References to figures are in italics.

*-integrity axiom, 337
*-property rule (star property rule), 334, 336
10Base2, 514
10Base5, 514
10Base-T, 514
3DES, 703
802.11a, 624
802.11b, 624
802.11e, 625
802.11f, 625
802.11g, 625
802.11h, 625
802.11i, 625–626
802.11j, 633
802.11n, 633
802.15, 634
802.16, 633
802.1X, 627–629

A
absolute addresses, 303
abstraction, 296, 962
access, defined, 155
access control administration, 222
centralized, 223
decentralized, 230
Diameter, 227–229
RADIUS, 223–224, 227
TACAS, 224–227
watchdog timers, 227
access control models, 210
discretionary access control, 211
identity-based, 212
mandatory access control, 212–214
role-based access control, 214–217
sensitivity labels, 213–214
access controls, 670
access control lists (ACLs), 220–221
access control matrix, 219–220
access criteria, 195–196
accountability, 159, 243–246
administrative controls, 232–233
auditing, 237
authentication, 158, 160–161
authorization, 158, 195
cabling, 234
capability tables, 220
computer controls, 234
constrained user interfaces, 218–219
content-dependent access control, 221
centralized, 223
decentralized, 230
Diameter, 227–229
RADIUS, 223–224, 227
TACAS, 224–227
watchdog timers, 227
access control models, 210
discretionary access control, 211
identity-based, 212
mandatory access control, 212–214
role-based access control, 214–217
sensitivity labels, 213–214
access controls, 670
access control lists (ACLs), 220–221
access control matrix, 219–220
access criteria, 195–196
accountability, 159, 243–246
administrative controls, 232–233
auditing, 237
authentication, 158, 160–161
authorization, 158, 195
cabling, 234
capability tables, 220
computer controls, 234
constrained user interfaces, 218–219
content-dependent access control, 221
centralized, 223
decentralized, 230
Diameter, 227–229
RADIUS, 223–224, 227
TACAS, 224–227
watchdog timers, 227
access control models, 210
discretionary access control, 211
identity-based, 212
mandatory access control, 212–214
role-based access control, 214–217
sensitivity labels, 213–214
access controls, 670
access control lists (ACLs), 220–221
access control matrix, 219–220
access criteria, 195–196
accountability, 159, 243–246
administrative controls, 232–233
auditing, 237
authentication, 158, 160–161
authorization, 158, 195
cabling, 234
capability tables, 220
computer controls, 234
constrained user interfaces, 218–219
content-dependent access control, 221
centralized, 223
decentralized, 230
Diameter, 227–229
RADIUS, 223–224, 227
TACAS, 224–227
watchdog timers, 227
access control models, 210
discretionary access control, 211
identity-based, 212
mandatory access control, 212–214
role-based access control, 214–217
sensitivity labels, 213–214
access controls, 670
access control lists (ACLs), 220–221
access control matrix, 219–220
access criteria, 195–196
accountability, 159, 243–246
administrative controls, 232–233
auditing, 237
authentication, 158, 160–161
authorization, 158, 195
cabling, 234
capability tables, 220
computer controls, 234
constrained user interfaces, 218–219
content-dependent access control, 221
centralized, 223
decentralized, 230
control zone, 234, 250
default to no access, 196–197
directory services, 209
emanation security, 248–250
encryption, 237
facilities, 447–454
groups, 196
identification, 158, 160–161, 162
intrusion detection systems (IDSs), 250–260
intrusion prevention systems (IPSs), 260–263
Kerberos, 200–205
layers, 231–232
logical access controls, 160
natural access control, 410–412
need-to-know principle, 197–198
network access, 236–237
network architecture, 235–236
network segregation, 233
object reuse, 248
overview, 155–156
perimeter security, 233
personnel, 454–455
personnel controls, 232
physical controls, 233
practices, 246–250
preventive, 239–240
protocols, 237
race condition, 159
roles, 195
rule-based, 217–218
security domains, 206–208
security-awareness training, 232
SESAME, 205–206
single sign-on, 198–200
supervisory structure, 232
system access, 235
technical controls, 234–237
Tempest, 249
testing, 233
thin clients, 209–210
threats, 263–269
types of, 237–242
unauthorized disclosure of information, 247–248
white noise, 249
work area separation, 234
See also identity management
access points (APs), 621
access triple, 339
accessing password files, 185
account management, 174
accountability, 159, 243–244
keystroke monitoring, 245–246
operations security, 1032–1033
protecting audit data and log information, 246
review of audit information, 245
accreditation, 371–372
ACLs, 220–221
active attacks, 753
ActiveX, 995
ActiveX Data Objects (ADO), 921
activity support, 415
Address Resolution Protocol (ARP), 529–530
administrative controls, 232–233
administrative interfaces, 984–985
Advanced Encryption Standard (AES), 697, 703–704
advisory policies, 112
adware, 645
aggregation, 927
AIC triad, 59–61
ALERT See annualized loss expectancy (ALE)
algebraic attacks, 756
algorithms, 666, 670
analog transmission signals, 505–506, 525
analytic attacks, 756
annualized loss expectancy (ALE), 95–97
annualized rate of occurrence (ARO), 96
anti-malware programs, 1005–1006
   See also malware
antivirus software, 1001–1004
   See also viruses
appliances, 559
application layer, 487, 494–495
application owners, responsibilities, 132
application security. See software security
application-level proxies, 554, 555–557
Arabo, Jason Salah, 25
architecture, 281
   and access control, 235–236
   additional storage devices, 317
   architectural view of network
   environments, 45–47
   central processing unit (CPU),
   281–286
   CPU modes and protection rings,
   308–310
domains, 312
enterprise architecture, 373–381
firewalls, 560–563
input/output device management,
   317–320
layered operating system architecture,
   311, 312–314
multiprocessing, 286–287
open network architecture, 484
operating systems, 287–294,
   310–311
process management, 287–292
security architecture, 322
Sherwood Applied Business Security
   Architecture (SABSA), 378
software, 966–967
system architecture, 321–330
terminology, 314–315
three-tier, 40–42
two-tier, 40
virtual machines, 315
Zachman Architecture Framework,
   376–378
   See also memory
arithmetic logic units (ALUs), 282
ARO. See annualized rate of
   occurrence (ARO)
ARP table poisoning, 530
artificial neural networks (ANNs),
   977–979
assembly code, 957
asset identification and management,
   1036–1037
Associate CISSP, 10
assurance, 355–356
assurance levels, 1034
asymmetric algorithms, 679
   types of, 706–713
asymmetric mode, 286–287
Asymmetrical DSL (ADSL), 607
asynchronous attacks, 383
asynchronous communication,
   507, 525
asynchronous token device, 189–190
Asynchronous Transfer Mode. See ATM
ATM, 594–596
attacks
   cramming, 1087
data diddling, 885
denial-of-service attacks,
   1010, 1086
distributed denial-of-service,
   1013–1014
dumpster diving, 886–887
emanations capturing, 887
 evolution of, 842–844
excessive privileges, 885
fake login screens, 1086
file descriptor attacks, 1096
fraggle, 1011
IP spoofing, 886
mail bombing, 1086
man-in-the-middle
attacks, 1086
password sniffing, 885–886
ping of death, 1086
salami attacks, 884
slamming, 1087
smurf, 1010–1011
SYN floods, 1011–1012
teadrop, 1012–1013, 1087
traffic analysis, 1087
wardialing, 1086
wiretapping, 887–888
See also hacking
attenuation, 512, 522–523
audit committee, responsibilities, 130
auditing, 237
physical access, 468–469
protecting audit data and log
information, 246
review of audit information, 245
auditors
compliance auditors, 90
responsibilities, 134
authentication, 158, 160–161, 669
open system authentication
(OSA), 623
protocols, 614–616
shared key authentication
(SKAL), 623
Authentication Header (AH), 750
authoritative sources, 175
authorization, 158, 195, 669
access criteria, 195–196
creep, 197
availability, 59–60
and access control, 157
Available Bit Rate (ABR), 595
awareness, security-awareness training,
139–142

