

# INDEX

Note: Page numbers followed by *f* and *t* indicate figures and tables respectively

723025

- A  
Abbreviations, for large numbers, 193t  
Abnagle, Frank, 14  
Above Top Secret classification, 758  
Abstraction, I/O system and, 212–213  
Acceptable use policy, 42, 564  
Access control, 221, 222  
effectiveness of encryption and, 377t  
pattern-based, 74  
strategies for, 71–76  
islands, 71  
puzzles and patterns, 71, 72–75  
vaults, 71, 72  
Access control lists, 146–149  
Macintosh OS-X, 146–149  
Microsoft Windows, 150–159  
Access matrix, 80–81, 118  
for processes, 81t  
for shared data section, 82t  
Access rights, 81  
determining, for Microsoft Windows ACLs, 152–153  
directory, 99–101  
to executable files, 120f  
file ownership and, 97–99  
managing, 117–119  
to personal files, 120f  
Access rules, ambiguous, 144t  
Access to Internet site, 614  
Accountability, companies, secrecy, and, 558  
Accreditation. *See* Certification and accreditation  
Acknowledgment numbers, TCP and, 518  
Acknowledgment protocol (ACK), 445–446, 446f, 447, 448f, 516  
ACLs. *See* Access control lists  
Acoustical signals, TEMPEST problem and, 787  
Acronyms, memory size names and, 192, 193t  
Active attacks, 27, 606, 607f  
Active Directory, Kerberos protocol and, 591  
Active Server Pages, 725  
Active Server Pages Extended, 725  
Active tokens, search space and, 258–259  
ActiveX, 725  
Adams, Carlisle, 309  
Addressing  
in tree network, 478  
web pages, 703–706  
default web pages, 706  
email URLs, 704  
hosts and authorities, 704–705  
path name, 705  
Address Resolution Protocol, 485, 495–496  
ARP cache, 495–496. *See also* ARP cache  
command to display ARP cache for, 496f  
packet contents and, 496f  
Address scope, 498  
reachability dependent on, 499f  
Address variables  
memory sizes and, 192–194  
size of, 192  
Adleman, Len, 344  
Administrative groups, basic file sharing on Windows and, 138–139  
Administrative users, Least Privilege and, 139–142  
Administrators, 23, 112  
separation of duty and, 579  
Admissible evidence, 175  
Advanced Encryption Standard, 292, 309, 321–322, 379  
choosing encryption algorithm and, 389  
development of, 384  
encrypting disk data with, 404f  
finalists, 384–385  
flexibility of RC4 *vs.* flexibility of, 381  
key sizes and average cracking times, 293t  
untrustworthy encryption and, 408  
Advanced Research Projects Agency, 482  
Advanced Technology Attachment, 52  
Advance fee fraud, 672  
Adversaries, 750  
AES. *See* Advanced Encryption Standard

- agent.btz worm, 429–430  
 Aggregation  
   challenge of secrecy and, 751  
   database security and, 734  
   inference and, 734  
 AIS. *See* Automated information systems  
 Alexander, Christopher, 586  
 Algorithms, 281  
   encryption, qualities of, 387–389  
   private label, cautionary note, 389  
   RC4, leaking and cracking, 386, 388  
 Aliases, website, 526  
 Altavista, 708  
 AM. *See* Amplitude modulation  
 Amazon.com, 729  
 American Bankers Association, 621  
 American Cancer Society, email hoaxes and, 679  
 American National Standards Institute, 382  
 Amplification attacks, 534  
 Amplitude, 442f  
 Amplitude modulation, 443  
 AM radio, 443–444  
 AM wave form, 443f  
 Analog-based digital networks, 545–546  
 Analog broadcast networks, 545  
 Analog signals, 440  
 Analog two-way radios, 547–548  
 Analysts, training and expertise for, 572  
 Anderson, Ross, 384  
 Anonymity, client, 743–744  
 Anonymous Diffie-Helman shared secret, creating, 625, 625f  
 Anonymous proxies, 744  
 ANSI. *See* American National Standards Institute  
 ANSI X9.17, 623  
   wrapping new keys for distribution and, 621, 622f  
 Antihacking laws, 41  
 Anti-tamper, working key storage and, 414  
 Antivirus software, 8  
 Apache, 703  
 API. *See* Application programming interface  
 Apple II, 103  
 Apple Macintosh OS-X, 57  
   choosing users for group in, 149f  
 Apple Mail, on OS-X, 663  
 Apple's HFS Plus, 205–206  
   volume format, 205f  
 Apple's Safari, 703  
 Application filtering, 683, 685, 685f  
 Application layer, OSI protocol model, 461  
 Application layer encryption with S/MIME or PGP, 612  
   in transit, 628f  
 Application programming interface, 210  
 Application programs, 103, 657  
 Application protocols, 457, 657  
 Application proxy, 685  
 Application transparency, 608  
   end-to-end crypto and, 635–636  
   IPsec and, 610  
 apps, 2–3  
 Arm, hard drive, 182  
 Armed robbery, 29  
 Armstrong, Edwin, 443  
 ARP. *See* Address Resolution Protocol  
 ARPA. *See* Advanced Research Projects Agency  
 ARPANET, 482, 483, 514, 528, 636, 658, 680  
   IMP, 486  
   protecting, 486–487  
 ARP cache  
   description of, 495–496  
   displaying, command for, 496f  
 ARP request, displayed in Wireshark, 504f  
 ARP response, displayed in Wireshark, 505f  
*Art of Deception, The* (Mitnick), 563  
 AS. *See* Autonomous systems  
 AS-400, 118  
 ASCII character set, 241  
 ASCII email, 660  
 ASPs. *See* Active Server Pages  
 ASPX. *See* Active Server Pages Extended  
 Assessment, 571  
 Assets, identifying, 15  
 Assured pipeline, 369  
 Asymmetric cryptography, 337  
 Asymmetric encryption algorithm, 339f  
 Asynchronous links, synchronous links *vs.*, 441  
 Asynchronous transfer mode services, 548  
 ATA. *See* Advanced Technology Attachment  
 Atlas computer, 77  
 ATM cards, 252  
 ATM services. *See* Asynchronous transfer mode services  
 Atomic bomb, development of, 750  
 Attack damage, 19  
 Attacker, 12  
 Attack matrix, 27–29, 28f  
 Attacks  
   calculating impact of, 34–35, 34t  
   defined, 12  
   detecting, by reviewing logs, 164  
 Attack strategy, low hanging fruit, 228–229  
 Attenuation, TEMPEST problem and, 787  
 Attribute entries, NT file system and, 207  
 Auditing, 570. *See also* Security audits  
   enterprises and, 584  
 Audit logs, audits of, 571  
 Auditors, training and expertise for, 572  
 Audits, 564  
 Audit trail, 160  
 AUP. *See* Acceptable use policy  
 Authenticated email, 670–671  
 Authenticated software updates, 367–369  
 Authentication, 221–273  
   base secret and, 223

- basic external attacks  
on, 227f  
biometric, 261–265  
database thefts, 229–231  
digest, 255–256  
direct, 588–589  
disk-based, 417–418  
enterprise network, 585–594  
of hard drive, 179  
indirect, 590–593  
    properties of, 593  
local, 587–588  
objective of, 223  
off-line, 593–594  
performing, steps in, 222, 222f  
with personal information,  
    230–231  
preboot, 417–418  
to protect computer resources,  
    222f  
redirected, 592–593  
risks and, 225–228  
security services and, 86  
server, 714–719  
service-based, 591–592  
techniques, examples of, 224t  
threats and, 225  
ticket-based, 591  
Authentication database, 223  
Authentication factors, 223–225  
three-factor authentication,  
    225  
two-factor authentication,  
    224–225  
types of, 223–224  
Authentication Header, within  
    IPsec, 639  
Authentication policy, 265–273  
    location and, 267  
    password selection and  
        handling, 271–273  
        password managers, 273  
        simple passwords, 272  
    strong but memorable  
        passwords, 272–273  
    strongest passwords, 273  
strong and extreme threat  
    environments  
constructing policy, 269–270  
    passwords alone for strong  
        threats, 268  
    passwords plus biometrics,  
        269, 270t  
    passwords plus tokens, 269,  
        271t  
    strong threats, risks  
        from, 266  
weak threat environments  
    household policy, 267, 267t  
    workplace policy:  
        passwords and tokens,  
            268  
        workplace policy:  
            passwords only, 268  
    weak threats, risks  
        from, 266  
Authentication server, 586  
Authentication tokens, 251–261  
    active, 252  
    challenge-response, 252,  
        255–256  
    denial of service, 260, 261t  
    one-time password tokens,  
        252, 257–259  
    passive, 252–253  
vulnerabilities of, 260–261,  
    261f, 261t  
clone credential, 260, 261t  
clone or borrow the  
    credential, 260, 261t  
denial of service, 260, 261t  
retrieve from backup, 260,  
    261t  
sniff credential, 260, 261t  
trial and error guessing,  
    260, 261t  
Authenticity, 607  
Authorities, email URLs  
    and, 704–705, 705f  
Automated information  
    systems, 773  
Automated teller machine, 224  
Automatic Encryption, 614  
Automobiles, computer-  
    controlled, security  
    vulnerabilities with, 3  
Autonomous systems, 488–489  
Availability  
    security services and, 9–11, 86  
    Web, 741–743  
Average attack space, 247, 259  
Average cracking time, 292  
B  
b (lower case), storage in bits,  
    194  
B (upper case), storage in bytes,  
    194  
Back door, opening for attacker,  
    62  
Backdoor attack, laptop risk  
    assessment and, 29  
Back doors, 367  
Background investigations, 576,  
    762  
Back Orifice program, 541  
Backups  
    full vs. partial, 595–596  
    image, 595  
    incremental, 597  
    RAID as, 597–598  
    synchronized, 596–597  
Balanced trees (B-trees), 206  
Bandwidth, 442  
Base secret, 223  
Basic language, 103  
Basic principle of information  
    security, 8  
Chain of Control, 75–76  
    control flow integrity and,  
        75  
Defense in Depth, 18–19  
Deny by Default, 116–117,  
    116f  
Least Privilege, 15–16  
Open Design, 73–74  
Separation of Duty, 333–335  
Transitive Trust, 159  
Bastion-host topology, 690, 691  
Baudot, Émile, 433, 442  
Bayesian filtering, 675  
BBN. *See* Bolt, Beranek, and  
    Newman  
Bcc field, in emails, 660  
BCP. *See* Business continuity plan  
Beale, T. J., 280  
Beale Papers, 279–280  
Bell-LaPadula model, properties  
    enforced by, 795  
Bell-LaPadula rules  
    covert channels and, 797  
    virus problem and, 797  
Bell Telephone Laboratories, 142  
Berners-Lee, Tim, 631, 700

- Beyond Fear* (Schneier), 4
- BIA. *See* Business impact analysis
- Biased password selection, 247–250
- four-digit luggage lock, 248–250, 249f
- independent guesses and, 248
- measuring likelihood, not certainty, 248
- Bi-directional satellite communications, 549
- Biham, Eli, 384
- Bill of Rights, Fourth Amendment of, 175–176
- Binary encryption, 293
- Binary exponents, relationship between decimals and, 192
- Binary keys, textual keys *vs.*, 321
- Binary matches, 675
- Biological viruses, 105
- Biometric authentication, 261–265
- accuracy of, 262–263
- fingerprint reader on laptop keyboard, 261f
- vulnerabilities of, 264–265
- Biometrics, 74–75
- Biometric sensor, 263
- Biometric spoofing, 589
- Biometric systems, 224
- elements of, 262f
- BIOS (Basic Input/Output System), 54, 75–76
- BIOS-integration, preboot authentication and, 417–418
- BIOS parameter block (BPB), 196
- Birthday attacks, 354–355
- Birthday paradox game, 354
- Bit-flipping attacks, 351–352, 407
- on encryption with xor, 352f
- BitLocker (Microsoft), 401
- Bits, estimating number of, 192–194
- Bittorrent, 463–464
- Black-hat hackers, defined, 14
- Black hats
- exploit and, 127
- windows of vulnerability and, 127
- Black Hat USA 2005 Briefings, 44
- Black key, 782
- Blacklists, 674, 710
- Black programs, 767–768
- Block cipher modes, 379–399
- applying, 379
- building, 379–381
- data encrypted in fixed-sized blocks, 380f
- encryption failure with, 390f
- features of, 381
- mixing mode used with, 392f
- Block encryption procedure, description of, 380–381
- Blogs, 557
- Blue Screen of Death, 83
- Blu-ray disks, 311
- Bogus certificate authority, 719, 720
- Bogus certificates, 718, 719
- Bogus primes attack, on RSA, 351
- Bogus purchase, laptop risk assessment and, 29
- Bogus sites, 533, 714
- Bolt, Beranek, and Newman, 486
- Boot, 75
- Boot blocks, 196–197
- contents of FAT 32 boot block, 196t
- Booting, 54
- Bootstrap, defined, 75
- Bootstrapping, 54
- Border routers, 489
- Botnet herders, 22
- Botnets, 2, 13, 430–432
- DDOS attacks on DNS servers and, 534
- fighting, 431–432
- in operation, 431
- operators, identifying specific attacks by, 28, 28t
- bots, 431, 534
- Boundaries
- analyzing, 15–18, 17
- insider threats and, 17–18
- Least Privilege principle and, 15–16
- security, 15–18
- in store, 16, 16f
- Boundary marker, 661
- Boyce, Christopher, 776
- bpn.gov certificate, browser authentication for, 718f
- Bredolab botnet, 432
- British Standard BS7799, 566
- Broadcast networks, 544
- Browser cookies, 729–730
- adding to header in subsequent visits, 730f
- defined, 729
- producing, 729f
- Browsers, 703, 705
- sandboxing, 728
- Browser software, 462
- Browsing, private, 744–745
- B-trees (balanced trees), 206
- Bucket brigade attacks, 359, 360f
- bogus certificates and, 718
- Buffer overflows, Morris worm and, 62–71
- Buffers, 57, 184
- Bugs, 125
- Built-in file encryption, 302–304
- Burst transmissions, countering EW attacks and, 783
- Bus, 52, 183
- Bush, Vannevar, 699
- Business continuity plan, 601
- Business impact analysis, 600, 601
- Business records, legal issues and, 176
- Bus interface, 184
- Bus interface connector, 184
- Bus network, 473, 476–477, 476f
- benefits and shortcomings with, 477
- C
- CA. *See* Certificate authority
- C&A. *See* Certification and accreditation
- Cable modem, 536
- Cables, 53f
- network, 451
- Cable TV, 548–549
- Cache poisoning, DNS and, 533
- Caesar, Julius, 605
- Caesar cipher, 287, 379, 605
- Cain, 644
- Callahan, Edward, 433

