

Index

- *-property (star property), 255–256
- 1 x 1 GIF. *See* Web bugs.
- 12-step password attacks, 226
- 802.11 (wireless) standards, 383, 467

- A1, TCSEC class, 297–298, 299–300
- Acceptance testing, 170–171
- Access acceptability, databases, 337–338
- Access control
 - databases, 325, 327–328
 - e-mail, 636
 - file protection
 - all-none, 215–216
 - group, 216–217
 - individual permissions, 217
 - per-object, 219
 - persistent permissions, 218
 - per-user, 219
 - SUID (set userid), 218–219
 - temporary acquired permissions, 218–219
 - memory and address protection
 - base/bounds registers, 195–196
 - context switch, 195–196
 - fences, 193–194
 - page frames, 202
 - paging, 202–203, 203–204
 - relocation, 194–195
 - relocation factor, 195
 - segment address table, 199
 - segmentation, 199–202, 203–204
 - selective protection. *See* Tagged architecture.
 - tagged architecture, 196–199
 - principles of trusted systems, 266
 - privacy in computing, 606
 - privacy principles and policies, 618
 - protected objects
 - AS (authentication server), 213–214
 - access control matrix, 210–211
 - ACLs (access control lists), 208–210
 - capability, 210–213
 - directories, 205–208
 - domains, 211
 - erasing deleted files, 207
 - KDC (key distribution center), 213–214
 - Kerberos, 213–214
 - local name space, 211
 - procedure-oriented, 214–215
 - protection goals, 205
 - pseudonyms, 207–208
 - revocation of access, 206–207
 - role-based, 215
 - single sign-on, 214
 - TGS (ticket-granting server), 213–214
 - types of, 204–205
 - wild cards, 208–210
- Access control matrix, 210–211
- Access decisions, databases, 337–338
- Access policy ambiguity, 288
- Access triples security policy, 250
- Accountability principle, 272
- Accuracy
 - cost of security, 581
 - of information, ethical issues, 706–707
- ACK (acknowledgment), 429
- ACLs (access control lists), 208–210, 464–466
- ACM (Association for Computing Machinery), code of ethics, 710, 712
- Acquisti, Alessandro, 597
- Acrobat PDF, deleting text, 271
- Action phrases, 301
- Active code, network threat, 433, 435–437
- Active fault detection, 172–173
- Active server pages (ASP), 435
- Active wiretapping, 409
- ActiveX controls, 435–437
- Add subkey, 753
- Addresses (IP). *See* IP addresses.
- Addresses (memory). *See* Memory and address protection.
- Adequate protection principle, 17
- Adjusting future earnings, 575–576
- Administering security. *See* Physical security; Risk analysis; Security plan; Security policies.
- Advertising, web privacy, 628–629
- Adware, 633–634
- AES (Advanced Encryption System). *See also* DES.
 - add subkey, 753
 - byte substitution, 750–751
 - cryptanalysis of, 753–754
 - definition, 72
 - versus* DES, 73–75
 - design contest, 72
 - MARS algorithm, 748
 - mix column, 752–753
 - RC6 algorithm, 749
 - Rijndael algorithm, 73, 749

816 Index

- AES (Advanced Encryption System).
(*continued*)
Serpent algorithm, 749
shift row, 751–752
structure of, 749–753
symmetric encryption, 748–754
Twofish algorithm, 749
- Affected subject, 605–606
- Agents, malicious, 114
- Aggregation of data, 350–351, 625–626
- AH (authentication header), 455
- Airport security, case study, 370
- Al Qaeda computer case study, 24
- Alarms, 468, 489. *See also* Alerts.
- ALE (annualized loss expectation), 544
- Alerts, 468. *See also* Alarms.
- Algebra, Euclidean, 726
- Algorithm design, DES, 742–743
- Algorithms, encryption. *See* Encryption, algorithms.
- Aliasing errors, 103
- All-none file protection, 215–216
- Allocation of general objects, 266–267
- Amateur computer criminals, 21–22
- Ambiguous access policies, 288
- Amplifiers, network, 383
- Analog network communication, 382
- Analysis, risk. *See* Risk analysis.
- Ancheta, Jeanson James, 403
- Anderson, Ross, 296, 351, 601, 622
- Angle of dispersion, 384–385
- Annualized loss expectation (ALE), 544
- Anomaly-based intrusion detection, 485
- Anonymity, 397, 614
- Anonymization, 618, 622–623
- Anonymous e-mail, 637–638
- Antipiracy feature, 653–654
- Antón, Annie, 645
- Appended viruses, 118
- Applets, hostile, 436, 499
- Application layer, 386, 391
- Application proxy gateways, 478–480
- Applications
code errors, 426
security. *See* Programs, security.
viruses, 124
- Architecture, networks, 442–443
- Arithmetic properties of cryptography, 725–730
- Arora, Ashish, 598
- ARPANET, 112, 325
- AS (authentication server), 213–214
- ASINTOER code, 59
- ASP (active server pages), 435
- Asperger syndrome, 401
- Assertions, 293
- Assessment
quality. *See* Evaluation.
risk. *See* Risk analysis.
- Asset identification, 526–527
- Association for Computing Machinery (ACM), code of ethics, 710, 712
- Associativity, 727
- Assurance. *See* Trusted systems, assurance.
- Assurance arguments, 184
- Asymmetric encryption. *See also* Public key encryption; RSA.
authentication, 62
characteristics of, 757–758
cryptanalysis of knapsack algorithm, 764–765
definition, 39
flow diagram, 40
general knapsacks, 759–760
hard knapsacks, 763–764
key distribution, 62
key management, 62
knapsack decryption algorithm, 764–765
knapsacks, and modular arithmetic, 761–763
knapsacks, as cryptographic algorithms, 761–763
Merkle–Hellman knapsacks, 758–761, 766–767
overview, 62
relatively prime values, 762
RSA (Rivest-Shamir-Adelman), 767–772
simple knapsacks, 760–761, 763
superincreasing knapsacks, 760–761, 763–764
- AT&T, 677
- Attachment viruses, 117–119
- Attackers. *See also* Crackers; Hackers.
amateurs, 21–22
career criminals, 22–23
motives, 399–404
network threat, 399–404
psychological profile, 401
terrorists, 23–24
- Attacks. *See also* Threats; Vulnerabilities.
attractive targets, 9
controls, 7
definition, 7
information leaks, 16
MOM (method, opportunity, motive), 8–9
reprocessing used data items, 18
sources, 588
types, 587
universities, as prime targets, 9
vulnerabilities, 6
- Attacks, methods
12-step password attacks, 226
brute force. *See* Brute force attack.
brute force password, 223
chosen plaintext, 66
ciphertext only, 65
cryptanalytic. *See* Cryptanalysis.
cyber, 101–102
database inference
combined results control, 348
concealing control, 347
controls for, 347–349
count attacks, 343–344
direct attack, 342–343
indirect attack, 343–350
limited response suppression, 347–348
linear system vulnerability, 346–347
mean attacks, 344
median attacks, 344–345
problem summary, 349–350
query analysis, 349
random data perturbation, 349
random sample control, 348–349
statistical inference attacks, 347
sum attacks, 343
suppression control, 347
tracker attacks, 345–346
denial of service. *See* DDoS; DoS.
encrypted password file, 227–228
exhaustive password, 223
full plaintext, 65–66
logic bombs, 16
man-in-the-middle, 149
partial plaintext, 65–66
password
12-step process, 226
brute force, 223
encrypted password file, 227–228
exhaustive, 223
indiscreet users, 228–229
plaintext password list, 226

- probability, 224
- salt extension, 228
- trial and error, 222
- weak passwords, 224–227
- probable plaintext, 66
- salami
 - definition, 19, 144
 - examples, 144–145
 - persistence of, 145
- timing, 150
- trapdoors, 16
- Trojan horses, 16
- viruses, 16
- Attractive targets, 9
- Attributes, 321, 620
- Audience for security policies, 547–548
- Audit trails, 618
- Auditability of databases, 326
- Audits
 - data overload, case study, 273
 - log reduction, 272–273
 - principles of trusted systems, 272
- Australian Computer Crime and Security Survey, 582
- Authentication
 - asymmetric encryption algorithms, 62
 - certificates, 87–89
 - Digital distributed, 460–461
 - distributed, 398
 - flaws, 103
 - mutual, 463
 - network vulnerabilities
 - avoidance, 416–417
 - eavesdropping, 416
 - guessing passwords, 415–416
 - man-in-the-middle attack, 420
 - masquerade, 418–419
 - nonexistent authentication, 417
 - phishing, 419
 - session hijacking, 419–420
 - spoofing, 418
 - trusted authentication, 418
 - well-known authentication, 417–418
 - wiretapping, 416
 - nonexistent, 417
 - privacy in computing
 - anonymized records, 622–623
 - attributes, 620
 - identity, 619, 621–622
 - individual, 619, 620
 - meaning of, 619–620
 - overview, 619
 - privacy principles and policies, 617
 - strong, networks, 459–464
 - symmetric encryption algorithms, 62
 - trusted, network vulnerability, 418
 - users. *See* User authentication.
- Authentication header (AH), 455
- Authentication server (AS), 213–214
- Authenticity, databases, 338
- Automatic exec by file type, 437
- Availability of data
 - data and services, 12
 - data mining, 370
 - databases, 328–329
 - definition, 10
 - denial of service. *See* DDoS; DoS.
- Avoidance, 416–417
- B1, TCSEC class, 297–298, 299
- B2, TCSEC class, 297–298, 299
- B3, TCSEC class, 297–298, 299
- Backdoors. *See* Trapdoors.
- Backing up data, 563–566
- Balanced scorecard, 573–574
- Base registers, 195–196
- Baseline, 244
- Bastion host, 478–480
- Beacon gif. *See* Web bugs.
- Beizer, Boris, 678
- Bell–La Padula security model, 254–256
- Beneficiaries of security policies, 548
- Benign viruses, 132–133
- Best practices, 34, 568
- BestBuy, 413
- Biba integrity security model, 256
- BIND (Berkeley Internet Name Domain), 431
- Binding of functionality, 304
- Biometrics, 219–220, 234–236. *See also* Face recognition authentication.
- “Black hole” failure, 325
- Black-box testing, 170
- Blaze, Matt, 677
- Block ciphers, 62–63. *See also* AES; DES.
- Bombs, software. *See* Logic bombs; Time bombs.
- Book ciphers, 52–54
- Boot sector viruses, 122
- Bootstrapping, 122
- Botnets, 437–438
- Bots, 437–438
- Boundaries, network, 381–382
- Boundary condition errors, 103
- Bounds disclosure, 338
- Bounds registers, 195–196
- Brain virus, 133–134
- Breakable encryption, 42–43
- Breaking encryption. *See also* Cryptanalysis.
 - chosen plaintext attacks, 66
 - ciphertext only attacks, 65
 - full plaintext attacks, 65–66
 - partial plaintext attacks, 65–66
 - probable plaintext attacks, 66
 - weaknesses, 66–67
- Britain. *See* United Kingdom.
- British evaluation criteria, 301–302
- Broadcast mode, 428–429
- Brute force attack, 223, 744–745
- Buffer overflow, 178, 425
- Bugs
 - software, 100
 - web, 105631, 139–141
- Bulletin boards, 407
- Business case
 - adjusting future earnings, 575–576
 - balanced scorecard, 573–574
 - cost estimates, 578
 - definition, 573
 - determining economic value, 574–578
 - discount rate, 576
 - false positives, 578
 - influences on investment strategy, 572
 - IRR (internal rate of return), 577
 - net present value, 574–577
 - opportunity cost, 576
 - overview, 572–574
 - ROI (return on investment), 577–578
 - web application, case study, 579
- Business continuity plan, 518–521
- Byte substitution, 750–751
- C1, TCSEC class, 297–298
- C2, TCSEC class, 297–298, 299
- Cables, network
 - coaxial, 382
 - eavesdropping, 409–410
 - Ethernet, 383
 - impedance, 410
 - inductance, 409
 - networking, 382–383
 - UTP (unshielded twisted pair), 382
 - wiretapping, 409–410

818 Index

- Caesar cipher, 44–46
- California Breach Act, 686
- CAN (campus area network), 395
- CAN SPAM Act, 685–686
- Capability, 210–213
- Capability Maturity Model (CMM), 181
- Capstone, 691
- Career computer criminals, 22–23
- CartManager International, 612
- CARVER (criticality, accessibility, recuperability, vulnerability, effect, and recognizability) method, 530
- Case studies
 - airport security, 370
 - al Qaeda computer, 24
 - analysis of Shakespeare's plays, 353
 - attacker profile, 401
 - "black hole" failure, 325
 - business case, 579
 - CartManager International, 612
 - computerized text analysis, 353
 - copyright, 655
 - data mining, 370
 - database integrity failure, 325
 - database precision, 341
 - deceptive practices, 612–613
 - difficulties of securing code, 140
 - Earl of Buckingham, 621
 - e-mail theft
 - Hollywood, 20
 - New Zealand Herald, 413
 - Wilshire Associates, Inc., 28
 - ethical issues
 - accuracy of information, 706–707
 - cracking, 707–710
 - DoS (denial of service), 701–702
 - fraud, 705–706
 - hacking, 707–710
 - ownership of programs, 702–704
 - privacy rights, 700–701
 - proprietary resources, 704
 - use of computer services, 698–699
 - FAIS (Foreign Affairs Information System), 312
 - hacker sting operation, 403
 - Hollywood e-mail theft, 20
 - human fallibility, 67
 - identity theft, 621
 - JetBlue airlines, 612–613
 - Kennedy, Edward, 370
 - Key Online Banking, 452
 - Lewis, John, 370
 - Lloyd's Bank, 452
 - mafia boss, 45
 - microcontrollers in automobiles, 3
 - MP3.com, 655
 - Napster, 655
 - online banking, 452
 - PKI (public key infrastructure), 452
 - privacy, 615
 - privacy, government intrusion
 - Icelandic DNA database, 351
 - U.K. RIPA (Regulation of Investigatory Powers Act), 287
 - screening for terrorists, 615
 - security, as add-on, 312
 - silken codes, 41
 - Stopford, Charlie, 621
 - Torch Concepts, 612–613
 - tracking Russian nuclear weapons, 140
 - U.S. Government
 - audit data overload, 273
 - security report card, 29
 - U.S. Census Bureau, 341
 - V.A. (Veterans Administration), 14
 - Wilshire Associates, e-mail theft, 28
 - wireless vulnerabilities, 413
 - WW II
 - ASINTOER code, 59
 - Enigma code machine, 67
 - Japanese codes, 42
 - poem codes, 48
 - silken codes, 41
 - Soviet Union codes, 59
- Catastrophe, recovering from. *See* Backing up data; Physical security; Recovery from backup.
- CCB (configuration and change control board), 176
- CDs (compact disks)
 - copy protection, 145–147, 654–655
 - fair use, 654–655
 - XCP (extended copy protection) rootkit, 145–147
- Census Bureau, 341
- Centralization, 326–327
- CERT (Computer Emergency Response Team), 432
- Certificate authority, 8, 451
- Certificates
 - authentication, 87–89
 - encryption, 84–91
 - encryption, uses for, 84–91
 - trust
 - through common respected individual, 85–87
 - without a single hierarchy, 89–91
 - trust threshold, 85
- CGI (Common Gateway Interface), 434–435
- Chain of custody, 680
- Chaining, 80
- Challenge, attack motive, 400
- Challenge-response systems, 231–232, 233–234, 460
- Change logs, 326
- Change management. *See* Configuration.
- Channels, covert. *See* Covert channels.
- Chats, 407
- Checksums, cryptographic
 - definition, 79–80
 - multilevel databases, 358–359
 - networks, 458–459
- Children's Online Privacy Protection Act (COPPA), 610
- Chinese Wall security policy, 251–252
- Chosen ciphertext attack, 66
- Chosen plaintext attacks, 66
- Ciphers
 - block, 62–63. *See also* AES; DES.
 - book, 52–54
 - Caesar, 44–46
 - complexity, 47–48
 - cryptanalysis, 48–49
 - cryptographer's dilemma, 49
 - keyless, 40
 - keys, 47
 - one-time pads, 50–54
 - permutations, 46–47
 - product, 58, 733
 - random number sequences, 50
 - RC2, 754–755
 - RC4, 755–756
 - RC5, 756
 - stream, 62–63
 - substitution
 - book ciphers, 52–54
 - Caesar cipher, 44–46
 - complexity, 47–48
 - cryptanalysis, 48–49
 - cryptographer's dilemma, 49
 - keys, 47
 - one-time pads, 50–54
 - permutations, 46–47
 - random number sequences, 50
 - Vernam cipher, 50–52