B
backdoors, 1085–1087
background checks, 137–138
backups, 1066–1067
choosing a software backup
facility, 806
data backup alternatives, 801–803
differential process, 802
electronic backup solutions, 803–806
full backup, 802
hardware, 796
incremental process, 802
software, 796–797
bandwidth, 506, 519
Bank of America, 27
base registers, 297, 298
baseband, 507–508, 525
Basel II Accord, 858
baselines, 113–114
See also security policies
Basic Security Theorem, 335
bastion hosts, 560
BCP. See business continuity plan (BCP)
BEDO DRAM, 300
Bell-LaPadula model, 333–336
vs. Biba model, 338
Biba model, 336–338
vs. Bell-LaPadula model, 338
biometrics, 179–182, 183–184
crossover error rate (CER),
179–180
facial scans, 183
fingerprints, 182
hand geometry, 182
hand topography, 183
iris scans, 182
keyboard dynamics, 183
palm scans, 182
processing speed, 181
retina scans, 182
signature dynamics, 182–183
Type I and Type II errors, 179, 180
voice prints, 183
blackout, 434
block ciphers, 685–687
blocked state, 290
Blowfish, 704–705
Bluejacking, 634
blueprints, 78–79
Bluetooth, 634
board of directors, responsibilities, 123–124, 125–126
Boeing, 36
bollards, 458
Boot Protocol (BOOTP), 531
boot sector viruses, 996
Border Gateway Protocol (BGP), 534–535
botnets, 839, 999
Brewer and Nash model, 348–349
bridges, 536–538
vs. routers, 540
British Standard 7799 (BS7799), 71
broadband, 507–508, 525
broadcast storms, 537
broadcast transmission, 524–525
brownout, 434
browsing, 1082–1083
brute force attacks, 185, 264–265
buffer overflows, 384–388, 1096
burst EDO DRAM (BEDO DRAM), 300
bus topology, 510
business continuity, 770–771
planning, 771
steps, 772–774
business continuity coordinator, 776
business continuity plan (BCP), 770
business impact analysis (BIA), 778–783
business process recovery, 788–789
checklist test, 818
choosing a software backup facility, 806
certainty planning policy statement, 777
damage assessments, 810
data backup alternatives, 801–803
data recovery solutions, 807–808
development products, 813
disk shadowing, 804
documentation, 798–799
digital backup solutions, 803–806
electronic vaulting, 804–805
emergency response, 820–821
end-user environment, 800–801
facility recovery, 789–795
full-interruption test, 819
goals, 814–815
hardware backups, 796
human resources, 799–800
implementing strategies, 815–816
insurance, 808–809
interdependencies, 783–785
life cycles, 824
maintaining the plan, 821–823
maximum tolerable downtime (MTD), 781–782
parallel test, 819
as part of the security policy and program, 774–775
preventive measures, 786, 787
project initiation, 776–777
recovery and restoration, 809–813
recovery strategies, 786–788
remote journaling, 805
requirements, 778
restoration team, 810
salvage team, 810
simulation test, 819
software backups, 796–797
storing the BCP, 798
structured walk-through test, 818–819
supply and technology recovery, 795–800
tape vaulting, 805–806
testing and revising the plan, 816–821
training, 820
types of, 817
business enablement, 380
business impact analysis (BIA), 778–783

C
CA. See certificate authorities
cable modems, 606–608
cabling, 234, 519
  attenuation, 522–523
  bandwidth, 519
  coaxial, 520
  crosstalk, 523
  data throughput rate, 519
  fiber-optic, 522
  fire rating, 523–524
  noise, 522
  twisted-pair, 520–521
cache memory, 302
Caesar ciphers, 677
caller ID, 617
Canadian Information Processing Society. See CIPS
Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), 49
CAP, 11
Capability Maturity Model (CMM), 955–956
capability tables, 220
care-of addresses, 228
carrier sense multiple access with collision avoidance. See CSMA/CA
carrier sense multiple access with collision detection. See CSMA/CD
cascading errors, 87
CBC-MAC, 717, 718
CBK security domains, 5, 6–7
  ISO 17799 domains, 71–72
  See also security domains
CCTA Risk Analysis and Management Method (CRAMM), 89
CCTV, 461–464, 465
CD-ROM, accompanying this book, 1109
  Final mode, 1111
  installing test software, 1111
  navigation, 1111
  Practice mode, 1111
  running the QuickTime cryptography video sample, 1110
  system requirements, 1112
  technical support, 1112
  troubleshooting, 1111
cell phone cloning, 637
cell suppression, 929
central processing units, 281–286
  See also processors
CER. See crossover error rate (CER)
certificate authorities, 726–729
certificates, 729, 730
certification, 370–371
  other certification exams, 11
  reasons for getting, 1–2
  recertification requirements, 9–10
  requirements, 2–4, 9
Certification and Accreditation Professional. See CAP
Certified Information Systems Security Professional. See CISSP
Challenge Handshake Authentication Protocol (CHAP), 615, 616
change control analysts, responsibilities, 132–133
change control documentation, 1047–1048
change control process, 1045–1047
Channel Service Unit/Data Service Unit. See CSU/DSU
Chief Executive Officer (CEO), responsibilities, 124–125
Chief Financial Officer (CFO), responsibilities, 125
Chief Information Officer (CIO), responsibilities, 126–127
Chief Information Security Officer (CISO), responsibilities, 129
Chief Privacy Officer (CPO), responsibilities, 127
Chief Security Officer (CSO), responsibilities, 128–129
Chinese Wall model, 348–349
Choicepoint, 26–27
chosen-ciphertext attacks, 754
CIA triad. See AIC triad
cipher locks, 451–452
cipher-only attacks, 753
ciphers, 670
  block, 685–687
  confusion and diffusion, 685–686
  initialization vectors, 688
  stream, 687–688, 689
  types of, 676–679
ciphertext, 665
CIPS, 8
client/server model, 908
clipping levels, 1033
clock speed, 288
closed environments, 19–20
closed systems, 372–373
  See also open systems
closed-circuit TV, 461–464, 465
clustering, 1064–1065
coaxial cable, 520
CobiT, 69–72
cognitive passwords, 160, 187
cohesion, 967–968
collision domains, 527–528
collusion, 136
COM, 971
commits, 926
committed information rate (CIR), 592
Common Criteria, 49, 366–369
  components of, 370
compartmented security mode, 352–353
compliance auditors, 90
compression viruses, 996
Computer Ethics Institute, 889
Computer Fraud and Abuse Act, 856–857
Computer Security Act of 1987, 859
Computer Security Institute. See CSI
compartmented security mode, 352–353
compliance auditors, 90
corporate security, 29–31
management, 35–37
Corporate Security Officer (CSO). See security officer
COSO framework, 69–70
cost/benefit analysis, 102–103
cost/benefit comparisons, 84
countermeasures, 46–47
to brute force attacks, 265
to buffer overflow attacks, 388
to covert channels, 344
defined, 62
to dictionary attacks, 264
to distributed denial-of-service attacks, 1014
to fraggle attacks, 1011
functionality and effectiveness of, 104–105
to maintenance hooks, 382–383
selection, 102–103
to smurf attacks, 1010–1011
to SYN floods, 1012
to teardrop attacks, 1013
to time-of-check/time-of-use attacks, 383–384
counter-synchronization, 188–189
coupling, 968–969
covet timing channel, 344
CRAMM, 89
cramming, 1087
crime
common Internet crime schemes, 843
complexities, 839–841
computer-assisted crime, 836–838  
computer-targeted crime, 836–838  
defining and protecting electronic assets, 842  
evolution of attacks, 842–844  
investigations, 866–872  
other jurisdictions, 844–846  
See also laws  
Crime Prevention Through Environmental Design (CPTED), 409–414  
activity support, 415  
crossover error rate (CER), 179–180  
crosstalk, 523  
cryptanalysis, 664, 670  
differential cryptanalysis, 755  
linear cryptanalysis, 755  
cryptographic keys, 190  
cryptography, 659–660, 670  
asymmetric, 681–684  
attacks, 753–757  
concealment ciphers, 674  
digital envelopes, 693  
government involvement, 675–676  
hardware vs. software systems, 737  
history of, 660–665  
notation, 705  
out-of-band method, 680  
quantum cryptography, 741–742  
running key ciphers, 673–674  
security through obscurity, 64  
substitution ciphers, 660  
symmetric, 679–681  
terminology, 665–667  
See also ciphers; encryption; steganography  
cryptology, 670  
cryptosystems, 665, 666, 670  
services, 669–670  
strength, 668–669  
work factor, 668  
CSL, 8  
CSMA, 526–527  
CSMA/CA, 527  
CSMA/CD, 526–527  
CSO. See security officer  
CSU/DSU, 589  
Cyber Czar, 33, 49  
cybercrime. See crime  
cyberlaw. See laws  
cyberterrorism, 28–29  
D  
DAC, 211, 217  
data analysts, responsibilities, 133  
data buses, 285–286  
data centers, 424–428  
Data Circuit-Terminating Equipment (DCE), 592  
data custodians, responsibilities, 131  
data definition language (DDL), 921  
data dictionary, 922  
data diddling, 885  
Data Encryption Algorithm (DEA), 696  
Data Encryption Standard (DES), 696–698  
Cipher Block Chaining (CBC) mode, 699–700  
Cipher Feedback mode, 700–701  
Counter Mode (CTR), 702  
Electronic Code Book (ECB) mode, 698–699  
Output Feedback mode, 701–702  
See also Triple-DES (3DES)  
data hiding, 295, 312  
data inspection, 560  
data leakage, 1054–1055  
data link layer, 492–494, 496  
data manipulation language (DML), 922  
data mining, 933–935  
data modeling, 966  
data origin authentication, 670, 717
Data owners, 57
responsibilities, 130, 131
Data Processing Management Association. See DPMA
data remanence, 1050
data structures, 503, 967
Data Terminal Equipment (DTE), 592
data throughput rate, 519
data warehousing, 932–933
data width, 288
database management, 912–913
ActiveX Data Objects (ADO), 921
data mining, 933–935
data warehousing, 932–933
Extensible Markup Language (XML), 921
integrity, 924–927
Java Database Connectivity (JDBC), 921
models, 914–919
Object Linking and Embedding Database (OLE DB), 920–921
Open Database Connectivity (ODBC), 920
programming interfaces, 919–921
relational database components, 921–924
security issues, 927–932
software, 913–914
terminology, 918
database views, 929–930
databases, roles, 42–44
datagrams, 503
DCOM, 47, 972
DDR SDRAM, 300
decipher, 670
dedicated security mode, 352
degaussing, 1049
delayed loss, 88
Delphi technique, 100
demilitarized zones (DMZs), 549
denial-of-service attacks, 1010, 1086
DES. See Data Encryption Standard (DES)
device locks, 452
dialog management, 489
Diameter, 227–229
dictionary attacks, 185, 263–264
differential cryptanalysis, 755
differential power analysis, 193
Diffie-Hellman algorithm, 706–708
digital envelopes, 693
Digital Forensics Science (DFS), 873
See also forensics
digital identities, 177
digital signals, 506, 525
Digital Signature Standard (DSS), 725
digital signatures, 722–725
Digital Subscriber Line. See DSL
Direct Access Storage Devices, 1060–1061
direct memory access (DMA), I/O using, 320
Direct Sequence Spread Spectrum (DSSS), 620–621
directories, 165–167
object organization, 166
role in identity management, 167–168
directory services, 165, 209, 575–576
disaster recovery, 770–771
disaster recovery plan, life cycles, 824
discretionary access control (DAC), 211, 217
ORBs, 970–971
Discretionary Security Property (ds-property), 336
disk shadowing, 804
distance-vector routing protocols, 533
Distributed Component Object Model. See DCOM
distributed computing, 969
COM, 971
CORBA, 969–970
DCOM, 972
Distributed Computing Environment (DCE), 974–975
Enterprise JavaBeans (EJB), 972–973
object linking and embedding (OLE), 973
distributed denial-of-service attacks, 1013–1014
DNS, 569–570
Internet DNS and domains, 570–571
poisoning, 572
dogs, 468
Domain Name Service. See DNS
domains, 312
doors, 421–423
double data rate SDRAM (DDR SDRAM), 300
DPMA, 8
DRAM, 299
drills, 469–470
DSL, 606
DSW Shoe Warehouse, 27
dual control, 138
dual-homed firewalls, 560
due care, 57–58, 116, 861, 1028
due diligence, 116, 861, 1028
dumpster diving, 886–887
dynamic analysis, 1002
Dynamic Host Configuration Protocol (DHCP), 530–531
dynamic keys, 629–631
dynamic link libraries (DLLs), 297
dynamic mapping, 578
dynamic packet filtering, 557–558
dynamic RAM (DRAM), 299
dynamic routing protocol, 533