- Called procedure, 56  
Caller ID feature, 546  
Calling procedure, 56  
Capability(ies), 118  
  defined, 118  
  resource-oriented permissions  
    and, 118–119  
Capability-based security, 118  
Capability Maturity Model, 565–566  
Capitalization, for Internet protocols, 482  
Carnegie-Mellon University (CMU), 565  
Cascading Style Sheets, 702–703  
CAST, 309  
*Catch Me if You Can* (film), 14  
Category 5 Enhanced wiring (Cat 5E), 451  
Category 5 wiring (Cat 5), 451  
CB. *See* Citizen's band  
CBC  
  calculating, 647  
  sector encryption with, 405f  
CBC encryption, integrity issues with, 405–406  
CBC mode, drive encryption with, 404–406  
Cc field, in emails, 660  
CCI. *See* Controlled cryptographic item  
CCM. *See* Counter with CBC MAC  
CD-R (recordable CD), 308  
CD-RW (rewritable CD), 308  
CDs. *See* Compact disks  
CEK. *See* Content encryption key  
Cell phones, 61, 548  
Cell phone towers, 542, 543f  
Censorware, 117  
Central Intelligence Agency, 302, 754, 776  
Central processing unit, 50, 50f, 51  
CEO. *See* Chief executive officer  
CERT. *See* Computer Emergency Response Team  
CERT Advisories, 67  
CERT Coordination Center (CERT/CC), 66  
Certificate authority, 361, 362  
  bogus, 719, 720  
  subsidiary, 362  
  tricked, 722  
  untrusted: difficult to verify, 717–719  
Certificate chain, 363  
  email authenticated with, 363f  
Certificate hierarchy, for spanning multiple enterprises, 365f  
Certificate names, mismatched, Firefox alert for, 715f  
Certificates  
  bogus, defined, 719  
  expired: possibly bogus, probably not, 719  
  revoked: always bogus, 719  
Certification, information security and, 574–575  
Certification and accreditation, 775  
Certified Information Security Auditor, 574  
Certified Information Systems Security Professional, 574, 575  
CFB mode. *See* Cipher feedback mode  
CFM. *See* Cold Fusion Markup Language  
CGI. *See* Common Gateway Interface  
Chain letters  
  email, 678–680  
  virus hoax, 679–680  
Chain of Control, 75–76, 113  
  computer viruses and, 105  
control flow integrity (CFI) and, 75  
  executable files and, 103  
  subverting, 76  
Challenge-response authentication, 252, 253–257, 254f  
challenge-response calculation, 256f  
hand-operated token, 254f  
implementing, 254–255  
for network, 589  
nonce and, 254  
using challenge-response token, 255f  
Change control process, 566  
Character set, 241  
Checks, signing, with digital signature, 356–357, 357f  
Checksums, 188–189, 235, 352, 445, 639  
  data encrypted with, 353f  
  simple, calculating, 188, 188f  
Check value, 179, 184  
Chief executive officer, 567, 568f  
Chief information officer, 569  
Chief information security officer, 570, 573  
Chief technical officer, 569  
China Telecom, 490  
Chosen ciphertext attack, on RSA, 351  
Christian canon law, 174  
Chrome browser (Google), sandboxing and, 728  
CIA. *See* Central Intelligence Agency  
CIA properties, 9. *See also* Availability; Confidentiality; Integrity  
CIO. *See* Chief information officer  
Cipher block chaining, 391, 397–399  
mode decryption diagram for, 398f  
mode encryption diagram for, 398f  
Cipher feedback, 391  
Cipher feedback code, mode encryption diagram for, 396f  
Cipher feedback mode, 396–397  
  ciphertext errors, 396–397  
Cipher machine, Friedman with, 290f  
Cipher mode, choosing, 400  
Ciphers, 282, 282f  
  Caesar, 287  
  stream, 295–298  
  substitution, 282, 282f, 286, 287  
  Vignère, 287–289

- Cipher.suites, 613  
Ciphertext, 281  
  identical blocks encrypting to identical ciphertext, 391f  
  IV included with, when required, 392  
  key wrapping and, 330  
  symmetric encryption and, 283f  
Ciphertext errors  
  for CBC, 399  
  for CFB, 396–397  
  effects of, 299, 381–382  
  for OFB, 392  
Ciphertext Stealing, 406, 407  
Circuit board, hard drive controller, 183  
Circuit filtering, 684  
Circuit-switched telephone systems, 545  
Circuit switching, 434, 435–438  
  advantages with, 435–438  
  disadvantages with, 438  
  between two phones, phone call circuit and, 437f  
CISA. *See* Certified Information Security Auditor  
Cisco, 44  
  certifications through, 574  
CISO. *See* Chief information security officer  
CISSP. *See* Certified Information Systems Security Professional  
Citizen's band, 444  
Civil complaint, 175  
Civil law, 174  
Civil War, Confederate cipher used during, 287–289, 288f  
Clancy, Tom, 751  
C language, 66, 106  
Classification levels, 757–758  
  enforcing access to, 769–770  
Classifications and clearances, 756–770  
  classification levels, 757–758  
  classification levels in practices, 763–764  
  compartments and other special controls, 764–770  
  restrictions in, 757–758  
  security clearances, 761–763  
  security labeling, 759–761  
Classification system, legal basis for, 758  
Classified information  
  classification guide, 759  
computer modes of operation  
  and, 797–799  
  compartmented or partitioned mode and, 797, 798–799  
  dedicated mode, 797–798  
  multilevel mode, 797, 799  
  system-high mode, 797, 798  
government secrecy and, 750–751  
minimizing amount of, 758–759  
security labeling and, 759–760  
working with, 763–764  
Clearances  
  defined, 576  
  employee, 576–577  
  modern security classification system and, 757  
  security, 761–763  
Clear-to-Send, 457  
Client  
  network services and, 463  
  resource sharing and, 465  
  service request and reply, 463f  
Client anonymity, 743–744  
Client policy issues, Web security and, 709  
Client/server mode, 463  
Client-side scripts, 724, 726–728  
  executing, 727f  
  HTML, in JavaScript, 726f  
  risks with, 727–728  
  “same origin” policy and, 728  
  sandboxing and, 728  
Clone credential  
  authentication tokens and, 260, 261t  
  biometric authentication and, 264  
Cluster chain, 198  
Clusters, 742  
  building FAT files from, 197–199  
  in file, FAT pointing to, 199f  
  on hard drive, 186  
  NT file-system and, 206–207  
  parts of files in, 198f  
  storage of, 198  
  Unix file system, 203  
CMM. *See* Capability Maturity Model  
CMS. *See* Content management systems  
CMW. *See* Compartmented Mode Workstation  
CNSS. *See* Committee on National Security Systems  
Coaxial cable, 448  
Cobol, 106  
Code analysis procedures, 584  
Code reviews, 584  
Codes, 282, 282f, 286, 287  
Codes of conduct, 42  
Code word, classified, 767  
Coding activities, formalized enterprises and, 583–585  
  auditing and monitoring, 584  
  avoiding risky practices, 584  
code analysis procedures, 584  
code reviews, 584  
coding standards, 584  
software-based access controls, 585  
Coding standards, 584  
Cohen, Fred, 104, 703  
Cold-boot attacks, 420  
Cold Fusion Markup Language, 725  
Cold standby, 601  
Cold War  
  government secrecy and, 750  
  nuclear operations during, 793  
  TEMPEST problem and, 787  
College degrees, information security field, 573  
Collisions  
  avoiding, wireless protocol for, 456f  
  handling, 455–457  
  wireless collisions, 456–457  
  wireless retransmission, 457  
Command injection attacks, 736–740  
  defined, 737  
  inside of, 738–739

- login masquerade and, 738f  
password-oriented, 737–738  
resisting website command injection, 740  
input validation, 740
- Command logic, 184  
reading encrypted data from hard drive and, 413
- Commercial enterprises, information security and, 556
- Committee on National Security Systems, 574, 770  
communications security and cryptography instructions by, 776  
communications security policies published by, 775  
information assurance requirements for national defense systems, 792
- Common Criteria*, 165
- Common Criteria evaluation, 565
- Common Criteria Protection Profiles, modern high-assurance computing systems and, 791
- Common Gateway Interface, 725
- Common law, 174
- Common Vulnerability Enumeration (CVE) database, 67
- Communication networks, history behind, 542–544
- Communications intelligence (COMINT), 768
- Communications security (COMSEC), 605–615, 768, 775–784
- crypto by layers, 608–613  
application layer encryption with S/MIME or PGP, 612  
link layer encryption and 802.11 wireless, 608–609  
network layer encryption and IPsec, 609–610  
socket layer encryption with SSL/TLS, 610–611
- cryptographic technology, 777–779
- crypto security procedures for, 779–782  
key leakage through spying, 776–777  
layer-oriented variations in, 612–613  
national system security and, 773  
transmission security and, 782–784
- Compact access rules, 122, 122f  
for isolation policy, 123t
- Compact disks, 51
- Companies and information control, 556–559  
accountability, 558  
managing publicity, 558  
Need to Know, 558–559  
obligations, 557  
reputation: speaking with one voice, 556–557  
secrecy culture, 558  
trade secrets, 557–558
- Company ID cards, 577
- Company identity, processes tied to, 557
- Company statements (official), personal statements *vs.*, 557
- Compartmented mode, computer modes of operation and, 797, 798–799
- Compartmented Mode Workstation, 798–799
- Compartments, 764  
clearances, lattice of, 769f  
data processing with, 765  
enforcing access to, 769–770
- Compatible Time-Sharing System, 224, 228, 231
- Competitors, 22
- Compiler, 106
- Compliance, 569
- Compliance audits, 571–572
- Compression, 635
- Compromised systems, 13, 172
- Compromising emanations, TEMPEST and, 776
- CompTIA certification, 574
- Computer-based encryption, 291–301
- Advanced Encryption Standard, 292
- Data Encryption Standard, 291–292
- exclusive or, 293–295
- key stream security, 298–299
- one-time pad, 299–301
- predicting cracking speeds, 292–293
- stream ciphers, 295–298
- Computer customization, 15
- Computer dissection, 50–51
- Computer Emergency Response Team, 66–67, 630
- Computer modes of operation, classified information and, 797–799
- compartmented or partitioned mode, 797, 798–799  
dedicated mode, 797–798  
multilevel mode, 797, 799  
system-high mode, 797, 798
- Computer networking, 425–468  
Ethernet: modern LAN, 448–457
- network applications, 462–468
- network security problem, 425–432
- protocol stack, 457–462
- putting bits on a wire, 440–448
- transmitting data, 432–440
- Computer network operations, military information operations and, 755
- Computer networks  
combining, 481–491  
emergence of Internet, 482–483  
evolution of Internet security, 485–488  
early Internet attacks, 487  
early Internet defenses, 487–488  
protecting the ARPANET, 486–487
- hopping between, 483–485  
counting hops, 485  
routing Internet packets, 485
- traversing, 482

- Computers  
 classified information and, 763  
 executing machine instruction in, 55f  
 programs and, 49–57  
 working insides of, 50f
- Computer Technology Industry Association, 574
- Computer viruses, 75, 103–107  
 malicious viruses, 105–106  
 removable storage devices and, 8  
 virus infection, 103–106
- COMSEC. *See* Communications security
- COMSEC materials, 779
- Con artists, 21
- Concurrency problem, 210
- Confederate Army, Vignère cipher used by, 287–289
- Confederate cipher disk, reproduction of, 288f
- Conficker or Downadup, 107, 108–109
- Confidential classification, 757
- Confidential clearances, 762
- Confidential documents, protecting, 763
- Confidential information, color code for, 759
- Confidentiality, 607  
 security services and, 9–11, 86  
 on the Web, 740–741
- Configuration management process  
 enterprises and, 582–583  
 repeatability and traceability in, 583  
 software development security, 582–583
- Connection-based email attacks, 671–672
- Consent to search, 176
- Consultants, enterprises and, 579
- Containers, 100
- Content control, Internet traffic control and, 682
- Content control software, 117, 710
- Content encryption key, 331
- KEK encryption of, key wrapping and, 330
- Separation of Duty and, 334–335
- Contention, bus network and, 477
- Content management systems, 730–740, 731f  
 database management systems, 732–734  
 description of, 730–732  
 password checking: example, 734–736  
 logging-in to website, 735  
 login process, 735–736, 736f
- Content-Type header, MIME formatting in Internet email and, 660–661
- Contingency planning, 595–602  
 components of, 595  
 data backup and restoration, 595–598  
 file-oriented incremental backups, 597  
 full vs. partial backups, 595–596  
 image backups, 597  
 RAID as backup, 597–598  
 defined, 595  
 disaster preparation and recovery, 600–602  
 business impact analysis, 600  
 process for, 601–602  
 recovery strategies, 600–601  
 handling serious incidents, 598–599
- Continuous availability, 742, 743
- Continuous Improvement, 8
- Continuous operation, 742
- Contractual obligations, companies, secrecy, and, 557
- Controlled access protection, 796
- Controlled Access Protection Profile, system-high mode of operation and, 798
- Controlled cryptographic item, 780–781
- Controlled sharing, 110–112, 133–142  
 basic, on Windows, 135–136  
 administrative groups, 138–139  
 user groups, 136–139
- Least Privilege and administrative users, 139–142  
 sharing dilemma, 134–135  
 tailored file security policies, 134
- Control section, 55  
 shared by two processes, 80f
- Cookies, 462, 744–745  
 browser, 729–730, 729f, 730f
- Corbató, Fernando, 77, 224
- Corporate espionage, 750
- COSMEC custodian, duties of, 779
- Cost centers, 568–569
- Counterintelligence, 754–755
- Counterintelligence polygraph examination, SCI clearances and, 765
- Counter mode, 391, 395
- CCM encryption and, 646  
 drive encryption with, 405  
 constructing counter, 405  
 integrity risk, 404  
 encrypting disk data with, 404f  
 key stream with, 395f
- Counter with CBC MAC, 646–647
- Country codes, 524
- Coupling, 789
- Covers, 754
- Covert channels, multilevel security and, 796–797
- CPU. *See* Central processing unit
- Crackers, defined, 13
- Cracking feasibility, different degrees of, 244t
- Cracking speeds, 244–245  
 predicting, 292–293
- CRCs. *See* Cyclic redundancy checks
- Credentials, 221, 225–226  
 guessing, 259  
 sniffing, 226, 228, 236–237

