), 24
 RPC (Remote Procedure Call) port, 236
 RRAS (Routing and Remote Access Services), 119
 RSA encryption, 314, 336
 RSH (Remote Shell) utility, 341
 rubber hose attacks, 469–470
 rules of evidence, 186–187

S

S/FTP (Secure FTP), 140
 S-HTTP (Secure Hypertext Transport Protocol), 344
 S/MIME (Secure Multipurpose Internet Mail Extensions), 340
 sandbox, 136
 SANS (SysAdmin, Audit, Network, Security) certification, 464
 SANS Institute, 438
 scanning
 networks, 198
 ports, 71–72
 wireless cells, 264–265, 264
 Schneier, Bruce, 313, 484
 scope and purpose
 in guidelines, 278
 in policies, 276
 in standards, 277
 screensavers, 77
 script kiddies, 458
 scripts, 193, 232
 secret information, 284
 Secure Electronic Transaction (SET), 340, 341
 Secure FTP (S/FTP), 140
 Secure Hash Algorithm (SHA), 311
 Secure Hypertext Transport Protocol (S-HTTP), 344
 Secure Multipurpose Internet Mail Extensions (S/MIME), 340
 Secure Shell (SSH) protocol, 130, 340–342, 342, 473
 Secure Sockets Layer (SSL), 135–136, 338–339, 338
 security concepts and process, 3–4, 4
 access control, 14–15
 antivirus software, 14
 authentication. *See* authentication
 exam essentials, 40–42
 goals, 13–14
 hands-on labs, 43
 management and policies, 9–13
 operational security, 7–9, 8
 physical security, 5–7
 review questions, 44–49
 services and protocols, 22–24
 summary, 39–40
 topologies. *See* topologies
 Security Enhanced Linux (SELinux) tools, 224
 security groups, 402, 402
 security guards, 257
 security logs, 90–91
 security management, 420
 awareness and education, 433–435
 best practices. *See* best practices
 computer forensics. *See* computer forensics, evidence in
 exam essentials, 445–446
 hands-on labs, 447
 privacy in, 440–444
 review questions, 449–453
 summary, 444–445
 updating, 436–439
 security professionals, 285
 security tokens, 18, 19
 security zones, 27–28, 257–259, 259
 demilitarized zones, 30–31, 30
 designing, 31
 extranets, 29–30, 30
 Internet, 28–29, 29
 intranets, 29, 29
 practical application, 481–482, 524
 SELinux (Security Enhanced Linux) tools, 224
 selling old computers, 355, 428
 sensitive but unclassified information, 283
 sensors in IDSs, 176
 Separation of Duties policies, 397
 sequence number attacks, 73, 74
 Sequenced Packet Exchange (SPX) protocol, 169
 Serial Line Internet Protocol (SLIP), 128
 server authentication, 127, 461
 servers, hardening, 125–126
 DNS, 234–235
 e-mail, 233, 233

