

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

- ~ or ! (NOT) operations, logical
 - operations, 341
- % (modulo) function, in cryptography, **342**
- * (star) Integrity Property
 - Bell-LaPadula state machine, 459
 - Biba state machine, 460
- ∨ (OR) operation, logical operations, 340
- ∧ (AND) operation, logical operations, 339–340
- 100Base-TX cable, 89
- 10Base-T cable, 89
- 10Base2 cable, 89
- 5-4-3 rule, for network design, 92
- 802.11. *see* wireless networking (IEEE 802.11)

A

- abstraction
 - overview of, **188**
 - security protection mechanisms, **436**
- abuse
 - access abuses, **705**
 - voice communication security, **161–162**
- acceptable use policies, 216
- access control
 - access control triple, 461
 - account administration, **29–30**
 - accountability. *see* accountability
 - auditing and monitoring and, 30
 - authentication. *see* authentication
 - brute-force attack countermeasure, 57–58
 - centralized and decentralized, **27–28**
 - compensation measures, **65**
 - context-dependent, 256
 - DACs (discretionary access controls), **23**
 - defined, **2**
 - email and, 157
 - lab and lab questions, 37–38
 - lattice-based, 26, 458
 - in layered environment, 4–5
 - malicious code countermeasure, 304
 - mandatory, **24–25**
 - nondiscretionary, **23–24**
 - to objects and subjects, **462–463**
 - overview of, 2
 - Q&A, 39–44
 - RADIUS and TACACS, 28
 - rights and permissions, 30–34
 - role-based, 25–26
 - summary and exam essentials, 34–37
 - techniques, 23
 - types of, 2–4
- access control lists (ACLs)
 - in access control matrix, 457
 - firewalls and, 117
- access control matrix, in security models, 457
- access control, physical
 - access abuses, 705
 - badges, 701
 - deploying, 697
 - fences, gates, turnstiles, and mantraps, 698
 - intrusion alarms, 702
 - keys and combination locks, 700–701
 - lighting, 698–699
 - motion detectors, 702
 - overview of, 4
 - preventing brute-force attacks, 57
 - secondary verification mechanisms, 702–703
 - security guards and dogs, 699–700
- Access Control Systems and Methodology
 - domain, CBK, 2, 46
- access control triple, 461
- access, defined, 2
- accessibility, factors in facility site selection, 695

- account administration, 29–30
 - creating accounts, 29–30
 - maintaining accounts, 30
- account lockout
 - login and, 12
 - preventing brute-force attacks, 58
- accountability
 - auditing and, 8–9, 529
 - authentication, 5–7
 - authorization, 7–8
 - government regulations, 531
 - identification, 5
 - monitoring and, 46–47, 529
 - overview of, 5, 186
 - security design and, 438–439
- accreditation
 - overview of, 476–477
 - standards and phases for, 477–478
- ACID model, 254–255
- ACLs (access control lists)
 - in access control matrix, 457
 - firewalls and, 117
- action phase, of incident response process, 675–677
- active content, malicious code and, 303
- active response, IDS, 48
- ActiveX controls
 - countermeasure to malicious code, 305
 - hostile applets, 303
 - overview of, 248
- actual cost evaluation (ACV), 602
- ACV (actual cost evaluation), 602
- ad hoc networks, wireless networking, 96
- Address Resolution Protocol. *see* ARP (Address Resolution Protocol)
- addresses, memory, 427–428
- Adleman, Leonard, 377
- administrative access control, 4
- administrative controls, 512–513
- administrative law, 632
- administrative management
 - antivirus management, 496–498
 - application controls, 512
 - assurance, 498–499
 - backup maintenance, 499
 - configuration and change management controls, 503–504
 - controls, generally, 512–513
 - due care and due diligence standards, 504
 - hardware controls, 511
 - I/O controls, 512
 - lab and lab questions, 517–519
 - legal issues, 505
 - media controls, 512
 - media management, 506–509
 - need to know and principle of least privilege, 500
 - operations controls, 510–511
 - Operations Security, 496
 - overview of, 496
 - personnel controls, 513–514
 - physical security controls, 693
 - privacy and protection, 505
 - privileged entity controls, 511
 - privileged operations functions, 501–502
 - Q&A, 520–525
 - record retention, 505–506
 - security controls, 509–510
 - summary and exam essentials, 514–517
 - trusted recovery, 502–503
 - workstations location changes, 499–500
- admissible evidence, 650
- advanced encryption standard (AES), 361–362
- advisory policies, security policies, 215
- adware, 303
- AES (advanced encryption standard), 361–362
- agents (bots), 246–247
- aggregation, SQL, 257–259
- AH (authentication header), IPSec, 143, 396
- alarm triggers, in auditing, 528
- alarms, intrusion detection, 702, 705–706
- ALE (annualized loss expectancy)
 - in BCP, 574
 - calculating, 225
 - cost functions in quantitative risk analysis, 224
- algorithms
 - asymmetric key, 353–356
 - cryptography based on, 338
 - hashing, 356–357
 - key space, 338
 - symmetric key, 352–353

- alternative sites
 - continuity planning, 577
 - recovery strategies, 604
- ALU (arithmetic-logical unit), 427
- amplifiers, network devices, 121
- analog, LAN technologies, 101
- analysis, gathering evidence and, 677
- analytic attacks, cryptographic, 399
- AND (\wedge) operations, logical operations, 339–340
- annualized loss expectancy (ALE)
 - in BCP, 574
 - calculating, 225
 - cost functions in quantitative risk analysis, 224
- annualized rate of occurrence (ARO)
 - in quantitative risk analysis, 224
 - for risks, 573
- anomaly detection, 260. *see also*
 - behavior-based IDS
- ANSI standards, for power, 709
- antivirus mechanisms. *see also* viruses
 - antivirus management, 496–498
 - filters, 304
 - overview of, 298
- APIPA (Automatic Private IP Addressing), 147
- applets
 - ActiveX, 248
 - countermeasure to malicious code, 304
 - hostile, 303
 - Java, 248
 - overview of, 247–248
- application attacks
 - buffer overflows, 314–315
 - lab and lab questions, 324–325
 - overview of, 314
 - Q&A, 326–331
 - rootkits, 315
 - summary and exam essentials, 323–324
 - TOCTOU
 - (time-of-check-to-time-of-use), 315
 - trap doors, 315
- application controls, 512
- Application layer (layer 7)
 - overview of, 86–87
 - TCP/IP working at, 87, 113–114
- application-level gateway firewalls, 118
- application security
 - agents (bots), 246–247
 - applets, 247–248
 - COM and DCOM and, 249
 - distributed environment, 246
 - lab and lab questions, 285–286
 - local/nondistributed environment, 244–245
 - logic bombs, 246
 - ORB (Object Request Broker), 248–249
 - overview of, 244
 - Q&A, 287–292
 - summary and exam essentials, 283–285
 - Trojan horses, 245
 - viruses, 245
 - worms, 246
- approval phase, BCP plan, 578
- arithmetic-logical unit (ALU), 427
- ARO (annualized rate of occurrence)
 - in quantitative risk analysis, 224
 - for risks, 573
- ARP (Address Resolution Protocol)
 - Data Link layer and, 83
 - as TCP/IP Network layer protocols, 112
- ARP spoofing attacks, 166–167
- artificial intelligence, 262. *see also*
 - knowledge-based systems
- AS (authentication service), Kerberos, 21
- assembly language, 267
- asset valuation, 218, 221–222
- asset value (AV), in BIA, 572
- assets
 - listing in BIA (business impact assessment), 572
 - risk terminology, 218
- assurance
 - Common Criteria, 473–474
 - controls, 265
 - ITSEC, 471
 - operational and lifecycle, 498–499
 - trust and, 465
- asymmetric cryptography, 354, 376–380
 - El Gamal, 379
 - elliptic curves and, 379–380
 - hash functions. *see* hash functions
 - lab and lab questions, 402–403
 - overview of, 353–356, 376

- PKI (public key infrastructure). *see* PKI (public key infrastructure)
- public and private keys and, 377, 377
- Q&A, 404–409
- RSA algorithm, 377–379
- summary and exam essentials, 400–402
- symmetric cryptography compared with, 356, 363
- asynchronous communication, LAN
 - technologies, 101
- asynchronous dynamic password tokens, 19
- asynchronous transfer mode (ATM), WAN
 - connection technologies, 153
- ATM (asynchronous transfer mode), 153
- atomicity, in ACID model, 254
- attackers
 - crackers and hackers compared with, 64
 - defined, 666
 - malicious, 548
- attacks
 - based on design flaws, 479
 - bluejacking, 95
 - botnets, 62
 - brute-force and dictionary, 56–58
 - crackers, hackers, and attackers, 64
 - cryptographic, 399–400
 - DoS (denial-of-service), 58–59
 - lab and lab questions, 65–68
 - man-in-the-middle, 63
 - overview of, 55–56
 - passwords and, 11–12
 - Ping-of-death, WinNuke, Teardrop, and Land, 61
 - Q&A, 70–75
 - risk terminology, 219
 - smurf, 60–61
 - sniffer, 64
 - spamming, 64
 - spoofing, 62
 - summary and exam essentials, 65–68
 - Syn flood, 59–60
- attacks, network, 164–167
 - ARP spoofing, 166–167
 - DNS spoofing, 167
 - eavesdropping, 164–165
 - hyperlink spoofing, 167
 - impersonation/masquerading, 166
 - modification, 166
 - overview of, 164
 - replay, 166
 - wireless, 99
- attenuation, cable degradation and, 92
- auctions, sniping, 247
- audit trails
 - overview of, 530–531
 - physical access control and, 705
 - reporting and, 532
- auditing. *see also* monitoring
 - access control and, 30
 - accountability, 8–9, 529
 - audit trails, 530–532, 705
 - compliance, 529
 - exam essentials, 552–553
 - external auditors, 534–535
 - lab and lab questions, 552–553
 - media maintenance and, 534
 - overview of, 185–186, 528
 - Q&A, 557–562
 - record retention and, 533
 - reporting and, 532
 - sampling and, 532
 - time frames for, 530
- auditors
 - external, 534–535
 - security roles, 212
- authentication
 - biometric factor ratings, 15–16, 16
 - biometric factors, 13–15
 - biometric registration, 16
 - biometrics, appropriate use, 16–18
 - challenge-response authentication, 337
 - factors, generally, 5–7
 - goals of cryptography, 337
 - Kerberos protocol for, 20–22
 - overview of, 9, 184–185
 - passwords, 10–13
 - protocols, 126
 - remote access security and, 123
 - SSO (single sign-on), 20, 22
 - tickets, 20
 - tokens (smart tokens), 18–20
- authentication header (AH), IPSec, 143, 396
- authentication service (AS), Kerberos, 21
- authorization, 7–8, 185
- automated recovery, types of trusted
 - recovery, 502–503

Automatic Private IP Addressing (APIPA), 147
 auxiliary alarm systems, intrusion detection, 702, 705
 AV (asset value), in BIA, 572
 availability, 183
 AVG() aggregate function, SQL, 258
 awareness, security awareness training, 230–231

B

back doors
 design flaws and, 479
 maintenance hooks and, 481
 Back Orifice Trojan, 301
 background checks, employees, 208
 backups
 best practices, 615
 electronic vaulting, 608–609
 maintenance program for, 499
 media formats, 614
 neglecting, 613–614
 recovery planning and, 612–614
 remote journaling, 609
 remote mirroring, 609–610
 restoring data from, 613
 tape rotation, 615
 badges, for controlling physical access, 701
 bandwidth on demand, 152
 baseband cable, 89–90
 baselines, 216
 base+offset addressing, memory addressing schemes, 428
 Basic Input/Output System (BIOS), 434
 bastion hosts, 119
 batch processing, by redundant servers, 127
 BCP (business continuity planning). *see also* DRP (Disaster Recovery Planning)
 benefits of, 569
 BIA (business impact assessment), 570–571
 business organization analysis, 566
 CBK domains, 564
 continuity planning, 575
 documentation in, 579
 DRP compared with, 565
 emergency-response guidelines, 581
 facility protection, 577
 goals, 579
 infrastructure protection, 577
 lab and lab questions, 583–584
 legal and regulatory requirements, 569–570
 maintenance program for, 581
 overview of, 564–565
 people, protecting, 576–577
 plan approval phase, 578
 plan implementation phase, 578
 priority identification, 571–572
 project scope and planning, 565
 provisions and processes phase, 576
 Q&A, 585–590
 resource prioritization, 575
 resource requirements, 567–569
 risk acceptance/mitigation document, 580
 risk assessment document, 580
 risk identification, 572
 risk impact assessment, 573–575
 senior management and, 568
 statement of importance, 579
 statement of priorities, 579–580
 statement of urgency and timing, 579–580
 strategy development phase, 576
 summary and exam essentials, 582–583
 team approach to plan development, 568
 team selection, 566–567
 testing program for, 581
 threat likelihood assessment, 572–573
 training and education, 578
 vital records program, 581
 beacon frames, wireless networking (802.11), 97
 BEGIN TRANSACTION, database transactions, 254
 behavior-based IDS, 52
 behavior, OOP terminology, 269
 Bell-LaPadula security model, 458–461, 459
 best evidence rule, 650
 BIA (business impact assessment)
 overview of, 570–571
 priority identification, 571–572
 resource prioritization, 575
 risk identification, 572

800 **Biba security model – capabilities**

- risk impact assessment, 573–575
 - threat likelihood assessment, 572–573
- Biba security model, 460, 460–461
- binary mathematics
 - cryptography and, 339
 - decimal system compared with, 339
- biometrics
 - appropriate use, 16–18
 - controlling physical access, 704
 - factor ratings, 15–16, 16
 - factors, 13–15
 - registration, 16
 - Zephyr chart for comparing factor ratings, 16–17, 17
- BIOS (Basic Input/Output System), 434
- birthday attacks, 56–57, 400
- black box doctrine, 436
- black boxes
 - phreaking and, 163
 - software testing and, 280
- block ciphers
 - overview of, 350–351
 - Rijndael block cipher, 361
- Blowfish, 360
- blue boxes, 163
- bluejacking attacks, 95
- Bluetooth (802.15), 95–96
- Boehm, Barry, 274
- bombings/explosions, DRP and, 598
- boot sector, master boot record compared with, 296
- BootP (Bootstrap Protocol), 114
- bot herders, 62
- botnet controllers, 62
- botnets, 62, 301
- bots (agents), 246–247
- bounds, CIA techniques, 464
- breaches, risk terminology, 219
- Brewer and Nash (Chinese Wall) security model, 462, 483–485
- BRI ISDN, 151
- bridge mode, wireless networking (802.11), 96
- bridges, network devices, 121
- broadband cable, 89–90
- broadcast domains
 - Ethernet, 100
 - overview of, 120–121

- broadcasts
 - collisions and, 120
 - Ethernet as broadcast technology, 100
 - LAN technologies, 101
 - brouters
 - network devices, 122
 - Network layer and, 84
 - brute-force (dictionary) attacks
 - cryptographic attacks, 399
 - overview of, 56–58
 - password attacks, 12
 - buffer-overflows
 - checking code for, 480–481
 - input and parameter checking and, 480
 - overview of, 314–315
 - buffer-underflow, 614
 - buildings, protecting in continuity
 - planning, 577
 - burglar alarms, intrusion detection, 705
 - Bus topology, 104, 104
 - business attacks, categories of computer crime, 667–668
 - business continuity planning. *see* BCP (business continuity planning)
 - business impact assessment. *see* BIA (business impact assessment)
 - business organization analysis, 566
 - business units, prioritizing recovery of, 602