- Credential updates, enterprise network authentication and, 585
- Credit cards, 252  
online shopping and, 631
- Crime, via search engines, 708–709
- Criminal background checks, 576
- Criminal complaints, 175
- Criminal organizations, 21
- Critical data, identifying noncritical data *vs.*, 377–378
- Cross-domain sharing, system-high mode of operation and, 798
- Cross-site scripting, 727
- Crosstalk, TEMPEST separation and, 789
- CRUD (Create, read, update, delete access rights), 98
- Cryptanalysis, 298  
encryption and, 286–291
- Crypto atop protocol, 628–636  
adoption of secure email and application security, 630
- Pretty Good Privacy, 629–630  
privacy-enhanced mail, 629
- SSL handshake protocol, 632–634
- SSL record transmission, 634–636
- transport layer security—SSL and TLS, 630–632
- Cryptograms, 286
- Cryptographic building blocks, 236  
challenge-response, 253–257
- Diffie-Hellman secret sharing, 340–343, 624–625
- digital signature, 356–359
- exclusive-or, 293–295
- key distribution centers, 622–623
- key wrapping, 330–333, 621–622
- manual keying, 618–619
- one-way hash function, 234–236
- RSA, 344–345
- RSA secret wrapping, 345–347, 626
- shared secret hashing, 623–624
- stream cipher, 295–298
- Cryptographic function, 234
- Cryptographic product evaluation, 310
- Cryptographic protections, 607
- Cryptographic randomness, 243
- Cryptographic technology, governments, secrecy and classic Type I crypto technology, 777–779
- Cryptography, 72, 279, 317.  
*See also* Encryption; Public-key cryptography
- asymmetric, 337
- deploying on Internet, issues related to, 613
- access to Internet sites, 613
- automatic encryption, 613
- end-to-end crypto, 613
- keying, 613
- scope of sniffing protection, 613
- traffic filtering, 613
- elliptic curve, 343–344
- high-assurance, 777
- indirect authentication and, 593
- Open Design and, 74
- symmetric, 283, 339f
- Cryptography by layers, 608–613  
adding cryptography to Internet software, 608f  
application layer encryption with S/MIME or PGP, 612
- link layer encryption and 802.11 wireless, 608–609
- network layer encryption and IPsec, 609–610
- socket layer encryption with SSL/TLS, 610–611
- Crypto keys  
on a network, 615–628
- manual keying, 618–619
- public-key building blocks, 624–626
- public-key *vs.* secret-key exchanges, 626–628
- secret-key building blocks, 621–624
- simple rekeying, 619–621
- Walker spy ring and, 781
- Cryptolocker/ Cryptowall, 109–110  
ransomware, 109
- Crypto logic, reading encrypted data from hard drive and, 413
- Cryptology, 289, 387
- Cryptonets, 318  
rekeying and, 319
- Cryptoperiods, 319, 320  
key wrapping and, 332
- Crypto security procedures, 779–782  
controlled cryptographic items, 780–781
- key management processes, 781–782
- data transfer device, 781
- electronic key management system, 781–782
- two-person integrity, 779–780
- CSS. *See* Cascading Style Sheets
- CTO. *See* Chief technical officer
- CTR mode. *See* Counter mode
- CTS. *See* Clear to Send
- CTSS. *See* Compatible Time-Sharing System
- Culture, enterprise community and, 575
- Custodians, physical access and, 578
- Cutwail. *See* Pushdo/Cutwail
- Cyber assets, 30
- Cyberattacks, 67–71  
attack case study, 67, 68  
attack scenario, 67, 68
- Morris worm  
attack case study, 70–71  
attack scenario, 69–70
- Cybercrime organizations, 21–23
- Cyber-criminal teams, 21–22
- Cybersecurity, 2  
assessing risk, 8–19  
rule-based risk assessment, 9–11
- Cyclic redundancy checks, 189, 235, 352, 639
- Cylinder, 182

- D  
 Daemen, Joan, 384  
 DARPA, 482, 485  
 Data  
     file sharing and, 465–468  
     hiding with partitions, 191–192  
     sharing, 81–83  
 Data backup and restoration  
     file-oriented incremental  
         backups, 597  
     full *vs.* partial backups, 595–596  
     image backups, 597  
     RAID as backup, 597–598  
 Database management systems,  
     732–734  
     database security and, 734  
     enterprise databases and, 734  
     Structured Query Language  
         and, 733–734  
 Database management system  
     software, 731  
 Databases, 732  
     enterprise, 734  
     relational, 732  
 Database security, 734  
 Database thefts  
     authentication and, 229–231  
     authentication with personal  
         information, 230–231  
     identity theft, 229–230  
     masquerade attacks, 230–231  
 Data breach, 559  
 Data compression, SSL record  
     transmission and, 635  
 Data Encryption Standard,  
     291–292, 298, 379  
     evolution of, 382–385  
     Lucifer and, 382  
         triple, 382–383, 383f  
 Data execution prevention, 65  
 Data files, executable files *vs.*,  
     101  
 Data formats use, 584  
 Datagrams, 439  
 Data integrity, encrypting a  
     volume and, 409  
 Data link layer, OSI protocol  
     model, 461  
 Data loss prevention systems, 690  
 Data mining, 734  
 Data networks, 432  
 Data processing, compartments  
     used for, 766f  
 Data protection, 784–789  
     media handling, 784–785  
     media sanitization and  
         destruction, 785  
 Data recovery, low-level,  
     preventing, 307  
 Data section, 55  
 Data storage, on hard drive,  
     179–186  
 Data tables, 732  
     sample, from sample database,  
         732f  
 Data Transfer Device, keys  
     handled by, 781  
 Data transmission, 432–440  
     circuit switching, 435–438  
     message switching, 435  
     packet switching, 438–440  
 Data warehouses, 734  
 Daughterboards, 50, 50f  
 DBMS. *See* Database  
     management systems  
 DDOS. *See* Distributed denial of  
     service attacks  
 DEC. *See* Digital Equipment  
     Corporation  
 Decimals, relationship between  
     binary exponents and,  
     192  
 Decommissioning, 578  
 Decryption, 279, 347. *See also*  
     Encryption  
     for cipher block chaining  
         mode, 397, 398–399  
     of DVD sector, 336f  
     of files, security boundaries  
         for, 304f  
     RSA, 347  
     of stream ciphers, 381  
     symmetric encryption and, 283f  
 Decryption algorithm, 281  
 Dedicated digital network links,  
     548  
 Dedicated lines, 472, 474, 545  
     dial-up lines *vs.*, 546t  
 Dedicated mode, computer  
     modes of operation and,  
         797–798  
 Default Deny policy, low-cost  
     gateway products and,  
         536  
 Default file protection, Microsoft  
     Windows ACLs and,  
         154–156  
     dynamic ACLs, 154–156  
     inherited rights, 154  
 Default keying, 616  
 Default permit, 117  
 Default Permit policy, low-cost  
     gateway products and, 536  
 Defense, 13  
 Defense Advanced Research  
     Projects Agency. *See*  
         DARPA  
 Defense in Depth, 18–19  
     control of nuclear weapons  
         and, 793  
     discipline of secrecy and, 752  
     physical protection of  
         enterprise information  
         system and, 580  
 protecting classified data and,  
     763  
 two-factor authentication and,  
     224  
 Defense secrecy restrictions, 41  
 Defragment utility, 186  
 Degaussers, 785  
 Delayed recovery, 601  
 Delegation, of access to file  
     server, 467f  
 Delegation problem, 467  
 Deleting files, FAT directories  
     and, 200–201  
 Delivery protocols, 663, 664–665  
 Demilitarized zone, 689  
     dual-firewall topology with,  
         692, 693f  
     three-legged firewall with,  
         691–692, 692f  
 Deming cycle, 565  
 Denial of service, 27, 34, 38, 227,  
     427  
     authentication tokens and,  
         260, 261t  
     biometric authentication and,  
         264  
     bus network and, 477  
     distributed, 431

- on DNS servers, 533  
file protection policies and, 112  
power interruptions and, 580  
for social media, 35
- Deny access, for Microsoft Windows  
  ACLs, 151–154, 152f
- Deny by Default, 116–117, 116f
- Microsoft Windows ACLs  
    and, 153  
    opposite of, 117
- DEP. *See* Data execution prevention
- Department of Defense, 165, 636  
  FISMA and, 770–771  
  media sanitization procedures/standards of, 785
- Password Management Guideline, 238
- security labeling and, 760
- special access programs and, 767
- Department of Homeland Security, US-CERT and, 66–67
- Deployment, security-critical systems and, 567
- Deployment policy directives, 566–567  
  risk acceptance and, 567  
  steps related to, 566–567  
    deployment, 567  
    implementation, 566–567  
    planning, 566
- Derivative classification, 758
- DES. *See* Data Encryption Standard
- DESCHALL, 292
- DES Cracker, 244, 292, 408
- Design features, of dispatcher, 89
- Design patterns, types of, 586
- Detective controls, 160
- Device drivers, 61, 103
- Device-hosted volume, 402
- Device independence, I/O devices and, 208
- D-H. *See* Diffie-Hellman
- DHCP. *See* Dynamic Host Configuration Protocol
- Dial-back, 546
- Dial-up connections, 546
- Dial-up lines, dedicated lines vs., 546f
- Diameter protocol, 592
- Diaries, encrypted, 280–281
- Dictionary attacks, 245  
  analysis of, 246  
  by Morris worm, 245f, 250
- Diffie, Whitfield, 340, 343
- Diffie-Hellman, 339f, 340–343, 358, 617  
  background and description of, 340–341  
  cipher suites in SSL and, 613  
  IKE process and, 642–643  
  math basics and, 341–343  
  perfect forward secrecy and, 341  
  procedure for secret sharing, 340  
  RSA *vs.*, secret key sharing and, 347  
  secret sharing with, 624–625, 625f  
  variations of, 341
- Digest authentication, 255–256
- Digital circuits, minor signal glitches self-corrected with, 441f
- Digital devices, turning off, 178
- Digital Equipment Corporation, 481, 487
- Digital evidence, 175–179  
  collecting legal evidence, 177–178  
  documenting the scene, 178  
  securing the scene, 177–178  
  evidence log in, 178
- Fourth Amendment and, 175–176  
  procedures, 178–179  
    authenticating a hard drive, 179
- Digital forensics, 173
- Digital Millennium Copyright Act, 41
- Digital networks, 444, 545–546
- Digital rights management, 41, 310–313, 695, 741
- DVD Content Scrambling System, 312–313
- policy dilemmas, 311
- Digital satellite broadcasts, 549
- Digital signals, 440
- Digital signatures, 338, 341, 356–359, 360  
  invalid: always bogus, 719  
  nonrepudiation and, 359
- RSA, verifying, 357  
  RSA and, 344–345  
  signing a check-with, 356–357, 357f  
  in valid public-key certificates, 717
- Digital Signature Standard, 341, 358
- Digital steganography, 72
- Digital subscriber line, 536
- Digital systems, 440
- Digital video disks, erasure or destruction of, 785
- Digital Video Interface, 52
- Direct authentication, 588  
  description of, 588  
  poor scaling with, 589f  
  sniffing attacks and, 589
- Direct connect tokens, 256–257, 256f
- Direct design pattern, 586
- Directional transmissions, counteracting EW attacks and, 783
- Direction control, Internet traffic control and, 682
- Directories, 708  
  access rights for, 99–101  
  Unix, 204  
  Unix permission flags and, 143
- Directory name formats, 97t
- Directory ownership, 99f
- Directory path, 96–67
- Direct-sequence spread spectrum, 784
- Disaster preparation and recovery, 600–602  
  business impact analysis, 600  
  contingency planning process and, 601–602  
  recovery strategies, 600–601
- Disclosure, 26, 112, 426
- Disclosure attacks, 559, 606
- Discrete logarithm problem, 342
- Discretionary access control, 796

- Disengagement, serious attacks and, 599
- Disk-based authentication, 417–418
- Diskettes  
erasure or destruction of, 785  
virus-infected, 106*f*
- Disk keys, on DVDs, 335
- Disk platters, 182, 182*f*
- Dismount, 210
- Dispatcher, 77  
design features of, 89
- Dispatching procedure, 89–90
- DisplayPort, 52
- Distributed database, 528
- Distributed denial of service attacks, 431  
on DNS servers, 533
- Distributed DNS servers, 534
- Distributed processing, 445
- DMCA. *See* Digital Millennium Copyright Act
- DMZ. *See* Demilitarized zone
- DNS. *See* Domain Name System
- DNS Security Extensions (DNSSEC), 535
- Document markings, security labeling and, 759–760
- DOD. *See* Department of Defense
- Domain names, 523  
common top-level domain acronyms, 524*t*  
constructing, 524  
hierarchy of, 523*f*  
investigating, 531  
looking up, 526–527, 530*f*  
misleading, 720–722  
mismatched: may be legitimate, 715–717  
Firefox alert for mismatched certificate name, 715*f*  
phishing and, 677  
resolver software, 526  
resolving via redirection, 529–530  
taking possession of, 525  
three-part, example format, 525*f*  
using, 526
- Domain Name System, 523, 657
- attacking  
cache poisoning, 533  
DOS attacks on DNS resolvers, 534  
DOS attacks on DNS servers, 533–534  
DNS protocol, 528–531, 533–534  
DNS redundancy, 532  
Wireshark display of DNS response, 529*f*  
DNS Security Extensions (DNSSEC), 535  
security improvements for, 534–535
- Domain registrar, 525
- Doorknob rattling, 228
- DOS. *See* Denial of service
- Dotted decimal notation, 493  
examples of addresses in, 493  
for Internet addresses, 493*f*
- Downadup or Conficker, 107, 108–109
- Downlinks, 451
- Downloads subdirectory, 96*f*
- Draper, John, 13
- Drive-by downloads, 108, 676
- Drive concepts  
address variables, 192–194  
common, 186–194  
error correction, 187–189  
error detection, 187–189  
hard-drive partitions, 189–192  
memory sizes, 192–194
- Drive controller, 183  
adding encryption to hard drive and, 410
- Drive encryption  
with CBC mode, 404–406  
with counter mode, 405  
constructing counter, 403  
integrity risk, 404
- Drive formatting, encryption in hardware and, 411–412
- Drive locking/unlocking, encryption in hardware and, 412–413
- DRM. *See* Digital rights management
- Drupal, 731
- DSL. *See* Digital subscriber line
- DSS. *See* Digital Signature Standard
- DSSS. *See* Direct-sequence spread spectrum
- DTD. *See* Data Transfer Device
- Dual firewalls, 690, 692–693, 693*f*
- Due diligence, fault and, 173–174
- Dumb networks, “smart” networks *vs.*, 513–514
- Duplicated packet, delayed ACK and, 448*f*
- DVD content protection, 312*f*
- DVD Content Scrambling System (DVD-CSS), 311, 312–313, 335
- DVD key handling, 335–336  
decrypting DVD sector, 336*f*  
finalizing disk for publication, 336  
keys on DVD hidden track, 335*f*
- DVD publisher, 336
- DVD-R (recordable DVD), 308
- DVD-RW (rewritable DVD), 308
- DVDs. *See* Digital video disks
- DVI. *See* Digital Video Interface
- Dynamic ACLs, Microsoft Windows, 154–156
- Dynamic Host Configuration Protocol, 500, 501–502, 657  
configuring, NAT and, 538–540
- Dynamic inheritance, 154
- Dynamic-link libraries (.dll), 81, 103
- Dynamic websites, 723–730  
scripts on the Web, 724–728  
states and HTTP, 728–730  
web forms and POST, 723–724
- E
- E1/E3 services (Europe), 548
- EAM. *See* Emergency Action Message
- Eavesdropping  
bus network and, 477  
on encryption process, 420
- enterprise network authentication and, 585  
risks to volumes and, 375