552 service level agreements (SLAs) – steganography

- file and print, 236–237, 236
- FTP, 234
- NNTP, 235–236
- web servers, 232
- Windows Server 2003, 222–223
- service level agreements (SLAs), 390–392
- service packs, 228–229
- services, 22–24
 - enabling and disabling, 231
 - nonessential, 23–24
 - in TCP/IP, 67–69, 69–70
- sessions, terminating, 181, 181
- SET (Secure Electronic Transaction), 340, 341
- SHA (Secure Hash Algorithm), 311
- shadow copy backups, 380
- Shamir, Adi, 314, 336
- sharing files, 140, 236–237, 236, 477–478
- sheep-dip systems, 468
- Shielded Twisted Pair (STP) cable, 146–147, 146–147
- shielding, 268–269, 269
- shoulder surfing, 263
- shunning with IDSs, 180
- signal analysis and intelligence, 197–198
- signal strength, 118
- signatures
 - in applets, 137
 - in certificates, 399
 - in cryptographic systems, 313–318, 317
 - in IDSs, 176, 177, 187
 - and viruses, 80
 - in X.509, 324, 337
- Simple Mail Transport Protocol (SMTP), 64, 133
- Simple Network Management Protocol (SNMP), 24, 64, 141–142
- SIMs (Subscriber Identification Modules), 265
- single loss expectancy (SLE) values, 274–275
- single sign-on (SSO), 403–404
- site surveys for wireless systems, 194
- sites, alternate, 388–390
- SLAs (service level agreements), 390–392
- SLE (single loss expectancy) values, 274–275
- SLIP (Serial Line Internet Protocol), 128
- smart cards, 19, 21, 21, 154
- smoke damage, 266
- SMS (Systems Management Server), 70–71, 124
- SMTP (Simple Mail Transport Protocol), 64, 133
- SMTP ports with firewalls, 111
- SMTP relay, 138–139
- Smurf attacks, 75, 75, 141
- sniffers, 70–71, 123–124, 145, 196–197
- SNMP (Simple Network Management Protocol), 24, 64, 141–142
- snooping, 53
- social engineering, 88–89
 - for physical access, 261–263
 - preventing, 469–470
- sockets, Internet, 132–133, 132
- software
 - exploiting, 76–78
 - unauthorized, 125
 - working with, 108
- source ports, 133
- spam, 85
 - ACLs for, 233
 - from newsgroups, 235
- special ID numbers (SSIDs), 118
- spikes, 267
- split key generation systems, 347–348
- splitters, fiber optic, 148, 148
- spoofing attacks, 58–59, 59, 461, 466
- SPX (Sequenced Packet Exchange) protocol, 169
- Spybot program, 77
- spyware, 77
- Spyware Doctor program, 77
- SQL (Structured Query Language), 240
- SSH (Secure Shell) protocol, 130, 340–342, 342, 473
- SSIDs (special ID numbers), 118
- SSL (Secure Sockets Layer), 135–136, 338–339, 338
- SSL ports with firewalls, 111
- SSO (single sign-on), 403–404
- staffing issues, 430
- standards
 - cryptography. *See* cryptography
 - incorporating, 277–278
 - ISO 17799, 279–280, 345
- stateful inspection firewalls, 113–114
- static electricity, 266
- stealth viruses, 82, 82
- steganography, 304–306

storing
 information, 427
 keys, 348–350, 349
 onsite and offsite, 380–381
 STP (Shielded Twisted Pair) cable, 146–147,
 146–147
 stream ciphers, 312
 strong cryptographic systems, 312, 315
 Structured Query Language (SQL), 240
 Subscriber Identification Modules (SIMs), 265
 subscribers in trusted transactions, 399, 400
 substitution ciphers, 304
 support packs, 228–229
 surge protectors, 267
 suspending keys, 352
 switches
 operation of, 116, 116
 updating, 230
 Symantec Corporation, 438
 symmetric cryptographic algorithms,
 312–313, 312
 SYN floods, 72–73, 72
 SysAdmin, Audit, Network, Security (SANS)
 certification, 464
 system architecture, 430
 system hardening. *See* hardening
 system logs, 429
 system recovery, 387–388, 387
 systems development and maintenance in ISO
 17799 standard, 280
 Systems Management Server (SMS), 70–71,
 124

T

T-connectors, 145, 145
 TACACS (Terminal Access Controller Access
 Control System), 131
 TACACS ports with firewalls, 111
 tailgating, 262
 tangible impact analysis in BIA, 273
 tape, 151–152
 taps
 in monitoring, 173, 173
 vampire, 145, 145
 Tavares, Stafford, 313