- Vignère tableau, 50, 53
 - Vernam, 50–52
 - Vernam cipher, 50–52
 - Vignère tableau, 50, 53
 - Ciphertext, 26, 39
 - Ciphertext only attacks, 65
 - Civil law, 667
 - Claims language, 301
 - Clark-Wilson commercial security policy, 250
 - Classical probability, 534
 - Classification, 248
 - Clear gif. *See* Web bugs.
 - Clear-box testing, 170–171
 - Cleartext, 26. *See also* Plaintext.
 - CLEFs (Commercial Licensed Evaluation Facilities), 302
 - Clients, network, 378–379
 - Clipper, 691. *See also* Keys (encryption), escrow.
 - Clique problem, 720–722
 - Closed *versus* open organizations, 595
 - Clustering, key, 746
 - CMM (Capability Maturity Model), 181
 - Coaxial cable, 382
 - Code (program)
 - compatibility, 198–199
 - debugging, 142. *See also* Testing.
 - error correcting, 458
 - errors, 426
 - inspection, 166
 - malicious. *See* Malicious code.
 - mobile, 433
 - review, 168
 - security. *See* Programs, security.
 - signing, 457, 501
 - walk-through, 166
 - Code Red worm, 137–139, 675–676
 - Codes (encoding systems). *See also* Cryptography; Encryption.
 - hash, 458
 - Huffman, 458
 - Japanese, 42
 - poem, 48
 - silken, 41
 - Soviet Union, 59
 - Codes (of conduct)
 - of best practice. *See* Best practices.
 - of ethics. *See* Ethics.
 - Cohesion, 163
 - Cold site backups, 565
 - Columnar transpositions, 55–58
 - Combined Federal Criteria*, 304–307
 - Combined results control, 348
 - Command insertion, 142
 - Command structure, 259
 - Commercial Licensed Evaluation Facilities (CLEFs), 302
 - Commercial security policies, 248–250
 - Commit flag, 330
 - Commit phase, 331–332, 334
 - Committing database updates, 330
 - Common Criteria, 307–308
 - Common Gateway Interface (CGI), 434–435
 - Common Intrusion Detection Framework, 484
 - Communication mode, networks, 382
 - Community string, 418
 - Commutative filters, 361–363
 - Commutative ring, 727–728
 - Comparability, evaluating, 303
 - Comparable data, data mining, 369
 - Compartments, 246
 - Compatibility of
 - code, 198–199
 - evaluation, 309
 - Complements, DES, 745
 - Complete backups, 564
 - Complete mediation, 265–266, 270. *See also* Incomplete mediation.
 - Complex attacks, 438
 - Component testing. *See* Unit testing.
 - Components, software. *See* Modularity.
 - Composites, 725
 - Computational complexity, cryptography, 718
 - Computer crime
 - definition, 21
 - legal issues
 - California Breach Act, 686
 - CAN SPAM Act, 685–686
 - computer terminology and the law, 681
 - confidentiality threats, 680
 - Council of Europe Agreement on Cybercrime, 687
 - cryptography, 688, 688–692
 - defining, 681–682
 - E.U. Data Protection Act, 687
 - GLBA (Graham-Leach-Bliley Act), 684
 - HIPAA (Health Insurance Portability and Accountability Act), 684–685
 - integrity threats, 680
 - international dimensions, 686–688
 - overview, 679
 - prosecuting, 682–683
 - restricted content, 687–688
 - rules of evidence, 680
 - rules of property, 679–680
 - scope limitations, 688–689
 - statutes, examples, 683–686
 - U.S. Computer Fraud and Abuse Act, 683
 - U.S. Economic Espionage Act, 683
 - U.S. Electronic Communications Privacy Act, 684
 - U.S. Electronic Funds Transfer Act, 683
 - U.S. Freedom of Information Act, 684
 - U.S. Privacy Act, 684
 - USA Patriot Act, 685
 - value of data, 681
 - reporting, 21
 - statistics, 21
- Computer criminals. *See* Attackers; Crackers; Hackers.
- Computer Emergency Response Team (CERT), 432
- Computer Ethics Institute, 710, 713
- Computer Fraud and Abuse Act, 683
- Computer objects. *See* Objects, digital.
- Computer screen emanations, 562–563
- Computer terminology and the law, 681
- Computerized text analysis, 353
- Computing systems
 - components of, 6
 - definition, 4
 - intrusion characteristics, 4–5
- Concealing control, 347
- Concurrency, 333
- Conditional compilation, 175
- Conditions, security models, 259
- Confidence level, 244
- Confidentiality. *See also* Privacy.
 - data, 17, 19
 - databases, 329
 - definition, 10
 - e-mail, 492–493
 - multilevel databases, 355
 - overview, 11
 - threats, 680

820 Index

- Configuration
 - audit, 175–176
 - databases, 327
 - identification, 175
 - management, 174–176
- Configuration and change control
 - board (CCB), 176
- Confinement, 165
- Confusion, 63–64, 730
- Connection flooding, 427–428
- Connectivity. *See* Networks.
- Consequence-based ethics, 696–697
- Consistency, database, 332, 333
- Constrained data items, 250
- Constraints, 512–514
- Consumer products, privacy, 639–640
- Content integrity, 457–459
- Contests, web privacy, 629
- Context switch, 195–196
- Contingency planning. *See* Physical security; Risk analysis; Security plan.
- Continuity plan, 518–521
- Contract law, 668–669
- Control, network, 381–382
- Controlled disclosure, 604
- Controls. *See also* Defense methods.
 - data protection. *See* Encryption.
 - database inference attacks, 347–349
 - definition, 7
 - effectiveness, 28–30
 - export of cryptography, 690
 - hardware, 27
 - layered defense, 29
 - mapping to vulnerabilities, 537
 - for networks. *See* Networks, controls.
 - overlapping, 29
 - overview, 24–25
 - physical, 27
 - policies and procedures, 27
 - security plan, 512–514
 - selecting
 - criteria for, 537–542
 - mapping controls to vulnerabilities, 537, 539
 - positive and negative effects, 538–541
 - ratings, 541–542
 - VAM (Vulnerability Assessment and Mitigation), 537–542
 - software, 26–27
 - software development
 - acceptance testing, 170–171
 - active fault detection, 172–173
 - black-box testing, 170
 - CCB (configuration and change control board), 176
 - clear-box testing, 170–171
 - CMM (Capability Maturity Model), 181
 - components. *See* Modularity.
 - conditional compilation, 175
 - configuration audit, 175–176
 - configuration identification, 175
 - configuration management, 174–176
 - confinement, 165
 - coupling, 163
 - delta files, 175
 - design principles, 172–173
 - developer characteristics, 160–161
 - development standards, 178, 180
 - difference files, 175
 - encapsulation, 161–164
 - FMEA (failure modes and effects analysis), 168–169
 - formal methods, 179
 - FTA (fault tree analysis), 168–169
 - genetic diversity, 165
 - hazard analysis, 168–169
 - HAZOP (hazard and operability studies), 168–169
 - independent testing, 172
 - information hiding, 161–164
 - installation testing, 170
 - integration testing, 170
 - lessons from mistakes, 176
 - modularity, 161–164
 - mutual suspicion, 164
 - nature of software development, 160–161
 - overview, 26–27
 - passive fault detection, 172–173
 - peer reviews, 165–168
 - penetration testing, 172, 177
 - performance testing, 170
 - problem response, 173
 - process standards, 180–181
 - program practice conclusions, 178
 - program verification, 177–178
 - proof of correctness, 177–178
 - redundancy, 173
 - regression testing, 170
 - risk prediction, 173–174
 - security audits, 180
 - security requirements, 171
 - static analysis, 174
 - status accounting, 176
 - testing, 169–172
 - tiger team testing. *See* Penetration testing.
 - unit testing, 170
 - usage of cryptography, 688–690
- Convention 108, 613
- Cookies
 - network threat, 434
 - per-session, 434
 - persistent, 434
 - threats posed by, 434
 - user authentication, 236
 - viruses, 140
 - web privacy, 629–631
- COPPA (Children’s Online Privacy Protection Act), 610
- Copy protection, 145–147, 654–655
- Copyright
 - case study, 655
 - for computer software, 652–653
 - definition, 650
 - for digital objects, 653–655
 - DMCA (Digital Millennium Copyright Act), 649–650, 653
 - fair use, 651
 - first sale, 651
 - inappropriate references to, 656
 - infringement, 652
 - intellectual property, 650–651
 - legal issues, 649–655, 660
 - Napster, 655
 - originality of work, 651
 - ownership, 671
 - piracy, 651
 - public domain, 650
 - registering, 652
- Core. *See* Kernel.
- Correcting mistakes, data mining, 369
- Correction codes, database reliability, 332
- Correctness of data, data mining, 368–369
- Correlation of data, 624–625
- Cost of security. *See* Economics of cybersecurity.
- Cost/benefit risk analysis, 544
- Council of Europe, 613
- Council of Europe Agreement on Cybercrime, 687
- Count attacks, 343–344
- Coupling, 163
- Covert channels
 - creating, 152

- definition, 150
- file lock channel, 152
- identifying, 156–158
- information flow analysis, 158
- overview, 151–152
- shared resource matrix, 157–158
- signaling through images, 159–160
- steganography, 159–160
- storage channels, 152–155
- threat presented by, 158–160
- timing channels, 155–156
- Crackers, 22. *See also* Attackers; Hackers.
- Cracking, ethical issues, 707–710
- Credibility, 592
- Credit card payments, web privacy, 627
- Crime. *See* Computer crime.
- Criminal law, 667
- Criteria development, 309–311
- Criticality, accessibility, recuperability, vulnerability, effect, and recognizability (CARVER) method, 530
- Cryptanalysis
 - AES (Advanced Encryption System), 753–754
 - breaking encryption
 - chosen plaintext attacks, 66
 - ciphertext only attacks, 65
 - full plaintext attacks, 65–66
 - partial plaintext attacks, 65–66
 - probable plaintext attacks, 66
 - weaknesses, 66–67
 - Caesar cipher, 45–46
 - definition, 41
 - differential, 71–72, 747–748
 - digram analysis, 57–58
 - knapsack algorithm, 764–765
 - overview, 41–42
 - RSA (Rivest-Shamir-Adelman) encryption, 772
 - substitution ciphers, 48–49
- Cryptanalysts, 40
- Cryptographers, 40
- Cryptographer's dilemma, 49
- Cryptographic challenges
 - RSA (Rivest-Shamir-Adelman) encryption, 772–773
 - symmetric encryption, 756–757
- Cryptographic checksum
 - definition, 79–80
 - multilevel databases, 358–359
 - networks, 458–459
- Cryptographic hash functions, 79–80
- Cryptographic separation, 192, 279–280
- Cryptography. *See also* Encryption.
 - asymmetric encryption
 - characteristics of, 757–758
 - cryptanalysis of knapsack algorithm, 764–765
 - general knapsacks, 759–760
 - hard knapsacks, 763–764
 - knapsack decryption algorithm, 764–765
 - knapsacks, and modular arithmetic, 761–763
 - knapsacks, as cryptographic algorithms, 761–763
 - Merkle–Hellman knapsacks, 758–761, 766–767
 - relatively prime values, 762
 - RSA (Rivest-Shamir-Adelman), 767–772
 - simple knapsacks, 760–761, 763
 - superincreasing knapsacks, 760–761, 763–764
 - Capstone, 691
 - character representation, 43–44
 - ciphertext, 39
 - Clipper, 691
 - computer crime, 688, 688–692
 - current policy, 691–692
 - decryption, 38
 - definition, 40
 - DSA (Digital Signature Algorithm), 773–774
 - El Gamal algorithm, 773
 - encrypted text, 39
 - encryption, 38
 - export controls, 690
 - Fortezza, 691
 - and free speech, 690–691
 - interceptors, 38
 - intruders, 38
 - key escrow, 691
 - legal issues, 688–692
 - mathematics of
 - arithmetic properties, 725–730
 - commutative ring, 727–728
 - composites, 725
 - computational complexity, 718
 - division, 725
 - Euclidean algebra, 726
 - Fermat's theorem, 729–730
 - Galois fields, 727–728
 - greatest common divisor, 726
 - hierarchies of complexity, 723
 - identity (mathematical), 725
 - inherently hard problems, 724–725
 - instances, 722
 - inverses, computing, 728–730
 - inverses, definition, 725
 - knapsack problem, 719–720
 - modular arithmetic, 726–728
 - nondeterminism, 721
 - nondeterministic Turing machines, 721
 - NP class, 721
 - NP-complete problems, 719–724
 - oracles, 721
 - overview, 718
 - P class, 721
 - prime numbers, 725
 - problems, definition, 722–723
 - satisfiability, 719
 - modular arithmetic, 43
 - original text, 39
 - perfect cipher. *See* One-time pads.
 - permutations
 - columnar transpositions, 55–58
 - combined approaches, 58
 - definition, 55
 - digram analysis, 57–58
 - digrams, 56–57
 - encipherment/decipherment complexity, 56
 - patterns, 56–57
 - product ciphers, 58
 - substitution ciphers, 46–47
 - trigrams, 56–57
 - with photons, 775–776
 - plaintext, 39
 - quantum
 - cryptography with photons, 775–776
 - implementation, 776–778
 - overview, 774
 - photon reception, 775
 - polarizing filters, 774–775
 - quantum physics, 774–775
 - recipients, 38
 - senders, 38
 - substitution ciphers
 - book ciphers, 52–54
 - Caesar cipher, 44–46
 - complexity, 47–48
 - cryptanalysis, 48–49
 - cryptographer's dilemma, 49
 - keys, 47
 - one-time pads, 50–54
 - permutations, 46–47
 - random number sequences, 50

822 Index

- Cryptography (*continued*)
 substitution ciphers (*continued*)
 Vernam cipher, 50–52
 Vignère tableau, 50, 53
 substitutions, 43
 symmetric encryption. *See also*
 DES.
 AES (Advanced Encryption System), 748–754
 confusion, 730
 cryptographic challenges, 756–757
 diffusion, 730
 permutation, 730
 problems with, 730–732
 RC2 cipher, 754–755
 RC4 cipher, 755–756
 RC5 cipher, 756
 substitution, 730
 transmission medium, 38
 transpositions. *See* Permutations.
 usage controls, 688–690
 Cryptology, 40
 Cryptosystems, 38
 CSII/FBI Computer Crime and Security Survey, 582
 Culp, Scott, 675–676
 Culture of organizations. *See* Organizational culture.
 Cyber attacks, 101–102
 CyberCop Scanner, 405
 Cyberterrorism, 403
 Cycle, DES
 details, 736
 example, 735
 permutation, 734
 substitution, 734
- D, TCSEC class, 297–298
 DAC (discretionary access control), 269–270
 Daemen, John, 72
 Danseglio, Mike, 22
 Data. *See also* Information.
 access risks, 617
 anonymization, 618
 availability, databases, 337
 form checks, database, 334
 justifying cost of security
 accuracy, 581
 consistency, 581
 reliability, 581
 representative, 586
 left in place, 618
 minimization, 617–618
- perturbation
 data mining, 624–626
 database attacks, 349
 database inference, 349
 privacy, 624–626
 random, 349
 secrecy. *See* Confidentiality; Privacy.
 semantics, data mining, 369
 sensitivity, 551
 stored, protecting, 609–610
 Data Encryption Algorithm (DEA), 69. *See also* DES.
 Data Encryption Algorithm-1 (DEA-1), 69. *See also* DES.
 Data mining. *See also* Databases.
 case study, 370
 comparable data, 369
 correcting mistakes, 369
 data availability, 370
 data correctness, 368–369
 data semantics, 369
 definition, 367
 eliminating false matches, 370
 integrity, 368–369
 overview, 367
 privacy
 aggregation of data, 625–626
 correlation of data, 624–625
 data perturbation, 624–626
 government, 624
 preserving privacy, 624–626
 sensitivity, 368
 Data Protection Act, 687
 Database administrators, 319, 515
 Database management system (DBMS), 319
 Databases. *See also* Data mining.
 advantages of, 323
 aggregation, 350–351. *See also* Inference.
 attributes, 321
 components of, 319–323
 decentralization, 373
 definition, 319
 deleting fields and records. *See* Queries.
 editing fields and records. *See* Queries.
 elements, 319
 fields, 319
 front end. *See* DBMS.
 inference. *See also* Aggregation.
 combined results control, 348
 concealing control, 347
 controls for, 347–349
 count attacks, 343–344
 definition, 341
 direct attack, 342–343
 indirect attack, 343–350
 limited response suppression, 347–348
 linear system vulnerability, 346–347
 mean attacks, 344
 median attacks, 344–345
 problem summary, 349–350
 query analysis, 349
 random data perturbation, 349
 random sample control, 348–349
 statistical inference attacks, 347
 sum attacks, 343
 suppression control, 347
 tracker attacks, 345–346
 logical structure, 320
 manipulating. *See* Queries.
 protection laws, 666
 queries, 321–323
 records
 definition, 319
 manipulating. *See* Queries.
 projecting, 321–323
 selecting, 321–323
 relations, 321
 reliability
 commit flag, 330
 committing updates, 330
 concurrency, 333
 consistency, 332, 333
 correction codes, 332
 data form checks, 334
 definition, 329
 error detection, 332
 filters, 334
 intent phase, 330
 monitors, 334–335
 operating system protection features, 329–330
 patterns, 334
 recovery from backup, 332
 redundancy, 332
 shadow fields, 332
 shadow values, 331–332
 state constraints, 334–335
 transition constraints, 335
 two-phase update, 330–332
 retrieving fields and records. *See* Queries.
 schema, 320
 security requirements