E
EAP, 616
Economic Espionage Act of 1996, 859
EDO DRAM, 300
education, 51–52
security-awareness training, 139–142
EEPROM, 301
EF. See exposure factor (EF)
El Gamal algorithm, 711
electric power, 430–436
electrically erasable programmable ROM, 301
electromagnetic analysis, 193–194
electromagnetic interference (EMI), 432, 433
electronic access control (EAC) tokens, 455
electronic monitoring, 185
Electronic Registry Systems, 36–37
electronic vaulting, 804–805
elliptic curve cryptosystems, 712
e-mail, 1072–1073
how it works, 1074
Message Security Protocol (MSP), 739
Multipurpose Internet Mail Extension (MIME), 738
Pretty Good Privacy (PGP), 739–740
Privacy-Enhanced Mail (PEM), 738–739
quantum cryptography, 741–742
relaying, 1075–1076
standards, 737–742
emanation security, 248–250
emanations capturing, 887
emergency system restart, 1038
Emory University, 36
employee controls, 138
Encapsulating Security Payload (ESP), 750
capsulation, 295, 484–485, 503
encipher, 670
encryption, 237
  asymmetric and symmetric
  algorithms used together, 
  689–695
  defined, 665
  at different layers, 735
  Enigma machine, 663–664
  link vs. end-to-end, 735–736
  one-time pads, 671–673, 689
  ROT13, 662
  session keys, 692–695
  symmetric vs. asymmetric algorithms, 
  679–684
  See also cryptography
end-to-end encryption, vs. link encryption, 
735–736
end-user environment, 800–801
Enigma machine, 663–664
enterprise architecture, 373–381
Enterprise JavaBeans (EJB), 972–973
enticement, 262, 883
entity authentication, 670
entity integrity, 925
entrapment, 262, 883
entry points, 421–423
environmental issues, 436–438
EPROM, 301
erasable and programmable
  ROM, 301
Ethernet, 513–515
ethics, 888–889
  Computer Ethics Institute, 889
  corporate ethics programs, 891
  Internet Architecture Board (IAB), 
  890–891
European Union Principles on Privacy, 
845–846
evaluation
  accreditation, 371–372
  certification, 370–371
  Common Criteria, 
  366–369, 370
Information Technology Security
  Evaluation Criteria (ITSEC), 
  364–366
  reasons for evaluation, 
  356–357
  See also Orange Book
Evaluation Assurance Levels (EALs), 367
exam. See CISSP exam
excessive privileges, 885
execution domain switching, 325
execution domains, 324
executive succession planning, 799
expert systems, 975–977
exposure, defined, 62
exposure factor (EF), 96
extended data out DRAM (EDO 
  DRAM), 300
Extensible Authentication Protocol.
  See EAP
Extensible Markup Language. See XML
extranets, 579–580
facial scans, 183
  See also biometrics
Facilitated Risk Analysis Process (FRAP), 
88–89
facilities, 416–417
  access controls, 447–454
  cold sites, 790–791
  hot sites, 790–791
  multiple processing centers, 794
  offsite locations, 793
  reciprocal agreements, 793–794
  recovery, 789–795
  redundant sites, 794–795
  rolling hot sites, 794
  tertiary sites, 792
  warm sites, 790–791
Failure Modes and Effect Analysis (FMEA), 
89–92
failure states, 912
fake login screens, 1086
Faraday cage, 249
Fast Ethernet, 514–515
fault generation, 193
fault tree analysis, 91–92
tax security, 1076–1078
FDDI, 517–518
Federal Communications Commission (FCC), 482
Federal Privacy Act, 853, 857–858
Federal Sentencing Guidelines for Organizations, 891
federated identities, 178
fencing, 456–458
Fiber Distributed Data Interface.
  See FDDI
fiber-optic cable, 522
file access protection, 45
file descriptor attacks, 1096
financial fraud, 980
fingerprints, 182, 716
  See also biometrics
fire
  detection, 438, 439–442
  prevention, 438
  suppression, 439, 442–446
  testing and drills, 469–470
fire resistant ratings, 439
firewalls, 548–550, 563–566
  architecture, 560–563
  best practices, 559
  packet-filtering, 550–551
  proxy, 552–557
  stateful, 551–552
  web application, 982
flash memory, 301
Flury, Kenneth J., 25
FMEA, 89–92
footprint, 640
foreign key, vs. primary key, 922–924
forensics, 872–873
  best evidence, 881
  circumstantial evidence, 881
  conclusive evidence, 881
  corroborative evidence, 881
  direct evidence, 881
  enticement, 883
  entrapment, 883
  evidence admissible in court, 880–882
  exigent circumstances, 883
  field kits, 878
  forensics investigation process, 876–879
  hearsay evidence, 882
  incident investigators, 875
  International Organization on Computer Evidence (IOCE), 873–874
  interviewing and interrogating, 884
  means, 874
  motive, 874
  opinion evidence, 882
  opportunity, 874
  search and seizure, 883–884
  secondary evidence, 881
  surveillance, 883
forking, 289
forwarding tables, 537–538
fraggle, 1011
frame relay, 592–593
frameworks, 69–73
FRAP, 88–89
frequency analysis, 678
Frequency Hopping Spread Spectrum (FHSS), 619–620, 621
frequency-division multiplexing, 588
full-duplex, 490
fully mapped I/O, 320
functional requirements evaluation, 61
G

gap in the WAP, 636
gateways, 545–546
  H323 gateways, 600–601
general registers, 283
Generic Security Services Application Programming Interface (GSS-API), 205
governance, 73–75
Graham-Denning model, 349
Gramm-Leach-Bliley Act (GLBA), 124, 856
grid computing, 1065–1066
ground, 433
ground connectors, 419
groups, 196
GSS-API, 205
guards, 353, 467–468
guidelines, 114
  See also security policies