storing – three-way handshakes

TCP (Transmission Control Protocol), 64
 attacks on, 72–74, 72–74
 packets, 132, 133
 sequence number attacks, 73, 74
 SYN floods, 72–73, 72
 three-way handshakes, 69, 69
 wrappers, 224
 TCP/IP (Transmission Control Protocol/
 Internet Protocol), 61–63, 63
 Application layer, 64
 attacks on, 70–74, 72–74
 binding to, 219, 220
 encapsulation in, 66–67, 66–67
 hardening, 220
 Host-to-Host layer, 64–65
 Internet layer, 65
 Network Interface layer, 66
 network traffic in, 168
 protocols and services in, 67–69, 69–70
 SNMP, 141–142
 UDP attacks, 74–76, 75
 vulnerabilities in, 38
 TCSEC (Trusted Computer Systems
 Evaluation Criteria) system, 216
 technical staff, training, 434
 telecommunications capabilities, 120–122,
 121
 telnet ports with firewalls, 111
 Telnet protocol, 23–24, 64, 71
 TEMPEST project, 269
 Ten Commandments of Computer Ethics, 395
 Terminal Access Controller Access Control
 System (TACACS), 131
 terminating processes and sessions, 181, 181
 terminating resistors, 143
 termination policies, 394
 terminators, 143, 145
 test preparation. *See* practical application
 TFTP (Trivial File Transfer Protocol), 24
 theft, detecting and recovering from, 6
 thin clients, 154
 third-party CAs, 399, 400
 threats
 identifying, 36–38, 37
 network security, 213–215
 three-layer security model, 255, 255
 three-tier database models, 241
 three-way handshakes, 69, 69

554 tickets in KDCs – UTP (Unshielded Twisted Pair) cable

tickets in KDCs, 19
 timeframes in BIA, 273
 TLS (Transport Layer Security) protocol,
 135–136, 339, 339
 toolkits for acquiring evidence, 421
 top secret information, 284
 topologies, 24

- business concerns, 34–39
- design goals, 25–27
- newer technologies, 31–34, 32–34
- security zones, 27–31

 Tower-of-Hanoi tape rotation system, 152
 trade publications, 438–439
 traffic generation attacks, 466
 training, 433–435
 transactions, trusted, 399, 400
 transceivers, 117
 translating LAN framing to WAN framing, 114
 Transmission Control Protocol. *See* TCP
 (Transmission Control Protocol)
 Transmission Control Protocol/Internet
 Protocol. *See* TCP/IP (Transmission
 Control Protocol/Internet Protocol)
 transmission media, 142

- cabling, 142
 - coaxial, 142–145, 143–145
 - UTP and STP, 146–147, 146–147
- fiber optics, 147–148, 148
- infrared, 148
- microwaves, 149–150, 150
- radio frequency, 148–149, 149

 Transport layer, 64–65
 Transport Layer Security (TLS) protocol,
 135–136, 339, 339
 transposition ciphers, 304–305, 305
 trees in hierarchical trust models, 326, 327
 Triple-DES (3DES) encryption, 313
 Trivial File Transfer Protocol (TFTP), 24
 Trojan horses, 85
 trust models, 326, 327

- bridge, 327–328, 328
- hybrid, 329, 329
- mesh, 328–329, 328

 Trusted Computer Systems Evaluation
 Criteria (TCSEC) system, 216
 trusted transactions, 399, 400
 tunneling, 129–130

- ICMP, 75–76
- purpose of, 33–34, 34

2600: The Hacker Quarterly magazine, 438
 two-factor authentication system, 19, 20, 22
 two-tier database models, 241
 two-way authentication, 127
 Twofish encryption, 313
 Type factors for authentication, 460

U

UDP (User Datagram Protocol), 64–65

- attacks on, 74–76, 75
- ports, 168
- stateful inspection firewalls for, 113

 unauthorized software, 125
 unbreakable codes, myth of, 309–310
 unclassified information, 283
 unicasts, 142
 Uninterruptible Power Supplies (UPSs), 268
 Unix

- filesystems in, 226, 227
- hardening, 223–224
- interactive users in, 342

 Unix Remote Procedure Call, 24
 Unshielded Twisted Pair (UTP) cable,
 146–147, 146–147
 updating