- access control, 325, 327–328
- auditability, 326
- availability, 328–329
- change logs, 326
- confidentiality, 329
- configuration management, 327
- field checks, 325
- inference, 328
- integrity, 324–326, 329
- pass-through problem, 326
- release proliferation, 327
- user authentication, 328
- version proliferation, 327
- sensitive data
 - access acceptability, 337–338
 - access decisions, 337–338
 - authenticity, 338
 - bounds disclosure, 338
 - characteristics of, 336–337
 - data availability, 337
 - definition, 335
 - disclosures, types of, 338–339
 - exact data disclosure, 338
 - existence disclosure, 339
 - negative result disclosure, 339
 - overview, 335–337
 - probable value disclosure, 339
 - security *versus* precision, 339–341
 - subschema, 320
- Databases, multilevel
 - confidentiality, 355
 - differentiated security, 352–353
 - duplicate records, 355
 - granularity, 353
 - integrity, 354
 - polyinstantiation, 355
 - redundancy, 355
 - security designs
 - commutative filters, 361–363
 - distributed databases, 363
 - federated databases, 363
 - filtering, 365
 - guards, 360–361
 - integrity locks, 359–360
 - practical issues, 366
 - trusted front-end, 360–361
 - views, 363–366
 - windows, 363–366
 - security issues, 354–355
 - security proposals
 - cryptographic checksum, 358–359
 - encryption, 356–357
 - integrity lock, 357–359
 - partitioning, 356
 - sensitivity lock, 359
 - separation, 356–359
 - “spray paint” lock, 357–359
 - Summer Study on Database Security, 357
- Datagrams, 391
- DBMS (database management system), 319
- DDoS (distributed denial of service). *See also* Availability; DoS.
 - diagram of, 433
 - network threat, 431–433
 - TFN (Tribal Flood Network), 401, 432
 - TFN2K, 401, 432
- de Vere, Edward, 353
- DEA (Data Encryption Algorithm), 69. *See also* DES.
- DEA-1 (Data Encryption Algorithm-1), 69. *See also* DES.
- Debugging code, 142. *See also* Testing code.
- Decentralization, databases, 373
- Deceptive practices, 612–613
- Deciphering data. *See* Decryption.
- Decision making, 590–592
- Decoding data. *See* Decryption.
- Decryption
 - algorithm, 764–765
 - definition, 38
 - DES (Data Encryption Standard), 742
 - knapsacks, 764–765
- Defacing web sites, 424–425
- Defense methods. *See also* Controls.
 - privacy principles and policies, 617–618
 - viruses, 129–131
- Defining computer crime, 681–682
- Degaussing magnetic data, 562. *See also* Magnetic remanence.
- Deleting
 - database fields and records. *See* Queries.
 - PDF text, 271
 - Word text, 271
- Deloitte and Touche Tohmatsu Global Security Survey, 582–583
- Delphi approach, 533–534
- Delta (configuration control method), 175
- Denial of service (DoS). *See* DoS (denial of service).
- Deontology, 697
- Department of Energy (DOE) policy, 551–552
- Department of Trade and Industry (DTI), 18
- Depletion of information, 663
- DES (Data Encryption Standard). *See also* AES.
 - versus* AES, 73–75
 - algorithm design, 742–743
 - background, 68–69
 - brute force attack, 744–745
 - complements, 745
 - cycle, example, 735
 - cycle details, 736
 - decryption, 742
 - design weaknesses, 746
 - differential cryptanalysis, 71–72, 747–748
 - double DES, 70–71
 - encryption algorithm, 733–736
 - expansion permutations, 733, 736–741
 - final permutation, 739, 741
 - history, 68–69
 - initial permutation, 739, 741
 - inverse initial permutation, 739, 741
 - key clustering, 746
 - key length, 743–745
 - key transformation, 736
 - Lucifer algorithm, 68–69
 - number of iterations, 743
 - overview, 69–70, 732–733
 - parallel attack, 744–745
 - P-boxes, 739, 741
 - permutation cycle, 734
 - permutation types, 736
 - permuted choices, 733
 - product cipher, 733
 - S-boxes, 739, 740
 - security of, 71–72, 742–745, 748
 - semiweak keys, 745–746
 - substitution cycle, 734
 - triple DES, 71
 - weak keys, 745
 - weaknesses, 745–748
- Destination unreachable protocol, 438
- Determining economic value. *See* Economics of cybersecurity.
- DHCP (Dynamic Host Configuration Protocol), 412
- Diamond v. Bradley*, 658
- Diamond v. Diehr*, 658
- Difference files, 175
- Differential cryptanalysis, 71–72, 747–748

824 Index

- Differentiated security, multilevel
 - databases, 352–353
- Diffie-Hellman key exchange, 81–82
- Diffusion, 63–64, 730
- Digital distributed authentication, 460–461
- Digital Equipment Corporation, 460–461
- Digital Millennium Copyright Act (DMCA), 649–650, 653
- Digital network communication, 382
- Digital objects. *See* Objects, digital.
- Digital Signature Algorithm (DSA), 773–774
- Digital Signature Standard (DSS), 773
- Digital signatures, 82–84
- Digram analysis, 57–58
- Digrams, 56–57
- Direct attack, 342–343
- Directive 95/46/EC, 613
- Directories, 205–208
- “Dirty” power, 558
- Disaster, natural. *See* Natural disasters.
- Disaster recovery. *See* Backing up
 - data; Physical security; Recovery from backup.
- Disclosure
 - bounds, 338
 - controlled, 604
 - exact data, 338
 - existence, 339
 - negative result, 339
 - privacy issues, 606
 - probable value, 339
 - of software problems, 675–676
 - types of, 338–339
- Discount rate, 576
- Discretionary access control (DAC), 269–270
- Distributed authentication, 398
- Distributed databases, 363
- Distributed denial of service (DDoS). *See* DDoS.
- Division, cryptography, 725
- DMCA (Digital Millennium Copyright Act), 649–650, 653
- DNS attacks, 431
- DNS cache poisoning, 431
- Document viruses, 119–120
- Documentation
 - availability, network threat, 407
 - protection, legal issues, 662
- DOE (Department of Energy) policy, 551–552
- Domain errors, 103
- Domain names, 393, 662
- Domain switching, 276
- Domains, 211
- Dominance, 248
- DoS (denial of service). *See also* Availability; DDoS.
 - broadcast mode, 428–429
 - connection flooding, 427–428
 - DNS attacks, 431
 - DNS cache poisoning, 431
 - echo chargen, 428
 - estimated activity, 432
 - ethical issues, 701–702
 - network threat, 427–431
 - ping of death, 428
 - smurf attack, 428–429
 - SYN flood, 429
 - teardrop attacks, 430
 - traffic redirection, 430
 - transmission failure, 427
- Dot-dot-slash directory travel, 425–426
- Double DES, 70–71
- DoubleClick, 630–631
- Drive-by installation, 634
- Drops, electrical, 558
- DSA (Digital Signature Algorithm), 773–774
- DSS (Digital Signature Standard), 773
- DTI (Department of Trade and Industry), 18
- Dumpster diving, 406–407
- Dunham, Ken, 22
- Duplicate database records, 355
- Durability, 550
- Dynamic Host Configuration Protocol (DHCP), 412
- Earl of Buckingham, 621
- Ease of use, 266
- Easiest penetration principle, 5
- Eavesdropping, 408–414, 416
- Echo chargen attack, 428
- Echo protocol, 438
- Economic Espionage Act, 683
- Economics of cybersecurity
 - business case
 - adjusting future earnings, 575–576
 - balanced scorecard, 573–574
 - cost estimates, 578
 - definition, 573
 - determining economic value, 574–578
 - discount rate, 576
 - false positives, 578
 - influences on investment strategy, 572
 - IRR (internal rate of return), 577
 - net present value, 574–577
 - opportunity cost, 576
 - overview, 572–574
 - ROI (return on investment), 577–578
 - web application, case study, 579
- current and future
 - externalities, 599
 - free rides, 598
 - integrity, 598
 - policies, 597
 - regulation, 598–599
- modeling
 - credibility, 592
 - decision making, 590–592
 - framing the issue, 590–591
 - group behavior, 591–592
 - overview, 589
 - role of organizational culture, 592–597
 - transferring models, 589–590
 - trust as economic issue, 592
- organizational culture
 - cultural practices, 593–594
 - cultural values, 594
 - dimensions of, 595
 - employee *versus* job, 594
 - heroes, 593
 - loose *versus* tight control, 595
 - normative *versus* pragmatic, 595
 - open *versus* closed, 595
 - parochial *versus* professional, 595
 - process *versus* results, 594
 - rituals, 593
 - role of organizational culture, 592–597
 - security choices, examples, 596
 - symbols, 592
- quantifying value
 - accurate data, 581
 - attack sources, 588
 - attack types, 587
 - comparability of categories, 587
 - consistent data, 581
 - cost of U.K. security incidents, 586
 - economic impact, 580, 586, 588
 - ISBS (Information Security Breeches Survey), 581, 585–586

- justification data, 580–581
- overview, 578–580
- reliable data, 581
- representative data, 586
- respondent types, 587
- security practices, 581, 585–586
- timelines, 581
- security surveys
 - Australian Computer Crime and Security, 582
 - CSI/FBI Computer Crime and Security, 582
 - Deloitte and Touche Tohmatsu Global Security, 582–583
 - Ernst and Young Global Information Security, 583–584
 - IC3 (Internet Crime Complaint Center), 584
 - Imation Data Protection, 584–585
 - sources for, 585
 - trust, as economic issue, 593
- Economics of security policies, 551
- Economy of mechanism, 265
- EEye Digital Security, 675–676
- Effectiveness
 - of controls, 28–30
 - evaluating, 303
- Effectiveness principle, 28
- Egoism, 696–697
- e-Government Act of 2000, 611
- 802.11 (wireless) standards, 383, 467
- El Gamal algorithm, 773
- Electrical power, 558–559
- Electronic commerce, laws, 666–667
- Electronic Communications Privacy Act, 684
- Electronic Funds Transfer Act, 683
- Electronic publishing, laws, 666
- Electronic voting, 641–642
- Elements, databases, 319
- E-mail
 - attachment viruses, 117–118
 - government security policy example, 553
 - network encryption, 457
 - over networks. *See* Networks, secure e-mail.
 - privacy
 - access control, 636
 - anonymous, 637–638
 - interception, 636
 - mixmaster remailers, 637–638
 - monitoring, 637
 - overview, 635
 - remailers, 637–638
 - simple remailers, 637
 - spamming, 638
 - spoofing, 638
 - transmitting, 636
 - theft case studies
 - Hollywood, 20
 - New Zealand Herald, 413
 - Wilshire Associates, Inc., 28
- Emanations from computer screens, 562–563
- Emerging technologies
 - consumer products, 639–640
 - electronic voting, 641–642
 - overview, 638–639
 - privacy issues, 640–641
 - RFID (radio frequency identification), 640
 - security issues, 640–641
 - Skype, 642
 - VoIP (Voice over IP), 642
- Emphatic assertion, 311
- Employee contracts, 672
- Employee rights. *See* Rights of employees and employers.
- Employee *versus* job, 594
- Employer rights. *See* Rights of employees and employers.
- Encapsulated security payload (ESP), 455
- Encapsulation, 161–164
- Enciphered text, 26
- Enciphering data. *See* Cryptography; Encryption.
- Encipherment/decipherment complexity, 56
- Encoding data. *See* Cryptography; Encryption.
- Encrypted password file attacks, 227–228
- Encrypted tunnels, 449–450
- Encryption. *See also* Asymmetric encryption; Cryptography; Symmetric encryption.
 - algorithms. *See also* AES; DES; RSA.
 - block ciphers, 62–63
 - confusion, 63–64
 - definition, 39
 - diffusion, 63–64
 - secure, characteristics of, 60–62
 - stream ciphers, 62–63
 - trustworthy, properties of, 61–62
 - breakable, 42–43
 - breaking. *See* Cryptanalysis.
 - ciphertext, 26
 - cleartext, 26
 - cryptosystems, 38
 - definition, 26, 38
 - e-mail, 493–494
 - enciphered text, 26
 - factoring large numbers, 78, 325–330
 - key management, 62
 - keyless ciphers, 40
 - keys, 39
 - link, 445–446
 - multilevel databases, 356–357
 - networks
 - AH (authentication header), 455
 - certificate authorities, 451
 - comparison of methods, 447–449
 - e-mail, 457
 - encrypted tunnels, 449–450
 - end-to-end, 446–447
 - ESP (encapsulated security payload), 455
 - firewalls, 449–450
 - IKE (ISAKMP key exchange), 455–456
 - ISAKMP (Internet Security Association Key Management Protocol), 455
 - issues, 453
 - link, 445–446
 - overview, 444–445
 - PKI (public key infrastructure), 450–453
 - security associations, 454–455
 - signed code, 456–457
 - SPI (security parameter index), 455
 - SSH (secure shell), 453
 - SSL (Secure Sockets Layer), 453–454
 - TLS (transport layer security), 453–454
 - tunnels, 449–450
 - VPNs (virtual private networks), 449–450
 - private key, 39–40. *See also* AES; DES; Symmetric encryption.
 - protocols, 26
 - public key. *See also* Asymmetric encryption; RSA.
 - characteristics, 77
 - definition, 39
 - flow diagram, 40
 - key proliferation, 77
 - purpose of, 76

826 Index

- Encryption (*continued*)
 text, 39
 uses for
 certificates, 84–91
 chaining, 80
 checksums, 79–80
 cryptographic checksum, 79–80
 cryptographic hash functions, 79–80
 Diffie-Hellman key exchange protocol, 81–82
 digital signatures, 82–84
 key exchange, 80–82
 End-to-end encryption, 446–447
 Enforced sharing, 267
 England. *See* United Kingdom.
 Enigma code machine, 67
 Equivalent programs, 128
 Erasing deleted files, 207
 Ernst and Young Global Information Security Survey, 583–584
 Error checking, trapdoors, 142–143
 Error correcting codes, 458
 Error detection, 332, 458
 Errors. *See also* Faults; Flaws.
 buffer overflow, 178, 425
 definition, 100
 incomplete mediation. *See* Incomplete mediation.
 privilege escalation, 147–148
 time-of-check to time-of-use flaws, 288
 Escape-character attack, 434–435
 ESP (encapsulated security payload), 455
 Espionage, 402, 683
 Estimating security value. *See* Economics of cybersecurity.
 Ethernet cable, 383
 Ethical codes, 710–713
 Ethical hacking. *See* Penetration testing.
 Ethical issues. *See also* Legal issues.
 a case for, 696
 case studies
 accuracy of information, 706–707
 cracking, 707–710
 DoS (denial of service), 701–702
 fraud, 705–706
 hacking, 707–710
 ownership of programs, 702–704
 privacy rights, 700–701
 proprietary resources, 704
 use of computer services, 698–699
 overview, 647–649
 Ethical pluralism, 695
 Ethical principles
 consequence-based, 696–697
 deontology, 697
 duties of people, 697–698
 egoism, 696–697
 examples of, 696–698
 intrinsic good, 697–698
 rule-based, 697–698
 rule-deontology, 697–698
 teleological theory, 696–697
 utilitarianism, 697
 Ethical reasoning, 695–698
 Ethical systems, 693
 Ethics
 versus law, 692–694
 and religion, 694
 studying, 693–695
 universality, 694–695
 E.U. Data Protection Act, 687
 Euclidean algebra, 726
 Euler totient function, 769–771
 European Privacy Directive, 613
 Evaluating security value. *See* Economics of cybersecurity.
 Evaluation
 action phrases, 301
 British criteria, 301–302
 claims language, 301
 CLEFs (Commercial Licensed Evaluation Facilities), 302
 Combined Federal Criteria, 304–307
 Common Criteria, 307–308
 comparability, 303
 criteria development, 309–311
 effectiveness, 303
 emphatic assertion, 311
 Europe, 300–303
 German Green Book, 300–301
 ITSEC (Information Technology Security Evaluation Criteria), 300–303, 303–304
 marketability, 303
 overview, 296–297
 process description, 309
 protection profiles, 305
 security, as add-on, 312
 security targets, 306
 summary of criteria, 308–311
 target phrases, 301
 TCSEC (Trusted Computer System Evaluation Criteria), 297–300, 304
 TOE (target of evaluation), 303
 transferability, 303
 United States, 297–300, 304–307
 Even parity, 458
 Evidence
 destroying, 523
 gathering, 523
 physical, 682
 preserving, 523
 rules of, 680
 Exact data disclosure, 338
 Examples of problems. *See* Case studies.
 Execution domain switching, 276
 Executives, 189–190
 Exhaustive password attacks, 223
 Existence disclosure, 339
 Expansion permutations, 733, 736–741
 Exploitation examples, 289–290
 Export controls in cryptography, 690
 Exposing messages, 421–422
 Extended copy protection (XCP) rootkit, 145–147
 Externalities, 599
 F1-F10 functionality classes, 301–303
 Fabrications, 7–8
 Face recognition authentication, 619. *See also* Biometrics.
 Factoring large numbers, 78, 725–730
 Failover mode, 443
 Failure, 100, 443–444
 Failure modes and effects analysis (FMEA), 168–169, 528
 Fair Credit Reporting Act, 610
 Fair information policies, 609–610, 613–614
 Fair service guarantee, 267
 Fair use, 651
 Fairbrother, Peter, 287
 FAIS (Foreign Affairs Information System), 312
 False intrusion detection, 489–490
 False positives, 578
 Falsifying messages, 422–423
 Fame, attack motive, 402
 Fault tolerance, networks, 377
 Fault tree analysis (FTA), 168–169, 528
 Faults
 active detection, 172–173
 definition, 100
 fixing, 99–101
 passive detection, 172–173
 Faux environment, 468–469