H
H323 gateways, 600–601
hacker intrusion, liability for, 865–866
hacking, 1078–1082
  backdoors, 1085–1087
  browsing, 1082–1083
  and companies, 29–31
  evolution of, 23–27, 34–35
  Loki attacks, 1084–1085
  and military actions, 27–28
  password cracking, 1085
  session hijacking, 1084
  sniffers, 1083–1084
  See also attacks; cyberterrorism
half-duplex, 490
halon, 443–444
hand geometry, 182
  See also biometrics
hand topography
  See also biometrics
hardware backups, 796
Harrison-Ruzzo-Ulman model, 349
hashes, 718
hashing algorithms, 716, 718–720
hashing values, 716
HAVAL, 720
HDLC, 597
Health Insurance Portability and Accountability Act (HIPAA), 856
heat-activated fire detectors, 441
heuristic detection, 1001–1002
heuristic IDSs, 254
hierarchical data model, 915–916
Hierarchical Storage Management (HSM), 1067–1069
High-bit-rate DSL (HDSL), 607
High-level Data Link Control. See HDLC
High-Speed Serial Interface. See HSSI
hiring practices, 136–138
  See also personnel
HMAC, 715–717, 718
honeypots, 262, 566
hops, 736
host-based IDSs (HIDSs), 251
HSSI, 597
HTTP, 743–744
HTTP Secure (HTTPS), 744–745
hubs, 536

I
Idaho State University, 8
identification, 158, 160–161
  component requirements, 162
identifying threats, 87–88
identity management
  account management, 174
  assisted password reset, 172–173
  biometrics, 179–184
  cryptographic keys, 190
digital identities, 177
directories, 165–168
federation, 178
legacy single sign-on, 173
memory cards, 191
overview, 162–165
passphrases, 190–191
password management, 171
password synchronization, 171–172
passwords, 184–190
profile update, 176–177
provisioning, 175–176
self-service password reset, 172
smart cards, 191–194
web access management (WAM), 168–171
what companies need identity management, 178
identity repository, 175
identity theft, 268–269
Identity Theft Resource Center, 27
illogical processing, 87
IMAP, 1075
immunizers, 1002
i-Mode, 636–637
incident response, 866–869
incident investigators, 875
procedures, 869–872
inference, 927
inference attacks, 345
information classification.
See classification
information flow model, 342–344
information gathering, 983–984
information owners, 57
information risk management (IRM), 80–81
policy, 82
team, 82–83
Information Sharing and Analysis Centers.
See ISACs
Information Systems Audit and Control Association (ISACA), 69
Information Systems Security Association. See ISSA
Information Technology Security Evaluation Criteria (ITSEC), 49, 364–366
information warfare, 23
informative policies, 112
initialization vectors, 629–631, 688
input validation, 987–989
input/output device management, 317–320
in-rush current, 433–434
instant messaging (IM), 645–646
insurance, 107, 808–809
Integrated Services Digital Network.
See ISDN
integrity, 60, 669
and access control, 157
integrity models, goals of, 341–342
integrity verification procedures (IVPs), 339
intellectual property laws, 849
copyright, 850
internal protection of intellectual property, 851
patent, 851
software piracy, 852–853
trade secrets, 849–850
trademark, 850–851
Interior Gateway Routing Protocol (IGRP), 534
internal compartments, 423
International Data Encryption Algorithm (IDEA), 704
International Electrotechnical Commission (IEC), 73
International Information Systems Security Certification Consortium. See (ISC)²
International Organization on Computer Evidence (IOCE), 873–874
International Standards Organization. See ISO
International Telecommunication Union (ITU), 482
Internet, 37–40
    architecture, 40–42
    database roles, 42–44
Internet Architecture Board (IAB), 890–891
Internet Assigned Numbers Authority (IANA), 569
Internet Control Message Protocol (ICMP), 531–532
Internet Haganah, 29
Internet security, 743
    cookies, 747–748
    HTTP, 743–744
    HTTP Secure, 744–745
    Internet Security Protocol (IPSec), 749–753
    Secure Electronic Transaction (SET), 745–747
    Secure HTTP, 745
    Secure Shell (SSH), 748–749
Internet Security Association and Key Management Protocol (ISAKMP), 752
internetwork, 538
interrupt-driven I/O, 319
interrupts, 290–292, 318–319
intranets, 579–580
intrusion detection systems (IDSs), 250, 464–467
    characteristics, 467
    host-based IDSs (HIDSs), 251
    knowledge- or signature-based IDSs, 251–252
    network traffic, 259
    network-based IDSs (NIDSs), 250–251
    protocol anomaly–based IDSs, 254–255
    rule-based IDSs, 255–257
    sensors, 46, 258–259, 260
    state-based IDSs, 252–253
    statistical anomaly–based IDSs, 253–254
    traffic anomaly–based IDSs, 255
    types of, 257
intrusion prevention systems (IPSs), 260–261, 982
    honeypots, 262
    network sniffers, 262–263
invocation property, 337, 338
I/O device management, 317–320
IP, 498
IP addressing, 504
IP spoofing, 886
IP telephony. See Voice over IP (VoIP)
IPSec, 46, 610, 749–753
IPv6, 505
iris scans, 182
See also biometrics
Irish Republican Army, 28
IRM. See information risk management (IRM)
ISACs, 32
(ISC)², 8, 888
    process for earning credential, 4–5
    scenario-based exam questions, 4
ISDN, 604–606
ISDN DSL (IDSL), 607
ISO, 482, 483
ISO 17799, 71–73
ISO/IEC 14443, 194
isolation, 567
ISSA, 8
issue-specific policies, 111–112
IT Governance Institute (ITGI), 69
iterated tunneling, 610
ITSEC. See Information Technology Security Evaluation Criteria (ITSEC)
IVs. See initialization vectors
J
Java, 993–994
Java Database Connectivity (JDBC), 921
Java Virtual Machine (JVM), 316
Joint Analysis Development (JAD), 952

K
Kerberos, 200–201
  Key Distribution Center (KDC), 201
  and password-guessing attacks, 205
  principals, 201
  process, 201–204
  tickets, 201
  weaknesses, 204
Kerckhoffs’ Principle, 64, 668
kernel flaws, 1095
kernel mode, 285
kernel proxy firewalls, 558
key clustering, 671
key management, 732–733
  principles of, 733–734
  rules, 734
keyboard dynamics, 183
  See also biometrics
keys, 666, 667, 670
  asymmetric, 681
  session keys, 692–695
keyspaces, 666, 667, 671
keystroke monitoring, 245–246
KGB, 28
knapsack algorithms, 713
knowledge discovery in database (KDD). See data mining
knowledge-based IDSs, 251–252
knowledge-based systems, 975–977
Kosovo Air Campaign (1999), 28

L
L2TP, 613–614
LAN networking, 508
  broadcast transmission, 524–525
  cabling, 519–524
  collision domains, 527–528
  CSMA, 526–527
  Ethernet, 513–515
  FDDI, 517–518
  media access technologies, 512–519, 525–529
  multicast transmission, 524–525
  polling, 529
  protocols, 529–532
  token passing, 526
  Token Ring, 516
  topologies, 509–512
  unicast transmission, 524–525
LANs, 46
  protocols, 583
  See also Virtual LANs (VLANs)
laptop theft, 428–429
last mile, 506
lattice model, 346–347
laws
  administrative/regulatory laws, 848–849
  Basel II Accord, 858
  civil law, 846, 848
  common law, 846–847
  computer crime laws, 836–838
  Computer Fraud and Abuse Act, 856–857
  Computer Security Act of 1987, 859
  Economic Espionage Act of 1996, 859
  Federal Privacy Act, 853, 857–858
  Gramm-Leach-Bliley Act (GLBA), 856
  Health Insurance Portability and Accountability Act (HIPAA), 856
intellectual property laws, 849–853
mixed law systems, 847–848
overview, 836
Payment Card Industry Data Security Standards (PCI DSS), 858–859
and politics, 49–51
privacy, 853–861
religious law systems, 847
Sarbanes-Oxley Act of 2002 (SOX), 855–856
See also crime
layered approach to security, 44–45
an architectural view, 45–47
bringing layers together, 48–49
a missed layer, 48
layering, 312–314
LDAP. See Lightweight Directory Access Protocol (LDAP)
least privilege, 329–330
LexisNexis, 27
liability, 861–864
hacker intrusion, 865–866
personal information, 864–865
licensing, 1043
lighting, 459–460
limit registers, 297, 298
line conditioners, 434
linear cryptanalysis, 755
link encryption, 735–736
link-state routing protocols, 533
load, 418
local area networks. See LANs
local bridges, 537
local loop, 506
locks, 448–454
log scrubbers, 644
logic bombs, 1000
logical addresses, 303
logical location restrictions, 196
logon
limiting logon attempts, 187
spoofing at logon, 265
Loki attacks, 532, 1084–1085
loss
annualized loss expectancy (ALE), 95–97
delayed, 88
exposure factor (EF), 96
single loss expectancy (SLE), 95–97
loss potential, 88
LUC algorithm, 713
Lucifer, 644, 696
M
MAC, 212–214, 217
machine language, 957
macro languages, 997
MAID, 1063
mail bombing, 1086
mainframes, 21, 22, 1070–1072
maintenance hooks, 382–383
malware, 995–996
anti-malware programs, 1005–1006
components, 998
mandatory access control (MAC), 212–214, 217
mandatory vacation policy, 138
man-in-the-middle attacks, 1086
maskable interrupts, 291–292
masquerading, 530, 563
massive array of inactive disks. See MAID
maximum tolerable downtime (MTD), 781–782
MD2, 719
MD4, 719
MD5, 719–720
mean time between failures (MTBF), 1057
mean time to repair (MTTR), 1058
mechanical locks, 449–452
<table>
<thead>
<tr>
<th>Memory</th>
<th>Media Controls</th>
<th>Methods</th>
<th>Meme Viruses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Burst EDO DRAM (BEDO DRAM), 300</td>
<td>1048–1053</td>
<td>960</td>
<td></td>
</tr>
<tr>
<td>Cache, 302</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Double Data Rate SDRAM (DDR SDRAM), 300</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic RAM (DRAM), 299</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Electrically Erasable Programmable ROM, 301</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Erasable and Programmable ROM, 301</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extended Data Out DRAM (EDO DRAM), 300</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flash, 301</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leaks, 305–306</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management, 296–298</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mapping, 302–305</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Programmable ROM, 301</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection Issues, 298</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random Access Memory (RAM), 299–300</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Read-Only Memory (ROM), 300–301</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static RAM (SRAM), 299</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Synchronous DRAM (SDRAM), 300</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual, 306–307</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Memory Cards, 191</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mesh Topology, 510–511</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Authentication Code (MAC), 714–715</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Digest, 716</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Integrity, 713–714</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CBC-MAC, 717, 718</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HMAC, 715–717, 718</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>One-Way Hash, 714–715</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Integrity Code (MIC), 716</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message Security Protocol (MSP), 739</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Messages, 503</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Meta-Directories, 167, 168, 575</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
multiservice access technologies, 597–600
Multistation Access Units (MAUs), 516
multitasking, 289, 293
multithreaded applications, 293
multithreading, 293
MyDoom virus, 25–26