C

- C3 cipher, 334–335
- cable, network
 - attenuation, 92
 - baseband and broadband, 89–90
 - coaxial, 89
 - conductors, 91–92
 - overview of, 88
 - twisted-pair, 90–91
- Cache RAM, 426–427
- Caesar cipher, 334–335
- CALEA (Communications Assistance for Law Enforcement Act), 95, 645
- candidate keys, relational databases, 252
- capabilities
 - in access control matrix, 457
 - security, 453

- Capstone chip, 361
- cardinality, relational databases, 251
- Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA), 102
- Carrier-Sense Multiple Access with Collision Detection (CSMA/CD), 100, 102–103
- CAs (certificate authorities)
 - enrollment process, 388
 - overview of, 387–388
 - revocation process, 389–390
 - verification process, 388–389
- CASE (Computer-Aided Software Engineering), 269
- Cat5 cable, 91
- CBC (Cipher Block Chaining) mode, DES, 358
- CBK (Common Body of Knowledge)
 - Access Control Systems and Methodology domain, 2, 46
 - business continuity and disaster recovery domain, 564
 - hardware and software components and, 78
 - Law, Investigation, and Ethics domain, 666
 - Operations Security domain, 496, 528
 - Physical Security domain, 692
 - Security Management Practices domain, 180
 - Security Management Practices domain of, 206
 - Telecommunications and Network Security domain, 140
- CC. *see* Common Criteria
- CCTV (closed circuit TV)
 - access abuses and, 705
 - auditing and, 530–531
 - as perimeter protection, 699
 - secondary verification mechanisms for physical access, 703
 - technical physical security controls, 693
 - types of monitoring tools, 536–537
- CDDI (Copper Distributed Data Interface), 100
- CDI (constrained data item), in Clark-Wilson security model, 462
- cell phones, wireless communication, 93–95
- cell suppression, multilevel databases and, 256
- cell-switching. *see* circuit switching
- central processing units. *see* CPUs (central processing units)
- central station system, intrusion detection, 705
- centralized access control, 27–28, 126
- centralized alarm systems, 702
- CER (crossover error rate), biometric factor ratings, 15–16
- CERT (Computer Emergency Readiness Team), 55
- certificate authorities. *see* CAs (certificate authorities)
- certificate path validation (CPV), 388
- certificate revocation lists (CRLs), 389–390
- certificates, PKI, 386–387
- certification
 - overview of, 475–476
 - standards and phases for, 477–478
- CFAA (Computer Fraud and Abuse Act of 1984), 633–634
- CFR (Code of Federal Regulations), 632
- chain of evidence, 651
- Challenge Handshake Authentication Protocol (CHAP)
 - authentication protocols, 126
 - PPTP and, 142
- challenge-response authentication, 437
- challenge-response tokens, 19
- change control
 - overview of, 189
 - systems development and, 278–279
- change management controls, 503–504
- channel service unit/data service unit (CSU/DSU), 151
- channels, wireless, 97
- CHAP (Challenge Handshake Authentication Protocol)
 - authentication protocols, 126
 - PPTP and, 142
- Chauvaud, Pascal, 382
- checklist tests, in disaster preparedness, 618–619
- checklists, in disaster preparedness, 611–612
- Children’s Online Privacy Protection Act of 1998 (COPPA), 646
- Chinese Wall (Brewer and Nash) security model, 462, 483–485

802 Chipper chip – common routers

- Chipper chip, Skipjack and, 361
- choke points, workstation management and, 500
- chosen cipher attacks, cryptographic attacks, 399
- chosen plain-text attacks, cryptographic attacks, 399
- CIA triad
 - availability, 183
 - confidentiality, 180–181
 - integrity, 181–182
 - overview of, 180
 - prioritization in private and public sector, 182
 - techniques for ensuring, 463–464
- CIDR (Classless Inter-Domain Routing), 113
- Cipher Block Chaining (CBC) mode, DES, 358
- cipher-text messages, 338
- ciphers, 345–351
 - during American Civil War, 335
 - block ciphers, 350–351
 - Caesar cipher, 334–335
 - codes vs., 345–346
 - one-time pads, 349–350
 - overview of, 345
 - running key ciphers, 350
 - stream ciphers, 351
 - substitution ciphers, 347–348
 - transposition ciphers, 346–347
 - during WWII, 335–336
- CIR (Committed Information Rate), 152
- circuit encryption, networking security, 395–396
- circuit-level gateway firewall, 118
- circuit switching
 - overview of, 148–149
 - WAN connection technologies, 153
- CIRT (Computer Incident Response Team)
 - responsibilities of, 673
 - security roles, 211
- civil law, 632
- Civil War (U.S.), cryptography in, 335
- Clark-Wilson security model, 461–462
- classes, in OOP, 269, 436
- classes, IP classes, 113
- classification levels, in Bell-LaPadula model, 459
- Classless Inter-Domain Routing (CIDR), 113
- click-wrap licenses, 642
- clipping, types of sampling, 533
- closed circuit TV. *see* CCTV (closed circuit TV)
- closed head system, fire suppression, 713
- closed systems, security of, 463
- closure phase, of incident response process, 677
- clustering, in cryptography, 345
- clusters, redundant servers, 127
- CMWs (compartmented mode workstations), 422–423
- coaxial cable, 89
- CobiT (Control Objectives for Information and Related Technology), 193
- code of ethics, (ISC)², 680–681
- Code of Federal Regulations (CFR), 632
- Code Red example, worms, 301–302
- code review, systems development and, 272
- codes, ciphers compared with, 345–346
- cognitive passwords, 11
- cohesive, OOP terminology, 269
- cold rollover failovers, 127
- cold sites, recovery strategies, 604–605
- cold-swappable RAID, 129
- collision domains
 - Ethernet, 100
 - overview of, 120
- collisions, broadcasts and, 120
- collusion
 - job rotation and, 207
 - reducing opportunities for, 546
- COM (Component Object Model), 249–250
- .com files, file infector viruses and, 296
- combination locks, controlling physical access, 700–701
- Committed Information Rate (CIR), 152
- Common Body of Knowledge. *see* CBK (Common Body of Knowledge)
- Common Criteria, 472–475
 - comparing security evaluation standards, 475
 - overview of, 472
 - recognition of, 472–473
 - structure of, 473–475
- Common Object Request Broker Architecture (CORBA), 248–249
- common routers, 117

- communication
 - emergency communications, 603
 - external communications, 616
- communication paths. *see* virtual circuits
- Communications Assistance for Law Enforcement Act (CALEA), 95, 645
- communications security
 - disconnects as security issue, 482–483
 - email security, 156–159
 - lab and lab questions, 171–172
 - NAT (Network Address Translation), 144–147
 - network attacks, 164–167
 - Q&A, 173–176
 - security boundaries, 163–164
 - security controls, 154–156
 - summary and exam essentials, 168–171
 - switching technologies, 147–149
 - voice communication, securing, 160–163
 - VPNs (Virtual Private Networks), 140–143
 - WANs (wide area networks), 149–154
- companion viruses, 296
- compartmentalized environments, MAC and, 25
- compartmented mode, CPU security modes, 422–423
- compartmented mode workstations (CMWs), 422–423
- compensation, access control and, 4, 65
- compiled programming languages, 267
- compliance, verifying, 529
- Component Object Model (COM), 249–250
- composition passwords, 10
- composition theories, security models and, 456
- compromise, system, 672
- Computer-Aided Software Engineering (CASE), 269
- computer architecture, 434
 - abstraction and, 436
 - CPUs (central processing units). *see* CPUs (central processing units)
 - data hiding, 436
 - distributed architecture, 439–441
 - firmware, 434
 - hardware, 413
 - hardware segmentation, 437
 - I/O (input/output) structures, 431–434
 - lab and lab questions, 443–444
 - layering, 435–436
 - memory, 425–429
 - overview of, 412–413
 - process isolation, 436–437
 - Q&A, 445–450
 - security policies, 437–439
 - security protection mechanisms, 434–435
 - storage, 430–431
 - summary and exam essentials, 441–443
- computer crime, *see* crimes, computer
- Computer Emergency Readiness Team (CERT), 55
- computer ethics, 681–682. *see also* ethics
- computer export controls, 643
- Computer Fraud and Abuse Act of 1984 (CFAA), 633–634
- Computer Incident Response Team (CIRT)
 - responsibilities of, 673
 - security roles, 211
- Computer Security Act of 1987 (CSA), 634–635
- Computer Security Incident Response Teams (CSIRT), 673
- concentrators, network devices, 121
- concentric circle antivirus strategy, 497
- conceptual definition phase, of systems development, 270
- conclusive evidence, 650
- concurrency, multilevel databases and, 256
- conductors, network cabling, 91–92
- confidential level
 - commercial/private sector classification, 192
 - government/military classification, 191
- confidentiality
 - Bell-LaPadula model and, 459–460
 - goals of cryptography, 336
 - overview of, 180–181
 - TCSEC focus on, 471
- configuration management
 - controls, 503–504
 - systems development and, 278–279
- confinement, CIA techniques, 464
- confinement property, Bell-LaPadula state machine, 459

804 confusion and diffusion operations – CRCs

- confusion and diffusion operations, in
 - cryptography, 343
- connection technologies, WANs
 - ATM, 153
 - Frame Relay connections, 152–153
 - overview of, 151
 - SMDS, 153
 - X.25 WAN connections, 152
- connectivity. *see also* cable, network
- connectivity, network
 - overview of, 88
 - remote connectivity technology, 123
- consistency, in ACID model, 254
- constrained data item (CDI), in
 - Clark-Wilson security model, 462
- consultants, risk analysis by, 223
- content filters, 304
- contingency planning, 568
- continuity planning. *see also* BCP (business continuity planning)
 - overview of, 575
 - plan approval phase, 578
 - plan implementation phase, 578
 - protecting critical facilities, 577
 - protecting infrastructure, 577
 - protecting people, 576–577
 - provisions and processes phase of
 - continuity planning, 576
 - strategy development phase, 576
 - training and education, 578
- contractual licenses, 642
- Control Objectives for Information and Related Technology (CobiT), 193
- control zones
 - protection against EM, 483
 - TEMPEST countermeasures, 707
- controls. *see also* access control
 - administrative, 512–513
 - application, 512
 - configuration and change management, 503–504
 - hardware, 511
 - I/O, 512
 - media, 512
 - operations, 510–511
 - overview of, 464–465
 - physical security, 693–694
 - privileged entity, 511
 - security, 509–510
 - workplace, 500
- controls gap, 230
- COPPA (Children’s Online Privacy Protection Act of 1998), 646
- Copper Distributed Data Interface (CDDI), 100
- copyrights, 637–639
- CORBA (Common Object Request Broker Architecture), 248–249
- cordless phones, wireless
 - communication, 96
- corrective controls
 - access control, 3
 - security control types, 510
- cost functions, quantitative risk analysis, 223–224
- COUNT() aggregate function, SQL, 257
- counter (CTR) mode, DES, 359
- countermeasures
 - for indistinct threats, 545
 - malicious code, 304–305
 - password attacks, 307
 - physical security, 706–707
 - selecting, 230
 - SQL injection attacks, 319
- coupling, OOP terminology, 269
- covert channels, security issues, 478–479
- covert storage channel, 478
- covert timing channel, 478
- CPUs (central processing units)
 - execution methods, 414–416
 - operating modes, 424–425
 - operating states, 419–421
 - overview of, 413–414
 - processing types, 416–417
 - protection mechanisms, 417–419
 - security modes, 421–424
- CPV (certificate path validation), 388
- Crack program, dictionary attacks, 306
- crackers, hackers and attackers compared with, 64
- cracking
 - defined, 540
 - passwords, 57
- crashes (computer), initialization and failure states and, 479
- CRCs (cyclic redundancy checks), 155. *see also* message digests

- creeping privileges, 32
 - crimes, computer. *see also* laws
 - business attacks, 667–668
 - categories of computer crime, 666–667
 - evidence and, 670–671
 - financial attacks, 668
 - grudge attacks, 669–670
 - lab and lab questions, 684–685
 - laws and, 633–634
 - military and intelligence attacks, 667
 - Q&A, 686–690
 - summary and exam essentials, 683–684
 - terrorist attacks, 668
 - thrill attacks, 670
 - criminal law
 - civil law compared with, 632
 - overview of, 630–631
 - crisis management, recovery strategies, 602–603
 - critical path analysis, for secure facility plan, 693
 - criticality prioritization, 571. *see also* priorities
 - CRLs (certificate revocation lists), 389–390
 - cross-site scripting attacks. *see* XSS (cross-site scripting) attacks
 - crossover error rate (CER), biometric factor ratings, 15–16
 - cryptanalysis, 338
 - cryptography
 - in American civil war, 335
 - asymmetric. *see* asymmetric cryptography
 - attacks, 399–400
 - authentication and, 337
 - Caesar cipher, 334–335
 - ciphers, 345–351
 - concepts, 337–339
 - confidentiality and, 336
 - cryptographic keys, 351–352
 - defined, 338
 - e-commerce security, 394–395
 - email and, 391–393
 - goals of, 336
 - hashing algorithms, 356–357
 - integrity and, 336–337
 - key distribution and, 363–365
 - lab and lab questions, 367–368
 - mathematical concepts, 339–345
 - networking security, 395–398
 - nonrepudiation and, 337
 - overview of, 334
 - Q&A, 369–374
 - summary and exam essentials, 365–367
 - symmetric. *see* symmetric cryptography
 - Web communications and, 393–394
 - wireless networking security, 398–399
 - during WWII, 335–336
 - cryptology, 338
 - cryptovariables, 338. *see also* keys, cryptographic
 - CSA (Computer Security Act of 1987), 634–635
 - CSIRT (Computer Security Incident Response Teams), 673
 - CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance), 102
 - CSMA/CD (Carrier-Sense Multiple Access with Collision Detection), 100, 102–103
 - CSU/DSU (channel service unit/data service unit), 151
 - CTR (counter) mode, DES, 359
 - custodians, object access and, 32
 - CyberTrust, 466
 - cyclic redundancy checks (CRCs), 155. *see also* message digests
-
- D**
- DAA (Designated Approving Authority), 476
 - DACs (discretionary access controls), 23, 465
 - DARPA model. *see* TCP/IP (Transmission Control Protocol/Internet Protocol)
 - data classification, 190–193
 - benefits of, 190
 - commercial/private sector, 192–193
 - criteria for, 190
 - government/military sector, 191–192
 - implementation phases, 191
 - overview of, 190
 - data custodian, security roles, 212
 - Data Definition Language (DDL), 253
 - data dictionaries, for storing data, 259
 - data diddling, incremental attacks, 481

- Data Encryption Standard. *see* DES (Data Encryption Standard)
- data extraction, sampling and, 532–533
- data hiding
 - overview of, 188
 - security protection mechanisms, 436
- data integrity, incident handling and, 678
- Data Link layer (layer 2)
 - encapsulation/de-encapsulation, 81
 - overview of, 83
- Data Manipulation Language (DML), 253
- data mining, 259–260
 - for anomaly detection, 260
 - overview of, 259
 - tools, 46
- data owner, security roles, 212
- data remanence, 431
- data storage
 - lab and lab questions, 285–286
 - overview of, 260
 - Q&A, 287–292
 - summary and exam essentials, 283–285
 - threats to, 261
 - types of, 260–261
- data streams, 81
- data terminal equipment/data
 - circuit-terminating equipment (DTE/DCE), 151
- data transfer, remote journaling and, 609
- data warehouses, 259
- database management systems. *see* DBMS (database management systems)
- database security
 - aggregation and, 257–259
 - contamination, 255
 - data mining, 259–260
 - database transactions, 254–255
 - DBMS systems, 250
 - hierarchical and distributed databases, 250–251, 251
 - lab and lab questions, 285–286
 - multilevel databases, 255–257
 - ODBC and, 257, 257
 - Q&A, 287–292
 - relational databases, 251–253, 252
 - summary and exam essentials, 283–285
- databases
 - database-driven website architecture, 317, 317–318
 - recovering, 608
 - transactions, 254–255
- datagrams, UDP, 81
- DBMS (database management systems)
 - hierarchical and distributed databases, 250–251
 - overview of, 250
 - relational databases, 251–253
- DCOM (Distributed COM), 250
- DDL (Data Definition Language), 253
- DDoS (distributed denial of service) attacks, 59, 309
- de-encapsulation/encapsulation, OSI
 - model, 80, 80–81
- decentralized (distributed) access control, 27–28
- decimal system, binary compared with, 339
- decision making, BIA (business impact assessment) and, 571
- decision support systems (DSS), 263–264
- declassification, of media, 508
- decoy techniques
 - honey pots, 322
 - overview of, 322
 - pseudoflaws, 322
- dedicated lines, 149–150
- dedicated mode, CPU security, 422
- defense-in-depth. *see also* layering
 - access control and, 5
 - virus protection and, 498
- Defense Information Technology Security Certification and Accreditation Process (DITSCAP), 477
- degaussing, media, 508
- degrees, relational databases, 251
- delay feature, of mantraps, 698
- delegation, OOP terminology, 269
- deluge systems, fire suppression, 713
- denial-of-service attacks. *see* DoS (denial-of-service) attacks
- Department of Defense. *see* DoD (Department of Defense)
- Department of Defense Password Management, TCSEC green book, 469