Eavesdropping, enterprise network authentication and, 585  
ECB. *See* Electronic codebook mode  
ECCs. *See* Error correcting codes  
e-commerce, public-key certificates and, 362  
EDCs. *See* Error detecting codes  
Education, for information security professionals, 572  
EFF. *See* Electronic Frontier Foundation  
E-Government Act (2002), 770–771  
802.11 access, service-based authentication for, 592f  
802.11 link encryption, packet with, 609f  
802.11 wireless link encryption on, 643–649  
link layer encryption and, 608–609  
802.11 wireless network technology, 449  
EKMS. *See* Electronic Key Management System  
Electrical telegraph, 432  
Electric power management, in enterprises, 580  
Electromechanical encryption, 289–291  
Electronic codebook mode, 391  
Electronic Frontier Foundation, 292, 744  
Electronic keying, early forms of, 781  
Electronic Key Management System, 781–782  
Electronic warfare, 755, 782–783  
El Gamal cipher, 341, 358  
Elliptic curve cryptography, 343–344  
Elliptic curves, 339f  
email, 435, 557. *See also* Internet email  
aliases, 526  
authenticated, 670–671  
with certificate chain, 363f  
presidential, 669f

security problems, 671–680  
signed, excerpt from, 670f  
spam and, 13, 676  
tracking, 665–668, 666f, 667f  
from MMS01 to MMS02, 668  
from UC123 to USM01, 666  
from USM01 to USM02, 666–667  
from USM02 to MMS01, 668  
viruses, 671  
Email chain letters, 678–680  
email format, elements of, 659f  
email infection, Trojan malware and, 108  
email messages, forging, 668–671, 669f  
email protocol, port numbers for, 492  
email security problems, 671–680  
connection-based attacks, 671–672  
phishing, 675–677  
spam, 672–675  
viruses and hoaxes, 677–680  
email text, with MIME formatting, 662f  
email URLs, 704, 704f, 705  
email viruses, 671  
defined, 677  
execution of, 678  
Embezzlement, 29  
Embezzlers, 112  
Emergency Action Message, 793, 794  
Emergency destruction, 755  
Emissions Security Assessment Request, 73  
Employee clearances, 576–577  
Employee life cycle, 576, 577–578  
Employee roles, 576, 578–579  
Employees, insider attacks and, 561  
Employment history, verification of, 576  
Encapsulating Security Payload, 639–641  
packet format, 639–641  
transport mode, 641  
tunnel mode, 640–641  
Encapsulation of keys, with RSA public key, 346f  
retrieving key with RSA private key, 347f  
Encrypted drive  
automatic reboot, 418  
booting, 416–418  
preboot authentication, 417–418  
BIOS integration, 417, 417f  
disk-based authentication, 417–418, 417f  
Encrypted sector salt  
initialization vector.  
*See* ESSIV  
Encrypting a hash, two steps for, 355f  
Encrypting gateways, 610  
Encrypting volumes, 399–409  
block ciphers, 379–399  
choosing a cipher mode, 400  
encryption in hardware, 409–413  
drive controller, 410–412  
drive locking and  
unlocking, 412–413  
FDE implementations, objectives for, 399  
hardware *vs.* software, 400  
managing encryption keys, 413–421  
booting an encrypted drive, 416–418  
key-generation, 413  
key storage, 414–416  
rekeying, 414  
residual risks to keys, 418–421  
password volume for mounting, 402f  
policy for, 378–379  
policy statements for, 379t  
residual risks, 407–409  
data integrity, 409  
encryption integrity, 408  
looking for plaintext, 408  
untrustworthy encryption, 407–408  
securing a volume, 373–379  
in software, 400–402

- files as encrypted volumes, 402  
 "tweakable" mode, 406–407  
**Encryption**, 72–73, 279–313.  
*See also Cryptography; Decryption; Network encryption*  
 asymmetric, 282, 282f, 339f  
 automatic, deploying cryptography on Internet and, 613  
 automatic application of, 651  
 basics, 281–284  
 binary, 293  
 categories of, 282  
 for cipher block chaining mode, 398, 398f  
 computer-based, 291–301  
 cryptanalysis and, 286–291  
 crypto techniques to automate, 651t  
 digital rights management and, 310–313  
 effective, 284  
 effectiveness of access control and, 377t  
 for email, 629f  
 enterprise network authentication and, 585  
 file encryption software, 302–310  
 information states and, 284–286, 285f  
 procedure diagram of, 281f  
 process view of, 282–283  
 public-key, 337f, 340  
 secret-key, 340  
 security software and, 585  
 selective, reasons for, 651  
 Separation of Duty with, 334–335  
 symmetric, 339f  
     process diagram of, 283f  
 traditional purpose of, 605  
 untrustworthy, 407–408  
 with xor, bit-flipping attack on, 352f  
**Encryption algorithms**, 258, 339f  
     categories of, 282f  
     good, qualities of, 387–389  
 available for analysis, 387, 388  
 cryptographic evaluation, 389  
 explicitly designed for encryption, 387–388  
 no practical weaknesses, 387, 388–387  
 security does not rely on its secrecy, 387, 388  
 subjected to analysis, 387, 388  
**Encryption application programs**, 304–306  
     ensuring secure file encryption, 305  
     protecting the secret key, 305–306  
**Encryption key management**, 413–421  
     automatic reboot, 418  
     booting an encrypted drive, 416–418  
     key generation, 413  
     key storage, 414–416  
     persistent key storage, 414–416  
         key wrapping, 415–416  
         managing removable keys, 416  
         protected storage, 415  
     preboot authentication, 417–418  
         BIOS integration, 417f  
         disk-based authentication, 417f  
     rekeying, 414  
     residual risks to keys, 418–421  
         intercepted keys, 419–420  
         intercepted passphrase, 419  
         "master key" risk, 420–421  
     recycled CEK attack, 418–419  
**Encryption keys**, 281  
     distributing, 320  
     management. *See Encryption key management*  
     nonce used for constructing, 328f  
     text used for, 321–323  
 software checklist for key handling, 323  
 taking advantage of longer passphrases, 322–323  
**End tags**, HTML, 701  
**End-to-end crypto**, 628, 652  
     application transparency and, 635–636  
     deploying cryptography on Internet and, 613, 615  
     description of, 612  
     packet with, 612f  
**End-to-end networking**, 513–549  
     Internet gateways and firewalls, 535–542  
     Internet transport protocols, 514–523  
     long-distance networking, 542–549  
     names on the Internet, 523–535  
     "smart" vs. "dumb" networks, 513–514  
**End-to-end principle**, 514  
**End-to-end transport protocols**, 516  
**English Common Law**, 174, 176  
**Enigma** (film), 291  
**Enigma cipher machine** (German), 289  
**Enterprise computing**, 555–602  
     challenge of community, 555–563  
     contingency planning, 595–602  
     enterprise issues, 575–585  
     enterprise network authentication, 585–594  
     management processes, 563–575  
**Enterprise databases**, 734  
**Enterprise firewalls**, 680–688  
**Enterprise issues**, 575–585  
     education, training, and awareness, 575–576  
     culture, 575  
     formal training, 576  
     personal instructions, 575–576  
     public announcements, 576  
     written instructions, 575

- personnel security, 575, 576–579  
physical security, 575,  
579–582  
software security, 575,  
582–585
- Enterprise network  
authentication, 585–594  
credential updates and, 585  
crypto requirements and, 586  
direct authentication and,  
588–589  
eavesdropping and, 585  
fault tolerance and, 586  
indirect authentication and,  
590–593  
local authentication and,  
587–588  
multiple servers and, 585  
off-line authentication and,  
593–594  
redirected authentication and,  
592–593  
security boundary and, 586  
service-based authentication  
and, 591–592  
ticket-based, 591
- Enterprise point of presence,  
689–695  
attacking an enterprise site,  
693–695  
demilitarized zone, 689  
Internet service providers, 689  
intrusion detection, 689–690  
POP topology, 690–693  
real-time media challenge and,  
695
- Enterprise risks, 559–561  
disclosure attacks and, 559  
insiders and outsiders,  
560–561  
masquerade attacks and, 559  
physical theft, 560  
service loss attacks and, 560  
subversion attacks, 560
- Enterprises  
defined, 555  
information security and, 556
- Enterprise sites, attacking,  
693–695  
protocol attacks, 693–694  
tunneling, 694
- Entropy, bias and, 246  
Environmental management,  
enterprises and, 581–582
- Environmental risks, 23
- Equipment theft, at workplace,  
560
- Error correcting codes, 189
- Error detecting codes, 189
- Error detection and correction,  
187–189  
checksums, 188–189  
cyclic redundancy checks,  
189  
error correcting codes, 189  
error detecting codes, 189  
parity checking, 187–188  
by using odd parity on  
nine-track tape, 187
- Error propagation, 397
- Error results check, 584
- ESAR. *See* Emissions Security  
Assessment Request
- eSATA. *See* External SATA
- Escape character (ESC), 75
- ESMTP. *See* Extended SMTP
- ESP. *See* Encapsulating Security  
Payload
- Espionage, one-time pads and,  
300
- Espionage Act, 749
- ESP packet contents, 640f
- Essay file, information states of,  
125f
- ESSIV, 405  
sector encryption with, 405f
- Ethernet, 425, 439, 448–457  
bus topology and, 477  
as “dumb” network, 513  
frame format, 451–453  
address format, 452–453  
LAN addressing, 452  
MAC addresses and  
security, 453
- LAN connecting hosts on a  
bus, 448f  
optical fiber, 449  
packet (frame) contents, 451f  
today's, 449
- wired networks, 449  
wireless network technology,  
449
- Ethernet connection, 52
- Ethernet header, in Wireshark,  
503, 503f
- Ethernet hub, RJ-45 connectors  
on, 450f
- Ethical issues in security analysis,  
41–45  
laws, regulations, and codes of  
conduct, 41–42  
searching for vulnerabilities,  
42–43  
sharing or publishing  
vulnerabilities, 43–45
- Eudora (Qualcomm), 663
- Event, 162
- Event logging, in operating  
system, 163f
- Event logging mechanism, major  
elements of, 162–163
- Event logs  
for gateways, 536  
Microsoft Windows, 160f
- Evidence, admissible, 175
- EW. *See* Electronic warfare
- Exceptions, 542
- Exclusive-or (xor) cipher,  
293–295, 294f, 326f  
eliminating key streams with,  
326f  
encrypting image with, 295f  
encryption with, bit-flipping  
attack on, 352f  
key splitting with, 332
- Executable files, 101–110  
access rights to, 120f  
data files *vs.*, 101  
format of, 101f  
types of, 103  
virus infection in, 104f
- Execute right, 102
- Execution, serious attacks and,  
599
- Execution access rights, 102–103
- Executive Order 13526,  
classification system  
defined by, 758
- Expired certificates, possibly  
bogus, probably not, 719
- Explicit denial, 144
- Exploit, 127
- Exponentiation, 342

- Export Controlled marking, 761  
 Export Restricted marking, 761  
 Exposure and quarantine model, secrecy, information systems and, 753–754, 785  
 ext3 file system (Linux), 203  
 Extended SMTP (ESMTP), 668  
 Extensible Markup Language, 703  
**E**  
 Extents  
     Apple's HFS+ and, 205–206  
     NT file system and, 205–206  
 Exterior routing, autonomous systems and, 489  
 External files  
     effectiveness of access control and encryption, 377t  
     securing a volume and, 376  
 External SATA, 52  
 External security requirements, 164–167  
     laws, regulations, and industry rules, 165–166  
     security process and, 166–167  
 External storage traffic, protection of, 581  
 External wires, protecting, 429  
 Extortion, 560  
 Extreme threats, 226f  
     key management and, 318  
     key strength and, 325  
 Extremist political groups, 750
- F**  
 Facebook, 109, 679  
 Factories, security risks and, 3  
 Fair use, 311  
*Falcon and The Snowman, The* (Lindsey), 776  
 False acceptance rate, 263  
 False positives problem, spam and, 675  
 False rejection rate, 263  
 Family radio service bands, 547  
 FAR. *See* False acceptance rate  
 FAT. *See* File allocation table  
 FAT 12, 189, 195, 201  
     Microsoft's FAT file system formats, 197t  
     volume layout and, 195  
 FAT 16, 195, 201  
     flash storage and, 199  
     Microsoft's FAT file system formats, 197t  
     volume layout and, 195  
 FAT 32, 195  
     boot block, contents of, 196  
     flash storage and, 199  
     Microsoft's FAT file system formats, 197t  
 FAT directories, 200–201  
     deleting files, 200  
     long file names, 200  
     undeleting files, 201  
 FAT file system, 189  
 FAT-formatted volume, layout of, 195–196  
 Fault, due diligence and, 173–174  
 FBI. *See* Federal Bureau of Investigation  
 FCC. *See* Federal Communications Commission  
 FDDI. *See* Fiber distributed data interface  
 FDE. *See* Full-disk encryption  
 Feature extraction, biometric authentication and, 262  
 Federal Bureau of Investigation, 281  
 Federal Communications Commission, 443, 444, 547  
 Federal Information Processing Standard (FIPS), 9  
 Federal Information Processing Standard 180 (FIPS-180), 235  
 Federal Information Security Management Act, 165, 770–771  
     NIST standards and guidance for, 771  
     summary of, 771  
 Feistel structure, 382  
 Ferguson, Niels, 384  
 Fetch/store data, 184  
 Fiber distributed data interface, 549  
 Fields, in data tables, 732  
 File allocation table, 189  
 File allocation table: example file system, 195–201  
     boot blocks, 196–197  
     building files from clusters, 197–199  
     cluster storage, 198  
     example, 198–199  
     FAT and flash storage, 199  
     contents of FAT 32 boot block, 196t  
 FAT directories, 200–201  
     deleting files, 200  
     long file names, 200  
     undeleting files, 201  
     format variations of, 197  
     volume layout, 195–196  
 File encryption  
     enabling on Windows, 303f  
     secure, ensuring, 305  
 File encryption keys  
     hashing passphrases for, 322f  
     passphrase used for, 321f  
 File encryption programs  
     choosing, 308–310  
     cryptographic product evaluation, 310  
     file encryption security checklist, 309–310  
     software security checklist, 309  
 File encryption security checklist, 309–310  
 File encryption software, 302–310  
     built-in file encryption, 302–304  
     choosing file encryption program, 308–310  
     cryptographic product evaluation, 310  
     file encryption security checklist, 309–310  
     software security checklist, 309  
 encryption application programs, 304–306  
     ensuring secure file encryption, 305  
     protecting the secret key, 305–306  
     erasing a plaintext file, 306–308