N
namespaces, 165
naming distinctions, 295
NAT. See network address translation (NAT)
National Institute of Standards and Technology (NIST), 772
natural access control, 410–412
natural surveillance, 413
network access, 236–237
network address translation (NAT), 46, 577–579
network database model, 916
Network Information System (NIS), 573–575
network layer, 491–492, 495
network operating systems (NOS), 567–568
network segregation, 233, 567
network sniffers, 262–263, 1083–1084
network-based IDSs (NIDSs), 250–251
and switched environments, 258
Next-Generation Secure Computing Base (NGSCB), 324
nexus, 324
NIS. See Network Information System (NIS)
NIS+. See Network Information System (NIS)
NIST SP 800-30 and 800-66, 88
noise, 433, 434–435, 522
noise and perturbation, 929
nondisclosure agreements, 136
nondiscretionary access control.
See role-based access control (RBAC)
noninterference model, 345
nonkeyed message digests, 716
non-maskable interrupts, 292
nonplenum cables, 523
nonrepudiation, 669

O
Object Linking and Embedding Database (OLE DB), 920–921
object linking and embedding (OLE), 973
object organization in directories, 166
object reuse, 248
object-oriented analysis (OOA), 966
object-oriented database model, 917–918
object-oriented design (OOD), 966
object-oriented programming (OOP), 958–964
object-relational database model, 918–919
objects, defined, 155
obscurity, security through, 63–64
OCTAVE, 89
Office of Homeland Security. See ISACs
one-time pads, 671–673
vs. stream ciphers, 689
one-time passwords, 187–190
one-way functions, 710–711
one-way hash, 714–715
attacks against, 721–722
Online Certificate Status Protocol (OCSP), 729
online encryption. See link encryption
online transaction processing (OLTP), 931–932
OOP. See object-oriented programming (OOP)
Open Database Connectivity (ODBC), 920
open network architecture, 484
Open Shortest Path First (OSPF), 534
open system authentication (OSA), 623
open systems, 372
See also closed systems
Open Systems Interconnection reference model. See OSI model
operating system fingerprinting, 1080
operating systems, architecture,
287–294, 310–311
Operation French Fry, 26
operational goals, 66
operations security, 1027–1028
accountability, 1032–1033
administrative management,
1028–1031
asset identification and management,
1036–1037
assurance levels, 1034
climbing levels, 1033
clustering, 1064–1065
configuration management,
1045–1048
contingency planning, 1070
data leakage, 1054–1055
deveiations from standards,
1035–1036
Direct Access Storage Devices,
1060–1061
environmental controls, 1070
grid computing, 1065–1066
Hierarchical Storage Management
(HSM), 1067–1069
input and output controls,
1040–1041
licensing, 1043
MAID, 1063
mainframes, 1070–1072
mean time between failures
(MTBF), 1057
mean time to repair (MTTR), 1058
media controls, 1048–1053
network and resource availability,
1056–1070
RAID, 1061–1062
RAFT, 1063
remote access security, 1044
security and network personnel,
1031–1032
single points of failure,
1058–1060
Storage Area Networks (SANs),
1063–1064
system controls, 1037–1038
system hardening, 1042–1044
trusted recovery, 1038–1040
unexplained or unusual
occurrences, 1035
unscheduled initial program loads
(rebooting), 1036
See also backups
Orange Book, 49, 355–356,
357–358
Division A, 361
Division B, 360–361
Division C, 359
Division D, 359
and the Rainbow Series, 361–362
Red Book, 362–364
ORBs, 970–971
order of concepts, 63
Organisation for Economic Co-operation
and Development (OECD), 50–51
guidelines and transborder
information flow rules,
128, 845
organizational security model, 65–67
CobiT, 69–72
COSO framework, 69–70
frameworks, 69–73
operational planning, 66
private industry requirements vs. military requirements, 80
security governance, 73–75
security program components, 67–69
security program development, 76–79
strategic planning, 66
tactical planning, 66
organizational security policy, 110–112
Orthogonal Frequency-Division Multiplexing (OFDM), 621, 624
OSI model, 483
application layer, 487, 494–495
data link layer, 492–494, 496
functions and protocols, 494–496
network layer, 491–492, 495
physical layer, 494, 496
presentation layer, 487–489, 495
protocol, 483–486
session layer, 489–490, 495
transport layer, 490–491, 495
tying the layers together, 496
where devices and protocols appear within, 47

P
packet switching, 590–591
packet-filtering firewalls, 550–551
page frames, 306
paging, 306
palm scans, 182
See also biometrics
PAP, 614–615, 616
parameter validation, 989–992
partitioning, 929
passive attacks, 753
passphrases, 190–191
Password Authentication Protocol. See PAP
password sniffing, 885–886
passwords, 184
accessing password files, 185
aging, 187
assisted password reset, 172–173
cognitive, 160, 187
cracking, 1085
hashing and encryption, 186–187
limiting logon attempts, 187
management, 171, 184–185
one-time, 187–190
password checkers, 186
password-guessing attacks, 205
self-service password reset, 172
synchronization, 171–172
patch management, 1006–1007
best practices, 1009
limitations to patching, 1008–1009
steps, 1007–1008
patent, 851
patrol force, 467–468
Payment Card Industry Data Security Standards (PCI DSS), 858–859
PBXs, 547–548
penetration testing, 1090–1094
perimeter security, 233, 446–447
dogs, 468
external boundary protection mechanisms, 455–464
facility access control, 447–454
locks, 448–454
patrol force and guards, 467–468
personnel access controls, 454–455
See also intrusion detection systems (IDSs)
permanent virtual circuits (PVCs), 593
permissions, 1097
Persian Gulf War, 28
personnel
access controls, 454–455
employee controls, 138
hiring practices, 136–138
privacy issues, 859–861
responsibilities, 135
termination, 138–139
See also responsibility
pharming, 267–268
phisher scams, 27
phishing, 265–267
phreakers, 548
physical layer, 494, 496
physical location restrictions, 196
physical security, 401–404
activity support, 415
auditing physical access, 468–469
computer and equipment rooms, 424–428
construction, 418–421
Crime Prevention Through
Environmental Design (CPTED), 409–414
designing a physical security program, 414–428
doors and windows, 421–423, 424
electric power, 430–436
environmental issues, 436–438
facilities, 416–417
fire prevention, detection and suppression, 438–446
internal compartments, 423
natural access control, 410–412
natural surveillance, 413
planning, 404–408
protecting assets, 428–429
safes, 429
security zones, 411–412
territorial reinforcement, 413–414
testing and drills, 469–470
ventilation, 438
See also perimeter security
piggybacking, 455
ping of death, 1086
piracy, 852–853
PKI. See public key infrastructure
plaintext, 665, 671
chosen-plaintext attacks, 754
known-plaintext attacks, 753–754
planning horizon, 67
plenum areas, 442
plenum space, 523
point of presence (PoP), 611
Point-to-Point Protocol. See PPP
politics and laws, 49–51
polling, 529
polyinstantiation, 930–931
polymorphic viruses, 997
polymorphism, 964–965
POP, 1075
port address translation (PAT), 578
port scanning, 1081–1082
ports, well-known, 501, 557
positive drains, 436
postmortem review, 1097
PPP, 610–611
PPTP, 612–613
preemptive multitasking, 289
premapped I/O, 320
presentation layer, 487–489, 495
President’s Commission on Critical
Infrastructure Protection (PCCIP), 32, 406
Pretty Good Privacy (PGP), 739–740
primary key, vs. foreign key, 922–924
privacy, 853–854
Basel II Accord, 858
Computer Fraud and Abuse Act, 856–857
Computer Security Act of 1987, 859
Economic Espionage Act of 1996, 859
employee issues, 859–861
Federal Privacy Act, 853, 857–858
Gramm-Leach-Bliley Act (GLBA), 856
Health Insurance Portability and Accountability Act (HIPAA), 856
laws, directives and regulations, 854–855
Payment Card Industry Data Security Standards (PCI DSS), 858–859
Sarbanes-Oxley Act of 2002 (SOX), 855–856
Privacy-Enhanced Mail (PEM), 738–739
Private Branch Exchange. See PBXs
private keys, 190, 681
Privileged Attribute Certificates (PACs), 205
privileged mode, 285
problem state, 285
procedures, 114–115
   for classification, 121
   See also security policies
process activation, 324–325
process activity, 294–296
process enhancement, 380
process isolation, 294–295
process management, 287–292
process owners, responsibilities, 133
process scheduling, 293–294
processors, 288
product line managers, responsibilities, 134
profile update, 176–177
profile-based systems, 254
program counter registers, 283
program status word (PSW), 285
programmable I/O, 319
programmable ROM, 301
project sizing, 84
PROM, 301
protection profiles, 367–368
protection rings, 308–310
protocol anomaly–based IDSs, 254–255
protocols, 237, 483–486
   authentication, 614–616
   LAN networking, 529–532
   routing, 532–536
   tunneling, 609–614
prototyping, 953
provisioning, 175–176
proxy firewalls, 552–557
public algorithms, vs. secret algorithms, 754
public key cryptography, 683, 689, 709
public key infrastructure, 709, 725–726
   certificate authorities, 726–729
   certificates, 729, 730
   Registration Authority (RA), 729
   steps, 730–732
public keys, 190, 681
public-switched telephone network (PSTN), 598
purging, 1049