- Deploy Inward System Access (DISA), 162
- DES (Data Encryption Standard), 357–359
 - CBC (Cipher Block Chaining) mode, 358
 - CTR (counter) mode, 359
 - ECB (Electronic Codebook) mode, 357–358
 - Kerberos and, 20
 - OFB (Output Feedback) mode, 358
 - security of, 352
- design flaws, attacks based on, 479
- design review, systems development and, 271–272
- Designated Approving Authority (DAA), 476
- detectable weaknesses, penetration testing and, 54
- detective controls
 - access control, 3
 - security control types, 510
- deterrent access control, 3
- development life cycle, 269–270
- devices
 - firmware, 434
 - I/O (input/output), 431–432
 - nodes, 84
- DHCP (Dynamic Host Configuration Protocol), 114, 147
- dial-up protocols, 125
- DIAMETER, as decentralizing access control, 28
- dictionary attacks
 - overview of, 56–58, 306
 - password attacks, 12
- differential backups, recovery planning and, 612
- Diffie-Hellman algorithm, 364
- diffusion and confusion operations, in cryptography, 343
- digital IDs. *see* message digests
- digital, LAN technologies, 101
- Digital Millennium Copyright Act of 1998 (DMCA), 638–639
- Digital Signature Standard (DSS), 385–386
- digital signatures
 - DSS (Digital Signature Standard), 385–386
 - HMAC (Hashed Message Authentication Code) and, 385
 - overview of, 384
- digital subscriber line (DSL), 149–150
- direct addressing, memory addressing schemes, 428
- direct evidence, testimonial evidence and, 651
- Direct Memory Access (DMA), 433–434
- Direct Sequence Spread Spectrum (DSSS), 93
- directive controls
 - access control, 4
 - security control types, 509
- directory services, as SSO mechanism, 22
- DISA (Deploy Inward System Access), 162
- Disaster Recovery Planning. *see* DRP (Disaster Recovery Planning)
- disasters. *see also* DRP (Disaster Recovery Planning)
 - man-made. *see* man-made disasters
 - natural. *see* natural disasters
 - nature of, 592–593
- discretionary access controls (DACs), 23, 465
- discretionary protection (Categories C1,C2), TCSEC, 467–468
- Discretionary Security Property, state machine properties, 459
- distributed architecture, 439–441
- Distributed COM (DCOM), 250
- distributed databases, 250–251
- distributed denial of service (DDoS) attacks, 59, 309
- distributed environment, application security
 - agents (bots), 246–247
 - applets, 247–248
 - COM and DCOM, 249–250
 - ORB (Object Request Broker), 248–249, 249
 - overview of, 246
- distributed reflective denial of service attacks. *see* DRDoS (distributed reflective denial of service) attacks
- DITSCAP (Defense Information Technology Security Certification and Accreditation Process), 477
- DMA (Direct Memory Access), 433–434
- DMCA (Digital Millennium Copyright Act of 1998), 638–639

808 DML (Data Manipulation Language) – dual-homed firewalls

- DML (Data Manipulation Language), 253
- DNS (Domain Name System)
 - amplification attacks, 311
 - network-based IDS lookups, 51
 - poisoning attacks, 313
 - spoofing attacks, 167
- documentary evidence, 650
- documentation
 - DRP (Disaster Recovery Planning), 617–618
 - emergency-response guidelines, 581
 - goals, 579
 - maintenance program for, 581
 - overview of, 579
 - risk acceptance/mitigation document, 580
 - risk assessment document, 580
 - statement of importance, 579
 - statement of priorities, 579–580
 - statement of urgency and timing, 579–580
 - testing program for, 581
 - vital records program, 581
- DoD (Department of Defense)
 - Bell-LaPadula model, 458
 - light yellow book, 282
 - Orange Book, 282
 - TCP/IP model. *see* TCP/IP (Transmission Control Protocol/Internet Protocol)
 - TCSEC standards. *see* TCSEC (Trusted Computer System Evaluation Criteria)
- dogs, controlling physical access, 699–700
- Domain Name System. *see* DNS (Domain Name System)
- domains
 - access control, 28
 - broadcast domains and collision domains, 120–121
 - layering and, 435
- DoS (denial-of-service) attacks, 58–59
 - DDoS (distributed denial of service) attacks, 309
 - DNS amplification attacks, 311
 - DNS poisoning, 313
 - email security and, 157
 - Gibson Research and, 674
 - host-based IDS and, 50
 - incident handling and, 673
 - land attacks, 313
 - overview of, 308
 - ping-of-death, 314
 - smurf attacks, 309–311
 - Syn flood attacks, 308–309
 - teardrop attacks, 311–313
- DRDoS (distributed reflective denial of service) attacks
 - Fraggle example, 311
 - overview of, 59
 - vulnerability exploited by, 310
- DRP (Disaster Recovery Planning). *see also* BCP (business continuity planning)
 - BCP compared with, 565
 - bombings/explosions, 598
 - CBK domains, 564
 - earthquakes, 593–594
 - fires, 596–597
 - floods, 594–595
 - hardware/software failures, 599–600
 - lab and lab questions, 621–622
 - man-made disasters, 597
 - natural disasters, 593
 - nature of disasters, 592–593
 - overview of, 592
 - picketing and strikes, 600
 - power outages, 598–599
 - Q&A, 623–628
 - recovery plan. *see* recovery planning
 - recovery strategies. *see* recovery strategies
 - regional events, 597
 - storms, 596
 - summary and exam essentials, 620–621
 - terrorist-related, 597–598
 - testing and maintenance, 618–620
 - theft and vandalism, 601
 - training and documentation, 617–618
 - Unix and, 547
 - utility and infrastructure failures, 599
- dry pipe systems, fire suppression, 713
- DSL (digital subscriber line), 149–150
- DSS (decision support systems), 263–264
- DSS (Digital Signature Standard), 385–386
- DSSS (Direct Sequence Spread Spectrum), 93
- DTE/DCE (data terminal equipment/data circuit-terminating equipment), 151
- dual-homed firewalls, 118–119

due care
 Federal Sentencing Guidelines (1991), 635
 standards, 504

due diligence
 contingency planning and, 568
 standards, 504

dumb cards, technical controls for physical security, 704

dumpster diving
 overview of, 542–543
 reconnaissance attacks, 320–321

durability, in ACID model, 255

dwel time, keystroke patterns, 15

dynamic content, static web pages and, 317

Dynamic Host Configuration Protocol (DHCP), 114, 147

dynamic NAT, 146

dynamic passwords, 10

dynamic Web applications, 317–318

E

e-commerce security
 overview of, 394
 SET (Secure Electronic Transaction), 394–395

EAC (electronic access control), 701

EAP (Extensible Authentication Protocol)
 authentication protocols, 126
 PPTP and, 142

earthquakes
 DRP and, 593–594
 hazard map of U.S., 573

eavesdropping
 on networks, 165
 overview of, 164–165, 542
 work area design and, 696

ECB (Electronic Codebook) mode, DES, 357–358

Economic and Protection of Proprietary Information Act of 1996, 645

Economic Espionage Act (1996), 642

ECPA (Electronic Communications Privacy Act of 1986), 645

education
 continuity planning, 578
 disaster recovery, 617–618
 security awareness training, 231

EEPROM (electronically erasable programmable read-only memory), 426

EF (exposure factor), in BCP, 574

egress filtering, preventing smurf attacks, 310

eigenfeatures/eigenfaces, biometrics and, 13

El Gamal algorithm, 379

El Gamal, Dr. T., 379

electricity, environmental safety and, 708–709

electromagnetic (EM) radiation, security issues, 483

electromagnetic interference (EMI), 542, 709

electronic access control (EAC), 701

Electronic Codebook (ECB) mode, DES, 357–358

Electronic Communications Privacy Act of 1986 (ECPA), 645

electronic serial numbers (ESNs), 163

electronic vaulting, recovery strategies, 608–609

electronically erasable programmable read-only memory (EEPROM), 426

elliptic curve cryptography, 379–380

EM (electromagnetic radiation), security issues, 483

email security, 156–159
 goals of, 156–157
 issues, 157–158
 MOSS (MIME Object Security Services), 392
 overview of, 156
 PEM (Privacy Enhanced Mail), 392
 PGP and, 391
 S/MIME (Secure Multipurpose Internet Mail Extensions), 392–393
 solutions, 158–159
 spamming attacks, 64

emanation security, 706

emergency communications, 603

emergency response
 guidelines, 581
 recovery plan, 610–611

810 EMI (electromagnetic interference) – explosions/bombings

- EMI (electromagnetic interference), 542, 709
- employees
 - background checks, 208
 - employment agreements, 208–209
 - job descriptions, 206–208
 - NCAAs (noncompete agreements), 209
 - NDAAs (nondisclosure agreements), 208
 - sabotage by, 547
 - termination issues, 209–211
 - training for disaster preparedness, 617
- Encapsulating Security Payload (ESP),
 - IPSec, 143, 396–397
- encapsulation/de-encapsulation
 - abstraction and, 282
 - OSI model, 80, 80–81
- encrypted viruses, technologies for escaping
 - detection, 299
- encryption
 - end-to-end, 395–396
 - export controls, 643–644
 - overview of, 188
 - preventing brute-force attacks, 58
 - wireless networking (802.11), 98
- end-to-end encryption, 395–396
- END TRANSACTION, database
 - transactions, 254
- Enigma cipher, 335–336
- enrollment process, PKI, 388
- enterprise extended mode, wireless
 - networking (802.11), 96
- enticement, honey pots and, 53
- entrapment, honey pots and, 53
- environmental safety
 - fire detection and suppression, 710–714
 - noise and, 709
 - overview of, 707
 - personnel safety, 707
 - power and electricity and, 708–709
 - temperature, humidity, and static, 709–710
 - water and, 710
- EPROM (erasable programmable read-only memory), 426
- equal error rate (ERR), biometric factor
 - ratings, 15
- equipment failure, physical security
 - and, 715
- erasable programmable read-only memory (EPROM), 426
- erasing media, 508
- ERR (equal error rate), biometric factor
 - ratings, 15
- errors, vulnerabilities, 545
- ESNs (electronic serial numbers), 163
- ESP (Encapsulating Security Payload),
 - IPSec, 143, 396–397
- espionage
 - industrial, 667
 - overview of, 548–549
- Ethernet, 100
- ethical hacking, 540. *see also*
 - penetration testing
- ethics
 - 10 commandments of computer ethics, 681–682
 - Internet and, 681
 - (ISC)² code of, 680–681
 - overview of, 680
 - Q&A, 686–690
 - summary and exam essentials, 683–684
- event logs
 - access control and, 30
 - monitoring and, 46
- events, compared with incidents, 671
- evidence, 649–652
 - admissibility of, 650
 - chain of, 651
 - collecting, 652
 - computer crime and, 670–671
 - gathering in incident response process, 676–677
 - overview of, 649–650
 - types of, 650–652
- excessive privileges, 32
- exclusive OR (XOR) operation, logical
 - operations, 341
- .exe files, file infector viruses and, 296
- execution methods, CPUs, 414–416
- exit interviews, employee termination, 210
- expert opinions, testimonial evidence
 - and, 651
- expert systems, 262–263
- exploitation of collision attacks, 56–57
- explosions/bombings, DRP and, 598

export/import laws, 643–644
 exposure factor (EF)
 in BCP, 574
 cost functions in quantitative risk analysis, 223–224
 exposure, risk terminology, 219
 Extensible Authentication Protocol (EAP)
 authentication protocols, 126
 PPTP and, 142
 external auditors, 534–535
 external communications, recovery plan, 616
 external storage devices, workstation management and, 500
 extranets, 116

F

face scans, biometrics, 13
 facilities
 accessibility, 695
 cold sites, 604–605
 controls, 693–694
 designing for physical security, 695
 hot sites, 605–606
 mobile sites, 606
 multiple sites, 607
 natural disasters and, 695
 personnel safety and, 707
 physical security requirements, 692–693
 protecting in continuity planning, 577
 secure facility plan, 693
 server rooms, 696–697
 site selection, 694–695
 visibility, 695
 visitors and, 696
 warm sites, 606
 work areas, 696
 fail-open, avoiding system failure, 265–266
 fail-safe, failover solutions, 127
 fail-secure, failover solutions, 127, 265–266
 fail-soft, failover solutions, 127
 failover solutions, 127–128
 failure states, security issues, 479
 false acceptance rate (FAR), biometric factor ratings, 15–16
 false rejection rate (FRR), biometric factor ratings, 15–16
 Family Educational Rights and Privacy Act (FERPA), 647
 FAR (false acceptance rate), biometric factor ratings, 15–16
 Faraday cages
 protection against EM, 483
 TEMPEST countermeasures, 706
 fax communications, security of, 159
 FBI
 InfraGard program of, 677
 National Computer Crime Squad, 652
 FDDI (Fiber Distributed Data Interface), 100
 Federal Emergency Management Agency (FEMA)
 National Flood Insurance Program, 595
 on seismic hazards, 593–594
 Federal Information Processing Standard (FIPS) 1880, 381
 Federal Sentencing Guidelines (1991), 635
 feedback loop characteristic, in waterfall model, 273
 FEMA (Federal Emergency Management Agency)
 National Flood Insurance Program, 595
 on seismic hazards, 593–594
 fences, controlling physical access, 698
 FERPA (Family Educational Rights and Privacy Act), 647
 FHSS (Frequency Hopping Spread Spectrum), 93
 Fiber Distributed Data Interface (FDDI), 100
 fiber optic cable, 92
 fields, relational databases, 251
 file infector viruses, 296
 File Transfer Protocol (FTP), 114
 filters
 antivirus, 304
 firewalls, 117
 preventing smurf attacks, 310
 financial attacks, categories of computer crime, 668
 Finger, Internet Worm example, 302
 fingerprint checksums. *see* message digests
 fingerprints, biometrics and, 13
 finite state machine (FSM), 455
 FIPS (Federal Information Processing Standard) 1880, 381
 fire detection systems, 713