- erasing optical media, 307–308  
preventing low-level data recovery, 307  
requirements for key handling in, 323  
risks that demand overwriting, 306–307  
uses for, 302
- File folders, 95
- File-hosted volume, 402
- File management, I/O system and, 61
- File names, 96–67  
formats for, 97t
- File-oriented incremental backups, 597
- File-oriented synchronized backups, 596–597
- File ownership, 99f  
access rights and, 97–99
- File permission flags, 142–146  
for compact access rules, 122f  
set of, 121f
- File protection  
initial, 99  
from various threats, 112
- Files. *See also* Sharing files;  
Storing files  
access rights for, 98  
as encrypted volumes, 402  
encrypting with wrapped keys, 331  
executable, 101–110  
loss of, laptop risk assessment and, 29  
security controls for, 115–119  
sharing and protecting, 110–115  
policies for, 112–115
- File scavenging, 172
- File security controls, 119–125  
file permission flags, 121–123  
policy enforcement and, 123, 123t  
states and state diagrams, 123–125
- File server, delegating access to, 467f
- File sharing  
data and, 465–468  
on LAN, 466f
- on Microsoft Windows 8.1, 135–136, 136f  
security risk with, 466
- File-sharing policy, security controls for, 145, 146t
- File synchronization software, 84
- File system objectives, conflicting, 202–203
- File systems, 95–101  
categories of, 97  
design goals for, 202
- File system software, I/O system and, 209
- File transfer protocol  
application proxy and, 685  
port numbers for, 492
- Filtering  
connectivity and  
inbound connections, 541  
packet filtering, 540  
TEMPEST problem and, 787
- Finder, 147
- Finger, exploiting, 63–64
- Finger attack, 245
- Finger overflow, 62–66
- Fingerprint, 224t
- Finger process, attacking computer via, 64f
- Finger program, 62
- Finger service  
buffer overflow in, 64f  
data section for, 63f
- Finish TCP flag (FIN), 519
- FIPS 140-2, 310
- FIPS 140 certified products, 408
- FIPS-180. *See* Federal Information Processing Standard 180
- FIPS 199, 9
- FIPS documents, 771
- Firefox, 462, 703, 705  
alert for mismatched certificate names, 715f, 717  
certificate information displayed by, 716f
- Fires, 595
- Firewall proxies, 685
- Firewall rules  
additional mechanisms, 688  
implementing, 685–688
- format of simple firewall rules, 686, 686t  
proliferation of, 688
- Firewalls, 535, 693  
dual, 690, 692–693, 693f  
enterprise, 680–688  
HTTP tunnels and, 712  
national, 694–695  
single, 690, 691, 691f  
software-based, 541–542  
three-legged, 690, 691–692, 692f
- Firewall security controls, example of, 686–688, 687t
- Firewall vendors, Common Criteria evaluation and, 565
- Firewire, 52
- Firmware, 54
- First Amendment, government secrecy and, 751
- FISMA. *See* Federal Information Security Management Act
- Flags, wireless packet protection and, 646
- Flash drives, 186–187
- Flash memory, 54
- Flash storage, FAT and, 199
- Floods, 595
- Flow control problem, 518
- FM. *See* Frequency modulation
- FM radio, 443–444
- FM wave form, 443f
- Force surety, nuclear weapons and, 793–794
- Forensic investigators, training and expertise for, 572
- Forgeries, 27, 426, 606, 671  
distributing, 359  
of email messages, 668–671, 669f  
file protection policies and, 112
- Formal design specification, 790–791
- Formal security policies, 790
- Formatting standards  
for Internet email, 658  
for the Web, 700
- For Official Use Only, 761

- Fortran, 106  
 FOUO. *See For Official Use Only*  
 Fourth Amendment, surveillance and seizure restrictions and, 175–176  
 Four-way handshake, wireless LANs and, 648, 649f  
 Fragmentation, 186  
 partitioning and, 191  
 Frame, defined, 451  
 Frame relay services, 548  
 Fraud, 559, 560  
 financial, 672–673  
 workplace, 561, 562  
 Free Money virus hoax, 679  
 Free-space management, 202  
 Frequency, 442  
 Frequency analysis, 287  
 Frequency hopping, 784  
 Frequency modulation, 443  
 Frequency sharing, 443–444  
 Friedman, William, 290  
 with cipher machine, 290f  
 From: header, for Internet email, 659–660  
 FROTH keyword, 768  
 FRR. *See False rejection rate*  
 FRS bands. *See Family radio service bands*  
 FTP. *See File transfer protocol*  
 Full-disk encryption, 373, 376  
 hard drive volume with, 374f  
 techniques for, hardware *vs.* software, 400  
 Full-scope polygraphy  
 examination, SCI clearances and, 765  
 Functional managers, 567, 568f
- G**  
 GAO. *See Government Accountability Office*  
 Gardner, Martin, 349  
 Garfinkel, Simson, 375  
 Gates, Bill, 103  
 Gateways, 483, 535  
 construction of small LANs and, 536  
 filtering, connectivity and, 540–541  
 functions of, 500
- Internet traffic control and, 682  
 low-cost commercial, 501f  
 simple, configuring, 539f  
 Generic names, 524  
 Geolocation services, 531  
 GET command, 707  
 scripts and, 726  
 GIAC. *See Global information assurance certification*  
 GIF. *See Graphics Interchange Format*  
 GLBA. *See Gramm-Leach-Bliley Act*  
 Global information assurance certification, 574  
 Global IP addresses, 499  
 Global policies, 112  
 Gnu, 142  
 Gnu Privacy Guard, 630  
 Goldberg, Ian, 386  
*Gold Bug, The* (Poe), 279, 286, 287  
 Golden Shield project (China), 695  
 Good Times virus hoax, 679  
 Government  
 evolution of, in 20th century U.S., 749  
 hostile intelligence services, 750  
 information security, security classification and clearances and, 757  
 intelligence and counterintelligence, 754–755  
 military information operations, 755  
 operations security, 755–756  
 secrecy in classified information, 750–751  
 Government Accountability Office, 770  
 GPG. *See Gnu Privacy Guard*  
 Gramm-Leach-Bliley Act, 165  
 Graphical user interface, 57  
 Graphics Interchange Format, 707  
 Great Britain, evolution of classification system in, 756
- Grounding problems, TEMPEST emanations and, 789  
 Group rights, 136  
 Unix file permissions, 142, 142f  
 Guards, multilevel servers and, 799
- Guessing  
 authentication tokens and, 260, 261t  
 biometric authentication and, 264
- GUI. *See Graphical user interface*
- Gulf War (1991), operations security during, 755–756
- Guy, Mike, 232
- H**
- Hackers  
 black-hat, 14  
 defined, 14  
 white-hat, 14, 562
- Hacktivists, 22, 25–26
- Half-open connection, 519
- Hall, Chris, 384
- Hands-on certifications, 574
- Hard drive, 51, 53  
 authenticating, 179  
 cleaning of personal data, 375–376  
 discarded, risks to volumes and, 375–376  
 dissecting, 183  
 erasure or destruction of, 785  
 formatting, 184–186  
 high-level format, 185–186  
 low-level format, 184, 185f  
 fundamentals of, 180–183  
 history behind and description of, 180–183  
 magnetic recording, tapes and, 180  
 mechanism, 182f  
 partitions, 189–192  
 hiding data with, 191–192  
 partitioning and  
 fragmentation, 191  
 partitioning in modern systems, 191  
 partitioning to support older drive formats, 190

- rekeying, 414  
sectors and clusters on, 185–186, 185f  
speeds for, 184  
storing data on, 179–186  
typical, 181f
- Hard drive controller, 183–184  
hardware block diagram of, 183f
- Hard drive volume, with full-disk encryption, 374f
- Hardened protected distribution systems, 786
- Hardware, 15  
block diagram, 183, 183f  
encryption in, 409–413  
drive controller, 410–412  
drive formatting, 411–412  
recycling the drive, 409–410  
security boundary, 411  
physical damage to, 37  
working key storage in, 414
- Hardware failures, ensuring recovery from, 581
- Hash  
encrypting, two steps, 355f  
keying, one step, 356f
- Hashed MAC, 635
- Hash functions, modern, 235–236, 235t
- Hashing, 617  
constructing SSL keys through, 633f  
secret keys, 623–624  
to build a traffic key, 624f
- Hashing passphrase, for file encryption key, 322f
- Hash values, 234, 235t, 639  
changed, detecting, 355–356  
keyed hash, 356, 356f
- HDMI. *See* High-Definition Multimedia Interface
- Header, 184
- Head tags, HTML, 701
- Health Insurance Portability and Accountability Act, 165, 558, 565, 569
- Heating, ventilation, and air conditioning, 581
- Hebern, Edward, 289
- Hellman, Martin, 340, 343
- Heroditus, 542
- Hertz (Hz), 442
- HFS+. *See* Hierarchical file system plus
- Hibernation state, 420
- Hierarchical directory, 95
- Hierarchical file system plus, 201, 205–206
- Hierarchical levels, security clearances and, 761
- High-assurance cryptography, 777
- High-assurance systems, 790–791
- High availability, 742
- High-Definition Multimedia Interface, 52
- High-level format, 185–186  
fragmentation, 186  
quick format, 186
- Highlighted tag, hypertext links, 702
- HIPAA. *See* Health Insurance Portability and Accountability Act
- Hiring process, 577
- HMAC. *See* Hashed MAC
- Hoaxes, email, 679
- Holberton, Frances Betty, 733
- Honeywell Corporation, 481, 482
- Hops, counting, 485
- Host, 425  
network integrity and, 429–432
- Host addresses  
finding, 453–455  
addresses from keyboard commands, 453–454  
addresses from Mac OS, 454–455  
addresses from Microsoft Windows, 455  
retrieving, Windows command for, 454f
- Host control, Internet traffic control and, 681
- Hostile intelligence services, 750
- Hostile users  
effectiveness of access control, encryption and, 377t  
securing a volume and, 376
- Hosts  
address resolution protocol, 495–496  
behind NAT gateways, 538  
email URLs and, 704–705  
IP addresses and, 493–494  
IP packet format, 494–495  
packet fragmentation, 495  
talking between, 491–496  
socket addresses, 492  
socket API capabilities, 492–493  
socket interface, 491–492
- HOSTS.TXT, 528
- Hotel room card keys, 252
- Hot standby, 601
- Hourglass  
I/O and file systems, 208, 209f  
network protocols, 458f
- Household security policy, for weak threat environments, 267, 267t
- HR. *See* Human resources
- HTML. *See* Hypertext Markup Language
- HTTP. *See* Hypertext Transfer Protocol
- HTTP tunneling  
description of, 711–712  
firewalling and, 712  
packet format for, 712f
- Hubs, for wired LANs, 461
- Human-based intelligence gathering, 754
- Human resources, 363
- HUMINT. *See* Human-based intelligence gathering
- Hunter's dilemma, 4
- Hurricanes, 595
- HVAC. *See* Heating, ventilation, and air conditioning
- Hypercubes (topology), 473
- Hypertext, coining of term for, 699
- Hypertext fundamentals, 699–709  
addressing Web pages, 703–706  
formatting: Hypertext Markup Language, 700–703. *See also* Hypertext Markup Language

- Hypertext Transfer Protocol, 703. *See also* Hypertext Transfer Protocol  
 retrieving static web pages, 706–709  
 Web directories and search engines, 708–709  
 Web servers and statelessness, 707–708  
 Web standards, 700
- Hypertext links, 701–702, 702f
- Hypertext Markup Language, 700, 727  
 Cascading Style Sheets, 702–703  
 formatting with, 700–703  
 hypertext links, 701–702, 702f  
 source text, 701f
- Hypertext Transfer Protocol, 683, 703  
 retrieving data from other files or sites, 703  
 retrieving web page with, 706f  
 states and, 728–730  
 browser cookies, 729–730
- IBM, 77, 481  
 IBM System/38, 118
- ICANN. *See* Internet Corporation for Assigned Names and Numbers
- ICMP. *See* Internet Control Message Protocol
- ICV. *See* Integrity Check Value
- IDE. *See* Integrated Drive Electronics
- Identity-based access control, multilevel security and, 796
- Identity theft, 229–230  
 laptop risk assessment and, 29  
 online business, 34–35  
 social media, 35
- Identity thieves, identifying specific attacks by, 28, 28t
- IDS. *See* Intrusion detection systems
- IEC. *See* International Electrotechnical Commission
- IEEE. *See* Institute for Electrical and Electronics Engineers
- IETF. *See* Internet Engineering Task Force
- IIS. *See* Internet Information Services
- IKE Protocol. *See* Internet Key Exchange Protocol
- ILOVEYOU virus, 677–678
- Image backups, 597
- Image formats, common, 707
- IMAP. *See* Internet Message Access Protocol
- IMP. *See* Interface Message Processor
- Implementers, training and expertise for, 572
- Inbound connections, 541
- Incident response and attack, 171–175  
 aftermath of an incident, 173–174  
 digital forensics, 173  
 fault and due diligence, 173–174  
 compromised systems, 172  
 incidents and damage, 172  
 legal disputes, 174–175
- Incidents, aftermath of, 173–174
- Include instrumentation code, 584
- Incomplete page encryption, browser warning about, 636f
- Incremental backups, 597
- Independent guesses, making, 248
- Index variable, 192
- Indirect authentication, 590–593, 590f  
 description of, 590  
 properties of, 593  
 redirected authentication, 592–593  
 service-based authentication, 591–592  
 ticket-based authentication, 591
- Indirect design pattern, 586
- Industrial systems, security risks and, 3
- Inference  
 aggregation and, 734  
 challenge of secrecy and, 751  
 database security and, 734
- Infiltration, serious attacks and, 599
- Information, general types of attacks on, 26–27, 27f
- Information Assurance (IA) Courseware Evaluation (IACE) Program, 574
- Information networks  
 building, 471–481  
 bus network, 476–477, 476f  
 mesh network, 480–481  
 network topology, 473  
 point-to-point network, 473–474  
 star network, 474–476  
 tree network, 477–480
- Information resources  
 management, 569–570  
 lines of authority and, 569  
 managing information security and, 570
- Information security, national system security and, 773
- Information security architecture, 18–19
- Information security management system, 564
- Information security professionals, 572–575  
 college degrees for, 573
- information security certification for, 574–575  
 information security training for, 573  
 training and expertise of, 572
- Information security training  
 college courses, 573  
 hands-on training, 573  
 product-specific training, 573
- Information states, 124–125  
 encryption and, 284–286, 285f  
 illustrating policy with state diagram, 284–285  
 proof of security, 286
- of essay file, 125f
- network applications and, 464