Q
qualitative risk analysis, 98–101
   vs. quantitative risk analysis, 100–101
Quality of Service (QoS), 595–596
quantitative risk analysis, 92–93
   vs. qualitative risk analysis, 100–101
quantum cryptography, 741–742
query language (QL), 922

R
race condition, 159, 383, 1096–1097
radio frequency interference (RFI), 432, 433
RADIUS, 223–224, 227
RAID, 1061–1062
rainbow tables, 185
RAIT, 1063
RAM, 299–300
random access memory (RAM), 299–300
Rapid Application Development (RAD), 952
RBAC, 214–215, 217
core, 215
   hierarchical, 215–216
RC4, 705
RC5, 705
RC6, 705
read-only memory (ROM), 300–301
ready state, 290
rebooting, 1038
receipt, 671
recertification, requirements, 9–10
Red Book, 362–364
redundant array of independent tapes.
   See RAIT
reference monitor, 327–328
references, checking as part of hiring practices, 136–137
referential integrity, 925
Registration Authority (RA), 729
regulatory policies, 112
relational data model, 915
relative addresses, 303
remote access, 603
   administration, 1044
cable modems, 606–608
DSL, 606
guidelines, 616–617
ISDN, 604–606
Remote Access Service (RAS), 603–604
security, 1044
xDSL, 607
Remote Access Trojans (RATs), 1001
Remote Authentication Dial-In User Service (RADIUS), 223–224, 227
remote bridges, 537
remote journaling, 805
repeaters, 536
replay attacks, 185, 756
residual risk, 106
responsibility, 122–123, 134–135
   application owners, 132
   audit committee, 130
   auditors, 134
   board of directors, 123–124, 125–126
   change control analysts, 132–133
   Chief Executive Officer (CEO), 124–125
   Chief Financial Officer (CFO), 125
   Chief Information Officer (CIO), 126–127
   Chief Information Security Officer (CISO), 129
   Chief Privacy Officer (CPO), 127
   Chief Security Officer (CSO), 128–129
data analysts, 133
data custodians, 131
data owners, 130, 131
   international requirements, 128
personnel, 135
process owners, 133
product line managers, 134
security administrators, 131–132
security analysts, 132
security steering committee, 129
solution providers, 133
structure, 135–136
supervisors, 132
system owners, 131
users, 134
retina scans, 182
   See also biometrics
Reverse Address Resolution Protocol (RARP), 531
ring topology, 509
RISC chips, 281
risk
  accepting, 96, 107–108
defined, 62
handling, 107–108
See also information risk management (IRM)
risk analysis, 83–84, 938–940
  annualized loss expectancy (ALE), 95–97
  annualized rate of occurrence (ARO), 96
  automated methods, 93–94
  costs that make up the value of information and assets, 86–87
countermeasure selection, 102–103
Delphi technique, 100
exposure factor (EF), 96
Failure Modes and Effect Analysis (FMEA), 89–92
fault tree analysis, 91–92
functionality and effectiveness of countermeasures, 104–105
handling risk, 107–108
identifying threats, 87–88
methodologies, 88–89
ownership of risk, 85
protection mechanisms, 102–105
qualitative risk analysis, 98–101
quantitative risk analysis, 92–93, 100–101
results, 97
single loss expectancy (SLE), 95–97
steps of, 94–97, 105–106
team, 84–85
total vs. residual risk, 106
uncertainty, 98
value of information and assets, 85–86
See also risk assessment
risk assessment
  CRAMM, 89
  FRAP, 88–89
  NIST SP 800-30 and 800-66, 88
  OCTAVE, 89
  Spanning Tree Analysis, 89
  See also risk analysis
risk avoidance, 107
risk mitigation, 107
risk ownership, 85
Roaming Operations (ROAMOPS), 228
role-based access control (RBAC), 214–215, 217
core, 215
  hierarchical, 215–216
roles, 195
rollback, 925–926
ROM, 300–301
rootkits, 643–644
ROT13, 662
rotation of duties, 138
route flapping, 533
routers, 539–540
Routing Information Protocol (RIP), 534
routing protocols, 532–536
RSA, 708–711
rule-based access control, 217–218
rule-based IDSs, 255–257
rule-based programming, 976
running key ciphers, 673–674
running state, 290