812 fire extinguishers – half-duplex communication

fire extinguishers, 712–714
 fire suppression systems, 713–714
 fires
 damage caused by, 714
 detection and suppression, 710–714
 man-made disasters, 597
 natural disasters, 596
 firewalls
 deployment architectures, 119–120, 120
 IDS compared with, 48–49
 overview of, 116–117
 types of, 117–119
 firing employees, 210–211
 firmware, 434
 first-generation firewalls, 117
 flash floods, DRP and, 594
 Flask OS, Fluke research, 551
 flight time, keystroke patterns, 15
 flooding attacks
 DoS (denial-of-service) attacks and, 58
 email security and, 158
 floods
 DRP and, 594–595
 hazard map of Miami-Dade County, Florida, 595
 water leaks and, 710
 Fluke research OS, 551
 footers, OSI model, 80
 foreign keys, relational databases, 253
 formats
 Presentation layer, 85–86
 reporting and, 532
 Fourth Amendment, privacy rights in, 644
 fraggle attacks, 60, 311
 fragmentation attacks, 311–312, 312
 frames, layer 2, 81
 fraud
 voice communication security, 161–162
 vulnerabilities, 545–546
 frequency
 cordless phones, 96
 wireless communication, 93
 Frequency Hopping Spread Spectrum (FHSS), 93
 FRR (false rejection rate), biometric factor ratings, 15–16
 FSM (finite state machine), 455
 FTP (File Transfer Protocol), 114

full backups, 612
 full-duplex communication, 85, 100
 full-interruption test, disaster preparedness, 619
 Full-knowledge team, for penetration testing, 539
 functional requirements determination, systems development and, 271
 functionality, vs. user friendliness vs. security, 267
 FunLove virus, 497
 fuzzy logic, 263

G

Gantt charts, 277, 277–278
 gas discharge fire suppression system, 713–714
 gates, controlling physical access, 698
 gateways, network devices, 122
 generations, programming languages, 268
 GFS (Grandfather-Father-Son), tape rotation strategy, 615
 Gibson Research, 674
 GISRA (Government Information Security Reform of 2000), 635, 636–637
 GLBA (Gramm-Leach-Bliley Act of 1999), 646
 GnuPG, email security solutions, 158
 goals, documenting, 579
 Government Information Security Reform of 2000 (GISRA), 635, 636–637
 Gramm-Leach-Bliley Act of 1999 (GLBA), 646
 Grandfather-Father-Son (GFS), tape rotation strategy, 615
 gray boxes, 280
 Green book, rainbow series, 469–471
 grudge attacks, 669–670

H

hackers, 64
 hailstorms, DRP and, 596
 half-duplex communication, 85

- Halon/Halon substitutes, fire suppression, 714
 - hand geometry, biometrics and, 14
 - hardening provisions, for building and facilities and infrastructure, 577
 - hardware
 - CBK domains, 78
 - controls, 511
 - DRP and, 599–600
 - overview of, 413
 - replacement options in recovery, 607
 - hardware segmentation, security control architecture, 280, 437
 - hash functions, 380–383
 - MD2 (Message Digest 2), 382
 - MD4 (Message Digest 4), 382–383
 - MD5 (Message Digest 5), 383
 - overview of, 380–381
 - SHA (Secure Hash Algorithm), 381–382
 - hash totals, integrity verification, 154–155
 - Hashed Message Authentication Code (HMAC)
 - digital signatures and, 385
 - hashing algorithms, 356
 - hashing algorithms, 356–357
 - HDLC (High-Level Data Link Control), 153
 - headers
 - OSI model, 80
 - TCP, 108–109
 - UDP, 110
 - Health Insurance Portability and Accountability Act of 1996. *see* HIPAA (Health Insurance Portability and Accountability Act of 1996)
 - hearsay evidence, 652
 - heart/pulse patterns, biometrics and, 14
 - heating, ventilating, and air conditioning (HVAC), 693
 - heuristics-based detection. *see* behavior-based IDS
 - hierarchical databases, 250–251, 251
 - hierarchical environments, MAC and, 25
 - hierarchical storage management (HSM), 615
 - High-Level Data Link Control (HDLC), 153
 - high-level programming languages, 267
 - High Speed Serial Interface (HSSI), 153
 - hijack attacks, 63
 - HIPAA (Health Insurance Portability and Accountability Act of 1996)
 - disaster recovery and, 620
 - monitoring and, 47
 - privacy laws in U.S., 645
 - HMAC (Hashed Message Authentication Code)
 - digital signatures and, 385
 - hashing algorithms, 356
 - hoaxes, virus, 300
 - honey pots
 - decoy techniques, 322
 - overview of, 52–53
 - host-based IDS, 50
 - Host-to-Host layer (Transport layer), TCP/IP, 87
 - hostile applets, 303
 - hot rollover, failover solutions, 127
 - hot sites, recovery strategies, 605–606
 - hot-swappable RAID, 129
 - HSM (hierarchical storage management), 615
 - HSSI (High Speed Serial Interface), 153
 - HTTP (HyperText Transport Protocol), 114
 - hubs, network devices, 121
 - humidity, environmental safety and, 709–710
 - hurricanes, DRP and, 596
 - HVAC (heating, ventilating, and air conditioning), 693
 - hybrid attacks, password attacks, 12
 - hybrid environments, MAC and, 25
 - hybrid response, IDS, 48
 - hyperlink spoofing attacks, 167
 - HyperText Transport Protocol (HTTP), 114
-
- I/O (input/output)
 - controls, 512
 - structures, 431–434
 - IAB (Internet Advisory Board), 681

814 ICMP (Internet Control Message Protocol) DRDoS... – information security

- ICMP (Internet Control Message Protocol)
 - DRDoS attacks and, 310
 - smurf attacks and, 60
 - TCP/IP Network layer protocols, 111
- ID. *see* identification (ID)
- IDEA (International Data Encryption Algorithm), 360
- IDEAL model, 275–276, 276
- identification (ID). *see also* authentication
 - accountability, 5
 - overview of, 9, 184
 - physical access control, 701
 - smart cards and, 704
- identification phase, of incident response process, 675
- Identity Theft and Assumption Deterrence Act, 647
- IDL (Interface Definition Language), 249
- IDS (intrusion detection systems)
 - honeypots, 52–53
 - host-based, 50
 - knowledge and behavior-based, 51–52
 - lab and lab questions, 68–69
 - logon prompt attacks and, 12
 - monitoring and, 528
 - network-based, 50–51
 - overview of, 47–50
 - padded cells, 53
 - Q&A, 70–75
 - summary and exam essentials, 65–68
 - technical controls for physical security, 705–706
 - vulnerability scanners, 53–54
- IEEE 802.11. *see* wireless networking (IEEE 802.11)
- IETF (Internet Engineering Task Force), 396
- IGMP (Internet Group Management Protocol), 112
- IKE (Internet Key Exchange), 397
- illegal activities
 - software monitoring, 535. *see also* crimes, computer
 - types of, 505
- IMAP4 (Internet Message Access Protocol 4)
 - email security and, 156
 - TCP/IP application layer protocols, 114
- immediate addressing, memory addressing schemes, 428
- impact assessment, in BC, 573–575
- impersonation
 - second-tier attacks, 166
 - spoofing attacks and, 62
- implementation attacks, cryptographic attacks, 399
- implementation phase, BCP plan, 578
- implementation, team approach to, 569
- import/export laws, 643–644
- importance statement, in continuity planning, 579
- inappropriate activities, 544–545, 554–555
- incident handling
 - data integrity and retention, 678
 - DoS attacks, 673
 - interviews and interrogations, 678
 - lab and lab questions, 684–685
 - malicious code, 673
 - overview of, 671
 - Q&A, 686–690
 - reporting incidents, 678–679
 - response process, 675–677
 - response teams, 673–675
 - scanning attacks, 672
 - summary and exam essentials, 683–684
 - system compromise, 672
 - types of incidents, 672
- incidents, compared with events, 671
- incremental attacks, 481–482
- incremental backups, 612
- indirect addressing, memory addressing schemes, 428
- industrial espionage, 667
- inference attacks, database security and, 258–259
- inference engine, in expert systems, 262
- information flow models
 - Bell-LaPadula model, 458–460
 - Biba model, 460–461
 - noninterference models based on, 456
 - overview of, 455–456
- information gathering, dumpster diving, 542
- information security. *see* security models

- Information Systems Audit and Control Association (ISACA), 193
- Information Technology Infrastructure Library (ITIL), 193
- Information Technology Security Evaluation and Criteria. *see* ITSEC (Information Technology Security Evaluation and Criteria)
- informative policies, security policies, 215
- InfraGard program, of FBI, 677
- infrastructure
 - BCP and, 577
 - DRP and, 599
 - preventing loss of support, 547
- Infrastructure mode, wireless networking (802.11), 96
- inheritance, OOP terminology, 269
- initial program load (IPL), 550
- initialization states, security issues, 479
- input checking, security issues, 480
- input/output. *see* I/O (input/output)
- input validation, preventing SQL injection, 319
- insider threat, 669
- instances, OOP terminology, 269
- insurance, ACV (actual cost evaluation) and, 602
- Integrated Services Digital Network (ISDN), 150–151
- integrity
 - Biba model and, 460
 - Clark-Wilson model and, 461
 - of data in incident handling, 678
 - goals of cryptography, 336–337
 - overview of, 181–182
 - verifying, 154–155
- integrity verification procedure (IVP), in Clark-Wilson security model, 462
- intellectual property
 - copyrights, 637–639
 - Digital Millennium Copyright Act (1998), 638–639
 - licensing, 642–643
 - overview of, 637
 - patents, 640–641
 - trade secrets, 641–642
 - trademarks, 639–640
- intelligence attacks, computer crime, 667
- intent to use, trademarks and, 640
- Interface Definition Language (IDL), 249
- interim reports, of external auditors, 534
- International Data Encryption Algorithm (IDEA), 360
- International Information Systems Security Certification Consortium. *see* (ISC)²
- International Organization for Standardization (ISO), 78
- International Organization on Computer Evidence (IOCE), 652
- Internet Advisory Board (IAB), 681
- Internet Control Message Protocol. *see* ICMP (Internet Control Message Protocol)
- Internet Engineering Task Force (IETF), 396
- Internet ethics, 681–682
- Internet Group Management Protocol (IGMP), 112
- Internet Key Exchange (IKE), 397
- Internet layer (Network layer), TCP/IP, 87
- Internet Message Access Protocol 4 (IMAP4)
 - email security and, 156
 - TCP/IP application layer protocols, 114
- Internet Protocol Security. *see* IPsec (Internet Protocol Security)
- Internet Security Association and Key Management Protocol (ISAKMP), 397–398
- Internet Worm example, 302–303
- interpreted programming languages, 267
- interrogations, incident handling, 678
- interrupts (IRQ), 433
- interviews, incident handling, 678
- intranets, 116
- intrusion alarms, 702
- intrusion detection systems. *see* IDS (intrusion detection systems)
- intrusion prevention system (IPS), 54
- investigations
 - conducting, 653–654
 - evidence, 649–652
 - law enforcement and, 652
 - overview of, 649
 - search warrants and, 653

IOCE (International Organization on Computer Evidence), 652

IP addresses

- domain name resolution and, 115–116
- PAT and NAT and, 144
- private, 145
- RFC 1918, 146–147

IP (Internet Protocol)

- IP classes, 113
- IPv4 vs. IPv6, 111
- TCP/IP Network layer protocols, 110

IP Payload Compression (IPcomp) protocol, 397

IP probes (IP sweeps), reconnaissance attacks, 319

IP spoofing attacks, 321

IPcomp (IP Payload Compression) protocol, 397

IPL (initial program load), 550

IPS (intrusion prevention system), 54

IPSec (Internet Protocol Security)

- components of, 143
- NAT compatibility and, 146
- networking security, 396–397
- VPN links for securing TCP/IP, 106

Iris scans, biometrics and, 14

IRQ (interrupts), 433

ISACA (Information Systems Audit and Control Association), 193

ISAKMP (Internet Security Association and Key Management Protocol), 397–398

(ISC)²

- code of ethics, 680–681
- defining steps in BCP process, 564–565

ISDN (Integrated Services Digital Network), 150–151

ISO (International Organization for Standardization), 78

isolation

- in ACID model, 255
- CIA techniques, 464
- in incident response process, 676
- security control architecture, 280, 436–437

ITGI (IT Government Institute), 193

ITIL (Information Technology Infrastructure Library), 193

ITSEC (Information Technology Security Evaluation and Criteria)

- change management and, 189
- classes, 471
- comparing security evaluation standards, 475
- overview of, 466–467
- security baselines, 216

IVP (integrity verification procedure), in Clark-Wilson security model, 462

J

Jamming, protection against EM, 483

Java applets

- countermeasure to malicious code, 304
- hostile applets, 303
- overview of, 248

job descriptions, 206–208

job responsibilities, 207

job rotation, 207

journaling, remote journaling as Recovery strategy, 609

K

KDC (key distribution center), Kerberos, 20–21

KDD (Knowledge Discovery in Databases), 259. *see also* data mining

Kerberos, 20–22

- limitations of, 21–22
- logon process, 21
- overview of, 20–21
- as SSO mechanism, 20
- as ticket authentication system, 20

Kerchoff principle, 338

kernel mode, protection rings, 419

kernels

- program executive or process scheduler, 421
- protection rings and, 418
- security, 455

- key distribution center (KDC), Kerberos, 20–21
 - keyboards/mice, 432
 - keys and locks, controlling physical access, 700–701
 - keys, cryptographic
 - algorithms and, 338
 - asymmetric key algorithms, 353–356
 - clustering, 345
 - deciding which key to use, 385
 - distribution of, 363–365
 - key escrows, 344, 364
 - key space, 338
 - length of, 352, 378–379
 - managing within PKI infrastructure, 390
 - one-time pads and, 349
 - overview of, 351–352
 - public and private, 377
 - strengths of asymmetric keys, 355
 - symmetric key algorithms, 352–353
 - keystroke monitoring, types of monitoring tools, 536
 - keystroke patterns, biometrics and, 15
 - know plain-text attacks, cryptographic attacks, 399
 - knowledge base, expert systems, 262
 - knowledge-based systems
 - decision support, 263–264
 - expert systems, 262–263
 - intrusion detection, 51–52
 - lab and lab questions, 285–286
 - neural networks, 263
 - overview of, 261–262
 - Q&A, 287–292
 - security applications of, 264
 - summary and exam essentials, 283–285
 - Knowledge Discovery in Databases (KDD), 259. *see also* data mining
 - Koblitz, Neil, 379
 - KryptoKnight, as SSO mechanism, 20, 22
-
- L**
- L2F (Layer 2 Forwarding), 143
 - L2TP (Layer 2 Tunneling Protocol), 106, 143
 - labels, security, 453
 - LAN extenders, network devices, 123
 - land attacks, 61, 313
 - LANs (local area networks)
 - media access technologies, 102–103
 - primary LAN technologies, 99–100
 - subtechnologies, 101
 - WANs compared with, 88
 - lattice-based access control, 26, 27, 458
 - law enforcement, calling, 652
 - Law, Investigation, and Ethics domain, CBK, 666
 - laws. *see also* crimes, computer
 - administrative category, 632
 - categories, generally, 630
 - CFAA (Computer Fraud and Abuse Act of 1984), 633–634
 - civil category, 632
 - computer crime, 633
 - Computer Security Act (1987), 634–635
 - copyrights, 637–639
 - criminal category, 630–631
 - Digital Millennium Copyright Act (1998), 638–639
 - Economic Espionage Act (1996), 642
 - evidence, 649–652
 - Federal Sentencing Guidelines (1991), 635
 - Government Information Security Reform Act (2000), 636–637
 - import/export, 643–644
 - intellectual property and, 637
 - investigations, 649, 652–654
 - lab and lab questions, 656–657
 - law enforcement, calling in, 652
 - licensing, 642–643
 - National Information Infrastructure Protection Act (1996), 636
 - overview of, 633
 - Paperwork Reduction Act (1995), 635
 - patents, 640–641
 - privacy laws in European Union, 648–649
 - privacy laws in U.S., 644–648
 - Q&A, 658–663
 - summary and exam essentials, 654–655

818 layer 1 – MAC (mandatory access control)