Information system center, 581  
Information system protection, 580–581  
Information systems  
audits of, 162  
secrecy and, 753–754  
Information Systems Audit and Control Association, 574  
Infosec officer, 570  
Inheritance, static, 154  
Inherited rights  
  ACLs and, 154  
  adding to, in Windows ACL, 157f  
Initialization vector, 392  
  ESP packet format and, 640  
Inodes, 203–204  
Input/output  
  device independence and, 208  
  file system software and, 207–216  
  hourglass design and, 208  
  security and, 215–216  
  file access restrictions, 216  
  restricting devices themselves, 215–216  
  restricting parameters in I/O operations, 215  
  software layering and, 210–213  
    abstraction, 212–213  
    example of, 210–211  
    layering logic, 211–212  
  typical operation, 213–214  
  call-operating system, 213  
  driver starts actual I/O device, 214  
  I/O operation ends, 214  
  OS constructs the I/O operation, 213–214  
Input/output (I/O) circuits, 50f, 51  
Input/output (I/O) connections, 50f  
Input text validation, 584  
Insider attacks, 561  
Insider threats, 17–18, 432  
  reducing risks of, 561  
Insider trading, 559  
Institute for Electrical and Electronics Engineers, 52

Integrated Drive Electronics, 51  
Integrity  
  security services and, 9–11, 86, 607  
  Web, 741  
Integrity checking, security software and, 585  
Integrity check value, 179  
  ESP packet format and, 640  
Integrity of operations, 792–795  
  achieving nuclear high assurance, 794–795  
  force surety and, 793–794  
  for nuclear operations, 793  
  positive control and, 793  
Intelligence gathering, 754–755  
Interactive guessing, 238–239  
Interface logic, reading encrypted data from hard drive and, 413  
Interface Message Processor, 486, 486f  
Interior routing, autonomous systems and, 488  
Internal keys, 322  
  changing, 327  
  with nonce, software checklist for, 329  
Internal security labels, 585  
International Electrotechnical Commission, 564  
International Information Systems Security Certification Consortium (ISC<sub>2</sub>), 574  
International rerouting, 490  
International Standards Organization. *See* ISO  
International Telecommunications Union, 546  
International Traffic in Arms Regulation, 385  
Internet. *See also* Names on the Internet; Web security; World Wide Web  
  emergence of, 482–483  
  old and new routing structures, 489f  
Internet access policies  
  evolution of, 680–681  
  simple, 681, 681t  
Internet addresses  
  in practice, 497–502  
  IPv4 address classes, 498  
  network masks, 497–498, 497f  
Internet applications, traditional, 657–658  
Internet Assigned Numbers Authority, 485–486  
Internet Control Message Protocol, attacks on  
  ping attacks, 520–521  
  ping floods, 521  
  ping of death, 521  
  redirection attacks, 521–522  
  smurf attack, 521  
Internet Corporation for Assigned Names and Numbers, 525, 531, 722  
Internet email, 658–671  
  authenticated email, 670–671  
  categories of standards for, 658  
  elements of format for, 659f  
  forging email messages, 668–671  
  message formatting standards, 658–659  
  message headers, 659–660  
    additional headers, 660  
    From: header, 659–660  
    To: header, 660  
  MIME formatting, 660–663  
  presidential, 668–669  
  protocol standards, 663–665  
    email delivery, 664–665  
    mailbox protocols, 663–664  
    port number summary, 665  
    tracking an email, 665–668  
Internet Engineering Task Force, 488, 632, 695, 700  
Internet Explorer, 703  
Internet gateways and firewalls, 535–542  
  filtering and connectivity, 540–541  
  inbound connections, 541  
  packet filtering, 540  
network address translation, 536–540  
configuring DHCP and, 538–540

- overview of, 535–536  
 small LAN connects its ISP through a single gateway, 535f  
 software-based, 541–542
- Internet Information Services, 703
- Internet Key Exchange Protocol, 341, 625, 642–643  
 starting negotiation, 643f
- Internet layer, 483, 483f
- Internet Message Access Protocol, 663, 665
- Internet packets  
 routing, 485  
 scope of addressing information in, 498t
- Internet policy directives, Web security and, 709–710
- Internet Protocol, 461, 482, 483, 483f  
 displayed in Wireshark, 505f  
 layering, routing and, 516f
- Internet routing, 483, 484, 516
- Internet security  
 early attacks on Internet, 487  
 early defense of Internet, 487–488  
 evolution of, 485–488  
 protecting the ARPANET, 486–487
- Internet service providers, 483, 488  
 enterprise point of presence and, 689  
 starting, 490–491
- Internet services, 657–658
- Internet software, cryptography added to, 608f
- Internet Storm Center, 67
- Internet structure, 488–491  
 autonomous systems, 488–489  
 routing security, 489–490  
 starting an ISP, 490–491
- Internet traffic control, 681–683  
 gateways and, 682  
 packet headers and, 682f
- Internet transport protocols, 514–523  
 attacks on protocols, 520–523
- Transmission Control Protocol, 516–519
- User Datagram Protocol, 515–516
- Interpreter, 106
- Interpreter program, 103
- Intruders, catching, 160–161
- Intrusion detection systems, 689–690
- Intrusion prevention systems, 690
- Invisible partitions, 191
- I/O management; operating system and, 60
- I/O system, 61
- IOU, with adjustable check value, 354f
- IP. *See* Internet Protocol
- IP addresses, 483, 493–494  
 address locations in packet headers, 493f  
 dotted decimal notation for, 493f  
 global, 499
- IP version 4, 494
- IP version 6, 494
- private, 499–502  
 assigning, 500–501  
 dynamic host configuration protocol, 501–502  
 virtual private networks and, 642
- IP packet format, 494–495  
 major field contents, 494–495  
 major IP packet fields, 494f  
 packet fragmentation, 495
- IPsec gateways  
 encryption of packet and, 638f  
 virtual private networks and, 642
- IP Security Protocol (IPsec), 636  
 classified military networks and, 652  
 components of, 639  
 network layer encryption and, 609–610  
 packet protected with, 610f
- IP spoofing attacks, 518, 522–523
- IP version 4 (IPv4), 494, 498
- IP version 6 (IPv6), 494
- Iraq war, redaction problem and, 753
- Ironport, 668, 685
- ISACA. *See* Information Systems Audit and Control Association
- Islamic law, 174
- Islands, 71–72, 79, 117, 118
- ISMS. *See* Information security management system
- ISO 8859-1 character set, 661
- ISO 9000, 565
- ISO 9001, 565
- ISO 17799, 566
- ISO 27000, 165, 566
- ISO 27001, 571–572
- ISO/IEC 21827, 566
- ISO/IEC 27001, 564, 565, 566
- ISO/IEC 27002, 565, 566
- Isolation and mediation, islands and, 72
- Isolation policy  
 compact access rules for, 123t  
 enforcing, security controls and, 123, 123t
- ISPs. *See* Internet service providers
- ITAR. *See* International Traffic in Arms Regulation
- Iteration, security process and, 7
- ITU. *See* International Telecommunications Union
- IV. *See* Initialization-vector
- J
- Jamming, 782  
 electronic warfare and, 782–783  
 spread spectrum techniques and, 783
- Java, 106  
 buffer overflows checked with, 66
- JavaScript, 106, 725  
 client-side HTML script in, 726f
- Java Server Pages, 725
- Jerusalem virus, 105
- Jewish law, 174

- Job rotation, reducing risk of insider threats and, 561
- Joint Photographic Engineering Group, 707
- Joomla, 731
- JPEG. *See* Joint Photographic Engineering Group
- "JPEG of death,", 714
- JS. *See* JavaScript
- JSP. *See* Java Server Pages
- K
- Kaplan, Ray, 14
- Katz, Phil, 308
- KDC. *See* Key distribution centers
- KEKs. *See* Key encrypting keys
- Kelsey, John, 384
- Kerberos, 118, 591, 623  
ticket-based authentication by, 591f
- Kerckhoff's principle, 74, 282, 284, 388
- Kernel mode, 77
- Keyboard commands, host addresses from, 453–454
- Keyboards, 51
- Key distribution  
objectives, 616–617  
problem, 317  
strategies, 617  
techniques, 617–618
- Key distribution centers, 617, 621, 622–623  
keys wrapped in, 623f
- Keyed hash, 356
- Key encrypting keys, 331  
encryption of CEK, key wrapping and, 330f  
key encapsulation with RSA and, 347  
key wrapping and, 621, 622
- Separation of Duty and, 334–335  
wrapped keys and, 415–416
- Key expansion, 380
- Key field, in User tables, 732
- Key fingerprint, 366
- Key handling  
end-to-end, internet access, 651t
- software checklist for, 323
- Key ID, wireless packet protection and, 646
- Keying  
deploying cryptography on Internet and, 613, 615  
hash, one step, 356f
- Key leakage, through spying, 776–777
- Key management, 317–325  
cryptonets and, 318  
cryptoperiods and, 320  
distributing new keys, 320  
key-sharing procedures for, 319  
key strength and, 323–325  
levels of risk in, 318  
problems related to, 615–616  
public-key cryptography and, 320–321  
rekeying and, 319–321  
text used for encryption keys, 321–323
- Key rollover, 319
- Keys. *See also* Wrapped keys  
combining with nonce, 328–329  
on DVD hidden track, 335f  
employees and, 577  
encapsulation with RSA, 345–347, 346f  
intercepted, 419–420  
internal, 322  
new  
distributing, 320  
encrypted with old, 620–621, 620f  
private, 337  
public, 337  
sniffing from swap files, 420
- Key schedule, 380
- Key-sharing procedures, 319
- Key sizes  
comparable, 350t  
selecting, 349–350
- Key splitting, 332–333  
with xor, 332f
- Key storage  
persistent, 414–416  
key wrapping, 415–416
- managing removable keys, 416
- protected storage, 415
- Key stream, 295–296  
diagram of, 393  
eliminating with "xor,", 326  
generating, 295–296  
improved, from one-way hash, 297f
- Key stream security, 298–299
- RC4 biases  
effects of ciphertext errors, 299
- pseudo-random number generators, 298–299
- Key strength, operating recommendations, 324–325
- Keystroke loggers, 236, 237f
- Key update, 620
- Key wrapping, 320, 330–333, 347, 415–416, 617, 621–622  
content encrypting key in, 621
- cryptoperiods and, 332  
for email, 629f
- KEK encrypting CEK, 330f  
in key distribution centers, 623f
- key splitting and, 332–333  
multiple recipients and, 331–332  
software checklist for, 333
- Kismet, 644
- Klein, Daniel, password study by, 250–251, 324
- Knapsack, 339f
- Knudsen, Lars, 384
- Kohnfelder, Loren, 360
- Krebs, Brian, 23
- Kuwait, 755–756
- L
- LAMP, 732
- Lampson, Butler, 81
- Lampson's matrix, 80–81
- LAN addressing, 452
- Language-based password bias, estimating, 250–251
- LANs. *See* Local area networks

- Laptops, encrypted hard drives and, 418
- Laptop theft, at workplace, 560
- Large numbers, abbreviations for, 193
- Large-scale attacks, phases of, 599
- Lattice, of compartment clearances, 769, 769f
- Layer 2 devices, 461
- Layer 2 nodes, 483
- Layer 3 routers, 483
- Layer 7 protocols, network applications and, 657
- Layered defense, 19
- Layoffs, insider threats and, 561
- Layout information, executable files and, 101
- Least Privilege, 334, 560 access rights and, 100 administrative users and, 139–142 administration by regular users, 139–141 user account control on Windows, 141–142 boundaries and, 15–16 compartments and, 765 execute right and, 102 information resources management and, 569 sharing dilemma and, 135
- Legal disputes resolving, 174–175 security incidents and, 174–175
- Legal evidence collecting at scene, 177 documenting the scene, 178 securing the scene, 177–178
- Legal obligations, companies, secrecy, and, 557
- Legal systems, categories of, 174
- Lie detector tests, security clearances and, 763
- Life-cycle procedures, national system security and, 774
- Lindsey, Robert, 776
- Lines, on phone network, 472
- Link, 425
- LinkedIn, ZeuS and, 109
- Link encryption on 802.11 wireless, 643–649 Wi-Fi protected access: WPA and WPA2, 645
- Wired Equivalent Privacy, 645 wireless defenses, 644–645 wireless LAN security boundary, 644f wireless packet protection, 645–647
- Link layer encryption, 802.11 wireless and, 608–609
- Link protocol, 457
- Linksys, 645
- Linksys commercial wireless gateway, settings for, 539–540, 539f
- Linux, 57, 142, 462 ext3 file system, 203 local authentication and, 589 truly random sources and, 244
- Linux, Apache, MySQL, PHP. *See* LAMP
- Linux systems, synchronization programs for, 86
- Lisp, 103, 106
- LMDS. *See* Local management device
- Load-balancing, high Web availability and, 742
- Load balancing routers, 516
- Local area networks, 425, 426 file sharing on, 466f mapping with nmap, 505–508
- physical protection of, 428f protecting external wires, 429 protocols, 483, 483f sending a packet from one to another, 484, 484f simple, protocol software layers on, 461f small, firewalls and, 536 wireless security boundary, 644f
- Local authentication, 587–588, 587f benefits and shortcomings with, 587–588 description of, 587
- Local design pattern, 586
- Local management device, keys handled by, 781–782
- Log entry, 162
- Logging events, 161–164
- Logic bombs, 560
- Login process, 223
- Long-distance networking, 542–549 evolving technologies bidirectional satellite communications, 549 optical fiber networks, 549
- mature technologies cable TV, 548–549 cell phones, 548 dedicated digital network links, 548
- older technologies analog-based digital networks, 545–546 analog broadcast networks, 545
- analog two-way radios, 547–548
- circuit-switched telephone systems, 545
- microwave networks, 546–547
- overview of, 542–544
- Long file names, FAT directories and, 200
- Loop device, 402
- Lost control effectiveness of access control and encryption, 377t securing a volume and, 376
- Lost files, laptop risk assessment and, 29
- Lost packets, recovering, 447–448
- Lottery fraud, 672–673
- Lotus Notes, 630
- Lower bound, 247
- Low hanging fruit, 228
- Low-level format on hard drive, 184 of hard drive sector, 185f
- Low power transmissions, countering EW attacks and, 783
- Lucifer, DES and, 382

Luggage lock, four-digit, 248–250, 249f  
Lynn, Michael, 44

**M**

MAC. *See* Mandatory access control; Media access control; Message authentication code

MAC address

- format for, 452f
- network interfaces and, 452
- security and, 453
- uniqueness of, 453

Machine instructions, 49

Macintosh

- file and directory name formats for, 97t
- synchronization programs for, 86
- System Monitor application on, 60

Macintosh OS-X, 142, 401, 402

Macintosh OS-X ACLs, 146–149, 147f

- modifying rights on entry, 148f

Mac OS, host addresses from, 454–455

Macros, 107

Macro viruses, 106–107

- email viruses implemented as, 677

Macrovision copy protection, 311, 313

Magic number, executable files and, 101

Magnetic recording and tapes, hard drives and, 180

Magnetic stripe cards, 224t, 252

Magnetic tape drive, 181f

Mailbox protocols, 663

- POP3: an example, 663–664

Mail exchange, 667

Mainframe computers, 77

Maintenance crews, 22

Major attacks, handling, 599

Malicious acquaintances, 22, 112

Malicious changes

- detecting, 352–355
- birthday attacks, 354–355

one-way hash functions, 352–355

Malicious employees, identifying specific attacks by, 28, 28t

Malicious software. *See* Malware

Malicious viruses, 105–106

Malware, 2, 77, 107–110, 367.