- applications, 436
- network devices, 230, 436
- operating systems, 228–229, 436

 UPNs (User Principal Names), 239
 UPSs (Uninterruptible Power Supplies), 268
 uptime as design goal, 25
 usage auditing, 406
 usage policies, 11, 428
 User Datagram Protocol (UDP), 64–65

- attacks on, 74–76, 75
- ports, 168
- stateful inspection firewalls for, 113

 user files, backing up, 382
 user IDs for FTP, 140
 user management, 12, 401–402, 402, 430
 User Principal Names (UPNs), 239
 usernames, 16
 users of information, 285
 utilities in business continuity, 371–372
 UTP (Unshielded Twisted Pair) cable,
 146–147, 146–147

V

Valentine, Brian, 215
 valuing data assets, 36
 vampire taps, 145, 145
 .vbs extension, 196
 vendor support, 390
 code escrow, 392–393
 service level agreements, 390–392
 virtual local area networks (VLANs), 31, 32, 35
 virtual private networks (VPNs), 34, 122–123, 122, 473
 virus scanners on e-mail servers, 233, 233
 viruses, 78–79
 antivirus software for, 14, 87, 467–468
 hoaxes, 84
 network transmission of, 84
 operation of, 79–80, 80–81
 symptoms, 79
 types of, 80–83, 81
 VLANs (virtual local area networks), 31, 32, 35
 VPNs (virtual private networks), 34, 122–123, 122, 473
 vulnerabilities, 38–39

W

W3C (World Wide Web Consortium), 335
 Walker, John, 263
 wallets, electronic, 340, 341
 WAN framing, translating LAN framing to, 114
 WAP (Wireless Access Protocol), 192–193, 193, 479
 WAP (Wireless Applications Protocol), 127, 127, 191, 191
 WAPs (wireless access points), 117–118, 117
 war driving, 118
 warm sites, 389
 water damage, 266
 water fire suppression systems, 270–271, 271
 watermarks, electronic, 306
 WDP (Wireless Datagram Protocol), 127
 weak key attacks, 331
 weakest links in cryptography, 311
 Web, 134–135, 135
 add-ins, 136–139
 in mesh trust model, 328
 services, 23
 web servers, hardening, 232
 websites for security information, 437–438
 well-known ports, 67–69
 WEP (Wired Equivalent Privacy), 193, 345, 478
 in cryptographic systems, 331
 for man-in-the-middle attacks, 60
 whatis utility, 174
 whereis utility, 174
 white/black lists, 466
 WiFi standard, 192
 Wikipedia, 483
 Windows Internet Naming Service (WINS)
 service, 171–172, 172
 Windows systems, hardening
 Windows 2000, 220–222, 221
 Windows Server 2003, 222–223
 Windows XP, 222
 WINS (Windows Internet Naming Service)
 service, 171–172, 172
 WinSock (Windows socket) API, 69, 70
 Wired Equivalent Privacy (WEP), 193, 345, 478
 in cryptographic systems, 331
 for man-in-the-middle attacks, 60
 wireless access points (WAPs), 117–118, 117
 Wireless Access Protocol (WAP), 192–193, 193, 479
 Wireless Applications Protocol (WAP), 127, 127, 191, 191
 wireless cells, scanning, 264–265, 264
 Wireless Datagram Protocol (WDP), 127
 Wireless Ethernet protocol, 117
 Wireless Markup Language (WML), 193
 wireless protocols, 130
 Wireless Session Protocol (WSP), 127
 wireless systems
 monitoring, 191–194, 191, 193
 practical application, 478–479
 wireless technologies, 108
 Wireless Transaction Protocol (WTP), 127
 Wireless Transport Layer Security (WTLS), 127
 purpose of, 345
 in WAP environment, 191, 191
 in wireless devices, 265