- FBI
 - al Qaeda computer, 24
 - breaking WEP, 467
 - Computer Crime and Security Survey, 582, 585
 - loss from attacks, 588
 - organized crime, 403–404
 - stolen laptops, 15
 - survey of cyberattacks, 102
 - value of cybersecurity, 578
- Federal Educational Rights and Privacy Act, 610
- Federal Trade Commission (FTC), 610
- Federated databases, 363
- Felten, Edward, 654
- Fence register, 194–195
- Fences, 193–194
- Fermat's theorem, 729–730
- Field checks, databases, 325
- Fields, databases, 319
- File lock channel, 152
- File names, iishack problem, 425
- File protection
 - all-none, 215–216
 - group, 216–217
 - individual permissions, 217
 - per-object, 219
 - persistent permissions, 218
 - per-user, 219
 - SUID (set userid), 218–219
 - temporary acquired permissions, 218–219
- Files
 - access control. *See* Access control.
 - directory access, 425–426
 - erasing deleted, 207, 271
- Filters
 - database reliability, 334
 - multilevel databases, 365
 - polarizing, 774–775
- Final permutation, 739, 741
- fingerd* flaw, 136, 148
- Fingerprint, operating system or applications, 406–407
- Fingerprint authentication, 620–621. *See also* Biometrics.
- Fires, 557
- Firewalls
 - network encryption, 449–450
 - networks
 - application proxy gateway, 478–480
 - authentication, 466
 - comparison of, 481–482
 - definition, 474
 - design, 474–475
 - guards, 480
 - limitations, 483–484
 - overview, 474
 - packet filtering gateway, 475–477
 - personal, 481
 - sample configuration, 482–484
 - stateful inspection, 477–478
 - types of, 475–480
 - rules set, 477
- Firmware, legal issues, 660–661
- First sale, 651
- Flaws
 - aliasing, 103
 - ambiguous access policies, 288
 - authentication, 103
 - boundary conditions, 103
 - definition, 101
 - domain errors, 103
 - exploitation examples, 289–290
 - identification, 103
 - incomplete mediation, 288–289
 - known vulnerabilities, 288–289
 - logic errors, 103
 - overview, 101–103
 - serialization, 103
 - time-of-check to time-of-use flaws, 288
 - types of, 103
 - typical flaws, 288–290
 - user interface vulnerability, 288
 - validation errors, 103
- Floods, 556–557
- Flow analysis, 158
- FMEA (failure modes and effects analysis), 168–169, 528
- Follett, Ken, 52
- Footprints, satellite broadcast, 384–385
- Foreign Affairs Information System (FAIS), 312
- Forgery, 491, 640
- Formal methods, 179
- Formal verification, 292–294
- Format failures, 423–424
- Fortezza, 691. *See also* Keys (encryption), escrow.
- Frames, network, 388
- Framing the issue, 590–591
- Fraud
 - Computer Fraud and Abuse Act, 683
 - ethical issues, 705–706
 - laws, 667
- Free rides, 598
- Free speech, and cryptography, 690–691
- Freedom of Information Act, 684
- Frequency probability, 534
- Front end
 - databases, 319
 - trusted, 360–361
- FTA (fault tree analysis), 168–169, 528
- FTC (Federal Trade Commission), 610
- Full disclosure, 675–676
- Full plaintext attacks, 65–66
- Functional correctness, 244
- Future earnings, adjusting, 575–576

- Galois fields, 727–728
- Gates, Bill
 - on passwords, 229
 - on product quality, 678
- Gateways
 - application proxy, 478–480
 - packet filtering, 475–477
- General knapsacks, 759–760
- Genetic diversity, 165
- Geosynchronous orbit, 384
- German Green Book, 300–301
- Gibson, Steve, 432
- GISA (German Information Security Agency), 300–301
- GLBA (Graham-Leach-Bliley Act), 610, 684
- Goals of security, 10–12
- Gottschalk v. Benson*, 657–658
- Government. *See also specific governments.*
 - data mining, 624
 - e-mail, security policy example, 553
 - and privacy
 - Council of Europe, 613
 - European Privacy Directive, 613
 - Icelandic DNA database, 351
 - principles and policies, 616–618
 - U.K. RIPA (Regulation of Investigatory Powers Act), 287
- Graham–Denning security model, 257–259
- Grandin, Temple, 401
- Granularity, 193, 353
- Greatest common divisor, 726
- Group behavior, 591–592
- Group file protection, 216–217
- Guaranteed fair service, 267
- Guards, 360–361, 480, 560
- Guess function, 721
- Guessing passwords, 415–416

828 Index

- Hackers. *See also* Attackers; Crackers.
versus crackers, 22
 overview, 22
 sting operation, 403
- Hacking
 ethical. *See* Penetration testing.
 ethical issues, 707–710
- Hactivism, attack motive, 403
- Halting problem, 177, 261
- Hard knapsacks, 763–764
- Hardware. *See also* Cables; Networks.
 controls, 27
 legal issues, 660
 viruses, 132
- Hardware-enforced protection, 191
- Hash codes, 458. *See also* Hash function.
- Hash function, 493
- Hazard analysis, 168–169, 528. *See also* Physical security.
- HAZOP (hazard and operability studies), 168–169, 528
- Herald, New Zealand, 413
- Heroes, organizational, 593
- Heuristic intrusion detection, 485, 486–487
- Hierarchical security policies, 248
- Hierarchical structuring, 285–287
- Hierarchies of complexity, 723
- High-confidence software, 183
- Highjackers, 632–633
- HIPAA (Health Insurance Portability and Accountability Act), 610, 684–685
- Hollywood e-mail theft, 20
- Honeypots, 468–469
- Hoo, Soo, 551
- Host-based intrusion detection, 485
- Hostile applets, 436, 499
- Hosts, 379
- Hot site backups, 565–566
- HRU (Harrison–Ruzzo–Ullman) security model, 259–261
- Huffman codes, 458
- Human fallibility case study, 67
- Hyppönen, Mikko, 22
- IBM
 history of DES, 69
 Lucifer algorithm, 68–69
 MVS/ESA operating system, 281
 Processor Resources/System Manager (PR/SM), 282
 U.S. government suit, 191
- IC3 (Internet Crime Complaint Center), 584
- Icelandic DNA database, 351
- ICMP (Internet Control Message Protocol), 428
- Identification
versus authentication, 234–235
 errors, 103
 principles of trusted systems, 269
- Identity (authentication), 619, 621–622
- Identity (mathematical), 725
- Identity theft, 618, 621
- Ideology, attack motive, 403
- IDS (intrusion detection system)
 anomaly based, 485
 Common Intrusion Detection Framework, 484
 definition, 484
 false results, 489–490
 goals for, 488–490
 heuristic, 485, 486–487
 host based, 485
 misuse, 487
 model based, 487
 network based, 485
 networks. *See* Networks, IDS.
 overview, 484–485
 principles of trusted systems, 273
 response to alarms, 489
 signature based, 485, 486
 state based, 487
 statistical analysis, 486
 stealth mode, 487–488
 strengths and weaknesses, 490
 types of, 485–488
- IEEE (Institute for Electrical and Electronics Engineers)
 code of ethics, 710, 711
 Standard 729, 100
- IIS (Internet Information Server), 137–139, 140
- iishack problem, 425
- IKE (ISAKMP key exchange), 455–456
- Images, signaling through. *See* Steganography.
- Imation Data Protection Survey, 584–585
- Imbruglia, George, 28
- Impedance, electrical, 410
- Impersonation
 of login, 233–234
 man-in-the-middle attack, 420
 masquerade, 418–419
- network threat, 415–420
 phishing, 236, 419
 session hijacking, 419–420
 spoofing
 cryptographic protection, 462–463
 interface illusions, 148–149
 network vulnerability, 418
 trusted path, 270–271
 steganography, 159–160
 trusted systems, 236
 web bugs, 139–141, 631
- Implementation flaws, 424
- Incident response plans, 521–524
- Incident response teams, 522–523
- Incomplete mediation, 107–109, 288–289. *See also* Complete mediation.
- Independent testing, 172
- Indirect attack, 343–350
- Individual authentication, 619, 620
- Inductance, 409
- Industrial espionage, 402
- Inference, database attacks
 combined results control, 348
 concealing control, 347
 controls for, 347–349
 count attacks, 343–344
 direct attack, 342–343
 indirect attack, 343–350
 limited response suppression, 347–348
 linear system vulnerability, 346–347
 mean attacks, 344
 median attacks, 344–345
 problem summary, 349–350
 query analysis, 349
 random data perturbation, 349
 random sample control, 348–349
 statistical inference attacks, 347
 sum attacks, 343
 suppression control, 347
 tracker attacks, 345–346
- Information. *See also* Data; Databases.
 anarchy, 676
 collection, privacy issues, 606, 607
 commerce, 665–666
 depletion, 663
 disclosure, privacy issues, 606
 flow analysis, 158
 hiding, 161–164
 leaks, 16. *See also* Covert channels.

- replication, 664
- retention, privacy issues, 606
- security, privacy issues, 606
- usage, privacy issues, 606
- Information officers, security responsibilities, 515
- Information Security Breeches Survey (ISBS), 581, 585–586
- Information Technology Security Evaluation Criteria (ITSEC), 300–303, 303–304
- Informed consent, 607
- Infrared networks, 383–384
- Inherently hard problems, 724–725
- Initial permutation, 739, 741
- Inspection, code, 166
- Installation testing, 170
- Instances, 722
- Institute for Electrical and Electronics Engineers (IEEE)
 - code of ethics, 710, 711
 - Standard 729, 100
- Intangible transfer, 665
- Integrated viruses, 119
- Integrated Vulnerability Assessments (IVAs), 530
- Integration testing, 142, 170
- Integrity
 - data, 17, 19
 - data mining, 368–369
 - databases, 324–326, 329. *See also* Reliability.
 - definition, 10
 - economic, 598
 - enforcement, 244
 - locks, 357–359, 359–360
 - multilevel databases, 354
 - overview, 11–12
 - *-property, 256
 - threats, 680
- Intellectual property, 650–651
- Intelligence gathering, 406
- Intent phase, 330
- Intercepting sensitive information, 561–563
- Interception, 7–8, 412, 636
- Interceptors, 38
- Interface illusions, 148–149
- Internal networks, 395–396
- Internal rate of return (IRR), 577
- Internet, 552–553. *See also* Web sites.
- Internet Control Message Protocol (ICMP), 428
- Internet Crime Complaint Center (IC3), 584
- Internet Information Server (IIS), 137–139, 140
- Internet protocol. *See* IP.
- Internet Scanner, 405
- Internet Security Association Key Management Protocol (ISAKMP), 455
- Internet Security Systems (ISS), 677
- Internet worm, 134–137
- Internets, 395–396
- Interprocess communication, 267
- Interruptions, 7–8
- Intrinsic good, 697–698
- Intruders, 38
- Intrusion, characteristics, 4–5
- Intrusion detection system (IDS). *See* IDS.
- Inverse initial permutation, 739, 741
- Inverses, 725, 728–730
- Invisible gif. *See* Web bugs.
- I/O operation, 277
- IP addresses
 - resolution, 425
 - shortage of, 393, 454
 - spoofing. *See* Spoofing.
 - translation, 199, 202
- IPSec (IP Security Protocol Suite), 454–456
- IPv6, 454–456
- Iris pattern authentication. *See* Biometrics.
- IRR (internal rate of return), 577
- ISAKMP (Internet Security Association Key Management Protocol), 455
- ISAKMP key exchange (IKE), 455–456
- ISBS (Information Security Breeches Survey), 581, 585–586
- ISO OSI (Open Systems Interconnection) model, 386–390
- Isolation, 279–280
- ISS (Internet Security Systems), 677
- ITSEC (Information Technology Security Evaluation Criteria), 300–303, 303–304
- Ivanov, Alexey, 403
- IVAs (Integrated Vulnerability Assessments), 530
- Jacobi function, 771–772
- Japanese Naval code, 42
- Java code, 435–437
- JetBlue airlines, 612–613
- Job *versus* employee, 594
- JVM (Java virtual machine), 435–437
- Karger, Paul, 178
- KDC (key distribution center), 213–214
- Kennedy, Edward, 370
- Kerberos
 - access to protected objects, 213–214
 - network controls, 461–464
 - networks, 461–464
- Kernel, 274
- Kernelized design, 274–279
- Key Online Banking, 452
- Keyless ciphers, 40
- Keyrings, e-mail, 495
- Keys (encryption)
 - clustering, 746
 - definition, 47
 - distribution, 62
 - encryption, 39
 - escrow, 691
 - exchange, 80–82
 - length, 743–745
 - management, 62
 - private, 39–40. *See also* AES; DES; Symmetric encryption.
 - proliferation, 77
 - public. *See also* Asymmetric encryption; RSA.
 - characteristics, 77
 - definition, 39
 - flow diagram, 40
 - key proliferation, 77
 - purpose of, 76
 - RSA (Rivest-Shamir-Adelman) encryption, 769
 - transformation, 736
- Keystroke logging, 149, 632
- Klein, Joe, 353
- Knapsack problem, 719–720
- Knapsacks
 - as cryptographic algorithms, 761–763
 - decryption algorithm, 764–765
 - general, 759–760
 - hard, 763–764
 - Merkle–Hellman, 758–761, 766–767
 - and modular arithmetic, 761–763
 - simple, 760–761, 763
 - superincreasing, 760–761, 763–764
- Kneed-to-know security policies, 246

830 Index

- KSOS, 191, 311
KVM, 191, 311
- L0pht, 107, 405
L1-L6 assurance levels, 302
LAN (local area network), 394
Laptop computers, vulnerabilities, 14–15
Lattice security model, 253–254
Laws. *See also* Legal issues.
California Breach Act, 686
CAN SPAM Act, 685–686
civil, 667
contract, 668–669
Council of Europe Agreement on Cybercrime, 687
criminal, 667
versus ethics, 692–694
E.U. Data Protection Act, 687
fraud, 667
GLBA (Graham-Leach-Bliley Act), 684
HIPAA (Health Insurance Portability and Accountability Act), 684–685
information-related
database protection, 666
depletion, 663
electronic commerce, 666–667
electronic publishing, 666
information commerce, 665–666
intangible transfer, 665
marginal cost, 664
as object, 663–665
replication, 664
time-dependent value, 664–665
protecting computer artifacts, 669
RIPA (Regulation of Investigatory Powers Act), 287
statutes, definition, 667
statutes, examples, 683–686
tort, 667–668
U.S. Computer Fraud and Abuse Act, 683
U.S. Economic Espionage Act, 683
U.S. Electronic Communications Privacy Act, 684
U.S. Electronic Funds Transfer Act, 683
U.S. Freedom of Information Act, 684
U.S. Privacy Act, 684
USA Patriot Act, 685
Layered defense, 29
Layered trust, 283–287
Layering networks, 389
Leaking
access rights, 261
information, 16. *See also* Covert channels.
Least common mechanism, 266
Least privilege, 265
Legal control. *See* Laws; Legal issues.
Legal issues. *See also* Ethical issues; Laws.
computer crime
California Breach Act, 686
CAN SPAM Act, 685–686
Computer Fraud and Abuse Act, 683
computer terminology and the law, 681
confidentiality threats, 680
Council of Europe Agreement on Cybercrime, 687
cryptography, 688, 688–692
defining, 681–682
Economic Espionage Act, 683
Electronic Communications Privacy Act, 684
Electronic Funds Transfer Act, 683
E.U. Data Protection Act, 687
Freedom of Information Act, 684
GLBA (Graham-Leach-Bliley Act), 684
HIPAA (Health Insurance Portability and Accountability Act), 684–685
integrity threats, 680
international dimensions, 686–688
overview, 679
Patriot Act, 685
Privacy Act, 684
prosecuting, 682–683
restricted content, 687–688
rules of evidence, 680
rules of property, 679–680
scope limitations, 688–689
statutes, examples, 683–686
value of data, 681
cryptography, 688–692
overview, 647–649
program and data protection
computer objects, 659–662
copyright, 649–655, 660
documentation protection, 662
domain names, 662
firmware, 660–661
hardware, 660
object code software, 661
patents, 655–658, 660
reverse engineering, 658–659
source code software, 661–662
trade secrets, 658–659, 660
trademark, 662
URLs, 662
web content, 662
rights of employees and employers
copyright ownership, 671
employee contracts, 672
licensed software, 671
patent ownership, 670–671
product ownership, 670–672
trade secrets, 672
work for hire, 671
software failure
full disclosure, 675–676
overview, 673
quality demands, 674–675
quality software, 678–679
refunds, 674
reporting flaws, 675–679
selling correct software, 673–674
user interests, 676
vendor interests, 676
warranty of cyberworthiness, 675
Legislation. *See* Laws.
Levy, Elias, 148–149
Lewis, John, 370
Library viruses, 124
Licensed software, 671
Limited privilege, 244
Limited response suppression, 347–348
Linear system vulnerability, 346–347
Link encryption, 445–446
Links, network, 379
Linux, 295
Litchfield, David, 676
Lloyd's Bank, 452
Local area network (LAN), 394
Local name space, 211
Locks
access control, 560
integrity, 357–359, 359–360
sensitivity, 359
“spray paint,” 357–359
Logic bombs, 16, 116
Logic errors, 103
Logical separation, 191, 279–280
Logs
audit, 272–273
database changes, 326