- See also* Botnets

Conficker or Downadup, 107, 108–109

Cryptolocker/ Cryptowall, 109–110

exploit, 127

pattern detection, 74

Pushdo/Cutwail, 107, 109

Stuxnet, 107, 110

Waledac, 107, 108

Web traffic scanning and, 710

Zeus, 107, 109

Management hierarchies and delegation, 567–569

- in larger organization, 568f
- profit centers and cost centers, 568–569

implications for information security, 569

Management processes, 563–575

- auditing and review, 563
- delegation through management hierarchy, 563
- written policies and procedures, 563

Mandatory access control, multilevel security and, 795

Man-in-the-middle attack, 359

Manual keying, 617, 618–619

Mapping, of network drive, 467–468

Marine band, 444

Markup languages, 700

MARS, 309, 384

Masking, TEMPEST problem and, 787

Masquerade attacks, 230–231, 559

- direct authentication and, 589

Masquerades, 27, 427, 606

- bus network and, 477
- file protection policies and, 112

server, 719–722

social engineering and, 559, 563

Massachusetts Institute of Technology, 14, 66

Massey, Suzanne, 161

Master Boot Record, 105

Master file table, 206, 206f

“Master key” risk, 420–421

Master keys, employees and, 578

MBR. *See* Master Boot Record; Master boot record

McAfee, 308

MD4, 235t

MD5 hash value, 353

Media access control, 452

Media sanitation and destruction, 785

Mediation, 175

Melissa virus, 677

Memory mapped I/O, 215

Memory size names, acronyms and, 192, 193t

Memory sizes, address variables and, 192–194

Mesh-network, 473, 480–481, 480f

- benefits with, 481
- limitations with, 481

Message API (MAPI), 663

Message authentication code, SSL record transmission and, 635

Message Digest 5 (MD5), 235, 235t

Message headers

- for Internet email, 659–660
- additional headers, 660
- From: header, 659–660
- To: header, 660

Message integrity check, 646

- calculating, 647

Message switching, 435

- advantages and disadvantages of, 435

Message transfer agents, 664–666

Metcalfe, Robert, 475

Metcalfe’s law, 475

MFT. *See* Master file table

MIC. *See* Message integrity check

- Mice, 51  
Michelangelo virus, 105  
Microcomputers, 79  
Microphones, 545  
Microsoft Corporation, 57, 103  
certifications through, 574  
FAT file system formats, 197t  
Point to Point Tunnelling  
Protocol, 326  
Microsoft email products, 663  
Microsoft Windows, 791  
basic file sharing, 135–136  
dynamic link libraries (.dll), 81  
enabling file encryption, 303f  
file and directory name  
formats, 97t  
host addresses, 455  
resource oriented permissions, 119f  
security event log, 160f  
SYSTEM user identity, 122  
Task Manager, 60  
process display, 140f  
user account control, 141–142  
Microsoft Windows ACLs, 150–159, 150f  
default file protection, 154–156  
dynamic ACLs, 154–156  
inherited rights, 154  
denying access, 151–154  
determining access rights, 152–153  
effective, building, 153–154  
evolution of, 150–151  
for survey folder, 156f  
Microwave, 442  
Microwave antenna, tower with, 547f  
Microwave networks, 546–547  
Military deception, 755

Multipart Internet Message Extensions, 658  
Multiperson control, reducing risk of insider threats and, 561  
Multiple servers, enterprise network authentication and, 585  
Multiple single levels, system-high mode of operation and, 798  
Multitasking, 58–59, 77, 795  
MX. *See* Mail exchange  
MySpace, ZeuS and, 109. *See also* Negative acknowledgment

## N

NAK. *See* Negative acknowledgment  
Names on the Internet, 523–535.  
*See also* Domain names

attacking DNS, 531–535  
cache poisoning, 533  
DNS security improvements, 534–535  
DOS attacks and DNS resolvers, 534  
DOS attacks on DNS servers, 533–534  
common top-level domain acronyms, 524t  
DNS protocol, 528–531  
DNS redundancy, 530–531  
resolving domain name via redirection, 529–530

domain names hierarchy of, 523f  
investigating, 531  
in practice, 525–526  
three-part, 525f  
using, 526  
looking up, 526–527  
name space, 524–525

Napoleonic law, 174  
NAT. *See* Network address translation  
National Center of Academic Excellence, in IA education, 574

National defense systems, CNSS standards for information assurance requirements, 792  
National firewalls, 694–695  
*National Industrial Security Program Operating Manual*, 751  
National Institute of Standards and Technology. *See* NIST  
National policy issues, 770–775  
certification and accreditation, 775  
distinctive threats, vulnerabilities, and countermeasures, 772  
facets of national system security, 772–774  
legal elements, 770–771  
personnel roles and responsibilities, 771–772  
security planning, 774–775  
National security, legal basis for classification system and, 758  
National Security Agency, 292, 326, 636  
cryptographic standards and, 776, 777  
declassified intercepts from VENONA project, 768f  
elliptic-curve cryptography standards, 344  
Lucifer and, 382  
media erasure/destruction procedures approved by, 785  
redacted document, 753f  
Type 1 cryptographic products and, 778  
National security information, 41–42  
National Security Telecommunications and Information Systems Instruction 7003, national PDS guidance and, 786

National Security Telecommunications and Information Systems Security Committee, 770

National system security facets of, 772–774  
communications security, 773  
information security, 773  
life-cycle procedures, 774  
physical security, 772–773

*National Treasure* (film), 279

Natural threats, 23

Needham, Roger, 232

Need to Know classified information and, 761  
access to, 796  
companies, secrecy, and, 558–559  
controls, 585  
dedicated mode of operation and, 797

Negative acknowledgment lost packet recovery and, 447  
wireless retransmission and, 457

Nelson, Ted, 699

Netgear products, 645

Netscape Commerce Server, 631

Netscape Communications, 611, 631

Netscape Navigator, 631, 631f  
public-key certificates and, 362

Netscape software, 631

NetStumbler, 644

Network address translation, 500, 501, 536–540  
processing first packet with, 537f

Network applications, 462–468, 657

data and file sharing, 465–468  
delegation and, 467–468  
information states and, 464  
peer-to-peer strategy and, 463–464

resource sharing and, 464–465  
servers and, 463  
Network-based guessing, 239  
Network cables, 451  
Network defenses

- cryptographic, 427  
functional, 427  
logical, 427  
mechanical, 427  
physical, 427  
procedural, 427
- Network effect, 475
- Network efficiency, overhead and, 446–447
- Network encryption, 605–652  
administrative and policy issues, 613–615  
communications security, 605–615  
crypto atop protocol stack, 628–636  
cryptographic security requirements, 649–652  
crypto keys on a network, 615–628  
link encryption on 802.11 wireless, 643–649  
network layer cryptography, 636–643
- Network hub, 450
- Network Information System, 589
- Network inspection tools, 502–508  
nmap, 502, 505–508  
Wireshark, 502–505
- Network integrity, host and, 429–432
- Network layer, OSI protocol model, 461
- Network layer cryptography, 636–643  
encapsulating security payload, 639–641  
implementing a VPN, 641–642  
Internet Key Exchange protocol, 642–643
- Network layer encryption, IPsec and, 609–610
- Network layer protocols, evolution of, 636–637
- Network mapper utility, 506–507
- Network masks  
defined, 497  
interpreting, 497f
- Network message, unprotected, passive attack on, 606f
- Network protocol process, I/O system and, 61
- Network protocols  
attacks on, 520–523  
hourglass structure of, 458f
- Network security problem, 425–432  
basic network attacks and defenses, 426–428  
host and network integrity, 429–432  
botnets, 430–432  
insider threat, 432  
network worms, 430  
physical network protection, 428–429  
protecting external wires, 429
- Networks of networks, 471–508  
building information networks, 471–481  
combining computer networks, 481–491
- Internet addresses in practice, 497–502  
network inspection tools, 502–508  
talking between hosts, 491–496
- Network subversion, at workplace, 560
- Network switch, 450
- Network topology  
evolution of phone network, 472–473  
summary of properties for, 473
- Network transparency, 608  
crypto atop protocol stack and, 628  
IPsec and, 610
- Network worms, 430
- Next Header, ESP packet format and, 640
- “Nigerian scam,” 672
- 9/11 Commission, 757
- NIS. *See* Network Information System
- NISPOM. *See* *National Industrial Security Program Operating Manual*
- NIST, 5, 310, 347  
cryptographic standards, 777  
elliptic curve cryptography standards, 344
- NIST’s federal standards, guidance for FISMA and, 771
- NIST Special Publication, 165
- nmap, 502  
mapping LAN with, 505–508  
network mapper utility, 506–507  
output of simple command, 506f  
port listing using -sV option, 507f  
using with caution, 507–508  
of Windows 7 host, 507f  
with -PN and -O options, 508f
- nmap scans, 599
- Nodes, 472
- No foreign distribution (NOFORN), 757
- NOFORN. *See* No foreign distribution
- No lone zone, 780, 780f
- Nonce, 254  
constructing encryption keys and, 328f  
four-way handshakes and, 648, 649, 649f  
internal keys with, software checklist for, 329  
keys combined with, 328–329
- Nondisclosure agreements, 42
- Nonrepudiation, 607  
digital signatures and, 359  
security services and, 86
- North American Numbering Plan, 478, 479
- Norton, 308
- NSA. *See* National Security Agency
- nslookup, 527–528
- nslookup list, of “any” DNS records found for eifsc.com, 528f
- NSTISSC. *See* National Security Telecommunications and Information Systems Security Committee

- NSTISSI. *See* National Security Telecommunications and Information Systems Instruction
- NT file system (NTFS), 201, 206–207, 206*f*
- Nuclear threat, government secrecy and, 750
- Nuclear weapons detonating, two-step process for, 794 integrity of operations and, 792–795 achieving nuclear high assurance, 794–795 force surety and, 793–794 nuclear operations, 793 positive control and, 793 no lone zone and, 780, 780*f* risks posed by, 793 U.S. military policy for control of, 793
- Numbers large, abbreviations for, 193*t* truly random, 243
- Objects, 115
- Odd parity, detecting error in, 187, 187*f*
- OFB mode. *See* Output feedback mode
- Off-line attack, 239
- Off-line authentication, 593–594 description of, 593 with public-key certificates, 593–594, 594*f*
- Off-line design pattern, 586
- Off-line password cracking, 239–240
- Olympic Torch virus hoax, 679
- One big cryptonet strategy, 617
- One-time pads, 299–301 modular arithmetic and, 300–301, 301*f* practical, 301 Soviet espionage and, 300, 325
- One-time password, 224*t*
- One-time password tokens, 252, 257–259 attacking, 259
- generating one-time password, 258*f*
- SecurID, 257, 257*f* on smartphones, 258
- One-way hashes, 232, 279, 328*f* improved key stream from, 297*f*
- One-way hash functions, 234–236 cryptographic, 322 detecting malicious changes and, 352–355 performance of, 236 procedure diagram of, 234*f*
- Onion routing, 744
- Online shopping, 631
- Open Design, 387 cryptography and, 74 description of, 73
- OpenID authentication, 593
- Open source software, 142
- Open Systems Interconnect model, layers of, 460–462
- Operating system layers, procedure calls between, 211*f*
- Operating systems, 57, 60–61 access rights for files provided by, 98 event logging in, 163*f* I/O system, 60–61 security features with, 79
- Operating systems kernel, 103
- Operational key, 782
- Operations security, 755–756
- Operation Tovar, 109
- Operator errors, 77
- Opportunistic attacks, 231
- OPSEC. *See* Operations security
- Optical fiber, 449
- Optical fiber networks, 549
- Optical mechanisms, for communicating information, 544
- Optical media, erasing, 307–308
- Optical networks, 546
- Orange Book, 165, 565, 790, 796, 797
- ORCON. *See* Originator controlled
- Originator controlled (ORCON), 758
- Orphaned layers, 462
- OSI model. *See* Open Systems Interconnect model
- OS-X, resource oriented permissions, 119*f*
- OS-X padlock, unlocking with administrator's password, 140–141, 141*f*
- OTAR. *See* Over-the-air rekeying
- Other rights, in Unix, 142
- Outlook Exchange (Microsoft), 630
- Output feedback, 391
- Output feedback mode, 392 encrypting with, 393*f* key stream made with, 392 in practice, 393–394 weaknesses with, 395
- Over-the-air rekeying, 781, 782
- Overwriting, risks related to, 306–307
- Owner rights basic file sharing on Windows, 135 permission flags and, 121, 121*f* in practice, 122 Unix file permissions, 142, 142*f*
- P
- Packet addressing, IP addresses and, 484
- Packet capture file (pcap), 503
- Packet efficiency, 446
- Packet filtering, 540, 683, 683*f*
- Packet headers, 439 address locations in, 493*f* data in, 445 traffic controls and, 682*f*
- Packet number, wireless packet protection and, 646
- Packets with 802.11 link encryption, 609*f* acknowledgment protocol, 445–446 basic format of, 444*f* defined, 438 with end-to-end crypto, 612*f*