S
SABSA, 378
safe harbor requirements, 128, 845
safeguards
  defined, 62
  See also countermeasures
safes, 429
salami attacks, 884
salts, 186
SAM databases, 186–187
sandboxes, 316, 993
Sarbanes-Oxley Act of 2002 (SOX), 51, 124, 855–856
satellites, 640–641
savepoints, 926
screened hosts, 561
screened subnets, 561–563, 564
script kiddies, 842
script viruses, 998
scrubbing, 246
SDLC, 596–597
SDRAM, 300
secondary storage, 306
secret algorithms, vs. public
   algorithms, 754
Secure Electronic Transaction (SET), 745–747
Secure European System for Applications
   in a Multi-vendor Environment. See
   SESAME
Secure HTTP, 745
secure message format, 682
Secure MIME (S/MIME), 738
Secure Shell (SSH), 748–749
Secure Socket Layer. See SSL
SecureID, 188
security
   areas of, 22–23
   availability, 59–60
   and companies, 29–31
   confidentiality, 60–61
   education, 51–52
   history of, 19–22
   integrity, 60
   layered approach to, 44–45
   politics and laws, 49–51
   principles of, 59–61, 156–158
relationships among security
   components, 63
   terminology, 61–62
   through obscurity, 63–64
   and the U.S. government, 31–33
   See also corporate security; physical
   security; software security
Security Accounts Management (SAM)
   databases, 186–187
security administration, 56–59
security administrators, responsibilities,
   131–132
security analysts, responsibilities, 132
security architecture, 322
security domains, 206–208
   See also CBK security domains
security effectiveness, 380
security evaluation. See evaluation
security governance, 73–75
security kernel, 327–328
security management, 53–54
   administrative controls, 57
   example, 58
   physical controls, 57
   responsibilities, 54–55
   technical controls, 57
   top-down approach to building a
   security program, 55–56
   See also organizational security model
security model, 279–280, 330–331
   Bell-LaPadula model,
   333–336, 338
   Biba model, 336–338
   Brewer and Nash model, 348–349
   Chinese Wall model, 348–349
   Clark-Wilson model, 338–342
   formal models, 331
   Graham-Denning model, 349
   Harrison-Ruzzo-Ullman model, 349
   information flow model,
   342–344
lattice model, 346–347
noninterference model, 345
and security policies, 330
state machine models, 331–333
See also organizational security model
security modes of operation, 351
compartmented security mode, 352–353
dedicated security mode, 352
multilevel security mode, 353
system high-security mode, 352
security officer, 56, 67–68
security parameter index (SPI), 751
security perimeter, 326–327
security policies, 110–112, 279–280, 328–329
baselines, 113–114
due care and due diligence, 116
guidelines, 114
implementation, 115–116
procedures, 114–115
and security models, 330
standards, 112–113
security program development, 76–79
security standards, 112–113
See also security policies
security zones, 381, 411–412
security-awareness training, 139–140, 232
evaluating programs, 141–142
specialized security training, 142
types of, 140–141
segments, 503
self-garbling viruses, 997
semantic integrity, 925
sensitivity labels, 213–214
separation of duties, 135–136
and the Clark-Wilson model, 340–341
dynamic separation of duties (DSD) relations through RBAC, 216
static separation of duty (SSD) relations through RBAC, 216
system development, 945
Service Set ID (SSID), 622, 623
SESAME, 205–206
session hijacking, 1084
session keys, 692–695
session layer, 489–490, 495
session management, 992
SET, 745–747
SHA, 720
shared key authentication (SKA), 623
Sherwood Applied Business Security Architecture (SABSA), 378
shielded twisted pair (STP) cabling, 46, 520
shoulder surfing, 61
S-HTTP, 745
side-channel attacks, 193–194, 755–756
SIG-CS, 8
signature dynamics, 182–183
See also biometrics
signature-based detection, 1001
signature-based IDSs, 251–252
simple integrity axiom, 337
simple security rule, 334, 336
simpex, 490
single loss expectancy (SLE), 95–97
single sign-on technologies, 198–200
legacy single sign-on, 173
Six Sigma, 92
slamming, 1087
SLE. See single loss expectancy (SLE)
smart cards, 191–193
attacks, 193–194
interoperability, 194
SMDS, 596
smoke-activated fire detectors, 440–441
SMTP, 1074
smurf attacks, 1010–1011
sniffers, 262–263, 1083–1084
social engineering, 61, 185
SOCKS, 555–556
software, importance of, 905–906
software architecture, 966–967
software attacks, 194
software backups, 796–797
software development, 944–946
  Capability Maturity Model (CMM), 955–956
  change control, 953–955
  computer-aided software engineering (CASE), 952
  configuration management, 954
  methodologies, 957–969
  methods, 950–952
  prototyping, 953
software escrow, 957
software piracy, 852–853
Software Protection Association (SPA), 852
software security, 906–907
  complexity of functionality, 909
  data types, format and length, 910
  in different environments, 908
  environment vs. application, 908–909
  failure states, 912
  implementation and default issues, 910–912
  See also database management; patch management
solution providers, responsibilities, 133
SONET, 581–582, 585
source routing, 538, 565
SOX. See Sarbanes-Oxley Act of 2002 (SOX)
spam detection, 1004–1005
Spanning Tree Algorithm (STA), 538
Spanning Tree Analysis, 89
SPARC processors, 281
Special Interest Group for Computer Security. See SIG-CS
special registers, 283
Spectrum, Information Technologies and Telecommunications (SITT), 482
spiral development method, 952
split knowledge, 138
spoofing, 563
spoofing at logon, 265
spread spectrum, 619
  Direct Sequence Spread Spectrum (DSSS), 620–621
  Frequency Hopping Spread Spectrum (FHSS), 619–620, 621
  Orthogonal Frequency-Division Multiplexing (OFDM), 621
spyware, 645
SRAM, 299
SSL, 47
SSO. See single sign-on technologies
stacks, 284, 386
standards, 112–113
  See also security policies
star topology, 510
state machine models, 331–333
state-based IDSs, 252–253
stateful firewalls, 551–552
static analysis, 1002
static electricity, preventing, 437
static mapping, 578
static RAM (SRAM), 299
static routing protocol, 533
statistical anomaly–based IDSs, 253–254
statistical attacks, 757
statistical time-division multiplexing (STDM), 588
stealth viruses, 997
steering committee, responsibilities, 129
steganography, 674–675
Storage Area Networks (SANs), 1063–1064
storage devices, 317
star integrity axiom (*-integrity axiom), 337
star property rule (*-property rule), 334, 336
strategic alignment, 379
strategic goals, 66
stream ciphers, 687–688
vs. one-time pads, 689
strong authentication, 161
strong star property rule, 334, 336
subjects, defined, 155
substitution ciphers, 660, 676, 677
subsystems, 311
supercomputers, 1072
See also mainframes
supervisor mode, 285
supervisors, responsibilities, 132
surge, 434
surveillance devices, 460
swap space, 306
switched environments, 258
Switched Multimegabit Data Service. See SMDS
switched virtual circuits (SVCs), 593
switches, 541–542
Layer 3 and 4 switches, 542–543
switching, 590–591
symbolic links, 1096
symmetric algorithms, 679
types of, 695–705
symmetric mode, 286–287
Symmetrical DSL (SDSL), 607
SYN floods, 1011–1012
SYN proxies, 982
synchronous communication, 507, 525
Synchronous Data Link Control. See SDLC
synchronous DRAM (SDRAM), 300
Synchronous Optical Networks. See SONET
synchronous token device, 188–189
system architecture, 321–330
system authentication, 717
system development, 935–936
design specifications, 942–944
disposal, 947
functional design analysis and planning, 940–942
garbage collection, 949
installation/implementation, 946
life-cycle phases, 936–950
managing development, 936
operation and maintenance, 947
postmortem review, 949
project initiation, 937–938
risk analysis, 938–940
risk management, 938
separation of duties, 945
software development, 944–946
testing types, 947–949
verification vs. validation, 945
system hardening, 1042–1044
system high-security mode, 352
system owners, responsibilities, 131
system-specific policies, 112

T
TACAS, 224–227
TACAS+. See TACAS
tactical goals, 66
tape vaulting, 805–806
t-carriers, 586–587
TCP, 498–502
TCP handshake, 502
TCP/IP, 497–498
teardrop attacks, 1012–1013, 1087
telecommunications
defined, 482
evolution of, 583–586
Tempest, 249
temporal isolation (time-of-day restrictions), 196
Terminal Access Controller Access Control System (TACAS), 224–227
termination, 138–139
terminology, 61–62, 918
evolution of, 314–315
territorial reinforcement, 413–414
terrorism, 28–29
testing, physical security, 469–470
testing schedule, 1098
theft, 428–429
thin clients, 209–210
thrashing, 300
thread management, 292–293
threat agents, defined, 62
threats
defined, 61–62
identifying, 87–88
relationship of threats and vulnerabilities, 87
thunking, 316
Tiger, 720
time multiplexing, 295
time-of-day restrictions (temporal isolation), 196
time-of-check/time-of-use attacks, 383–384
TKIP, 630–631
token device, 187–188
asynchronous, 189–190
synchronous, 188–189
token passing, 526, 527
Token Ring, 516
topologies
bus topology, 510
mesh topology, 510–511
ring topology, 509
star topology, 510
Total Quality Management (TQM), 92
total risk, 106
trade secrets, 849–850
trademark, 850–851
traffic analysis, 1087
traffic anomaly–based IDSs, 255
traffic-flow security, 735
training, security-awareness, 139–142
tranquility principle, 335
transaction-type restrictions, 196
transformation procedures (TPs), 338
transient noise, 433
translation bridges, 537
transmission
analog and digital, 505–506
asynchronous and synchronous, 507
broadband and baseband, 507–508
transparent bridging, 537–538
transport adjacency, 610
transport layer, 490–491, 495
transposition ciphers, 676–679
Triple-DES (3DES), 703
Trojan horses, 1000–1001
trust, 355–356
Trusted Computer System Evaluation Criteria (TCSEC). See Orange Book
trusted computing base (TCB), 322, 323–326, 327
Trusted Network Interpretation (TNI). See Red Book
thrust path, 323
trusted recovery, 1038–1040
trusted shell, 323
tumbler locks, 449–451
tunneling protocols, 609–614
tunneling viruses, 998
twisted-pair cable, 520–521
two-factor authentication, 161
two-phase commits, 926–927
Type I and Type II errors, 179, 180
UDP, 498–502
unauthorized disclosure of information, 247–248
uncertainty, 98
unconstrained data items (UDIs), 339
unicast transmission, 524–525
uninterruptible power supplies. See UPSs
United States v. Jeansonne, 26
unshielded twisted pair (UTP) cabling, 520, 521
Unspecified Bit Rate (UBR), 595
UPSs
  online UPS systems, 430–431
  standby, 431
U.S. government, and security, 31–33
user errors, 88
user managers, responsibilities, 132
user mode, 285
user provisioning, 175
users, 338
  responsibilities, 134

costs that make up the value, 86–87
value-added networks (VAN), 580
vandalism, 980
Variable Bit Rate (VBR), 595
ventilation, 438
verification 1:1, 160–161
video cards, RAM, 318
virtual circuits, 593
virtual directories, 167
Virtual LANs (VLANs), 543, 544–545
virtual machines, 315
  Java Virtual Machine (JVM), 316
virtual mapping, 295–296
virtual memory, 306–307
virtual private networks. See VPNs
voices, 996–997
  antivirus software, 1001–1004
  immunizers, 1002
visual recording devices, 461–464
Voice over IP (VoIP), 598–599, 600
voice prints, 183
  See also biometrics
voltage regulators, 434
vulnerabilities
  buffer overflows, 1096
  defined, 61
  file and directory permissions, 1097
  file descriptor attacks, 1096
  kernel flaws, 1095
  race conditions, 1096–1097
  relationship of threats and vulnerabilities, 87
  symbolic links, 1096
vulnerability testing, 1087–1090
  penetration testing, 1090–1094
  schedule, 1098