556 wiring – zones

wiring, **142**
 coaxial, **142–145**, *143–145*
 fiber optic technology, **147–148**, *148*
 UTP and STP, **146–147**, *146–147*
WML (Wireless Markup Language), **193**
WMLScript environments, **193**
work factor of cryptographic systems, **315**
working copy backups, **380**
working documents, **282**
workstations, **125–126**
World Wide Web Consortium (W3C), **335**
WORM (write once, read many) devices, **471**
worms, **86**
wrappers, TCP, **224**
write down process, **286–287**
write once, read many (WORM) devices, **471**
WSP (Wireless Session Protocol), **127**
WTLS (Wireless Transport Layer Security), **127**
 purpose of, **345**
 in WAP environment, **191**, *191*
 in wireless devices, **265**
wtm file, **184**
WTP (Wireless Transaction Protocol), **127**

X

X.500 standard, **239**
X.509 standard
 certificates in, **399**
 cryptography, **337–338**
 PKI, **324–325**, *324*
X Windows service, **24**
XKMS (XML Key Management Service), **339**
XML (Extensible Markup Language), **135**

Z

ZENworks tool, **169**
Zimmerman, Phil, **336**
zones
 practical application, **481–482**
 router, **115**
 security, **27–31**

Wiley Publishing, Inc.

End-User License Agreement

READ THIS. You should carefully read these terms and conditions before opening the software packet(s) included with this book "Book". This is a license agreement "Agreement" between you and Wiley Publishing, Inc. "WPI". By opening the accompanying software packet(s), you acknowledge that you have read and accept the following terms and conditions. If you do not agree and do not want to be bound by such terms and conditions, promptly return the Book and the unopened software packet(s) to the place you obtained them for a full refund.

1. License Grant. WPI grants to you (either an individual or entity) a nonexclusive license to use one copy of the enclosed software program(s) (collectively, the "Software," solely for your own personal or business purposes on a single computer (whether a standard computer or a workstation component of a multi-user network). The Software is in use on a computer when it is loaded into temporary memory (RAM) or installed into permanent memory (hard disk, CD-ROM, or other storage device). WPI reserves all rights not expressly granted herein.

2. Ownership. WPI is the owner of all right, title, and interest, including copyright, in and to the compilation of the Software recorded on the physical packet included with this Book "Software Media". Copyright to the individual programs recorded on the Software Media is owned by the author or other authorized copyright owner of each program. Ownership of the Software and all proprietary rights relating thereto remain with WPI and its licensors.

3. Restrictions On Use and Transfer.

(a) You may only (i) make one copy of the Software for backup or archival purposes, or (ii) transfer the Software to a single hard disk, provided that you keep the original for backup or archival purposes. You may not (i) rent or lease the Software, (ii) copy or reproduce the Software through a LAN or other network system or through any computer subscriber system or bulletin-board system, or (iii) modify, adapt, or create derivative works based on the Software.

(b) You may not reverse engineer, decompile, or disassemble the Software. You may transfer the Software and user documentation on a permanent basis, provided that the transferee agrees to accept the terms and conditions of this Agreement and you retain no copies. If the Software is an update or has been updated, any transfer must include the most recent update and all prior versions.

4. Restrictions on Use of Individual Programs. You must follow the individual requirements and restrictions detailed for each individual program in the About the CD-ROM appendix of this Book or on the Software Media. These limitations are also contained in the individual license agreements recorded on the Software Media. These limitations may include a requirement that after using the program for a specified period of time, the user must pay a registration fee or discontinue use. By opening the Software packet(s), you will be agreeing to abide by the licenses and restrictions for these individual programs that are detailed in the About the CD-ROM appendix and/or on the Software Media. None of the material on this Software Media or listed in this Book may ever be redistributed, in original or modified form, for commercial purposes.

5. Limited Warranty.

(a) WPI warrants that the Software and Software Media are free from defects in materials and workmanship under normal use for a period of sixty (60) days from the date of

purchase of this Book. If WPI receives notification within the warranty period of defects in materials or workmanship, WPI will replace the defective Software Media.