- trade secrets, 641–642
 - trademarks, 639–640
 - Uniform Computer Information Transactions Act, 643
 - layer 1. *see* Physical layer (layer 1)
 - layer 2. *see* Data Link layer (layer 2)
 - Layer 2 Forwarding (L2F), 143
 - Layer 2 Tunneling Protocol (L2TP), 106, 143
 - layer 3. *see* Network layer (layer 3)
 - layer 4. *see* Transport layer (layer 4)
 - layer 5. *see* Session layer (layer 5)
 - layer 6. *see* Presentation layer (layer 6)
 - layer 7. *see* Application layer (layer 7)
 - layered environments, access control in, 4–5
 - layering
 - overview of, 187–188
 - security protection mechanisms, 435–436
 - leased lines, 149–150
 - least and most significant string bits, cryptography and, 343
 - least privilege, principle of, 438
 - least significant string bits, in cryptography, 343
 - legal defensible security, 187
 - legal requirements
 - for BCP, 569–570
 - organizations, 505
 - lessons learned, incident response process and, 677
 - levels, vs. protection rings in computer architecture, 435
 - licensing, 642–643
 - Life cycle models
 - IDEAL model, 275–276, 276
 - overview of, 272–273
 - software capability maturity model, 275
 - spiral model, 274, 274
 - waterfall model, 273, 273–274
 - life safety, 707. *see also* environmental safety
 - lifecycle assurance, 499
 - lighting, perimeter security and, 698–699
 - likelihood assessment, in BC, 572–573
 - limit checks, avoiding system failure, 265
 - Line Print Daemon (LPD), 114
 - link encryptions, protecting network data, 395
 - Linux vulnerabilities, 550–551
 - LLC (Logical Link Control), 83
 - local alarm systems, 702, 705
 - local area networks. *see* LANs (local area networks)
 - local environment, application security in. *see* nondistributed environment, application security in
 - locks, controlling physical access, 700–701
 - logic bombs, 246, 300
 - Logical Link Control (LLC), 83
 - logical location, authentication factors, 6–7
 - logical operations, cryptography, 339–341
 - logical security, vs. physical, 217
 - logical/technical access control, 4
 - logical topologies, 103
 - login
 - account lockout and, 12
 - brute-force (dictionary) attacks, 57
 - logistics, disaster recovery and, 616
 - logon scripts, as SSO mechanism, 22
 - logs
 - access control and, 30
 - analysis of, 528
 - monitoring with, 46
 - physical access control and, 705
 - problem identification and, 531
 - transmission logging, 155
 - LOMAC (Low Water-Mark Mandatory Access Control), Linux, 551
 - loopback addresses, 147
 - Low Water-Mark Mandatory Access Control (LOMAC), Linux, 551
 - LPD (Line Print Daemon), 114
-
- M**
- MAAs (mutual assistance agreements), 607–608
 - MAC addresses, ARP spoofing attacks, 166–167
 - MAC (mandatory access control)
 - overview of, 24–25
 - types of security controls, 465
 - user account management, 501

- MAC (Media Access Control), Data Link layer and, 83
- Mac OS, viruses and, 297
- machine languages, security and, 267
- macros, viruses, 296–297
- mail-bombing, 157
- main memory. *see* primary (real) memory
- maintenance
 - continuity planning documents, 581
 - disaster recovery and, 618–620
 - systems development and, 272
 - team approach to, 569
- maintenance hooks, 481
- malicious attackers, 548. *see also* attackers
- malicious code. *see also* application attacks
 - active content and, 303
 - countermeasures, 304–305
 - DoS attacks. *see* DoS
 - (denial-of-service) attacks
 - email security and, 157
 - incident handling and, 673
 - lab and lab questions, 324–325
 - logic bombs, 300
 - overview of, 294, 549
 - password attacks. *see* password attacks
 - Q&A, 326–331
 - sources of, 294–295
 - spyware and adware, 303
 - summary and exam essentials, 323–324
 - Trojan horses, 300–301
 - viruses. *see* viruses
 - worms, 301–303
- man-in-the-middle attacks, 63, 400
- man-made disasters
 - bombings/explosions, 598
 - DRP and, 597
 - fires, 597
 - hardware/software failures, 599–600
 - picketing and strikes, 600
 - power outages, 598–599
 - terrorist-related, 597–598
 - theft and vandalism, 601
 - utility and infrastructure failures, 599
- mandatory access control. *see* MAC (mandatory access control)
- mandatory protection (Categories B1, B2, B3), TCSEC, 468
- mantraps, controlling physical access, 698
- manual recovery, types of trusted recovery, 502
- marking/labeling media, 506
- Marzia virus, 299
- masquerading attacks
 - access abuses, 705
 - overview of, 321
 - second-tier attacks, 166
 - session hijacking attacks, 321–322
 - spoofing attacks and, 62, 321
- massively parallel processing (MPP), 414–415
- master boot record. *see* MBR (master boot record)
- mathematical concepts, in cryptography, 339–345
 - binary numbers, 339
 - clustering, 345
 - confusion and diffusion operations, 343
 - least and most significant string bits, 343
 - logical operations, 339–341
 - modulo function, 342
 - nonce, 343
 - one-way functions, 342
 - split knowledge, 344
 - work function, 345
 - zero-knowledge proof, 343–344, 344
- MAX() aggregate function, SQL, 258
- maximum tolerable downtime (MTD), 572
- MBR (master boot record)
 - boot sector compared with, 296
 - MBR virus, 295–296
 - stealth virus, 299
- MD2 (Message Digest 2), 356, 382
- MD4 (Message Digest 4), 356, 382–383
- MD5 (Message Digest 5), 356, 383
- mean time to failure (MTTF)
 - equipment failure and, 715
 - media life span, 507
- media, 506–509
 - formats of backup media, 613–614
 - handling, 506–507
 - life span of, 507–508
 - maintaining/destroying, 534
 - marking/labeling, 506
 - overview of, 506

- 820 Media Access Control (MAC) – Mueller, Frederic
- preventing disclosure via reuse, 508–509
 - security of, 431
 - storing, 507, 613
 - Media Access Control (MAC), Data Link layer and, 83
 - media access technologies, LANs, 102–103
 - media controls, 512
 - mediated-access model, 418
 - meet-in-the-middle attacks, 400
 - memory
 - addressing, 427–428
 - primary vs. secondary, 430
 - RAM, 426–427
 - registers, 427
 - ROM, 425–426
 - secondary, 428–429
 - security issues and, 429
 - memory cards, 704
 - memory-mapped I/O, 433
 - Merkle-Hellman Knapsack algorithm, 378
 - Mesh topology
 - network topologies, 106
 - overview of, 105
 - message digests. *see also* hash functions
 - hashing algorithms and, 356
 - integrity verification, 154
 - MD2, 356, 382
 - MD4, 356, 382–383
 - MD5, 356, 383
 - overview of, 380
 - messages, OOP terminology, 269
 - metamodels, spiral model as, 274
 - methods, OOP terminology, 269
 - mice/keyboards, 432
 - microcode. *see* firmware
 - Microsoft
 - Back Orifice trojan and Windows, 301
 - component models, 249–250
 - macro viruses infecting Office suite, 297
 - Trustworthy Computing Initiative, 480
 - viruses targeting Windows, 297
 - Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), 142
 - military attacks, categories of computer crime, 667
 - Miller, Victor, 379
 - MIME Object Security Services (MOSS), 158, 392
 - MIN() aggregate function, SQL, 258
 - MINs (mobile identification numbers), 163
 - minutia matching, biometrics and, 13
 - MIPS (million instructions per second), processor speeds, 413–414
 - mirrored ports, network-based IDS and, 51
 - mirroring, remote mirroring as recovery strategy, 609
 - mobile identification numbers (MINs), 163
 - mobile sites, recovery strategies, 606
 - modems, 432
 - modification attacks, second-tier attacks, 166
 - modulo (%) function, in cryptography, 342
 - Mondex payment system, 395
 - monitoring. *see also* auditing
 - access control and, 30
 - defined, 528
 - keystroke monitoring, 536
 - lab and lab questions, 65–68
 - overview of, 46–47, 535
 - Q&A, 70–75, 557–562
 - summary and exam essentials, 65–68, 552–553
 - tools for, 536–537
 - traffic/trend analysis, 536
 - warning banners, 535
 - monitors, 431
 - Morris, Robert Tappan, 302
 - MOSS (MIME Object Security Services), 158, 392
 - most significant string bits, in cryptography, 343
 - motion detectors (sensors), controlling physical access, 702
 - MPP (massively parallel processing), 414–415
 - MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 142
 - MTD (maximum tolerable downtime), 572
 - MTTF (mean time to failure)
 - equipment failure and, 715
 - media life span, 507
 - Mueller, Frederic, 382

multicasts, LAN technologies, 101
 multihomed firewalls, 118–119
 multilevel databases, 255–257
 multilevel mode, CPU security modes, 423
 multipartite viruses, 299
 multiple sites, recovery strategies, 607
 multiprocessing, processor execution methods, 414
 multiprogramming, processor execution methods, 415
 multistate processors, 416
 multitasking
 multiprogramming compared with, 415
 processor execution methods, 414
 multithreading, processor execution methods, 416
 multitier architecture, for firewalls, 119
 mutual assistance agreements (MAAs), 607–608

N

name resolution, TCP/IP, 115–116
 NAS (network attached storage), 614
 NAT (Network Address Translation), 144–147
 APIPA, 147
 overview of, 144–145
 private IP addresses and, 145
 stateful NAT, 146
 static and dynamic NAT, 146
 National Computer Crime Squad, of FBI, 652
 National Computer Security Association (NCSA), 297
 National Flood Insurance Program, FEMA, 595
 National Information Assurance Certification and Accreditation Process (NIACAP), 477–478
 National Information Infrastructure Protection Act (1996), 636
 National Institute of Standards and Technology. *see* NIST (National Institute of Standards and Technology)
 National Security Agency (NSA), 635

natural disasters
 earthquakes, 593–594
 facility site selection and, 695
 fires, 596
 floods, 594–595
 overview of, 593
 regional events, 597
 storms, 596
 NCAs (noncompete agreements), employment agreements, 209
 NCSA (National Computer Security Association), 297
 NDAs (nondisclosure agreements)
 employment agreements, 208
 trade secrets and, 641
 need-to-know
 access control, 24–25, 31
 overview of, 500
 negligence, Federal Sentencing Guidelines (1991), 635
 NetSP, as SSO mechanism, 20, 22
 NetWitness, sniffers, 165
 Network Access (Data Link layer), TCP/IP, 87
 Network Address Translation. *see* NAT (Network Address Translation)
 network attached storage (NAS), 614
 network-based IDS, 50–51
 network devices
 firewalls. *see* firewalls
 list of, 121–123
 Network layer and, 83–84
 Physical layer and, 82
 Network File System (NFS), 114
 Network layer (layer 3)
 encapsulation/de-encapsulation, 81
 overview of, 83–84
 network layer protocols, TCP/IP, 110–113
 network protocols
 application layer protocols, 113–114
 network layer protocols, 110–113
 TCP/IP, 105–106
 transport layer protocols, 107–110
 network topologies
 Bus, 104, 104
 Mesh, 105, 106
 overview of, 103

822 networking – object-oriented programming (OOP)

- Ring, 103–104, 104
 - Star, 105, 105
 - networking
 - cabling. *see* cable, network
 - devices. *see* network devices
 - lab and lab questions, 131–132
 - local networks. *see* LANs (local area networks)
 - OSI model. *see* OSI model
 - protocols. *see* network protocols
 - Q&A, 133–138
 - redundancy/failover. *see* redundancy/failover
 - secure communications. *see* secure communications protocols
 - security, 123–124
 - summary and exam essentials, 129–131
 - TCP/IP. *see* TCP/IP (Transmission Control Protocol/Internet Protocol)
 - topologies. *see* network topologies
 - wireless communication. *see* wireless communication
 - networking security
 - circuit encryption, 395–396
 - cryptography, 395–398
 - IPSec and, 396–397
 - ISAKMPand, 397–398
 - overview of, 395
 - password attacks, 11
 - neural networks, 263
 - Next-Generation Intrusion Detection Expert System (NIDES), 264
 - NFS (Network File System), 114
 - NIACAP (National Information Assurance Certification and Accreditation Process), 477–478
 - NIDES (Next-Generation Intrusion Detection Expert System), 264
 - Nimda virus, 497
 - NIST (National Institute of Standards and Technology)
 - CSA (Computer Security Act of 1987), 635
 - DSS (Digital Signature Standard), 385–386
 - MSR (Minimum Security Requirements), 8
 - Rijndael block cipher, 361
 - SHA (Secure Hash Algorithm) and, 381
 - Skipjack and, 361
 - standards for perimeter protection, 699
 - noise
 - environmental safety and, 709
 - protection against EM, 483
 - nonce, in cryptography, 343
 - noncompete agreements (NCAs), employment agreements, 209
 - nondedicated lines, 149–150
 - nondisclosure agreements (NDAs)
 - employment agreements, 208
 - trade secrets and, 641
 - nondiscretionary access control, 23–24
 - nondistributed environment, application security in
 - logic bombs, 246
 - overview of, 244–245
 - Trojan horses, 245
 - viruses, 245
 - worms, 246
 - noninterference model, security models, 456
 - nonrepudiation
 - goals of cryptography, 337
 - overview of, 186
 - nonstatistical sampling, 533
 - nonvolatile storage, data storage, 261, 430
 - normal forms, databases, 253
 - normalization, databases, 253
 - NOT (~ or !) operations, logical operations, 341
 - NSA (National Security Agency), 635
-
- O**
- object evidence, 650
 - Object Management Group (OMG)
 - CORBA (Common Object Request Broker Architecture), 248–249
 - IDL (Interface Definition Language), 249
 - Object-Oriented Databases (OODBs), 252
 - object-oriented programming (OOP)
 - abstraction and, 436
 - overview of, 268–269

- Object Request Broker (ORB), 248–249, 249
- objects
 - access control and, 2
 - controlling access to, 462–463
- occupant emergency plans (OEPs), 707
- OCSP (online certificate status protocol), 390
- ODBC (Open Database Connectivity), 257, 257
- OEPs (occupant emergency plans), 707
- OFB (Output Feedback) mode, DES, 358
- OFDM (Orthogonal Frequency-Division Multiplexing), 93
- off-site storage, recovery plan, 612–614
- OMG (Object Management Group)
 - CORBA (Common Object Request Broker Architecture), 248–249
 - IDL (Interface Definition Language), 249
- omissions, vulnerabilities, 545
- one-time pads, 349–350
- one-time password generators, 19
- one-upped-constructed passwords, 12
- one-way functions
 - in cryptography, 342
 - MD2 and, 382
- online certificate status protocol (OCSP), 390
- OODBs (Object-Oriented Databases), 252
- OOP (object-oriented programming)
 - abstraction and, 436
 - overview of, 268–269
- Open Database Connectivity (ODBC), 257, 257
- Open Source Security Testing Methodology Manual (OSSTMM), 193
- open system authentication (OSA), wireless networking, 97
- open systems, security of, 463
- operating modes, CPUs, 424–425
- operating states (process states), CPUs, 419–421
- operating systems (OSs), viruses and, 297
- operational assurance, 498–499
- operational plans, security management, 213–214
- operations controls, 510–513
 - administrative controls, 512–513
 - application controls, 512
 - hardware controls, 511
 - I/O controls, 512
 - media controls, 512
 - overview of, 510
 - privileged entity controls, 511
 - resource protection, 510–511
- operations security
 - administrative controls, 512–513
 - antivirus management, 496–498
 - application controls, 512
 - assurance, 498–499
 - backup maintenance, 499
 - configuration and change management controls, 503–504
 - due care and due diligence standards, 504
 - hardware controls, 511
 - I/O controls, 512
 - legal issues, 505
 - media controls, 512
 - media management, 506–509
 - need to know and principle of least privilege, 500
 - operations controls, 510–511
 - overview of, 496
 - privacy and protection, 505
 - privileged entity controls, 511
 - privileged operations functions, 501–502
 - record retention, 505–506
 - security control types, 509–510
 - trusted recovery, 502–503
 - workstations location changes, 499–500
- Operations Security domain, CBK (Common Body of Knowledge), 496, 528
- operations security triple, 496
- OR (✓) operations, logical operations, 340
- Orange Book. *see also* TCSEC (Trusted Computer System Evaluation Criteria)
 - assurance levels, 498
 - DoD (Department of Defense), 282
 - penetration testing recommendations, 540
 - in rainbow series, 467–468