- database transactions, 324
 - reduction, 272–273
- Loose *versus* tight organizational control, 595
- Loose-lipped system, 222
- Lower bound, 254
- Lucifer algorithm, 68–69
- Lynn, Michael, 677

- MAC (mandatory access control), 269–270
- MAC (Media Access Control) address, 388
- Mafia boss case study, 45
- Mafiaboy, 404
- Magnetic remanence, 270
- Malformed packets, 423–424
- Malicious code. *See also* Nonmalicious errors; Programs, security; Viruses; Worms.
 - agents, 114
 - history of, 113–114
 - implementation time, 116
 - interface illusions, 148–149
 - keystroke logging, 149
 - logic bombs, 116
 - man-in-the-middle attacks, 149
 - potential for harm, 113
 - privilege escalation, 147–148
 - rabbits, 116
 - rootkit revealers, 146
 - rootkits, 145–147
 - Sony XCP (extended copy protection) rootkit, 145–147
 - spoofing, 148–149
 - threat assessment, 125
 - time bombs, 116
 - timing attacks, 150
 - Trojan horses, 116
 - types of, 114, 116–117
 - worms, 116
 - zero day exploits, 116
- Malware. *See* Malicious code.
- MAN (metropolitan area network), 395
- Managers, security responsibilities, 515
- Mandatory access control (MAC), 269–270
- Man-in-the-middle attacks, 149, 420. *See also* Impersonation; Masquerade; Spoofing.
- Mapping controls to vulnerabilities, 537, 539
- Marginal cost, 664

- Marketability, evaluating, 303
- Marks, Leo, 48
- MARS algorithm, 748
- Masquerade, 418–419. *See also* Man-in-the-middle; Spoofing.
- Mathematics of cryptography. *See* Cryptography, mathematics of.
- MD4 hash function, 80
- MD5 hash function, 80
- Mean attacks, 344
- Media, network, 382–385
- Media Access Control (MAC) address, 388
- Median attacks, 344–345
- Mediation
 - complete, 265–266, 270
 - incomplete, 107–109, 288–289
- Memory and address protection
 - base/bounds registers, 195–196
 - context switch, 195–196
 - fences, 193–194
 - page frames, 202
 - paging, 202–203, 203–204
 - Palladium (protect memory project), 238
 - principles of trusted systems, 266, 277
 - relocation, 194–195
 - relocation factor, 195
 - segment address table, 199
 - segmentation, 199–202, 203–204
 - tagged architecture, 196–199
- Memory-resident viruses, 123–124
- Merkle–Hellman knapsacks, 758–761, 766–767
- Message confidentiality, 420–422
- Message digests. *See* Cryptographic checksum.
- Message integrity, 422–423
- Method, opportunity, motive (MOM), 8–9
- Methods of
 - attack. *See* Attacks, methods.
 - defense. *See* Controls; Defense methods.
- Metropolitan area network (MAN), 395
- MIC (message integrity check), 493
- Microcontrollers, automobile control systems, 3
- Microcontrollers in automobiles, 3
- Microsoft
 - on career criminals, 22
 - on full disclosure, 675–676
 - passport, 232
 - on passwords, 229
 - patching flaws, 676
 - on product quality, 678
 - single sign-on, 232
- Microsoft Redaction Tool, 271
- Microsoft Word, deleting text, 271
- Microwave networks
 - description, 383
 - eavesdropping, 410–411
 - wiretapping, 410–411
- Military security policies, 246–248
- Mining, data. *See* Data mining.
- Misdelivering messages, 420–421
- Misuse intrusion detection, 487
- Mitnick, Kevin, 401
- Mix column, 752–753
- Mixmaster remailers, 637–638
- Mixer, 401
- Mobile agents, 444
- Mobile code, 433
- Model-based intrusion detection, 487
- Modeling security economics
 - credibility, 592
 - decision making, 590–592
 - framing the issue, 590–591
 - group behavior, 591–592
 - overview, 589
 - role of organizational culture, 592–597
 - transferring models, 589–590
 - trust as economic issue, 592
- Models, security. *See* Security models.
- Modular arithmetic, 43, 726–728
- Modularity of code, 161–164
- MOM (method, opportunity, motive), 8–9
- Money, attack motive, 402
- Monitoring
 - e-mail, 637
 - privacy, 606
- Monitors, 190, 334–335
- Monoalphabetic cipher, 44
- Moore’s Law, 43
- Morals. *See* Ethical issues.
- Morris, Robert, Jr., 134–137, 400
- Morris, Robert, Sr., 136
- Motives for attacks, 399–404
- MP3.com, 655
- Multics, 178, 191, 311
- Multifactor authentication, 222
- Multilevel databases. *See* Databases, multilevel.
- Multilevel security, 253–257
- Multiple identities, 614–616

832 Index

- Multiple virtual memory spaces, 281
- Multiplexed signals, 410
- Multiprogrammed operating systems, 190
- Mundie, Craig, 296, 676
- Mutual authentication, 463
- Mutual suspicion, 164

- Napster, 655
- National Institute of Standards and Technology (NIST), 72
- National Research Council (NRC), 691
- National Security Agency (NSA), 69, 181, 742–743
- Natural disasters, 556–558
- NBS (National Bureau of Standards), 68–69, 72
- NCSC (National Computer Security Center), 297, 304
- Negative result disclosure, 339
- Nessus, 405
- Net present value, 574–577
- netcat scanner, 405
- Network interface cards (NICs), 387–388
- Network-based intrusion detection, 485
- Networked backups, 565
- Networks
 - address shortage, 393, 454
 - amplifiers, 383
 - analog communication, 382
 - angle of dispersion, 384–385
 - boundaries, 381–382
 - cables
 - coaxial, 382
 - eavesdropping, 409–410
 - Ethernet, 383
 - impedance, 410
 - inductance, 409
 - networking, 382–383
 - UTP (unshielded twisted pair), 382
 - wiretapping, 409–410
 - CAN (campus area network), 395
 - clients, 378–379
 - coaxial cable, 382
 - communication mode, 382
 - control, 381–382
 - datagrams, 391
 - diagram of, 380
 - digital communication, 382
 - domain names, 393
 - environment of use, 379, 381
 - Ethernet cable, 383
 - fault tolerance, 377
 - firewalls
 - application proxy gateway, 478–480
 - comparison of, 481–482
 - definition, 474
 - design, 474–475
 - guards, 480
 - limitations, 483–484
 - overview, 474
 - packet filtering gateway, 475–477
 - personal, 481
 - sample configuration, 482–484
 - stateful inspection, 477–478
 - types of, 475–480
 - footprints, 384–385
 - frames, 388
 - geosynchronous orbit, 384
 - hosts, 379
 - IDS (intrusion detection system)
 - anomaly based, 485
 - definition, 484
 - false results, 489–490
 - goals for, 488–490
 - heuristic, 485, 486–487
 - host based, 485
 - misuse, 487
 - model based, 487
 - network based, 485
 - overview, 484–485
 - response to alarms, 489
 - signature based, 485, 486
 - state based, 487
 - statistical analysis, 486
 - stealth mode, 487–488
 - strengths and weaknesses, 490
 - types of, 485–488
 - infrared, 383–384
 - the Internet, 395–396
 - internets, 395–396
 - LAN (local area network), 394
 - layering, 389
 - links, 379
 - MAC (Media Access Control) address, 388
 - MAN (metropolitan area network), 395
 - media, 382–385
 - microwave, 383
 - NICs (network interface cards), 387–388
 - nodes, 379
 - opaqueness, 379
 - optical fiber, 383
 - OSI (Open Systems Interconnection) model, 386–390
 - overview, 378–379
 - ownership, 381–382
 - packets, 387, 391
 - peers, 386
 - port numbers, 391
 - protocol stack, 385
 - protocols, 385–393
 - repeaters, 383
 - resilience, 377
 - routers, 387
 - routing concepts, 393
 - satellite, 384–385
 - secure e-mail
 - confidentiality, 492–493
 - designs, 492–494
 - encryption, 493–494
 - keyrings, 495
 - MIC (message integrity check), 493
 - PGP (Pretty Good Privacy), 494–496
 - requirements, 491
 - ring of trust, 495
 - sample systems, 494–496
 - S/MIME (Secure MIME), 496
 - solutions, 491
 - threats, 491
 - servers, 378–379
 - sessions, 429
 - shape, 381–382
 - single point of failure, 377
 - size, 381–382
 - SYN_RECV connections, 429
 - TCP protocols, 391–392
 - TCP/IP protocol, 391–393
 - top-level domain, 393
 - topography, 381–382
 - types of, 394–396
 - UDP (user datagram protocol), 391–392
 - UTP (unshielded twisted pair) cable, 382
 - WAN (wide area network), 395
 - wireless, 383
 - workstations, 379
- Networks, controls
 - ACLs (access control lists), 464–466
 - alarms, 468
 - alerts, 468
 - architecture, 442–443

- challenge-response systems, 460
- content integrity, 457–459
- cryptographic checksum, 458–459
- design, 441–442
- Digital distributed authentication, 460–461
- encryption
 - AH (authentication header), 455
 - certificate authorities, 451
 - comparison of methods, 447–449
 - e-mail, 457
 - encrypted tunnels, 449–450
 - end-to-end, 446–447
 - ESP (encapsulated security payload), 455
 - firewalls, 449–450
 - IKE (ISAKMP key exchange), 455–456
 - ISAKMP (Internet Security Association Key Management Protocol), 455
 - issues, 453
 - link, 445–446
 - overview, 444–445
 - PKI (public key infrastructure), 450–453
 - security associations, 454–455
 - signed code, 456–457
 - SPI (security parameter index), 455
 - SSH (secure shell), 453
 - SSL (Secure Sockets Layer), 453–454
 - TLS (transport layer security), 453–454
 - tunnels, 449–450
 - VPNs (virtual private networks), 449–450
- error correcting codes, 458
- error detection, 458
- even parity, 458
- failover mode, 443
- failure tolerance, 443–444
- firewalls, 466
- hash codes, 458
- honeypots, 468–469
- Huffman codes, 458
- implementation, 441–442
- intrusion detection, 468
- Kerberos, 461–464
- mobile agents, 444
- odd parity, 458
- one-time password, 459–460
- onion routing, 470
- parity check, 458
- password tokens, 459–460
- redundancy, 443
- router access controls, 464–466
- segmentation, 442–443
- single points of failure, 443–444
- SSID (Service Set Identifier), 466–467
- strong authentication, 459–464
- summary of, 470–474
- threat analysis, 440–441
- tickets, 461
- TKIP (Temporal Key Integrity Protocol), 467–468
- traffic flow security, 469–470
- WEP (wired equivalent privacy), 467
- wireless security, 466–468
- WPA (WiFi Protected Access), 467–468
- Networks, threats
 - active code, 433, 435–437
 - active wiretapping, 409
 - ActiveX controls, 435–437
 - anonymity, 397
 - application code errors, 426
 - ASP (active server pages), 435
 - attackers, 399–404
 - authentication vulnerabilities
 - avoidance, 416–417
 - eavesdropping, 416
 - guessing passwords, 415–416
 - man-in-the-middle attack, 420
 - masquerade, 418–419
 - nonexistent authentication, 417
 - phishing, 419
 - session hijacking, 419–420
 - spoofing, 418. *See also* Man-in-the-middle; Masquerade.
 - trusted authentication, 418
 - well-known authentication, 417–418
 - wiretapping, 416
 - automatic exec by file type, 437
 - botnets, 437–438
 - bots, 437–438
 - broadcast mode, 428–429
 - buffer overflow, 425
 - bulletin boards, 407
 - cable
 - eavesdropping, 409–410
 - impedance, 410
 - inductance, 409
 - wiretapping, 409–410
 - challenge motive, 400
 - chats, 407
 - complex attacks, 438
 - connection flooding, 427–428
 - cookies, 434
 - cyberterrorism, 403
 - DDoS (distributed denial of service), 431–433
 - defacing web sites, 424–425
 - distributed authentication, 398
 - DNS attacks, 431
 - DNS cache poisoning, 431
 - documentation availability, 407
 - DoS (denial of service), 427–431
 - dot-dot-slash directory travel, 425–426
 - dumpster diving, 406–407
 - eavesdropping, 408–414
 - echo chargen, 428
 - escape-character attack, 434–435
 - espionage, 402
 - exposing messages, 421–422
 - falsifying messages, 422–423
 - fame motive, 402
 - format failures, 423–424
 - hactivism, 403
 - hostile applets, 436
 - ICMP (Internet Control Message Protocol), 428
 - ideological motive, 403
 - iishack problem, 425
 - impersonation, 415–420
 - implementation flaws, 424
 - intelligence gathering, 406
 - Java code, 435–437
 - JVM (Java virtual machine), 435–437
 - malformed packets, 423–424
 - message confidentiality, 420–422
 - message integrity, 422–423
 - microwave, 410–411
 - misdelivering messages, 420–421
 - in mobile code, 433
 - money motive, 402
 - motives for attacks, 399–404
 - multiple points of attack, 397
 - multiplexed signals, 410
 - noise, 423
 - optical fiber, 411
 - organized crime, 403
 - packet sniffers, 409–410
 - passive wiretapping, 409
 - ping of death, 428
 - port scans, 404–405
 - protocol failures, 424
 - protocol flaws, 414
 - reconnaissance, 404–408

834 Index

- Networks, threats (*continued*)
 replaying old messages, 422–423
 RFC (Request For Comment), 414
 rogue access points, 408
 sandbox, 435
 satellite, 411
 script kiddies, 438
 scripts, 434–435
 server-side includes, 427
 sharing, 397
 smurf attack, 428–429
 social engineering, 405–406
 SYN flood, 429
 system complexity, 397
 system fingerprinting, 406–407
 teardrop attacks, 430
 traffic flow analysis, 422
 traffic redirection, 430
 transmission failure, 427
 unknown path, 399
 unknown perimeter, 398–399
 vulnerabilities, 397–399
 vulnerabilities, summary of, 438
 war driving, 408
 web site vulnerabilities, 424–427
 wireless
 eavesdropping, 411–413
 interception, 412
 rogue access points, 408, 412
 theft of service, 408, 412
 vulnerabilities, 413
 war driving, 408
 wiretapping, 411–413
 wiretapping, 408–414
 zombies, 431–433
 New Zealand Herald, 413
 NICs (network interface cards), 387–388
 NIST (National Institute of Standards and Technology), 72
 nmap scanner, 405
 Nodes, network, 379
 Noise, in communications, 423
 Nondeterminism, 721
 Nondeterministic Turing machines, 721
 Nonexistent authentication, 417
 Nonhierarchical security policies, 248
 Nonmalicious errors. *See also* Malicious code; Programs, security.
 buffer overflows, 104–107
 causes of failures, 112
 combined flaws, 111
 incomplete mediation, 107–109
 synchronization, 109–111
 time-of-check to time-of-use errors, 109–111
- Normative *versus* pragmatic organizations, 595
 NP class, 721
 NP-complete problems, 719–724
 NRC (National Research Council), 691
 NSA (National Security Agency), 69, 181, 742–743
 Nuclear weapons, tracking, 140
 Nucleus. *See* Kernel.
 Number of iterations, 743
 Number theory, 78, 724
- Object code, legal issues, 661. *See also* Copyright.
 Objects, digital
 allocation, 266–267
 copying, 654–655
 copyright, 653–655
 information as, 663–665
 legal issues, 659–662
 patents, 657–658
 protected. *See* Protected objects.
 reusing, 270
 OCTAVE methodology, 511
 Odd parity, 458
 Odlyzko, Andrew, 597
 Offers, web privacy, 629
 Offsite backups, 564
 One-by-one gif. *See* Web bugs.
 One-time execution viruses, 122
 One-time pads, 50–54
 One-time passwords, 231–232, 459–460
 One-way functions, 79
 Onion routing, 470
 Online banking, 452
 Online environment, 626–627
 Online profiling, 631
 Opaqueness, of network, 379
 Opcodes, 143
 Open design, 265
 Open source, 295–296
 Open Systems Interconnection (OSI) model, 386–390
 Open *versus* closed organizations, 595
 Operating system data protection, 267–268
 Operating system protection features, 329–330
 Operating system security. *See also* Programs, security; Trusted systems.
 cryptographic separation, 192
 executives, 189–190
 file protection
 all-none, 215–216
 group, 216–217
 individual permissions, 217
 per-object, 219
 persistent permissions, 218
 per-user, 219
 SUID (set userid), 218–219
 temporary acquired permissions, 218–219
 granularity, 193
 hardware-enforced protection, 191
 history of, 189–190
 levels of protection, 192
 logical separation, 191
 memory and address protection
 base/bounds registers, 195–196
 context switch, 195–196
 fences, 193–194
 page frames, 202
 paging, 202–203, 203–204
 relocation, 194–195
 relocation factor, 195
 segment address table, 199
 segmentation, 199–202, 203–204
 selective protection. *See* Tagged architecture.
 tagged architecture, 196–199
 monitors, 190
 multiprogrammed operating systems, 190
 physical separation, 191
 protected objects, accessing
 AS (authentication server), 213–214
 access control matrix, 210–211
 ACLs (access control lists), 208–210
 capability, 210–213
 directories, 205–208
 domains, 211
 erasing deleted files, 207
 KDC (key distribution center), 213–214
 Kerberos, 213–214
 local name space, 211
 procedure-oriented, 214–215
 protection goals, 205
 pseudonyms, 207–208
 revocation of access, 206–207
 role-based, 215
 single sign-on, 214
 TGS (ticket-granting server), 213–214
 types of, 204–205
 wild cards, 208–210
 protection methods, 189–193