(b) WPI AND THE AUTHOR(S) OF THE BOOK DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WITH RESPECT TO THE SOFTWARE, THE PROGRAMS, THE SOURCE CODE CONTAINED THEREIN, AND/OR THE TECHNIQUES DESCRIBED IN THIS BOOK. WPI DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE ERROR FREE.

(c) This limited warranty gives you specific legal rights, and you may have other rights that vary from jurisdiction to jurisdiction.

6. Remedies.

(a) WPI's entire liability and your exclusive remedy for defects in materials and workmanship shall be limited to replacement of the Software Media, which may be returned to WPI with a copy of your receipt at the following address: Software Media Fulfillment Department, Attn.: CompTIA Security+ Study Guide, Deluxe Edition, Wiley Publishing, Inc., 10475 Crosspoint Blvd., Indianapolis, IN 46256, or call 1-800-762-2974. Please allow four to six weeks for delivery. This Limited Warranty is void if failure of the Software Media has resulted from accident, abuse, or misapplication. Any replacement Software Media will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

(b) In no event shall WPI or the author be liable for any damages whatsoever (including without limitation damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising from the use of or inability to use the Book or the Software, even if WPI has been advised of the possibility of such damages.

(c) Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation or exclusion may not apply to you.

7. U.S. Government Restricted Rights. Use, duplication, or disclosure of the Software for or on behalf of the United States of America, its agencies and/or instrumentalities "U.S. Government" is subject to restrictions as stated in paragraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, or subparagraphs (c) (1) and (2) of the Commercial Computer Software - Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR supplement, as applicable.

8. General. This Agreement constitutes the entire understanding of the parties and revokes and supersedes all prior agreements, oral or written, between them and may not be modified or amended except in a writing signed by both parties hereto that specifically refers to this Agreement. This Agreement shall take precedence over any other documents that may be in conflict herewith. If any one or more provisions contained in this Agreement are held by any court or tribunal to be invalid, illegal, or otherwise unenforceable, each and every other provision shall remain in full force and effect.

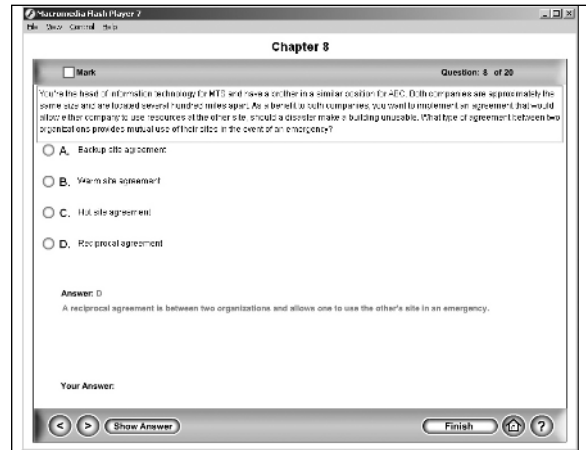
The Absolute Best Security+ Book/CD Package on the Market!



Get Ready for CompTIA's Security+ Exam with the most comprehensive and challenging sample tests anywhere!

The Sybex Test Engine features:

- All the review questions, as covered in each chapter of the book.
- Challenging questions representative of those you'll find on the real exam.
- Six full length bonus exams available only on the CD.
- An Assessment Test to narrow your focus to certain objective groups.



Use the Electronic Flashcards for PCs or Palm devices to jog your memory and prep last-minute for the exam!

- Reinforce your understanding of key concepts with these hardcore flashcard-style questions.
- Download the Flashcards to your Palm device and go on the road. Now you can study for the Security+ exam any time, anywhere.

Search through the complete book in PDF!

- Access the entire *Security+ Study Guide, Deluxe Edition*, complete with figures and tables, in electronic format.
- Search the *Security+ Study Guide, Deluxe Edition*, chapters to find information on any topic in seconds.