824 ORB (Object Request Broker) – penetration testing

ORB (Object Request Broker), 248–249, 249
 Orthogonal Frequency-Division Multiplexing (OFDM), 93
 OSA (open system authentication), wireless networking, 97
 OSI model, 79, 81
 application layer, 86–87
 data link layer, 83
 encapsulation/de-encapsulation, 80, 80–81
 functionality of, 79
 history of, 78–79
 network layer, 83–84
 overview of, 78
 physical layer, 82
 presentation layer, 85–86
 session layer, 85
 TCP/IP model compared with, 87, 87
 transport layer, 84–85
 OSs (operating systems), viruses and, 297
 OSSTMM (Open Source Security Testing Methodology Manual), 193
 output. *see* I/O (input/output)
 Output Feedback (OFB) mode, DES, 358
 overflows, input and parameter checking and, 480
 overt channels, 478
 overwriting (clearing) media, 508
 owners, object access and, 32

P

packages, of security components, 472
 packet switching
 Frame Relay connections, 152–153
 overview of, 148–149
 X.25 WAN connections, 152
 packets
 fragmentation, 312, 312
 layer 3, 81
 padded cells, IDS tools, 53
 paging, virtual memory and, 428
 pairing, Bluetooth and, 95
 palm scans (palm topography or palm geometry), biometrics and, 13, 14
 PANs (personal area networks), 95–96

PAP (Password Authentication Protocol), 126, 142
 Paperwork Reduction Act (1995), 635
 parallel runs, change management and, 189
 parallel tests, disaster preparedness, 619
 parameter checking, security issues, 480
 parole evidence rule, 650
 Paros, eavesdropping tools, 165
 Partial-knowledge team, for penetration testing, 539
 passive response, IDS, 48
 passphrases, 10
 password attacks
 countermeasures, 307
 dictionary attacks, 306
 Internet Worm example, 302
 overview of, 305
 password guessing, 305–306
 social engineering attacks and, 307
 Password Authentication Protocol (PAP), 126, 142
 passwords, 10–13
 attacks, 11–12
 brute-force (dictionary) attacks, 56–57
 cracking tools, 11
 improving security of, 12–13
 limitations as security mechanisms, 10
 list of commonly used, 306
 security policies, 11, 58
 selecting, 10–11
 PAT (Port Address Translation), 144
 patents, 640–641
 Patriot Act of 2001, 646
 PBX (private branch exchanges)
 fraud and abuse, 161–162
 securing voice communications, 160
 peer-to-peer networks, wireless networking, 96
 PEM (Privacy Enhanced Mail)
 email security solutions, 158, 392
 as example of end-to-end encryption, 396
 penetration, defined, 537
 penetration testing, 54–55
 dumpster diving, 542
 ethical hacking and, 540
 exam essentials, 554

- lab and lab questions, 65–68
- overview of, 537
- planning, 538
- Q&A, 70–75
- radiation monitoring, 542
- sniffing and eavesdropping, 541–542
- social engineering attacks and, 543–544
- summary and exam essentials, 65–68
- team for, 539–540
- war dialing and, 540–541
- perimeter security, 163–164, 698–699
- period analysis, in polyalphabetic substitution, 348
- permanent virtual circuits (PVCs), 149, 152–153
- permissions, access control, 30–34
- personal area networks (PANs), 95–96
- personal identification number (PIN), 5
- personally identifiable information, protecting, 546
- personnel
 - continuity plan, 576–577
 - controls, 513–514
 - recovery plan, 611–612
 - safety issues, 707
- PERT, 277–278
- PGP (Pretty Good Privacy)
 - email security solutions, 158, 391
 - IDEA (International Data Encryption Algorithm) and, 360
- phishing attacks, 167
- phone communications. *see* voice communication security
- phreaking, 162–163, 668
- physical access control. *see* access control, physical
- Physical layer (layer 1)
 - encapsulation/de-encapsulation, 81
 - overview of, 82
- physical security
 - access abuses, 705
 - accessibility, 695
 - badges, 701
 - controls, 693–694
 - emanation security, 706
 - equipment failure and, 715
 - facility design, 695
 - facility requirements, 692–693
 - fences, gates, turnstiles, and mantraps, 698
 - fire detection and suppression, 710–714
 - intrusion alarms, 702
 - intrusion detection systems, 705–706
 - keys and combination locks, 700–701
 - lab and lab questions, 718–719
 - lighting, 698–699
 - vs. logical or technical, 217
 - motion detectors, 702
 - natural disasters and, 695
 - noise and, 709
 - overview of, 692
 - personnel safety, 707
 - power and electricity and, 708–709
 - proximity readers, 704
 - Q&A, 720–724
 - secondary verification mechanisms, 702–703
 - secure facility plan, 693
 - security guards and dogs, 699–700
 - server rooms, 696–697
 - site selection and, 694–695
 - smart cards, 704
 - summary and exam essentials, 715–718
 - technical controls, 703
 - temperature, humidity, and static, 709–710
 - TEMPEST countermeasures, 706–707
 - visibility, 695
 - water and, 710
 - work areas, 696
- Physical Security domain, CBK (Common Body of Knowledge), 692
- physical support, preventing loss of, 547
- picketing, DRP and, 600
- piggybacking, access abuses, 705
- PIN (personal identification number), 5
- ping-of-death attacks, 61, 314
- PKI (public key infrastructure)
 - CAs (certificate authorities), 387–388
 - certificates, 386–387
 - enrollment process, 388
 - key management, 390
 - overview of, 386

- 826** plain-text messages – private branch exchanges (PBX)
- revocation process, 389–390
 - verification process, 388–389
 - plain-text messages
 - confusion and diffusion operations and, 343
 - cryptography and, 337–338
 - plan approval phase, continuity planning, 578
 - plan implementation phase, continuity planning, 578
 - planning
 - business continuity. *see* BCP (business continuity planning)
 - penetration testing, 538
 - project scope. *see* project scope and planning
 - recovery. *see* DRP (Disaster Recovery Planning)
 - security. *see* security planning
 - platforms, viruses and, 297
 - playback attacks, 63
 - point-to-point links, 149–150
 - Point-to-Point Protocol (PPP), 125, 154
 - Point-to-Point Tunneling Protocol (PPTP), 106, 142
 - policies. *see* security policies
 - polling, LAN technologies, 103
 - polyalphabetic substitution ciphers, 347–348
 - polyinstantiation, multilevel databases and, 256
 - polymorphic viruses, 299
 - polymorphism, OOP terminology, 269
 - POP3 (Post Office Protocol 3), 114, 156
 - Port Address Translation (PAT), 144
 - port-based access control, TCP wrappers, 106
 - port scans, reconnaissance attacks, 320
 - ports, for TCP/IP application layer protocols, 114
 - Post Office Protocol 3 (POP3), 114, 156
 - POST (power-on-self-test), 425
 - postmortem review, of incidents, 673
 - POTS, securing voice communications, 160
 - power and electricity, environmental safety and, 708–709
 - power-on-self-test (POST), 425
 - power outages
 - DRP and, 598–599
 - failover solutions, 128
 - NYC black out, 600
 - PPP (Point-to-Point Protocol), 125, 154
 - PPs (protection profiles), Common Criteria, 472
 - PPTP (Point-to-Point Tunneling Protocol), 106, 142
 - preaction systems, fire suppression, 713
 - Presentation layer (layer 6), 85–86
 - preset locks, for physical security, 700
 - pretexting attacks, 167
 - Pretty Good Privacy (PGP)
 - email security solutions, 158, 391
 - IDEA (International Data Encryption Algorithm) and, 360
 - preventive controls
 - overview of, 3
 - security control types, 509–510
 - PRI ISDN, 151
 - primary keys, relational databases, 252
 - primary (real) memory
 - data storage, 260
 - RAM and, 426
 - primary storage, 430
 - principle of least privilege, 31, 500
 - printers, 432
 - priorities
 - business unit recovery, 602
 - identifying in impact assessment, 571–572
 - resources, 575
 - statement documenting in continuity planning, 579–580
 - privacy
 - laws in European Union, 648–649
 - laws in U.S., 644–648
 - overview of, 183–184
 - protecting, 505
 - in workplace, 647–648
 - Privacy Act (1974), 644–645
 - Privacy Enhanced Mail (PEM)
 - email security solutions, 158, 392
 - as example of end-to-end encryption, 396
 - private branch exchanges (PBX)
 - fraud and abuse, 161–162
 - securing voice communications, 160

- private IP addresses, 145
- private keys, 352, 377. *see also*
 - symmetric cryptography
- private, levels of commercial/private sector classification, 191
- privilege programs, security issues, 481
- privileged entity controls, 511
- privileged mode, CPU operating modes, 424
- privileged mode (Level 0), protection rings, 281, 419
- privileged operations functions
 - list of, 501–502
 - managing, 501–502
- privileges
 - preventing SQL injection by limiting
 - account privileges, 319
 - principle of least privilege, 438
 - separation of, 438
- problem identification, log files and, 531
- problem management, 544
- problem state, 419
- procedures, security, 216–217
- process isolation, security control
 - architecture, 280, 436–437
- processes and provisions phase, continuity planning, 576
- processing types, CPUs, 416–417
- processor scheduler (program executive), 421, 421
- processors. *see* CPUs (central processing units)
- programmable read-only memory (PROM), 425–426
- programming flaws, 482
- programming languages
 - generations, 268
 - security implications related to, 266–267
- project scope and planning
 - business organization analysis, 566
 - legal and regulatory requirements, 569–570
 - overview of, 565
 - resource requirements, 567–569
 - team selection, 566–567
- PROM (programmable read-only memory), 425–426
- propagation techniques, viruses, 295–297
- proprietary data, 192
- proprietary system, intrusion detection systems, 705
- protected mode (level 3), protection rings, 281
- protection mechanisms
 - abstraction, 188
 - CPUs, 417–419
 - data hiding, 188
 - encryption, 188
 - layering, 187–188
 - overview of, 187
- protection profiles (PPs), Common Criteria, 472
- protection rings, 418
 - levels vs. rings, 435
 - overview of, 417–419
 - security control architecture, 281, 281
- protection specifications development, systems development and, 271
- protocols
 - Application layer, 86
 - Data Link layer, 83
 - defined, 78
 - Network layer, 84
 - protocol discovery, 110
 - Session layer, 85
 - Transport layer, 85
 - VPNs, 142
 - WANs, 153–154
- provisions and processes phase, continuity planning, 576
- proxies, network devices, 122
- proximity readers, technical controls for physical security, 704
- proxy firewalls, 118
- prudent man rule, Federal Sentencing Guidelines (1991), 635
- pseudoflaws, decoy techniques, 322
- public key cryptography. *see* asymmetric cryptography
- public key infrastructure. *see* PKI (public key infrastructure)
- public keys, 377
- public, levels of commercial/private sector classification, 193

828 purging – recovery strategies

purging
 media, 507–508
 memory, 431
 PVCs (permanent virtual circuits), 149,
 152–153

Q

qualitative decision making, BIA and, 571
 qualitative risk analysis, 227–228
 Delphi technique, 228
 quantitative risk analysis compared
 with, 228
 scenarios, 227–228
 techniques for performing, 227
 quantitative decision making, BIA and, 571
 quantitative risk analysis, 223–227
 cost functions, 223–224
 qualitative risk analysis compared
 with, 228
 steps in, 223
 threat/risk calculation, 225–227

R

race conditions, 482
 radiation monitoring, 542
 radio frequency identification devices
 (RFID), for controlling physical
 access, 704
 radio frequency interference (RFI), 709
 radio frequency (RF), 542
 RADIUS (Remote Authentication Dial-In
 User Service), 28, 126
 RAID (Redundant Array of Independent
 Disks), 128–129
 rainbow series
 Green book, 469–471
 Orange book (TCSEC classes), 467–468
 overview of, 466–467
 publications, 469–470
 Red book, 469
 RAM (random access memory)
 dynamic vs. static, 427
 memory, 426–427
 memory security issues, 429
 random access storage, 261, 430
 random number generation, 343
 RARP (Reverse Address
 Resolution Protocol)
 Data Link layer and, 83
 network-based IDS lookups, 51
 TCP/IP Network layer protocols, 112
 RAs (registration authorities), digital
 certificates, 388
 RC5 (Rivest Cipher 5), 361
 RDBMS (relational database management
 systems), 251–253
 read-only memory (ROM), 425–426
 ready state, process states, 420
 real evidence, 650
 reasonableness checks, software testing
 and, 279
 reciprocal agreements, 607–608
 reconnaissance attacks
 dumpster diving, 320–321
 IP probes, 319
 overview of, 319
 port scans, 320
 vulnerability scans, 320
 record retention
 organizational policies, 505–506
 overview of, 533
 record sequence checking, 155
 recovery controls
 overview of, 3
 security control types, 510
 recovery planning
 backup best practices, 615
 backup media formats, 614
 backups and off-site storage, 612–614
 emergency response, 610–611
 external communications, 616
 logistics and supplies, 616
 overview of, 610
 personnel notification, 611–612
 recovery vs. restoration, 616–617
 software escrow arrangements, 615–616
 tape rotation, 615
 utilities, 616
 recovery strategies
 alternative processing sites, 604
 business unit priorities, 602
 cold sites, 604–605

- crisis management, 602–603
- database recovery, 608
- electric vaulting, 608–609
- emergency communications, 603
- hot sites, 605–606
- MAAs (mutual assistance agreements), 607–608
- mobile sites, 606
- multiple sites, 607
- overview of, 602
- remote journaling, 609
- remote mirroring, 609
- service bureaus, 607
- warm sites, 606
- work group recovery, 603
- recovery time objective (RTO), 572
- recovery, vs. restoration, 616–617
- Red book, rainbow series, 469
- red box, phreaking and, 163
- redundancy/failover
 - failover solutions, 127–128
 - RAID (Redundant Array of Independent Disks), 128–129
 - redundant servers, 127
- Redundant Array of Independent Disks (RAID), 128–129
- redundant servers, 127
- reference monitor, in TCB (trusted computing base), 454–455
- reference profile/reference template, stored samples of biometric factors, 16
- referential integrity, relational databases, 253
- reflective attacks, 59
- regional events, DRP and, 597
- register addressing, memory addressing schemes, 428
- registers, memory, 427
- registration authorities (RAs), digital certificates, 388
- regulatory policies, types of security policies, 215
- regulatory requirements, for BCP, 569–570
- rejecting risk, 229
- relational database management systems (RDBMS), 251–253
- relational databases, 252
- release control phase, of change control process, 279
- remanence, purging media and, 508
- remote access, techniques for, 151–152
- Remote Authentication Dial-In User Service (RADIUS), 28, 126
- remote authentication protocols, 126–127
- remote controls. *see also* thin clients
 - remote access via, 151
 - tools, 20
- remote journaling, recovery strategies, 609
- remote mirroring, recovery strategies, 609
- remote nodes, remote access via, 152
- remote security management, 123–124
- remote users, assisting, 124
- removable media, marking/labeling, 506
- repeaters, network devices, 121
- replay attacks
 - cryptographic attacks, 400
 - overview of, 63
 - second-tier attacks, 166
- reporting
 - audit trails and, 532
 - gathering evidence and, 677
 - incidents, 678–679
 - interim reports, 534
- request control phase, of change control process, 278
- residual risks, 229
- resources
 - operations controls, 510–511
 - prioritizing, 575
 - requirements, for BCP, 567–569
- response process, incident handling, 675–677
- response teams, for incident handling, 673–675
- restoration
 - incident response process and, 677
 - vs. recovery, 616–617
- restricted interface model, Clark-Wilson model and, 462
- retina scans, biometrics, 14
- Reverse Address Resolution Protocol. *see* RARP (Reverse Address Resolution Protocol)
- reverse hash matching attacks, 56–57