- separation, 190–193
- system functions, 188–189
- temporal separation, 191
- user authentication
 - additional authentication information, 221–222
 - biometrics, 219–220, 234–236
 - challenge-response system, 231–232, 233–234
 - cookies, 236
 - flaws, 233–234
 - versus* identification, 234–235
 - impersonating trusted systems, 236
 - impersonation of login, 233–234
 - multifactor authentication, 222
 - one-time passwords, 231–232
 - overview, 219
 - password attacks, 222–229
 - password selection criteria, 229–231
 - passwords as authenticators, 221
 - phishing, 236
 - process description, 232–234
 - single sign-on, 232
 - two-factor authentication, 222
- Opportunity cost, 576
- Optical fiber networks
 - description, 383
 - eavesdropping, 411
 - wiretapping, 411
- Oracle, estimating security costs, 578
- Oracles, 721
- Orange Book. *See* TCSEC.
- Organizational culture
 - cultural practices, 593–594
 - cultural values, 594
 - dimensions of, 595
 - employee *versus* job, 594
 - heroes, 593
 - loose *versus* tight control, 595
 - normative *versus* pragmatic, 595
 - open *versus* closed, 595
 - parochial *versus* professional, 595
 - process *versus* results, 594
 - rituals, 593
 - role of organizational culture, 592–597
 - security choices, examples, 596
 - symbols, 592
- Organized crime, 403
- Originality of work, 651
- OSI (Open Systems Interconnection) model, 386–390
- Overlapping controls, 29
- Overwriting magnetic data, 562
- Owners, 548
- Ownership
 - of data, 608
 - networks, 381–382
 - programs, 702–704
 - web sites, 628–629
- Ozment, Andy, 598
- P class, 721
- Packet filtering gateways, 475–477
- Packet sniffers, 409–410
- Packets, network, 387, 391
- Page address translation, 202
- Page frames, 202
- Page size, 202
- Page translation table, 203–204
- Paged segmentation, 203–204
- Paging, 202–203, 203–204
- Palladium (protect memory project), 238
- Parallel attack, 744–745
- Parity check, 458
- Parker, Donn, 401
- Parochial *versus* professional organizations, 595
- Partial ordering, 254
- Partial plaintext attacks, 65–66
- Partitioning multilevel databases, 356
- Passenger Name Record (PNR), 615
- Passive fault detection, 172–173
- Passive wiretapping, 409
- Passport, 232
- Pass-through problem, 326
- Password attacks
 - 12-step process, 226
 - brute force, 223
 - encrypted password file, 227–228
 - exhaustive, 223
 - guessing, 464
 - indiscreet users, 228–229
 - plaintext password list, 226
 - probability, 224
 - salt extension, 228
 - trial and error, 222
 - weak passwords, 224–227
- Passwords
 - as authenticators, 221
 - frequency of change, 230–231
 - guessing, 415–416
 - with Kerberos, 462
 - Microsoft, 229
 - mnemonic qualities, 230
 - network tokens, 459–460
 - one-time, 231–232
 - selection criteria, 229–231
- Patents
 - for computer objects, 657–658
 - definition, 655
 - Diamond v. Bradley*, 658
 - Diamond v. Diehr*, 658
 - Gottschalk v. Benson*, 657–658
 - infringement, 657
 - legal issues, 655–658, 660
 - ownership, 670–671
 - registering, 656–657
 - requirements of novelty, 656
- Path, trusted. *See* Trusted path.
- Patriot Act, 685
- Patterns
 - cryptographic permutations, 56–57
 - database reliability, 334
 - virus signatures, 125–127
- Payment schemes, web privacy, 627
- Payments online, web privacy, 627
- P-boxes, 739, 741
- PDF, deleting text, 271
- Peer reviews, 165–168
- Peers, network, 386
- Penetrate-and-patch technique, 100
- Penetration testing, 172, 177, 291
- Performance testing, 170
- Permission based principles of trusted systems, 266
- Permissions. *See also* Privilege.
 - individual, 217
 - persistent, 218
 - temporary acquired, 218–219
- Permutation cycle, 734
- Permutations
 - columnar transpositions, 55–58
 - combined approaches, 58
 - definition, 55
 - digram analysis, 57–58
 - digrams, 56–57
 - encipherment/decipherment complexity, 56
 - patterns, 56–57
 - product ciphers, 58
 - substitution ciphers, 46–47
 - symmetric encryption, 730
 - trigrams, 56–57
 - types, 736
- Permuted choices, 733
- Per-object file protection, 219
- Per-session cookies, 434
- Persistent cookies, 434
- Personal computer users, security responsibilities, 514
- Personal firewall, 481
- Personal identification number (PIN), 219

836 Index

- Personnel staff members, security responsibilities, 516
- Per-subject protection, 208–210
- Per-user file protection, 219
- PGP (Pretty Good Privacy), 494–496
- Phishing, 236, 419. *See also* Impersonation.
- Photon reception, 775
- Photons, cryptography with, 775–776
- Physical controls, 27
- Physical security
- backing up data, 563–566
 - cold site backups, 565
 - complete backups, 564
 - computer screen emanations, 562–563
 - contingency planning, 563–566
 - definition, 556
 - degaussing magnetic data, 562
 - “dirty” power, 558
 - fires, 557
 - floods, 556–557
 - guards, 560
 - hot site backups, 565–566
 - intercepting sensitive information, 561–563
 - locks, 560
 - natural disasters, 556–558
 - networked backups, 565
 - offsite backups, 564
 - overwriting magnetic data, 562
 - power loss, 558
 - revolving backups, 564
 - selective backups, 564
 - shell backups, 565
 - shredding paper data, 562
 - smart cards, 560
 - surge suppressors, 558–559
 - Tempest program, 562–563
 - theft prevention, 559–561
 - unauthorized access, 559
 - UPS (uninterruptible power supply), 558
 - vandalism, 559–561
- Physical separation, 191, 279–280
- PIN (personal identification number), 219
- Ping of death, 428
- Ping protocol, 438
- Piracy, 651
- Pixel tags. *See* Web bugs.
- PKI (public key infrastructure), 450–453
- Plaintext
- chosen plaintext attacks, 66
 - ciphertext only attacks, 65
 - definition, 39
 - full plaintext attacks, 65–66
 - partial plaintext attacks, 65–66
 - password list attacks, 226
 - probable plaintext attacks, 66
- Planning, security. *See* Risk analysis; Security plan.
- PNR (Passenger Name Record), 615
- Poem codes, 48
- Polarizing filters, 774–775
- Policies. *See also* Principles; Security policies; Standards.
- economic, 597
 - privacy. *See* Privacy, principles and policies.
 - security. *See* Security policies.
- Polyinstantiation, 355
- Polymorphism, viruses, 127–128
- Port numbers, 391
- Port scans, 404–405
- Power, electrical, 558–559
- Power, Richard, 9
- Power off, virus defense, 132
- Pragmatic *versus* normative organizations, 595
- Precision *versus* security, 339–341
- Prediction, of risk. *See* Risk analysis.
- Pretty Good Privacy (PGP), 494–496
- Prevention. *See* Controls; Defense methods.
- Prime numbers, 725
- Primitive operations, 259–260
- Principles. *See also* Policies; Standards.
- economic, 597
 - privacy. *See* Privacy, principles and policies.
 - security
 - adequate protection, 17
 - easiest penetration, 5
 - effectiveness, 28
 - weakest link, 29–30
 - trusted systems. *See* Trusted systems, design principles.
- Privacy. *See also* Confidentiality.
- access control, 606
 - affected subject, 605–606
 - aspects of, 604–606
 - authentication
 - anonymized records, 622–623
 - attributes, 620
 - identity, 619, 621–622
 - individual, 619, 620
 - meaning of, 619–620
 - overview, 619
 - case study, 615
 - computer-related problems, 606–608
 - controlled disclosure, 604
 - data mining
 - aggregation of data, 625–626
 - correlation of data, 624–625
 - data perturbation, 624–626
 - government, 624
 - preserving privacy, 624–626
 - sensitive data, 368
 - dimensions of privacy, 606–608
 - e-mail
 - access control, 636
 - anonymous, 637–638
 - interception, 636
 - mixmaster remailers, 637–638
 - monitoring, 637
 - overview, 635
 - remailers, 637–638
 - simple remailers, 637
 - spamming, 638
 - spoofing, 638
 - transmitting, 636
 - emerging technologies
 - consumer products, 639–640
 - electronic voting, 641–642
 - overview, 638–639
 - privacy issues, 640–641
 - RFID (radio frequency identification), 640
 - security issues, 640–641
 - Skype, 642
 - VoIP (Voice over IP), 642
 - government and
 - Council of Europe, 613
 - European Privacy Directive, 613
 - Icelandic DNA database, 351
 - principles and policies, 616–618
 - U.K. RIPA (Regulation of Investigatory Powers Act), 287
 - history of, 603
 - information collection, 606, 607
 - information disclosure, 606
 - information retention, 606
 - information security, 606
 - information usage, 606
 - informed consent, 607
 - loss of control, 607–608
 - monitoring, 606
 - ownership of data, 608
 - policy changes, 607
 - principles and policies

- access control, 618
- anonymity, 614
- audit trails, 618
- authentication, 617
- Convention 108, 613
- COPPA (Children's Online Privacy Protection Act), 610
- Council of Europe, 613
- data access risks, 617
- data anonymization, 618
- data left in place, 618
- data minimization, 617–618
- deceptive practices, 612–613
- defense methods, 617–618
- Directive 95/46/EC, 613
- e-Government Act of 2000, 611
- European Privacy Directive, 610
- Fair Credit Reporting Act, 610
- fair information, 609–610
- Fair Information Policies, 613–614
- Federal Educational Rights and Privacy Act, 610
- FTC (Federal Trade Commission), 610
- GLBA (Graham-Leach-Bliley Act), 610
- government policies, 616–618
- HIPAA (Health Insurance Portability and Accountability Act), 610
- identity theft, 618
- multiple identities, 614–616
- non-U.S., 613–614
- Privacy Act (5 USC 552a), 610
- protecting stored data, 609–610
- pseudonymity, 616
- quality, 618
- restricted usage, 618
- training, 618
- U.S. laws, 610–611
- Ware committee report, 610
- web site controls, commercial, 612–613
- web site controls, government, 611
- rights, ethical issues, 700–701
- RIPA (Regulation of Investigatory Powers Act), 287
- sensitive data, 604–605
- on the web
 - advertising, 628–629
 - adware, 633–634
 - contests, 629
 - cookies, 629–631
 - credit card payments, 627
 - drive-by installation, 634
 - highjackers, 632–633
 - keystroke loggers, 632
 - offers, 629
 - online environment, 626–627
 - online profiling, 631
 - payment schemes, 627
 - payments online, 627
 - precautions, 629–631
 - registration, 628
 - shopping, 634–635
 - site ownership, 628–629
 - spyware, 632–634
 - third-party ads, 628–629
 - third-party cookies, 630–631
 - web bugs, 631
- Privacy Act, 610, 684
- Privacy-preserving data mining, 624–626
- Private key encryption, 39–40. *See also* AES; DES; Symmetric encryption.
- Privilege. *See also* Permissions.
 - escalation, 147–148
 - limited, 244
- Probability, 534
- Probability password attacks, 224
- Probable plaintext attacks, 66
- Probable value disclosure, 339
- Problems, cryptographic, 722–723
- Procedure-oriented access control, 214–215
- Process activation, 276
- Process *versus* results organizations, 594
- Product cipher, DES, 733
- Product ciphers, 58
- Product ownership, 670–672
- Professional *versus* parochial organizations, 595
- Profile, of attackers, 401
- Programs
 - definition, 98. *See also* Application; Code; Software.
 - protection legal issues
 - computer objects, 659–662
 - copyright, 649–655, 660
 - documentation protection, 662
 - domain names, 662
 - firmware, 660–661
 - hardware, 660
 - object code software, 661
 - patents, 655–658, 660
 - reverse engineering, 658–659
 - source code software, 661–662
 - trade secrets, 658–659, 660
 - trademark, 662
 - URLs, 662
 - web content, 662
- Programs, security. *See also* Operating system security; Trusted systems.
 - controls. *See* Controls, software development.
 - cyber attacks, 101–102
 - errors, 100
 - failures, 100
 - faults, 100
 - fixing faults, 99–101
 - flaws
 - aliasing, 103
 - authentication, 103
 - boundary conditions, 103
 - definition, 101
 - domain errors, 103
 - identification, 103
 - logic errors, 103
 - overview, 101–103
 - serialization, 103
 - types of, 103
 - validation errors, 103
 - IEEE Standard 729, 100
 - intentional incidents. *See* Cyber attacks.
 - malicious code. *See also* Attacks, methods; Trapdoors; Viruses.
 - agents, 114
 - back doors. *See* Trapdoors.
 - history of, 113–114
 - implementation time, 116
 - interface illusions, 148–149
 - keystroke logging, 149
 - leaking information. *See* Covert channels.
 - logic bombs, 116
 - man-in-the-middle attacks, 149
 - potential for harm, 113
 - privilege escalation, 147–148
 - rabbits, 116
 - rootkit revealers, 146
 - rootkits, 145–147
 - Sony XCP (extended copy protection) rootkit, 145–147
 - spoofing, 148–149
 - threat assessment, 125
 - time bombs, 116
 - timing attacks, 150
 - Trojan horses, 116
 - types of, 114, 116–117

838 Index

- Programs, security (*continued*)
 - malicious code (*continued*)
 - worms, 116
 - zero day exploits, 116
 - nonmalicious errors
 - buffer overflows, 104–107
 - causes of failures, 112
 - combined flaws, 111
 - incomplete mediation, 107–109
 - synchronization, 109–111
 - time-of-check to time-of-use errors, 109–111
 - overview, 99
 - penetrate-and-patch technique, 100
 - unexpected behavior, 101–103
- Project leaders, security responsibilities, 514
- Proliferation of keys, 77
- Proof of program correctness, 177–178
- Propagation of errors, 64
- *-property (star property), 255–256
- Proprietary resources, ethical issues, 704
- Prosecuting computer crime, 682–683
- Protected objects, accessing
 - AS (authentication server), 213–214
 - access control matrix, 210–211
 - ACLs (access control lists), 208–210
 - capability, 210–213
 - directories, 205–208
 - domains, 211
 - erasing deleted files, 207
 - KDC (key distribution center), 213–214
 - Kerberos, 213–214
 - local name space, 211
 - procedure-oriented, 214–215
 - protection goals, 205
 - pseudonyms, 207–208
 - revocation of access, 206–207
 - role-based, 215
 - single sign-on, 214
 - TGS (ticket-granting server), 213–214
 - types of, 204–205
 - wild cards, 208–210
- Protecting stored data, 609–610
- Protection. *See* Controls; Defense methods.
- Protection profiles, 305
- Protection system commands, 258
- Protection systems, 260
- Protocols
 - destination unreachable, 438
 - echo, 438
 - encryption, 26
 - failures, 424
 - flaws, 414
 - networking, 385–393
 - ping, 438
 - SMTP (simple mail transport protocol), 392
 - SNMP (simple network management protocol), 392
 - source quench, 438
 - stack, 385
 - TCP/IP, 391–393
 - UDP (user datagram protocol), 391–392
- Provenzano, Bernardo, 45
- Proxies, 478–480
- Proxy firewall, 482–483
- PR/SM. *See* IBM, Processor Resources/System Manager.
- Pseudonymity, 616
- Pseudonyms, 207–208
- PSOS (Provably Secure Operating System), 284–287
- Public domain, 650
- Public key encryption. *See also* Asymmetric encryption; RSA.
 - characteristics, 77
 - definition, 39
 - flow diagram, 40
 - key proliferation, 77
 - purpose of, 76
- Public key infrastructure (PKI), 450–453
- Q
- Q0-Q7 quality levels, 301
- Quality
 - demands, 674–675
 - privacy principles and policies, 618
 - software, 678–679
- Quantifying security value
 - accurate data, 581
 - attack sources, 588
 - attack types, 587
 - comparability of categories, 587
 - consistent data, 581
 - cost of U.K. security incidents, 586
 - economic impact, 580, 586, 588
 - ISBS (Information Security Breaches Survey), 581, 585–586
 - justification data, 580–581
 - overview, 578–580
 - reliable data, 581
 - representative data, 586
 - respondent types, 587
 - security practices, 581, 585–586
 - timelines, 581
- Quantum cryptography
 - cryptography with photons, 775–776
 - implementation, 776–778
 - overview, 774
 - photon reception, 775
 - polarizing filters, 774–775
 - quantum physics, 774–775
- Quantum physics, 774–775
- Queries database, 321–323
- Query analysis, database inference, 349
- Rabbits, 116
- Radio frequency identification (RFID), 640
- RAND Corporation, 184, 609
- Random number sequences, 50
- Random sample control, 348–349
- Ranum, Marcus, 296
- RC2 cipher, 754–755
- RC4 cipher, 755–756
- RC5 cipher, 756
- RC6 algorithm, 749
- Read-only files, viruses, 131
- Realism, 550
- Rearrangement. *See* Permutation.
- Recipients, 38
- Reconnaissance, 404–408
- Records, database, 319, 321–323
- Recovery from backup, 332
- Redaction Tool, 271
- Redundancy
 - database reliability, 332
 - multilevel databases, 355
 - networks, 443
 - process comparison, 173
- Reference monitor, 275
- Refunds, 674
- Registration
 - copyright, 652
 - patents, 656–657
 - web privacy, 628
- Regression testing, 170
- Regulation, economics, 598–599
- Regulation of Investigatory Powers Act (RIPA), 287
- Relational operators, 254
- Relations, database, 321