WAM. See web access management (WAM)
WANs, 46, 583
  CSU/DSU, 589
  dedicated links, 586–587
  protocols, 583
  T-carriers, 586–587
telecommunications evolution, 583–586
WAP, 635–636
  gap in the WAP, 636
wardriving for WLANs, 639–640
wardialing, 264, 603–604, 1086, 1094–1095
watchdog timers, 227, 292
water sprinklers, 445–446
waterfall development method, 952
The Web, 37, 38
vulnerabilities, 43–44
See also Internet
web access management (WAM), 168–171
Web security, 979–980
administrative interfaces, 984–985
authentication and access control, 985–986
configuration management, 986–987
denial-of-service attacks, 981
financial fraud, 980
firewalls, 982
information gathering, 983–984
input validation, 987–989
intrusion prevention systems (IPSs), 982
parameter validation, 989–992
privileged access, 980–981
quality assurance process, 982
session management, 992
SYN proxies, 982
theft of intellectual property, 981
theft of transaction information, 981
vandalism, 980
Weisburd, Aaron, 29
well-known ports, 501, 557
Wells Fargo Bank, 36
white noise, 249
wide area networks. See WANs
windows, 421–423, 424
Wired Equivalent Privacy (WEP), 623, 695
Wireless Application Protocol. See WAP
wireless communications, 618
Bluetooth, 634
current implementations, 626–627
Direct Sequence Spread Spectrum (DSSS), 620–621
dynamic keys, 629–631
Frequency Hopping Spread Spectrum (FHSS), 619–620, 621
i-Mode, 636–637
initialization vectors, 629–631
spread spectrum, 619
standards, 623–634
third generation, 641–642
Wireless Application Protocol (WAP), 635–636
See also mobile phone security; satellites; WLANs
wireless LANs. See WLANs
Wireless Transport Layer Security (WTLS), 635
wiretapping, 887–888
WLANs
ad hoc WLANs, 622
components, 621–623
infrastructure WLANs, 622
war driving for, 639–640
work area separation, 234
work factor, 671
wormhole attacks, 535
worms, 999–1000
X
X.25, 594
xDSL, 607
XML, 47, 921
Y
Yahoo, 27
Z
Zachman Architecture Framework, 376–378
zero knowledge proof, 713
zeroization, 1049
zombies, 563, 839
zone transfers, 570
zones, 569
THE BEST

in Microsoft Certification Prep

VISIT MHPROFESSIONAL.COM TO READ SAMPLE CHAPTERS AND LEARN MORE.
LICENSE AGREEMENT

THIS PRODUCT (THE "PRODUCT") CONTAINS PROPRIETARY SOFTWARE, DATA AND INFORMATION (INCLUDING DOCUMENTATION) OWNED BY THE McGRAW-HILL COMPANIES, INC. ("McGRAW-HILL") AND ITS LICENSORS. YOUR RIGHT TO USE THE PRODUCT IS GOVERNED BY THE TERMS AND CONDITIONS OF THIS AGREEMENT.

LICENSE: Throughout this License Agreement, “you” shall mean either the individual or the entity whose agent opens this package. You are granted a non-exclusive and non-transferable license to use the Product subject to the following terms:

(i) If you have licensed a single user version of the Product, the Product may only be used on a single computer (i.e., a single CPU). If you licensed and paid the fee applicable to a local area network or wide area network version of the Product, you are subject to the terms of the following subparagraph (ii).

(ii) If you have licensed a local area network version, you may use the Product on unlimited workstations located in one single building selected by you that is served by such local area network. If you have licensed a wide area network version, you may use the Product on unlimited workstations located in multiple buildings on the same site selected by you that is served by such wide area network; provided, however, that any building will not be considered located in the same site if it is more than five (5) miles away from any building included in such site. In addition, you may only use a local area or wide area network version of the Product on one single server. If you wish to use the Product on more than one server, you must obtain written authorization from McGraw-Hill and pay additional fees.

(iii) You may make one copy of the Product for back-up purposes only and you must maintain an accurate record as to the location of the back-up at all times.

COPYRIGHT: RESTRICTIONS ON USE AND TRANSFER: All rights (including copyright) in and to the Product are owned by McGraw-Hill and its licensors. You are the owner of the enclosed disc on which the Product is recorded. You may not use, copy, decompile, disassemble, reverse engineer, modify, reproduce, create derivative works, transmit, distribute, sublicense, store in a database or retrieval system of any kind, rent or transfer the Product, or any portion thereof, in any form or by any means (including electronically or otherwise) except as expressly provided for in this License Agreement. You must reproduce the copyright notices, trademark notices, legends and logos of McGraw-Hill and its licensors that appear on the Product on the back-up copy of the Product which you are permitted to make hereunder.

All rights in the Product not expressly granted herein are reserved by McGraw-Hill and its licensors.

TERM: This License Agreement is effective until terminated. It will terminate if you fail to comply with any term or condition of this License Agreement. Upon termination, you are obligated to return to McGraw-Hill the Product together with all copies thereof and to purge all copies of the Product included in any and all servers and computer facilities.

DISCLAIMER OF WARRANTY: THE PRODUCT AND THE BACK-UP COPY ARE LICENSED “AS IS.” McGRAW-HILL, ITS LICENSORS AND THE AUTHORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE RESULTS TO BE OBTAINED BY ANY PERSON OR ENTITY FROM USE OF THE PRODUCT, ANY INFORMATION OR DATA INCLUDED THEREIN AND/OR ANY TECHNICAL SUPPORT SERVICES PROVIDED HEREUNDER, IF ANY (“TECHNICAL SUPPORT SERVICES”). McGRAW-HILL, ITS LICENSORS AND THE AUTHORS MAKE NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT TO THE PRODUCT. McGRAW-HILL, ITS LICENSORS, AND THE AUTHORS MAKE NO GUARANTEE THAT YOU WILL PASS ANY CERTIFICATION EXAM WHATSOEVER BY USING THIS PRODUCT. NEITHER McGRAW-HILL, ANY OF ITS LICENSORS NOR THE AUTHORS WARRANT THAT THE FUNCTIONS CONTAINED IN THE PRODUCT WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PRODUCT WILL BE UNINTERRUPTED OR ERROR FREE. YOU ASSUME THE ENTIRE RISK WITH RESPECT TO THE QUALITY AND PERFORMANCE OF THE PRODUCT.

LIMITED WARRANTY FOR DISC: To the original licensee only, McGraw-Hill warrants that the enclosed disc on which the Product is recorded is free from defects in materials and workmanship under normal use and service for a period of ninety (90) days from the date of purchase. In the event of a defect in the disc covered by the foregoing warranty, McGraw-Hill will replace the disc.

LIMITATION OF LIABILITY: NEITHER McGRAW-HILL, ITS LICENSORS NOR THE AUTHORS SHALL BE LIABLE FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES, SUCH AS BUT NOT LIMITED TO, LOSS OF ANTICIPATED PROFITS OR BENEFITS, RESULTING FROM THE USE OR INABILITY TO USE THE PRODUCT EVEN IF ANY OF THEM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL APPLY TO ANY CLAIM OR CAUSE WHATSOEVER WHETHER SUCH CLAIM OR CAUSE ARISES IN CONTRACT, TORT, OR OTHERWISE. Some states do not allow the exclusion or limitation of indirect, special or consequential damages, so the above limitation may not apply to you.

U.S. GOVERNMENT RESTRICTED RIGHTS: Any software included in the Product is provided with restricted rights subject to subparagraphs (c), (1) and (2) of the Commercial Computer Software-Restricted Rights clause at 48 C.F.R. 52.227-19. The terms of this Agreement applicable to the use of the data in the Product are those under which the data are generally made available to the general public by McGraw-Hill. Except as provided herein, no reproduction, use, or disclosure rights are granted with respect to the data included in the Product and no right to modify or create derivative works from any such data is hereby granted.

GENERAL: This License Agreement constitutes the entire agreement between the parties relating to the Product. The terms of any Purchase Order shall have no effect on the terms of this License Agreement. Failure of McGraw-Hill to insist at any time on strict compliance with this License Agreement shall not constitute a waiver of any rights under this License Agreement. This License Agreement shall be construed and governed in accordance with the laws of the State of New York. If any provision of this License Agreement is held to be contrary to law, that provision will be enforced to the maximum extent permissible and the remaining provisions will remain in full force and effect.