830 revocation process – SAs (security associations)

revocation process, PKI (public key infrastructure), 389–390
 RF (radio frequency), 542
 RFC 1087, on Internet ethics, 681
 RFC 1918, IP addresses, 146–147
 RFI (radio frequency interference), 709
 RFID (radio frequency identification) devices, for controlling physical access, 704
 rights
 access control, 30–34
 excessive privileges and creeping privileges, 32
 Rijndael block cipher, 361–362
 Ring topology
 network topologies, 104
 overview of, 103–104
 rings, vs. levels in computer architecture, 435
 risk management
 analyzing risk, 218, 220
 assessing risk, 220
 asset valuation and, 221–222
 auditing based on risk analysis, 530
 calculating risk, 225–227
 elements of, 220, 220
 handling risk, 229–230
 mitigating risk, 229
 overview of, 217–218
 qualitative risk analysis, 227–228
 quantitative risk analysis, 223–227
 reducing, assigning, accepting, rejecting risk, 229
 terminology, 218–219
 types of risk, 572
 risk management, in BCP
 defined, 217
 identifying risk, 572
 impact assessment, 573–575
 likelihood assessment, 572–573
 risk acceptance/mitigation document, 580
 risk assessment document, 580
 Rivest Cipher 5 (RC5), 361
 Rivest, Ronald, 377, 382
 Rivest, Shamir, and Adleman (RSA). *see* RSA (Rivest, Shamir, and Adleman)

Rogier, Nathalie, 382
 role-based access control (RRBAC), 25–26
 ROM (read-only memory), 425–426
 rootkits, 315
 Rosenberger, Rob, 300
 ROT3 cipher, 334–335
 rotation of duties, managing privileged functions, 502
 routers
 network devices, 122
 Network layer and, 84
 routing protocols, Network layer and, 84
 Royce, Winston, 273
 RRBAC (role-based access control), 25–26
 RSA (Rivest, Shamir, and Adleman) algorithm, 377–379
 Data Security, 361, 381
 RTO (recovery time objective), 572
 rule-based access control, 465
 rule-based security policy, 24
 rules, expert systems, 262
 running key ciphers (book ciphers), 350
 running state (problem state), process states, 420

S

S-HTTP (Secure HTTP), 394
 S/MIME (Secure Multipurpose Internet Mail Extensions), 158, 392–393
 S-RPC (Secure Remote Procedure Call), 125
 sabotage, employees, 547
 safeguards
 calculating cost/benefits, 226–227
 calculating costs, 225–226
 distributed architecture, 440–441
 risk terminology, 219
 salami attacks, 481–482
 sampling, data analysis and, 532
 SAN (storage-area networks), 614
 sandbox, Java, 304
 sanitization
 of media, 508
 of memory, 431
 Sarbanes-Oxley Act, 47, 531, 620
 SAs (security associations), 398

- satellite connections, 150
- scanning attacks, 672
- Schneier, Bruce, 360, 362
- scope, of projects. *see* project scope and planning
- screening employees, 208
- screening routers, 117
- script kiddies
 - sources of malicious code, 294–295
 - thrill attacks, 670
- scripted access, as SSO mechanism, 22
- SDLC (Synchronous Data Link Control), 153
- search warrants, 652, 676
- second-tier attacks, 165, 166–167
- secondary memory, 428–429
- secondary storage, data storage, 260, 430
- secondary verification mechanisms,
 - controlling physical access, 702–703
- secret key cryptography. *see* symmetric cryptography
- secret, levels of government/military classification, 191
- secure communications protocols
 - authentication protocols, 126
 - dial-up protocols, 125
 - overview of, 124–125
 - remote authentication protocols, 126–127
- Secure Electronic Transaction (SET)
 - e-commerce security, 394–395
 - secure communications protocols, 125
- Secure European System for Applications in a Multivendor Environment (SESAME), 20, 22
- secure facility plan, 693
- Secure Hash Algorithm (SHA), 356, 381–382
- Secure Hash Standard (SHS), 381
- Secure HTTP (S-HTTP), 394
- Secure Multipurpose Internet Mail Extensions (S/MIME), 158, 392–393
- Secure Remote Procedure Call (S-RPC), 125
- Secure Shell (SSH), 396
- Secure Sockets Layer. *see* SSL (Secure Sockets Layer)
- secure state machines, 455
- security associations (SAs), 398
- security awareness training, 230–231
- security boundaries, 163–164
- security concepts
 - accountability, 186
 - auditing, 185–186
 - authentication, 184–185
 - authorization, 185
 - availability and, 183
 - confidentiality and, 180–181
 - identification, 184
 - integrity and, 181–182
 - nonrepudiation, 186
 - overview of, 180
 - privacy, 183–184
- security controls, 154–156
 - architecture for, 280–283
 - integrity verification, 154–155
 - transmission mechanisms, 155
 - transparency, 154
 - types of, 509–510
- security domains, 24
- security guards, controlling physical access, 699–700
- security IDs, physical access
 - control, 701
- security issues
 - attacks based on design flaws, 479
 - covert channels, 478–479
 - electromagnetic radiation, 483
 - incremental attacks, 481–482
 - initialization and failure states and, 479
 - input and parameter checking, 480
 - maintenance hooks and privilege programs, 481
 - memory, 429
 - networks and, 123–124
 - overview of, 478
 - programming flaws, 482
 - timing, state changes, and communication disconnects, 482–483
 - vs. user friendliness vs. functionality, 267
- security kernel, 455
- security labels, 453

832 security management – separation of duties

- security management. *see also*
 - security planning
 - change control, 189
 - data classification, 190–193
 - lab and lab questions, 196
 - planning and, 193
 - protection mechanisms. *see* protection mechanisms
 - Q&A, 198–203
 - summary and exam essentials, 193–196
- security management, human aspect
 - baselines, 216
 - employment agreements, 208–209
 - job descriptions, 206–208
 - lab and lab questions, 235–236
 - overview of, 206
 - planning process, 212–214
 - Q&A, 237–242
 - risk management. *see* risk management
 - screening and background checks, 208
 - security awareness training, 230–231
 - security policies, 214–215
 - security procedures, 216–217
 - security roles, 211–212
 - summary and exam essentials, 231–235
 - termination issues, 209–211
- Security Management Practices domain,
 - CBK (Common Body of Knowledge), 180, 206
- security models
 - access control matrix, 457
 - Bell-LaPadula, 458–460, 459
 - Biba, 460, 460–461
 - Brewer and Nash (Chinese Wall), 462
 - CIA triad and, 463–464
 - Clark-Wilson, 461–462
 - closed vs. open systems, 463
 - controlling access to objects and
 - subjects, 462–463
 - controls, 464–465
 - information flow, 455–456
 - noninterference, 456
 - overview of, 452–454
 - security issues and. *see* security issues
 - state machine, 455
 - system security evaluation. *see* system security evaluation
 - Take-Grant, 456–457
 - TCB (trusted computing base), 454–455
 - trust and assurance and, 465
- security modes, CPUs, 421–424
 - comparing, 424
 - compartmented mode, 422–423
 - dedicated mode, 422
 - multilevel mode, 423
 - overview of, 422–423
 - system high mode, 422
- security perimeter, in TCB (trusted computing base), 454
- security planning, 212–214
 - as management process, 193
 - overview of, 212–213
 - types of plans, 213
- security policies
 - acceptable use policies, 216
 - access control and, 31
 - not addressed to specific individuals, 215
 - overview of, 214–215
 - password policies, 11
 - rule-based security policy, 24
 - security protection mechanisms, 437–439
- security procedures, 216–217
- security professional, security roles, 211
- security protection mechanisms, computer architecture, 434–435
- security roles, 211–212
- security standards, 215–216
- security targets (STs), Common Criteria, 472
- security tokens, 453
- segments, TCP, 81
- SEI (Software Engineering Institute), 275
- seismic hazards, FEMA on, 593–594
- Sendmail, 156
- senior management, BCP and, 568
- senior manager, security roles, 211
- sensitive but unclassified, levels of
 - government/military classification, 191
- sensitive information, 506
- sensitive, levels of commercial/private
 - sector classification, 193
- separation of duties
 - for access control, 32–34
 - job descriptions, 207
 - overview of, 438

- separation of privileges, 438
- sequential access storage, data storage, 261, 430–431
- Serial Line Protocol (SLIP), 125
- server farms, 127
- server rooms, facility security and, 696–697
- servers, making inaccessible, 697
- service bureaus, recovery strategies, 607
- service-level agreements. *see* SLAs
 - (service-level agreements)
- service ports, TCP and UDP, 107
- SESAME (Secure European System for Applications in a Multivendor Environment), 20, 22
- session hijacking attacks, 321–322
- Session layer (layer 5), 85
- SET (Secure Electronic Transaction), 125, 394–395
- SHA (Secure Hash Algorithm), 356, 381–382
- Shamir, Adi, 377
- shared key authentication (SKA), 97
- shielded twisted pair (STP) cable, 90
- shimming attacks, 700
- Shiva Password Authentication Protocol (SPAP), 142
- shoulder surfing, 696
- shrink-wrap licenses, 642
- SHS (Secure Hash Standard), 381
- signature-based detection. *see also* knowledge-based systems
 - antivirus filters, 304
 - antivirus mechanisms, 298
- signature dynamics, biometrics and, 15
- signatures, knowledge-based IDS and, 51
- Simple Integrity Property, Biba state machine, 460
- Simple Key Management for IP (SKIP), 124
- Simple Mail Transfer Protocol (SMTP), 114, 156
- Simple Network Management Protocol (SNMP), 114
- Simple Security Property, Bell-LaPadula state machine, 459
- simplex communication, 85
- simulation tests, disaster preparedness, 619
- single loss expectancy (SLE), 224, 574
- single sign-on (SSO), 20, 22
- single state processors, 416
- site selection, facility security, 694–695
- sites, in DRP
 - alternative processing sites, 604
 - cold sites, 604–605
 - hot sites, 605–606
 - mobile sites, 606
 - warm sites, 606
- SKA (shared key authentication), 97
- SKIP (Simple Key Management for IP), 124
- Skipjack, 361
- SLAs (service-level agreements)
 - equipment failure and, 715
 - legal and regulatory requirements in BCP, 570
 - systems development and, 283
- slaves/zombies, in DDoS attacks, 59
- SLE (single loss expectancy), 224, 574
- sliding windows, TCP and, 107
- SLIP (Serial Line Protocol), 125
- smart cards
 - identification process and, 5
 - technical controls for physical security, 704
- SMDS (Switched Multimegabit Data Service), 153
- SMP (symmetric multiprocessing), 414–415
- SMTP (Simple Mail Transfer Protocol), 114, 156
- smurf attacks, 309–311, 310
 - DNS amplification attacks compared with, 311
 - as DoS attack, 309–310
 - how it works, 310–311
 - overview of, 60–61
- sniffing attacks
 - overview of, 64, 541
 - as password attacks, 11
 - sniffers, as eavesdropping tools, 165
- sniping, auctions, 247
- SNMP (Simple Network Management Protocol), 114
- snooping attacks, 64
- social engineering attacks
 - overview of, 307, 543–544
 - password attacks and, 12
 - voice communication security, 160–161
- SOCKS firewall, 118

834 software – strategic plans

- software
 - development, 264
 - escrow arrangements, 615–616
 - failure and disaster recovery, 599–600
 - illegal software monitoring, 535
 - testing, 279–280
- Software Capability Maturity Model (SW-CMM), 275
- Software Engineering Institute (SEI), 275
- Software IP encryption (SWIPE), 125
- “something you are”
 - authentication factors, 6
 - biometrics and, 13
- “something you do”, authentication factors, 6
- spamming attacks
 - email security and, 158
 - overview of, 64
- SPAP (Shiva Password Authentication Protocol), 142
- spiral model, 274, 274
- split knowledge
 - in cryptography, 344
 - managing privileged functions, 502
- spoofing attacks, 62, 157
- spread spectrum, wireless communication and, 93
- spyware
 - defense-in-depth and, 498
 - overview of, 303
- SQL injection attacks, 318–319
 - how it works, 318–319
 - overview of, 317
 - protecting against, 319
- SQL (Structured Query Language)
 - aggregation, 257–259
 - relational databases using, 253
 - views, 255
- SSH (Secure Shell), 396
- SSID (station set identifier), wireless networking, 96–97
- SSL (Secure Sockets Layer)
 - secure communications protocols, 125
 - TCP/IP application layer protocols, 114
 - Web communication security, 393
- SSO (single sign-on), 20, 22
- stand-alone mode, wireless networking, 96
- standards
 - due care and due diligence, 504
 - security management, 193
 - security standards, 215–216
- Star topology, 105, 105
- state changes, security issues, 482–483
- state, defined, 455
- state machine
 - Bell-LaPadula security properties, 459
 - Biba security properties, 460
 - security models, 455
- state transitions, 455
- stateful inspection firewalls, 118
- stateful NAT, 146
- static electricity, environmental safety and, 709–710
- static NAT, 146
- static packet-filtering firewalls, 117
- static passwords, 10
- static tokens, 18
- static web pages, 317
- station set identifier (SSID), wireless networking, 96–97
- statistical attacks, cryptographic attacks, 399
- statistical intrusion detection. *see*
 - behavior-based IDS
- statistical sampling, 533
- stealth viruses, 299
- steganography, Web communication security, 394
- stopped state, process states, 420
- storage, 430–431
 - electronic vaulting, 608–609
 - off-site, 612–614
 - primary vs. secondary, 430
 - random vs. sequential access, 430–431
 - secondary memory and, 428
 - security of storage media, 431
 - volatile vs. nonvolatile, 430
- storage-area networks (SANs), 614
- storage media, 500
- storing media, 507
- storms, DRP and, 596
- STP (shielded twisted pair) cable, 90
- strategic plans, security management plans, 213