- Relatively prime values, 762
- Release proliferation, 327
- Reliability
 - databases. *See also* Integrity.
 - commit flag, 330
 - committing updates, 330
 - concurrency, 333
 - consistency, 332, 333
 - correction codes, 332
 - data form checks, 334
 - definition, 329
 - error detection, 332
 - filters, 334
 - intent phase, 330
 - monitors, 334–335
 - operating system protection features, 329–330
 - patterns, 334
 - recovery from backup, 332
 - redundancy, 332
 - shadow fields, 332
 - shadow values, 331–332
 - state constraints, 334–335
 - transition constraints, 335
 - two-phase update, 330–332
- Religion, and ethics, 694
- Relocation, 194–195
- Relocation factor, 195
- Remailers, 637–638
- Remanence, magnetic, 270
- Repeaters, network, 383
- Replay attack, 422–423
- Reporting
 - computer crime, 21
 - program flaws, 675–679
- Reprocessing used data items, 18
- Request For Comment (RFC), 414
- Requirements checking, 295
- Requirements of novelty, 656
- Resident viruses, 114–116
- Resilience, network, 377
- Resorla, Eric, 598
- Respondent types, 587
- Response
 - to alarms, 489
 - CERT (Computer Emergency Response Team), 432
 - intrusion detection, 489
 - limited response suppression, 347–348
 - plans, 521–524
 - teams, 522–523
- Responsibility for security, 514–516
- Restricted content, 687–688
- Restricted usage, 618
- Results *versus* process organizations, 594
- Retina pattern authentication. *See* Biometrics.
- Return on investment (ROI), 577–578
- Reverse engineering, 658–659
- Reviews, design and code, 295
- Revocation of access, 206–207
- Revolving backups, 564
- RFC (Request For Comment), 414
- RFID (radio frequency identification), 640
- .rhosts file, 417–418
- Right, *versus* wrong. *See* Ethics.
- Rights of employees and employers
 - copyright ownership, 671
 - employee contracts, 672
 - licensed software, 671
 - patent ownership, 670–671
 - product ownership, 670–672
 - trade secrets, 672
 - work for hire, 671
- Rijmen, Vincent, 72
- Rijndael algorithm, 73, 749. *See also* AES.
- Ring of trust, 495
- RIPA (Regulation of Investigatory Powers Act), 287
- Risk analysis. *See also* Security plan.
 - classical probability, 534
 - Delphi approach, 533–534
 - FMEA (failure modes and effects analysis), 528
 - frequency probability, 534
 - FTA (fault tree analysis), 528
 - hazard analysis techniques, 528
 - HAZOP (hazard and operability studies), 528
 - IVAs (Integrated Vulnerability Assessments), 530
 - nature of risk, 525
 - probability, 534
 - pros and cons, 544–547
 - steps involved in
 - alternative steps, 526
 - asset identification, 526–527
 - control selection, 536–542
 - cost/benefit analysis, 544
 - expected loss computations, 535–536
 - exploitation estimation, 531–535
 - savings projections, 542–544
 - vulnerability identification, 527–531
 - subjective probability, 534
- VAM (Vulnerability Assessment and Mitigation), 527
- Risks
 - definition, 524
 - exposure, 524
 - impact, 524
 - leverage, 525
 - nature of, 525
 - prediction, 173–174. *See also* Risk analysis.
- Rituals, organizational, 593
- Rivest, Ron, 754
- Rivest-Shamir-Adelman (RSA) encryption. *See* RSA.
- .rlogin file, 417–418
- Rochefort, Joseph, 42
- Rogue access points, 408
- Rogue programs. *See* Malicious code.
- ROI (return on investment), 577–578
- Role-based access control, 215
- Rootkit revealers, 146
- Rootkits, 145–147
- Roundoff error, 3%145
- Router access controls, 464–466
- Routers, 387
- Routing concepts, 393
- RSA (Rivest-Shamir-Adelman) encryption
 - cryptanalysis of, 772
 - cryptographic challenges, 772–773
 - description, 769
 - Euler totient function, 769–771
 - Jacobi function, 771–772
 - key choice, 769
 - mathematical foundations, 769–771
 - overview, 77–78, 767–769
 - using the algorithm, 771–772
- Rule-based ethics, 697–698
- Rule-deontology, 697–698
- Rules of evidence, 680
- Rules of property, 679–680
- Rules set, firewall, 477
- Russian nuclear weapons, tracking, 140
- Salami attack, 19
- Salt extension, 228
- Sandbox, 435
- SAS Institute, 353
- Satellite networks
 - description, 384–385
 - eavesdropping, 411
 - wiretapping, 411
- Satisfiability, cryptography, 719
- S-boxes, 739, 740

840 Index

- Scanners
 - port, 405
 - virus, 124
- Schechter, Stuart, 598
- Schell, Roger, 178
- Schema, database, 320
- Schneier, Bruce, 599
- SCOMP, 191, 311
- Scrambling data. *See* Cryptography; Encryption.
- Screening router, 475–476, 480
- Script kiddies, 438
- Scripts, 434–435
- Secrecy. *See* Confidentiality; Privacy.
- Secret key encryption. *See* Symmetric encryption.
- Secure encryption algorithms, 60–62
- Secure Hash Algorithm (SHA), 80
- Secure Hash Standard (SHS), 80
- Secure MIME (S/MIME), 496
- Secure shell (SSH), 453
- Secure Sockets Layer (SSL), 453–454
- Security
 - as add-on, 312
 - associations, 454–455
 - audits, 180
 - availability, 10, 12
 - confidentiality, 10–11. *See also* Privacy.
 - definition, 1–2
 - features, 266–273
 - goals, 10–12
 - integrity, 10, 11–12
 - kernel, 274
 - money *versus* information, 2
 - physical. *See* Physical security.
 - versus* precision, databases, 339–341
 - software. *See* Operating system security; Programs, security.
 - targets, 306
 - value of. *See* Economics of cybersecurity.
 - weaknesses. *See* Vulnerabilities.
- Security models
 - Bell–La Padula, 254–256
 - Biba integrity, 256
 - command structure, 259
 - conditions, 259
 - definition, 243
 - Graham–Denning, 257–259
 - Harrison–Ruzzo–Ullman, 259–261
 - integrity *-property, 256
 - lattice model, 253–254
 - leaking access rights, 261
 - lower bound, 254
 - multilevel security, 253–257
 - partial ordering, 254
 - primitive operations, 259–260
 - *-property (star property), 255–256
 - protection system commands, 258
 - protection systems, 260
 - relational operators, 254
 - simple integrity property, 256
 - simple security property, 255–256
 - Take–Grant, 261–263
 - theoretical limitations of systems, 257–263
 - upper bound, 254
 - uses for, 252–253
 - write-down, 256
- Security parameter index (SPI), 455
- Security plan. *See also* Risk analysis; Security policies.
 - business continuity plan, 518–521
 - commitment to, 517–518
 - constraints, 512–514
 - contents of, 510–516
 - continuing attention, 516
 - controls, 512–514
 - current status, 511–512
 - definition, 509
 - framework for, 511
 - history of, 509
 - incident response plans, 521–524
 - incident response teams, 522–523
 - OCTAVE methodology, 511
 - policy statement, 510–511
 - requirements, 512–514
 - responsibilities, 514–516
 - team members, 517
 - timetable, 516
- Security policies. *See also* Policies; Principles; Security plan.
 - access triples, 250
 - audience, 547–548
 - beneficiaries, 548
 - characteristics of, 549–550
 - Chinese Wall, 251–252
 - Clark–Wilson commercial, 250
 - classification, 248
 - commercial, 248–250
 - compartments, 246
 - constrained data items, 250
 - contents, 548–549
 - definition, 243, 245, 547
 - dominance, 248
 - durability, 550
 - economics of, 551
 - examples
 - data sensitivity, 551
 - DOE (Department of Energy) policy, 551–552
 - government e-mail, 553
 - Internet policy, 552–553
 - hierarchical, 248
 - issues, 554–555
 - kneed-to-know, 246
 - military, 246–248
 - nonhierarchical, 248
 - owners, 548
 - purpose, 547
 - realism, 550
 - separation of duty, 250–251
 - transformation procedures, 250
 - usefulness, 550
 - users, 547–548
 - well-formed transactions, 250
- Segment address table, 199
- Segment address translation, 199
- Segmentation
 - combined wit paging, 203–204
 - networks, 442–443
 - overview, 199–202
- Selective backups, 564
- Selective protection. *See* Tagged architecture.
- Self-healing code, 184
- Self-stabilizing code, 184
- Selling correct software, 673–674
- Semiweak keys, 745–746
- Senders, 38
- Sendmail* flaw, 135–136
- Sensitive data
 - data mining, 368
 - databases
 - access acceptability, 337–338
 - access decisions, 337–338
 - authenticity, 338
 - bounds disclosure, 338
 - characteristics of, 336–337
 - data availability, 337
 - definition, 335
 - disclosures, types of, 338–339
 - exact data disclosure, 338
 - existence disclosure, 339
 - negative result disclosure, 339
 - overview, 335–337
 - probable value disclosure, 339
 - security *versus* precision, 339–341
 - overview, 604–605
- Sensitivity lock, 359
- Separation
 - of duty, 250–251
 - multilevel databases, 356–359
 - overview, 190–193

- principles of trusted systems, 279–280
- of privilege, 266
- Serialization error, 103
- Serpent algorithm, 749
- Servers, network, 378–379
- Server-side includes, 427
- Service, denial of. *See* DDoS; DoS.
- Service Set Identifier (SSID), 466–467
- Session hijacking, 419–420. *See also* Impersonation.
- Sessions, network, 429
- Set userid (SUID), 218–219
- SHA (Secure Hash Algorithm), 80
- Shadow fields, 332
- Shadow values, 331–332
- Shakespeare, authorship debate, 353
- Shannon, Claude, 60
- Shape, networks, 381–382
- Shared resource matrix, 157–158
- Sharing
 - access, 323
 - enforced, 267
 - network threat, 397
 - session keys, 454
- Shell backups, 565
- Shift row, 751–752
- Shneiderman, Ben, 515
- Shopping online, privacy, 634–635
- Shredding paper data, 562
- SHS (Secure Hash Standard), 80
- Signaling through images. *See* Steganography.
- Signature-based intrusion detection, 485, 486
- Signatures, viruses
 - definition, 124
 - execution patterns, 125–126
 - polymorphism, 127–128
 - scanners, 124
 - storage patterns, 125
 - transmission patterns, 126–127
- Signed code, 456–457
- Silken codes case study, 41
- Simple integrity property, 256
- Simple knapsacks, 760–761, 763
- Simple remailers, 637
- Simple security property, 255–256
- Single point of failure, networks, 377, 443–444
- Single sign-on, 214, 232
- Size, networks, 381–382
- Skype, 642
- Smart cards, 560
- S/MIME (Secure MIME), 496
- SMTP (simple mail transport protocol), 392
- Smurf attack, 428–429
- SNMP (simple network management protocol), 392
- Social engineering, 405–406
- SOE (Special Operations Executive), 48
- Software. *See also* Application; Code; Programs.
 - access control, 15
 - configuration management, 15
 - controls. *See* Controls, software development.
 - failure, legal issues
 - full disclosure, 675–676
 - overview, 673
 - quality demands, 674–675
 - quality software, 678–679
 - refunds, 674
 - reporting flaws, 675–679
 - selling correct software, 673–674
 - user interests, 676
 - vendor interests, 676
 - warranty of cyberworthiness, 675
 - malicious modification, 15–16
 - security. *See* Operating system security; Programs, security.
- Sony XCP (extended copy protection) rootkit, 145–147
- Source code, legal issues, 661–662
- Source quench protocol, 438
- Soviet Union codes, 59
- Spafford, Eugene, 296
- Spam, 598–599, 638
- Special Operations Executive (SOE), 48
- SPI (security parameter index), 455
- Spikes, electrical, 558
- Spoofing. *See also* Impersonation.
 - cryptographic protection, 462–463
 - e-mail, 638
 - interface illusions, 148–149
 - network vulnerability, 418
 - trusted path, 270–271
- “Spray paint” lock, 357–359
- Spying, 402, 683
- Spyware, 632–634
- SSH (secure shell), 453
- SSID (Service Set Identifier), 466–467
- SSL (Secure Sockets Layer), 453–454
- Stack pointer, 106
- Standards. *See also* Policies; Principles.
 - IEEE Standard 729, 100
 - process, 180–181
 - software development, 178, 180
- Star property (*-property), 255–256
- State constraints, 334–335
- State-based intrusion detection, 487
- Stateful inspection firewalls, 477–478
- Static code analysis, 174
- Statistical analysis, intrusion detection, 486
- Statistical inference attacks, 347
- Statistics, computer crime, 21
- Status accounting, 176
- Statutes, 667, 683–686. *See also* Laws.
- Stealth mode intrusion detection, 487–488
- Steganography, 159–160
- Stevens, Thomas, 28
- Stoll, Cliff, 137, 468
- Stopford, Charlie, 621
- Storage channels, 152–155
- Stream ciphers, 62–63
- Strong authentication, 459–464
- Subjective probability, 534
- Subschema, database, 320
- Substitution, symmetric encryption, 730
- Substitution ciphers
 - book ciphers, 52–54
 - Caesar cipher, 44–46
 - complexity, 47–48
 - cryptanalysis, 48–49
 - cryptographer’s dilemma, 49
 - keys, 47
 - one-time pads, 50–54
 - permutations, 46–47
 - random number sequences, 50
 - Vernam cipher, 50–52
 - Vignère tableau, 50, 53
- Substitution cycle, DES, 734
- Substitutions, 43
- SUID (set userid), 218–219
- Sum attacks, 343
- Summer Study on Database Security, 357
- Superincreasing knapsacks, 760–761, 763–764
- Suppression control, 347
- Surge suppressors, 558–559
- Surges, electrical, 558
- Surrounding viruses, 118–119
- Surveys of security
 - Australian Computer Crime and Security, 582

842 Index

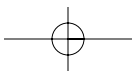
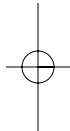
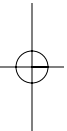
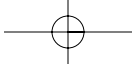
- Surveys of security (*continued*)
 CSI/FBI Computer Crime and Security, 582
 Deloitte and Touche Tohmatsu Global Security, 582–583
 Ernst and Young Global Information Security, 583–584
 IC3 (Internet Crime Complaint Center), 584
 Information Data Protection, 584–585
 sources for, 585
 Swallow, William, 404
 Symantec, 125, 147–148
 Symbols, organizational, 592
 Symmetric encryption. *See also* AES; DES; Private key encryption.
 algorithms, 62
 authentication, 62
 confusion, 730
 cryptographic challenges, 756–757
 definition, 39
 diffusion, 730
 flow diagram, 40
 key distribution, 62
 key management, 62
 overview, 62
 permutation, 730
 problems with, 730–732
 RC2 cipher, 754–755
 RC4 cipher, 755–756
 RC5 cipher, 756
 substitution, 730
 SYN flood, 429
 Synchronization, 267
 SYN_RECV connections, 429
 System complexity, 397
 System security policy. *See* Security policies.
 System testing, 295. *See also* Testing.
- Tagged architecture, 196–199
 Take-Grant security model, 261–263
 Tapping wires, 408–414, 416
 Target of evaluation (TOE), 303
 Target phrases, 301
 TCB (trusted computing base), 245, 275–279
 TCP (Transmission Control Protocol), 391–392
 TCP/IP protocol, 391–393
 TCSEC (Trusted Computer System Evaluation Criteria), 297–300, 304
 Teardrop attacks, 430
- Telang, Rahul, 598
 Teleological theory, 696–697
 Telnet, 392, 477, 525
 Tempest program, 562–563
 Temporal Key Integrity Program (TKIP), 467–468
 Temporal separation, 191, 279–280
 Temporary permissions, 218–219
 Ten Commandments of Computer Ethics, 713
- Terrorists
 computer criminals, 23–24
 cyberterrorism, 403
 screening airline passengers, 615
- Testing code
 acceptance, 170–171
 assuring trusted systems, 290–291
 black-box, 170
 clear-box, 170–171
 debugging, 142
 formal methods, 179
 independent, 172
 installation, 170
 integration, 142, 170
 peer reviews, 165–168
 penetration, 172, 177, 291
 performance, 170
 regression, 170
 reviews, 168, 295
 tiger team, 172, 177, 291
 unit, 142, 170
 walk-throughs, 166
- Text analysis, computerized, 353
 TFN (Tribal Flood Network), 401, 432
 TFN2K, 401, 432
 TGS (ticket-granting server), 213–214
 The Internet, 395–396
 Theft of service, 408, 412
 Theft prevention, 559–561
 Theorem provers, 292
 Theoretical limitations of systems, 257–263
 Third-party ads, 628–629
 Third-party cookies, 630–631
 Thompson, Ken, 136
- Threats
 definition, 6
 e-mail, 491
 fabrications, 7–8
 interceptions, 7–8
 interruptions, 7–8
 modifications, 7–8
 to networks. *See* Networks, threats.
 types of, 7–8
versus vulnerabilities, 6
- Ticket-granting server (TGS), 213–214
 Tickets, networks, 461
 Tiger team testing, 172, 177, 291
 Tight *versus* loose organizational control, 595
 Time bombs, 116
 Time-dependent value of information, 664–665
 Timelines, quantifying security value, 581
 Time-of-check to time-of-use flaws, 288
 Timestamps, 463
 Timetable for security planning, 516
 Timing attacks, 150
 Timing channels, 155–156
 TKIP (Temporal Key Integrity Program), 467–468
 TLS (transport layer security), 453–454
 TOE (target of evaluation), 303
 Tokens, password, 459–460
 Top-level domain, 393
 Topography, networks, 381–382
 Torch Concepts, 612–613
 Tort law, 667–668
 Totient function, 769–771
 Tracker attacks, 345–346
 Tracking Russian nuclear weapons, 140
 Trade secrets, 658–659, 660, 672
 Trademark, 662
 Traffic flow analysis, 422
 Traffic flow security, 469–470
 Traffic redirection, 430
 Training, privacy principles and policies, 618
 Transferability, evaluating, 303
 Transferring models, 589–590
 Transformation procedures, 250
 Transient viruses, 114
 Transition constraints, 335
 Transmission Control Protocol (TCP), 391–392
 Transmission failure, 427
 Transmission medium, 38
 Transmitting e-mail, 636
 Transport layer security (TLS), 453–454
 Transposition. *See* Permutation.
- Trapdoors
 causes of, 144
 definition, 16, 116
 error checking, 142–143
 examples, 142–144
 integration testing, 142


- undefined opcodes, 143–144
- unit testing, 142
- Tribal Flood Network (TFN), 401, 432
- Triggering viruses, 117–119
- Trigrams, 56–57
- Trin00, 432
- Triple DES, 71
- Tripwire, 488
- Trojan horses, 16, 116
- Trust. *See also* Trusted systems, design principles.
 - definition, 243
 - as economic issue, 592–593
 - threshold, 85
 - through common respected individual, 85–87
 - without a single hierarchy, 89–91
- Trusted authentication, 418
- Trusted Computer System Evaluation Criteria (TCSEC), 297–300, 304
- Trusted computing base (TCB), 245, 275–279
- Trusted front-end, 360–361
- Trusted path, 270–271
- Trusted processes, 245
- Trusted product, 245
- Trusted software, 245
- Trusted systems. *See also* Operating system security; Programs, security.
 - appropriate confidence level, 244
 - characteristics of, 244
 - definition, 242
 - design principles. *See also* Trust.
 - access control, 266
 - accountability, 272
 - allocation of general objects, 266–267
 - assurance, 268
 - audit, 272
 - audit log reduction, 272–273
 - complete mediation, 265–266, 270
 - cryptographic separation, 279–280
 - DAC (discretionary access control), 269–270
 - definition, 243
 - ease of use, 266
 - economy of mechanism, 265
 - enforced sharing, 267
 - execution domain switching, 276
 - guaranteed fair service, 267
 - hierarchical structuring, 285–287
 - identification, 269
 - importance of, 264
 - intrusion detection, 273
 - I/O operation, 277
 - isolation, 279–280
 - kernelized design, 274–279
 - layered trust, 283–287
 - least common mechanism, 266
 - least privilege, 265
 - logical separation, 279–280
 - MAC (mandatory access control), 269–270
 - magnetic remanence, 270
 - memory protection, 266, 277
 - multiple virtual memory spaces, 281
 - object reuse, 270
 - open design, 265
 - operating system data protection, 267–268
 - permission based, 266
 - physical separation, 279–280
 - process activation, 276
 - reference monitor, 275
 - security features, 266–273
 - separation, 279–280
 - separation of privilege, 266
 - synchronization, 267
 - system elements, 265–266
 - TCB (trusted computing base), 275–279
 - temporal separation, 279–280
 - trusted path, 270–271
 - user authentication, 266, 269
 - virtual machines, 282–283
 - virtual memory, 282
 - virtualization, 280–283
 - enforcement of integrity, 244
 - functional correctness, 244
 - limited privilege, 244
 - overview, 243–245
 - qualities of, 245
 - versus* secure, 244
 - security models
 - Bell–La Padula, 254–256
 - Biba integrity, 256
 - command structure, 259
 - conditions, 259
 - definition, 243
 - Graham–Denning, 257–259
 - Harrison–Ruzzo–Ullman, 259–261
 - integrity *-property, 256
 - lattice model, 253–254
 - leaking access rights, 261
 - lower bound, 254
 - multilevel security, 253–257
- partial ordering, 254
- primitive operations, 259–260
- *-property (star property), 255–256
- protection system commands, 258
- protection systems, 260
- relational operators, 254
- simple integrity property, 256
- simple security property, 255–256
- Take–Grant, 261–263
- theoretical limitations of systems, 257–263
- upper bound, 254
- uses for, 252–253
- write-down, 256
- security policies
 - access triples, 250
 - Chinese Wall, 251–252
 - Clark–Wilson commercial, 250
 - classification, 248
 - commercial, 248–250
 - compartments, 246
 - constrained data items, 250
 - definition, 243, 245
 - dominance, 248
 - hierarchical, 248
 - knead-to-know, 246
 - military, 246–248
 - nonhierarchical, 248
 - separation of duty, 250–251
 - transformation procedures, 250
 - well-formed transactions, 250
- trust, definition, 243
- underpinnings of, 242–243
- Trusted systems, assurance evaluation
 - action phrases, 301
 - British criteria, 301–302
 - claims language, 301
 - CLEFs (Commercial Licensed Evaluation Facilities), 302
 - Combined Federal Criteria*, 304–307
 - Common Criteria, 307–308
 - comparability, 303
 - criteria development, 309–311
 - effectiveness, 303
 - emphatic assertion, 311
 - Europe, 300–303
 - German Green Book, 300–301
 - ITSEC (Information Technology Security Evaluation Criteria), 300–303, 303–304

844 Index

- Trusted systems, assurance
(*continued*)
evaluation(*continued*)
marketability, 303
overview, 296–297
process description, 309
protection profiles, 305
security, as add-on, 312
security targets, 306
summary of criteria, 308–311
target phrases, 301
TCSEC (Trusted Computer System Evaluation Criteria), 297–300, 304
TOE (target of evaluation), 303
transferability, 303
United States, 297–300, 304–307
- flaws
ambiguous access policies, 288
exploitation examples, 289–290
incomplete mediation, 288–289
known vulnerabilities, 288–289
time-of-check to time-of-use flaws, 288
typical flaws, 288–290
user interface vulnerability, 288
- methods
formal verification, 292–294
penetration testing, 291
requirements checking, 295
reviews, design and code, 295
system testing, 295
testing, 290–291
theorem provers, 292
validation, 295
open source, 295–296
overview, 287–288
- Tunnels, network encryption, 449–450
Turing machines, 721
12-step password attacks, 226
Two-factor authentication, 222
Twofish algorithm, 749
Two-phase update, 330–332
- UCC (Uniform Commercial Code), 674–675
UDP (user datagram protocol), 391–392
Unauthorized access, 559
Undefined opcodes, 143–144
Unexpected behavior, 101–103
Uninterruptible power supply (UPS), 558
Unit testing, 142, 170. *See also* Testing.
- United Kingdom
cost of security incidents, 586
RIPA (Regulation of Investigatory Powers Act), 287
- United States
California Breach Act, 686
CAN SPAM Act, 685–686
Census Bureau, 341
Computer Fraud and Abuse Act, 683
Economic Espionage Act, 683
Electronic Communications Privacy Act, 684
Electronic Funds Transfer Act, 683
evaluating trusted systems, 297–300, 304–307
Freedom of Information Act, 684
GLBA (Graham-Leach-Bliley Act), 684
government
audit data overload, 273
security report card, 29
HIPAA (Health Insurance Portability and Accountability Act), 684–685
laws. *See* Laws, U.S..
Patriot Act, 685
Privacy Act, 684
privacy principles and policies, 610–611
Universality of ethics, 694–695
Universities, as prime targets, 9
Unknown path, 399
Unknown perimeter, 398–399
Unshielded twisted pair (UTP) cable, 382
Upper bound, 254
UPS (uninterruptible power supply), 558
URLs, legal issues, 662
Usage controls on cryptography, 688–690
Use of computer services, ethical issues, 698–699
Usefulness, 550
User authentication. *See also* Authentication.
additional authentication information, 221–222
biometrics, 219–220, 234–236
challenge-response system, 231–232, 233–234
cookies, 236
databases, 328
flaws, 233–234
versus identification, 234–235
impersonating trusted systems, 236
impersonation of login, 233–234
multifactor authentication, 222
one-time passwords, 231–232
overview, 219
password attacks, 222–229
password selection criteria, 229–231
passwords as authenticators, 221
phishing, 236
principles of trusted systems, 266, 269
process description, 232–234
single sign-on, 232
two-factor authentication, 222
User datagram protocol (UDP), 391–392
User interests, 676
User interface vulnerability, 288
User-group-world protection, 218
Users
human fallibility case study, 67
security policies, 547–548
security responsibilities, 514
Utilitarianism, 697
UTP (unshielded twisted pair) cable, 382
- V.A. (Veterans Administration), 14
Validation, 295
Validation errors, 103
Value of data, 681
Value of security. *See* Economics of cybersecurity.
VAM (Vulnerability Assessment and Mitigation), 527, 537–542
Vandalism, 559–561
Varian, Hal, 597
Vendor interests, 676
Verifying program code. *See* Testing code.
Verisign, 22, 229, 457
Vernam, Gilbert, 50
Vernam cipher, 50–52
Version proliferation, databases, 327
Views, multilevel databases, 363–366
Vignère tableau, 50, 53
Virtual machines, 282–283
Virtual memory, 282
Virtual private networks (VPNs), 449–450
Virtualization, 280–283
Virus scanners, 124

- Viruses. *See also* Malicious code.
 appended to a program, 118
 application programs, 124
 attachment, 117–119
 benign, 132–133
 boot sector, 122
 bootstrapping, 122
 Brain, 133–134
 Code Red, 137–139
 cookies, 140
 defense methods, 129–131
 definition, 16
 document, 119–120
 effects and causes, 127–128
 e-mail attachment, 117–118
 gaining control, 120–121
 homes for, 121–124, 131–132
 infecting hardware, 132
 integrated, 119
 Internet worm, 134–137
 libraries, 124
 memory-resident, 123–124
 misconceptions, 131
 one-time execution, 122
 platform limitations, 131
 qualities of, 121
 in read-only files, 131
 resident, 114–116
 signatures
 definition, 124
 execution patterns, 125–126
 polymorphism, 127–128
 scanners, 124
 storage patterns, 125
 transmission patterns, 126–127
 source of, 128–129
 spreading media, 132
 surrounding a program, 118–119
 surviving power off, 132
 transient, 114
 triggering, 117–119
 web bugs, 139–141
- Voice recognition authentication. *See* Biometrics.
- VoIP (Voice over IP), 642
- Voting, electronic, 641–642
- VPNs (virtual private networks), 449–450
- Vulnerabilities. *See also* Attacks; *specific vulnerabilities*.
 data, 16–19
 definition, 6
 hardware, 13–15
 laptop computers, 14–15
 mapping to controls, 537
 network threat, 397–399, 438
 risk analysis, 527–531
 software, 15–16
versus threats, 6
- Vulnerability Assessment and Mitigation (VAM), 527, 537–542
- Walk-through, code, 166
- WAN (wide area network), 395
- War driving, 408
- Ware, Willis, 609–610
- Ware committee report, 610
- Warranty of cyberworthiness, 675
- Watermarking, 93–94
- Weak keys, DES, 745
- Weak passwords, 224–227
- Weakest link principle, 29–30
- Weakest point, 5
- Weakness. *See* Risk analysis; Risks; Threats; Vulnerabilities.
- Weaknesses, 66–67
- Web bugs, 139–141, 631
- Web servers, escape-character attack, 434–435
- Web sites. *See also* Internet.
 content, legal issues, 662
 defacing, 424–425
 posting privacy policies, 611
 privacy
 advertising, 628–629
 adware, 633–634
 contests, 629
 cookies, 629–631
 credit card payments, 627
 drive-by installation, 634
 highjackers, 632–633
 keystroke loggers, 632
 offers, 629
 online environment, 626–627
 online profiling, 631
 payment schemes, 627
 payments online, 627
 precautions, 629–631
 registration, 628
 shopping, 634–635
 site ownership, 628–629
 spyware, 632–634
 third-party ads, 628–629
 third-party cookies, 630–631
 web bugs, 631
 privacy controls, commercial, 612–613
 privacy controls, government, 611
 tracking usage, 396
 vulnerabilities, 424–427
- Well-formed transactions, 250
- Well-known authentication, 417–418
- WEP (wired equivalent privacy), 467
- White-box testing, 170–171
- Wide area network (WAN), 395
- WiFi. *See* Wireless.
- WiFi Protected Access (WPA), 467–468
- Wild cards, 208–210
- Wilshire Associates, e-mail theft, 28
- Windows, distributed authentication, 398
- Windows, multilevel databases, 363–366. *See also* Views.
- Wireless networks
 description, 383
 eavesdropping, 411–413
 interception, 412
 rogue access points, 408
 security, 466–468
 theft of service, 408, 412
 vulnerabilities, 413
 vulnerabilities, case study, 413
 war driving, 408
 wiretapping, 411–413
- Wiretapping, 408–414, 416
- Woods, Alan, 452
- Word, deleting text, 271
- Work for hire, 671
- Workstations, 379
- World War II case studies
 ASINTOER code, 59
 Enigma code machine, 67
 Japanese codes, 42
 poem codes, 48
 silken codes, 41
 Soviet Union codes, 59
- Worms. *See also* Malicious code; Viruses.
 Code Red, 137–139, 675–676
 definition, 116
 Internet worm, 134–137
- WPA (WiFi Protected Access), 467–468
- Write-down, 256
- XCP (extended copy protection) rootkit, 145–147
- Xu, Hao, 598
- Zero day exploits, 116
- Zimmerman, Phil, 691
- Zombie, 431–432





Register Your Book

at www.awprofessional.com/register

You may be eligible to receive:

- Advance notice of forthcoming editions of the book
- Related book recommendations
- Chapter excerpts and supplements of forthcoming titles
- Information about special contests and promotions throughout the year
- Notices and reminders about author appearances, tradeshow, and online chats with special guests

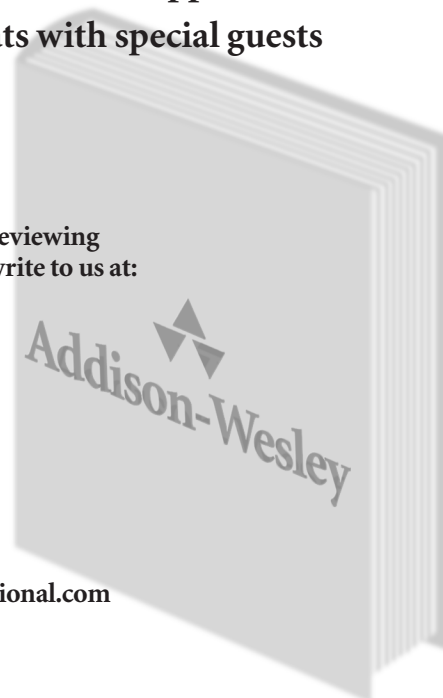


Contact us

If you are interested in writing a book or reviewing manuscripts prior to publication, please write to us at:

Editorial Department
Addison-Wesley Professional
75 Arlington Street, Suite 300
Boston, MA 02116 USA
Email: AWPro@aw.com

Visit us on the Web: <http://www.awprofessional.com>





THIS BOOK IS SAFARI ENABLED

INCLUDES FREE 45-DAY ACCESS TO THE ONLINE EDITION

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

TO GAIN 45-DAY SAFARI ENABLED ACCESS TO THIS BOOK:

- Go to <http://www.prenhallprofessional.com/safarienabled>
- Complete the brief registration form
- Enter the coupon code found in the front of this book on the "Copyright" page

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.



Wouldn't it be great
if the world's leading technical
publishers joined forces to deliver
their best tech books in a common
digital reference platform?

They have. Introducing
InformIT Online Books
powered by Safari.

■ **Specific answers to specific questions.**

InformIT Online Books' powerful search engine gives you relevance-ranked results in a matter of seconds.

■ **Immediate results.**

With InformIT Online Books, you can select the book you want and view the chapter or section you need immediately.

■ **Cut, paste and annotate.**

Paste code to save time and eliminate typographical errors. Make notes on the material you find useful and choose whether or not to share them with your work group.

■ **Customized for your enterprise.**

Customize a library for you, your department or your entire organization. You only pay for what you need.

Get your first 14 days FREE!

For a limited time, InformIT Online Books is offering its members a 10 book subscription risk-free for 14 days. Visit <http://www.informit.com/online-books> for details.



POWERED BY
Safari
TECH BOOKS ONLINE

informIT
Online Books

informit.com/onlinebooks