- strategy development phase, continuity
 - planning, 576
- stream attacks, 61
- stream ciphers, 351
- strikes (labor), DRP and, 600
- Structured Query Language. *see* SQL (Structured Query Language)
- structured walk-through, disaster preparedness, 619
- STs (security targets), Common Criteria, 472
- subjects
 - access control and, 2, 462–463
 - security perimeter and, 454
 - trusted subjects in Bell-LaPadula model, 459
- subpoena, for gathering evidence, 676
- substitution ciphers
 - Caesar cipher, 334–335
 - one-time pads, 349–350
 - overview of, 347–348
- SUM() aggregate function, SQL, 258
- super-increasing sets, 378
- supervisor state, operating states, 419
- supervisory state, process states, 420
- supplies, disaster recovery and, 616
- SVCs (switched virtual circuits), 149, 152–153
- SW-CMM (Software Capability Maturity Model), 275
- SWIPE (Software IP encryption), 125
- Switched Multimegabit Data Service (SMDS), 153
- switched networks, network-based IDS and, 51
- switched virtual circuits (SVCs), 149, 152–153
- switches, network devices, 121
- switching technologies, 147–149
 - circuit switching, 148–149
 - overview of, 147
 - packet switching, 148–149
 - virtual circuits, 149
- symmetric cryptography
 - AES (advanced encryption standard), 361–362
 - asymmetric algorithms compared with symmetric, 356
 - Blowfish, 360
 - DES (Data Encryption Standard), 357–359
 - IDEA (International Data Encryption Algorithm), 360
 - key distribution and, 363–365
 - overview of, 357
 - Skipjack, 361
 - symmetric key algorithms, 352–353, 353
 - Triple DES, 359–360
 - weaknesses of, 353
- symmetric multiprocessing (SMP), 414–415
- SYN/ACK packets, 59–60, 107
- Syn flood attacks
 - SYN/ACK packets and, 59–60
 - three-way handshake and, 308–309, 309
- synchronous communication, LAN technologies, 101
- Synchronous Data Link Control (SDLC), 153
- synchronous dynamic password tokens, 19
- system compromise, 672
- system failure
 - avoiding, 265–266
 - monitoring and, 46
- system high mode, CPU security modes, 422
- system security evaluation
 - certification and accreditation, 475–478
 - Common Criteria, 472–475
 - ITSEC classes, 471
 - lab and lab questions, 486–487
 - overview of, 466
 - Q&A, 488–493
 - rainbow series, 466–471
 - summary and exam essentials, 483–485
 - TCSEC classes, 467–468
- systems development controls
 - assurance controls, 265
 - avoiding system failure, 265–266
 - change control and configuration management, 278–279
 - code review, 272
 - conceptual definition phase of, 270
 - design review, 271–272
 - development life cycle, 269–270
 - functional requirements determination, 271

Gantt charts and PERT, 277, 277–278
 lab and lab questions, 285–286
 Life cycle models, 272–276
 maintenance, 272
 object-oriented programming, 268–269
 overview of, 264
 programming languages for, 266–267
 protection specifications
 development, 271
 Q&A, 287–292
 security control architecture, 280–283
 SLAs (service-level agreements), 283
 software development, 264
 software testing, 279–280
 summary and exam essentials, 283–285
 test review, 272
 systems, open and closed, 463

T

T-sight, eavesdropping tools, 165
 TACACS (Terminal Access Controller
 Access Control System), 28, 126
 tactical plans, security management
 plans, 213
 Take-Grant model, security models,
 456–457
 tape rotation, backups, 615
 target of evaluation (TOE), ITSEC, 471
 task-based access control (TBAC), 26
 TBAC (task-based access control), 26
 TCB (trusted computing base), 454–455
 overview of, 454
 reference monitors and kernels and,
 454–455
 security perimeter in, 454
 TCP/IP (Transmission Control Protocol/
 Internet Protocol)
 application layer protocols, 113–114
 domain name resolution and, 115–116
 model, 87, 87–88, 106
 network layer protocols, 110–113
 OSI model compared with, 87, 87
 overview of, 105–106
 three-way handshake, 308, 308
 transport layer protocols, 113–114
 vulnerabilities, 115
 TCP (Transport Control Protocol)
 segments, 81
 TCP/IP transport protocols, 107
 wrappers, 106
 TCSEC (Trusted Computer System
 Evaluation Criteria)
 assurance levels, 498
 categories, 467
 comparing security evaluation
 standards, 475
 discretionary protection (Categories
 C1, C2), 467–468
 Green book, 469–470
 ITSEC compared with, 471
 mandatory protection (Categories B1,
 B2, B3), 468
 Orange book, 467–468
 penetration testing
 recommendations, 540
 rainbow series, 466–467
 Red book, 469
 security baselines, 216
 verified protection (Category A1), 468
 weaknesses of, 470–471
 teams
 incident response, 673–675
 for penetration testing, 539–540
 selecting for BCP, 566–567
 teardrop attacks
 as DoS attack, 311–313, 312
 overview of, 61
 technical controls, physical security
 access abuses, 705
 emanation security, 706
 intrusion detection systems, 705–706
 overview of, 703
 proximity readers, 704
 smart cards, 704
 TEMPEST countermeasures, 706–707
 technical physical security controls, 693
 technical security, vs. physical, 217
 Telecommunications and Network Security
 domain, CBK (Common Body of
 Knowledge), 140
 Telnet protocol, 114
 temperature, environmental safety and,
 709–710

- TEMPEST (Transient Electromagnetic Pulse Equipment Shielding Techniques)
 - physical security countermeasures, 706–707
 - protection against EM, 483
 - radiation monitoring, 432, 542
- Terminal Access Controller Access Control System (TACACS), 28, 126
- termination, of employees, 209–211
- terrorist attacks, categories of computer crime, 668
- terrorist-related disasters, DRP and, 597–598
- test review, systems development and, 272
- testimonial evidence, 651–652
- testing
 - business continuity plan, 569
 - disaster recovery plan, 618–620
- testing program, continuity planning documents, 581
- TFN (Tribal Flood Network), 309
- TFTP (Trivial File Transfer Protocol), 114
- TGS (ticket-granting service), Kerberos, 21
- theft
 - DRP and, 601
 - vulnerabilities, 545–546
- thicknet, coaxial cable, 89
- thin clients, as SSO mechanism, 20, 22
- thinnet, coaxial cable, 89
- threats
 - calculating in quantitative risk analysis, 225–227
 - to data storage, 261
 - risk terminology, 218
- thrill attacks, categories of computer crime, 670
- throughput rate, in biometrics, 16
- ticket authentication, 20
- ticket-granting service (TGS), Kerberos, 21
- time frames
 - auditing and, 530
 - record retention and, 533
 - reporting and, 532
- time-of-check-to-time-of-use (TOCTOU)
 - attacks, 482
 - overview of, 315
- time of check (TOC), 482
- time of use (TOU), 482
- time slices, operating states and, 419
- timing
 - security issues, 482–483
 - statement documenting in continuity planning, 579–580
- TNI (Trusted Network Interpretation), 469
- TOC (time of check), 482
- TOCTOU (time-of-check-to-time-of-use)
 - attacks, 482
 - overview of, 315
- TOE (target of evaluation), ITSEC, 471
- token passing, LAN technologies, 103
- Token Ring, 100
- tokens, security tokens, 453
- tokens (smart tokens)
 - one-time passwords and, 10
 - overview of, 18–20
 - strengths and weaknesses of, 19–20
 - types of, 18–19
- top secret, levels of government/military classification, 191
- total risk, 230
- TOU (time of use), 482
- TPs (transformation procedures), in Clark-Wilson security model, 462
- trade secrets, 641–642
- trademarks, 639–640
- traffic/trend analysis, 536, 550
- training
 - continuity planning, 578
 - disaster recovery, 617–618
 - security awareness, 231
- transformation procedures (TPs), in Clark-Wilson security model, 462
- Transient Electromagnetic Pulse Equipment Shielding Techniques. *see* TEMPEST (Transient Electromagnetic Pulse Equipment Shielding Techniques)
- Transmission Control Protocol/Internet Protocol. *see* TCP/IP (Transmission Control Protocol/Internet Protocol)
- transmission mechanisms, 155
- transmission, remote access security and, 123
- transmission windows, TCP and, 107
- transparency, 154

- Transport Control Protocol. *see* TCP
(Transport Control Protocol)
- Transport layer (layer 4), 84–85
- transport layer protocols, TCP/IP, 113–114
- transport mode, IPSec, 397
- transposition ciphers, 346–347
- trap doors (back doors), 315
- Tribal Flood Network (TFN), 309
- Trinoo, common DDoS toolkits, 309
- triple, access control, 461
- Triple DES, 359–360
- Tripwire
as countermeasure to malicious code, 304
data integrity assurance package, 298
- Trivial File Transfer Protocol (TFTP), 114
- Trojan horses
Back Orifice example, 301
email security and, 157
functionality of, 300
as malicious code, 300–301
overview of, 245
- trust, assurance and, 465
- trust relationships, Internet Worm example, 302–303
- Trusted Computer System Evaluation Criteria. *see* TCSEC (Trusted Computer System Evaluation Criteria)
- trusted computing base. *see* TCB (trusted computing base)
- Trusted Network Interpretation (TNI), 469
- trusted paths, TCB, 454
- trusted recovery, 479, 502–503
- trusted subjects, Bell-LaPadula model, 459
- trusted systems, 465
- Trustworthy Computing Initiative, Microsoft, 480
- tsunamis, disaster recovery and, 594
- tunneling, 141–142
drawbacks of, 142
IPSec tunnel mode, 397
need for, 141–142
- tuples, relational databases, 251
- turnstiles, controlling physical access, 698
- twisted-pair cable, 90–91
- two-factor authentication, 7, 58
- two-person controls, managing privileged functions, 502
- Twofish algorithm, 362
- Type 1 authentication factor, 5
- Type 2 (something you have) authentication factor, 6, 18
- Type 3 (something you are) authentication factor, 6, 13
-
- ## U
- UCITA (Uniform Computer Information Transactions Act), 643
- UDI (unconstrained data item), 462
- UDP (User Datagram Protocol)
datagrams, 81
DNS amplification attacks and, 311
overview of, 109–110
- Ultra program, as counter to Enigma cipher, 336
- unclassified, levels of government/military classification, 191
- unconstrained data item (UDI), 462
- underflow, 614
- unicasts, LAN technologies, 101
- Uniform Computer Information Transactions Act (UCITA), 643
- uninterruptible power supply (UPS), 598, 708
- United States Patent and Trademark Office (USPTO), 640
- Unix
Internet Worm example, 302–303
viruses and, 297
vulnerabilities, 547–548
- unshielded twisted pair (UTP) cable, 90, 91
- UPS (uninterruptible power supply), 598, 708
- urgency and timing, statement documenting in continuity planning, 579–580
- U.S. Constitution
laws and, 631
privacy rights, 644
- USA Patriot Act of 2001, 646
- USC (United States Code), for civil law, 632
- User Datagram Protocol. *see* UDP (User Datagram Protocol)
- user friendliness, vs. security and functionality, 267

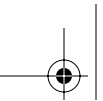
user mode, CPU operating modes, 424
 user mode (level 3), protection rings,
 281, 419
 users
 assisting remote users, 124
 managing user accounts, 501
 object access and, 32
 security roles, 212
 USPTO (United States Patent and
 Trademark Office), 640
 utilities
 failure of, 599
 troubleshooting during disasters, 616
 UTP (unshielded twisted pair) cable, 90, 91

V

Van Eck radiation, 432
 vandalism, disaster recovery and, 601
 VENONA project, 349
 verification process
 in PKI, 388–389
 secondary verification mechanisms for
 physical access, 702–703
 verified protection (Category A1),
 TCSEC, 468
 Vernam ciphers, 349
 Vernam, Gilbert Sandford, 349
 views, restricting database access with, 255
 Vigenere cipher, 347–348
 violation analysis, types of sampling, 533
 virtual circuits
 overview of, 149
 TCP, 107
 virtual machines (VM), 424
 virtual memory, 260, 428–429
 Virtual Private Networks. *see* VPNs
 (Virtual Private Networks)
 virtual storage, data storage, 261
 virus decryption routine, 299
 viruses. *see also* antivirus mechanisms
 antivirus management, 496–498
 antivirus mechanisms, 298
 email security and, 157
 file infector, 296
 hoaxes and, 300
 macro, 296–297
 MBR virus, 295–296
 overview of, 245, 295
 platforms effected, 297
 propagation techniques, 295
 virus technologies for escaping
 detection, 299
 visibility, facility site selection and, 695
 visitors, facility security and, 696
 vital records program, continuity planning
 documents, 581
 VM (virtual machines), 424
 voice communication security, 160–163
 fraud and abuse, 161–162
 overview of, 160
 phreaking, 162–163
 social engineering attacks and, 160–161
 voice pattern recognition, biometrics
 and, 14
 volatile storage, data storage, 261, 430
 volcanoes, natural disasters, 597
 VPNs (Virtual Private Networks), 140–143
 how they work, 142
 implementing, 142–143
 IPSec and, 396
 overview of, 140
 tunneling, 141–142
 VPN links for securing TCP/IP, 106
 vulnerabilities
 distributed architecture and, 439
 risk terminology, 218
 TCP/IP, 115
 Unix/Linux, 547–548
 vulnerabilities, indistinct
 collusion, 546
 errors and omissions, 545
 espionage, 548–549
 IPL (initial program load), 550
 malicious attackers, 548
 malicious code, 549
 preventing loss of physical and
 infrastructure support, 547
 sabotage, 547
 theft and fraud, 545–546
 traffic and trend analysis and, 550
 vulnerability scanners, IDS tools, 53–54
 vulnerability scans, reconnaissance
 attacks, 320

W

- waiting state, process states, 420
- WANs (wide area networks), 149–154
 - ATM and, 153
 - connection technologies, 151
 - Frame Relay connections, 152–153
 - LANs compared with, 88
 - overview of, 149–151
 - protocols, 153–154
 - SMDS and, 153
 - X.25 WAN connections, 152
- WAP (Wireless Application Protocol), 95
- war dialing, 540–541
- war-driving attacks, 99
- warm sites, recovery strategies, 606
- warm-swappable RAID, 129
- warning banners, types of monitoring tools, 535
- water, environmental safety and, 710
- water fire suppression systems, 713
- waterfall model, 273, 273–274
- Web application security
 - dynamic Web applications and, 317–318
 - overview of, 316
 - SQL injection attacks, 318–319
 - XSS (cross-site scripting) attacks, 316–317
- web bots, 247
- Web communication security
 - cryptography and, 393–394
 - overview of, 393
 - S-HTTP (Secure HTTP), 394
 - SSL (Secure Sockets Layer), 393
 - steganography, 394
- well-known ports, TCP and UDP, 107
- WEP (Wired Equivalent Privacy), 97–98, 398
- wet pipe systems, fire suppression, 713
- white boxes
 - phreaking and, 163
 - software testing and, 280
- wide area networks. *see* WANs (wide area networks)
- WiFi Protected Access. *see* WPA (WiFi Protected Access)
- wildfires, 596
- WinNuke attacks, 61
- WIPO (World Intellectual Property Organization), 638
- Wired Equivalent Privacy (WEP), 97–98, 398
- wired extension mode, wireless networking, 96
- Wireless Application Protocol (WAP), 95
- wireless channels, 97
- wireless communication, 92–99
 - Bluetooth, 95–96
 - cell phones, 93–95
 - cordless phones, 96
 - overview of, 92–93
 - wireless channels, 97
 - wireless networking (802.11), 96–99
- wireless networking (IEEE 802.11)
 - cryptography, 398–399
 - WEP (Wired Equivalent Privacy), 398
 - wireless communication, 96–99
 - WPA (WiFi Protected Access), 398–399
- Wireless Transport Layer Security (WTLS), 95
- Wireshark, sniffers, 165
- work areas, facility security and, 696
- work function, in cryptography, 345
- work group recovery, recovery strategies, 603
- workplace, privacy in, 647
- workstations, managing location changes, 499–500
- World Intellectual Property Organization (WIPO), 638
- World War II, cryptography in, 335–336
- worms, 301–303
 - Code Red example, 301–302
 - email security and, 157
 - Internet Worm example, 302–303
 - overview of, 246
 - risk represented by, 301
- WPA (WiFi Protected Access)
 - overview of, 398–399
 - wireless networking (802.11), 98
 - WPA-2 (IEEE 80211i), 98
- WTLS (Wireless Transport Layer Security), 95



X

- X Window protocol, 114
- X.400 standard, 156
- X.509 standard, 386–387
- Xbox, Trojan horse example, 300
- XOR (exclusive OR) operations, logical operations, 341
- XSS (cross-site scripting) attacks, **316–317**
 - overview of, 316
 - protecting against, 316–317

Z

- Zephyr chart, for comparing biometric factor ratings, 16–17, 17
- zero-knowledge proof, in cryptography, **343–344, 344**
- Zero-knowledge team, for penetration testing, 539
- Zimmerman, Phil, 360, 391
- zombies/slaves, in DDoS attacks, 59