- fragmentation of, 495  
 IPsec gateway and encryption of, 638f  
 with IPsec protection, 610f  
 network efficiency and overhead, 446–447  
 sending from one LAN to another, 484, 484f  
 with SSL encryption, 611f  
 transmitting, 444–447  
 wireless protection of, 645–647
- Packet's CRC value, wireless packet protection and, 646
- Packet switching, 434, 438–440  
 advantages with, 439  
 disadvantages with, 439  
 mix-and-match network switching, 440  
 packet messages travelling and, 438f
- Padding Data, ESP packet format and, 640
- Padding length, ESP packet format and, 640
- Pagetable, 78
- Paging files, 420
- Pairwise transient key, 648
- Palo Alto Research Center, 425, 448
- Parallel construction, 177
- Parallel wiring, serial wiring *vs.*, 52–53
- PARC. *See* Palo Alto Research Center
- Parity checking, 187–188
- Partial insiders, enterprises and, 579
- Partitioned mode, computer modes of operation and, 797, 798–799
- Partitioning  
 fragmentation and, 191  
 in modern systems, 191
- Partitions  
 hard drive, 189–192  
 hiding data with, 191–192
- Passive attacks, 27  
 defined, 606  
 on unprotected network message, 606f
- Passive authentication tokens, 252–253, 253f
- Passive tokens, search space and, 258–259
- Passphrase interception  
 risks to keys and, 419, 419f  
 cold-boot attacks, 420  
 eavesdropping on encryption process, 420  
 sniffing keys from swap files, 420
- Passphrases, 241, 242t  
 hashing for file encryption key, 322  
 key strength and, 324  
 longer, taking advantage of, 322–323  
 reusing, 327  
 using for file encryption key, 321  
 wrapped keys and, 415–416
- Password bias  
 entropy and, 246  
 language-based, estimating, 250–251
- Password bias attacks, 245–251
- Password checking, CMS example  
 logging-in to website, 735  
 login process, 735–736, 736f
- Password cracking, 239
- Password cracking utilities, 246
- Password guessing, 238–245  
 cracking speeds, 244–245
- DOD password guideline, 238
- interactive guessing, 238–239  
 network-based guessing, 239  
 off-line password cracking, 239–240  
 password search space, 240–242  
 stories about, 238  
 truly random password selection, 242–244
- Password hashes, off-line trial-and-error attack on, 239
- Password hashing, 232–233  
 attacking, 250–251  
 procedure diagrams, 233
- Password Management Guideline (DOD)*, 238
- Password manager, 273
- Password-oriented injection attacks, 737–738  
 password that always matches in SQL, 737
- Passwords, 224  
 cracking, 324  
 matches in SQL, 739f  
 memorized, 224t  
 selection and handling of, 271–273  
 typing, masking space for, 232f
- Password search space, 240–242
- Password systems  
 evolution of, 231–237  
 one-way hash functions, 234–236  
 password hashing, 232–233  
 sniffing credentials, 236–237
- Password theft, laptop risk assessment and, 29
- Patch, defined, 126
- Patching process, 126
- Patching security flaws, 125–129
- Patent protection, 385
- Path name, email URLs and, 705
- Pattern-based access control, 74
- Patterns, 72–75
- Payload data  
 ESP packet format and, 640  
 wireless packet protection and, 646
- Payment Card Industry Data Security Standard, 165, 569, 571, 572
- PC. *See* Program counter
- pcap. *See* Packet capture file
- PCI DSS. *See* Payment Card Industry Data Security Standard
- PCIe. *See* Peripheral Component Interconnect Express
- PDS. *See* Protected distribution systems
- Peer-to-peer strategy, network services and, 463–464
- Penalties, modern security classification system and, 757

- Penetration test (pen test), 571, 572  
pen test. *See* Penetration test  
Pepys, Samuel, encrypted diaries of, 280, 284  
Perfect forward secrecy, Diffie-Hellman and, 341  
Periods processing, dedicated mode of operation and, 798  
Peripheral Component Interconnect Express, 51  
Perl, 103, 725  
Permission flags, 121–123, 121f, 122f  
ambiguities and, 143–144  
examples of, 144–146  
Permutations, rounds and, 380  
Persistent key storage, 414–416  
key wrapping, 415–416  
managing removable keys, 416  
protected storage, 415  
Persistent storage, working storage *vs.*, 53–54  
Personal computers evolution of, 78–79  
identity theft and, 375  
security on, 79  
Personal data, cleaning hard drive of, 375–376  
Personal files, access rights to, 120f  
Personal Home Page/Hypertext Preprocessor, 103, 106, 725, 732  
Personal identification numbers, 223, 224t  
Personal information authentication, 230–231  
Personal statements, official company statements *vs.*, 557  
Personnel security, 575, 576–579  
administrators and separation of duty, 579  
employee clearances, 576–577  
employee life cycle, 577–578  
employee roles, 578–579  
partial insiders, 579  
PGP. *See* Pretty Good Privacy
- PGP Directory, 367  
PGPDisk, 401, 402  
PGP MIME, 671  
Philby, Kim, 326, 768  
Phil Katz’ “Zip” compression program. *See* PKZIP  
Phishing, 671, 675–677  
bogus certificates and, 718  
misleading syntax and, 721  
tracking attacks of, 676–677  
window from early phishing attack, 676f  
Phone phreak, defined, 13  
Photo ID cards, pattern-based access control and, 74  
PHP. *See* Personal Home Page/Hypertext Preprocessor  
Physical disasters, ensuring recovery from, 581  
Physical layer, OSI protocol model, 461  
Physical network protection, 428–429  
external wires, 429  
for LAN, 429  
Physical security, 575  
in enterprises, 579–582  
environmental management, 581–582  
information system protection, 580–581  
power management, 580  
national system security and, 772–773  
Physical theft, 27, 426, 560  
PID. *See* Process identifier  
Ping, 496  
Ping attacks, ICMP and, 520–521  
Ping floods, ICMP and, 521  
Ping of death, 521  
Ping packet, displayed in Wireshark, 521f  
PINs. *See* Personal identification numbers  
Pins, input/output and, 51  
PKCS. *See* Public Key Cryptography Standards  
PKI. *See* Public-key infrastructure  
PKZIP, 308
- Plaintext, 281  
encrypting a volume and looking for, 408  
symmetric encryption and, 283f  
Plaintext files, erasing, 306–308  
Planning, security process and, 7  
Platters, hard drive, 182, 182f  
PLCs. *See* Programmable logic controllers  
PNG. *See* Portable Network Graphics  
Poe, Edgar Allan, 279  
Pointer variables, 192  
Point of presence. *See also* POP topology  
enterprise, 689–695  
Point-to-point network, 472, 473–474, 473f  
advantages with, 474  
disadvantages with, 474  
Point-to-Point Protocol, 636  
Point-to-Point Tunneling Protocol, 326, 636  
Policy directives, 564  
Policy motivations and objectives, 709–710  
Policy specifications, 564  
Polygraph examinations, security clearances and, 763  
POP3, 663–664, 665  
transcript of, 664  
POP topology, 690–693  
bastion-host, 690, 691  
dual firewalls, 690, 692–693, 693f  
single firewall, 690, 691, 691f  
three-legged firewall, 690, 691–692, 692f  
Portable Network Graphics, 707  
Portable Operating System Interface, 142  
Portion markings, for classified documents, 760f  
Port numbers, 491–492  
for email protocols, 665, 665t  
User Datagram Protocol and, 515–516  
Positive control, nuclear weapons and, 792, 793

- POSIX. *See Portable Operating System Interface*
- Postal systems, 543  
message switching and, 434
- POST command  
example login process and, 735–736, 736f  
password-oriented injection attacks and, 737  
web forms and, 723–724, 723f
- Postel, Jon, 486, 491
- Post Office Protocol, version 3.  
*See POP3*
- Potter, Beatrix, encrypted diary of, 280, 282, 284, 287
- Power alarms, 580
- Power cabling, protected, 580
- Power filtering, types of, 580
- Power grids, security risks and, 3
- PPP. *See Point-to-Point Protocol*
- PPTP. *See Point-to-Point Tunneling Protocol*
- Preboot authentication  
encrypted drives and, 417–418  
BIOS integration, 417, 417f  
disk-based authentication, 417–418, 417f  
with software encryption, 417f
- Predator drones, 615–616
- Presentation layer, OSI protocol model, 461
- Pretty Good Privacy, 308, 364, 671  
crypto atop protocol stack and, 629–630
- Preventative controls, 160
- Prime factors problem, public-key cryptography and, 339
- Printers, 51  
directly connected *vs.* sharing across LAN, 465f  
sharing, risks related to, 427  
policy statements, 427  
potential controls, 427–428
- Privacy  
reasonable expectation of, 176  
tailored policies and, 113  
Web, 743–745
- Privacy Enhanced Mail, crypto atop protocol stack and, 629
- Private action, 174
- Private browsing, 744–745
- Private codes, 224. *See also* Passwords
- Private IP addresses  
assigning, 500–501  
networks and use of, 501  
virtual private networks and, 642
- Private keys, 337  
stolen, 722
- Private key value, in Diffie-Hellman calculation, 342
- Private label algorithms, cautionary note, 389
- Private/public key pair, constructing, 338f
- Private searches, 176
- PRMF. *See Proprietor's RMF*
- PRNGs. *See Pseudorandom number generators*
- Procedure diagrams, 233  
of encryption, 281f  
of one-way hash function, 234f
- Process diagrams, 233
- Processes  
access matrix for, 81t  
active, observing, 59–60  
control section shared by, 81  
data section shared by, 82f  
partial list of, displayed by Unix ps command, 59, 60f  
programs and, 57–61  
running two at once, 58f  
security controls, 83–86  
separation of, 77–83  
switching between, 59–60
- Process identifier, 59–60
- Processing state, 124
- Process management, operating system and, 60
- Process protection  
dispatcher's design description, 88–90  
design features, 89  
dispatching procedure, 89–90  
functional security controls, 88  
risk assessment and, 87–88  
security controls for, 90, 90t
- security plan for, 86–90  
security requirements, 88, 89t
- Process state, 59
- Product-specific certifications, 574
- Professional certifications, 574
- Profit centers, 568–569  
information security and, 569
- Program counter, 54
- Programmable logic controllers, 3
- Programmed I/O, 215
- Programming languages, 106
- Programs  
computers and, 49–57  
executing, 54–56  
procedures and, 56–57  
processes and, 57–61  
separate control and data sections, 55–56, 56f  
sharing, 79–83  
access matrix and, 80–81  
access rights and, 81
- Program size, executable files and, 101
- Project and program managers, 568f
- Property thieves, 28t
- Proprietor's RMF, 6, 7f, 11–14
- Protected distribution systems, 786
- Protected power controls, 580
- Protecting files, policies for, 112–115
- Protections, modern security classification system and, 757
- Protocol attacks, 693–694
- Protocol layers  
headers added to packets with, 459f  
in ordering pizza, 460, 460f
- Protocols, defined, 439
- Protocol stack, 457–462  
adoption of secure email and application security, 630  
crypto on top of, 628–636  
hourglass structure of, 457, 458f
- OSI protocol model, 460–462
- Pretty Good Privacy, 629–630

- privacy-enhanced mail, 629  
relationships between layers, 459–460  
SSL handshake protocol, 632–634  
SSL record transmission, 634–636  
transport layer security—SSL and TLS, 630–632
- Protocol standards  
for Internet email, 658  
for the Web, 700
- Provisioning requirements, 577
- Proxies, 536  
anonymous, 744  
encryption of, 638  
firewall, 685
- ps command (Unix), 60  
partial list of processes displayed by, 59, 60f
- Pseudorandom number generators, 243
- key stream security and, 298–299  
self-rekeying and, 619–620
- Pseudorandom numbers, 243
- Psychological operations, 755
- Public announcements, enterprise community and, 576
- Publicity; companies, secrecy, and, 558
- Public-key building blocks, 624–626  
secret sharing with Diffie-Hellman, 624–625  
wrapping a secret key with RSA, 626, 626f
- Public-key certificates, 118, 360–362  
certificate authorities, 361–362  
constructing, 360–361, 361f  
expired: possibly bogus, probably not, 719  
information in, 360  
off-line authentication with, 593–594, 594f  
secure email and, 671  
self-signed, 366–367  
trickery with, 367  
valid, digital signatures in, 717
- Public-key cryptography, 320–321, 336–344  
asymmetric encryption algorithms, 339f  
attacking public keys, 340  
constructing public/private key pair, 338f  
Diffie-Hellman, 340–343  
elliptic curve cryptography, 343–344  
secret-key cryptography *vs.*, 338t  
secret-key *vs.* public-key crypto, 338t
- Public Key Cryptography Standards, 351
- Public-key encryption, 340
- Public-key infrastructure, 364
- Public keys, 303, 337  
attacking, 339–340  
distribution of, 617  
encryption of, 337f  
publishing, 359–369  
authenticated software updates, 367–369  
certificate authorities, 361–362  
certificate hierarchy, 364  
chains of certificates, 362–367  
public-key certificates, 360–362  
self-signed certificates, 366–367  
trickery with certificates, 367  
web of trust, 364–366, 366f  
techniques, 617
- Public-key techniques, choosing, 627–628
- Public opinion, psychological operations and, 755
- Public/private key pair, constructing, 338f
- Pushdo/Cutwail, 107, 109, 432
- Puzzles, 72–75
- PY. *See* Python
- Python (PY), 103, 106, 726
- Q
- QSA. *See* Qualified Security Assessor
- Qualified security assessor (QSA), 571
- Quantum computing techniques, key cracking and, 245
- Quantum cryptanalysis, 350
- R
- Radar signals, risks related to, 782
- Radio, 544, 545  
AM and FM, 443–444  
analog two-way, 547–548  
frequency sharing and, 443–444  
propagation and security, 444
- Radio frequency identification, 252–253
- Radio interference, spread spectrum techniques and, 783
- Radio signals, 442, 442f
- Radio transmissions, 442
- RADIUS, 592
- RAID, as backup, 597–598
- RAID 1 system, reliability of, 598
- RAID system, 414
- RAM. *See* Random access memory
- RAM management, operating system and, 60
- RAM protection, 78
- Random access, hard drives and, 180
- Random access memory, 50, 50f, 51, 222–223  
cold-boot attacks, 420  
separating data and control, 55–56
- sniffing keys from swap files, 420
- Random password selection, 242–244
- RB. *See* Ruby
- RC. *See* Replay count
- RC2, 386
- RC4, 298, 321, 325, 326, 330, 343  
cracking rapid penetration of WEP encryption and, 645  
flexibility of AES *vs.* flexibility of, 381
- RC4 biases, 298  
effects of ciphertext errors, 299
- pseudorandom number generators and, 298–299

RC4 story, 385–387  
 export restrictions, 385–386  
 leaking, then cracking of algorithm, 386  
 lessons learned, 386–387

RC6, 309, 384

Reachability  
 address scope dependent on, 499f  
 Layer 2 reachability matrix, 500t

Read, write, execute access rights, 102

Reader rights, basic file sharing on Windows and, 135

Reading, shared, tailored policies and, 113

Read-only (RO) access restriction, 80

Read-only memory, 54

Read-only sharing, 115

Read right, 100

Read/write (RW) access, 81

Read/write head, hard drive, 180, 181, 181f, 182f

Real-time media, challenge of, 695

Real-time Transport Protocol, 695

Recommended Standard 232 (RS-232), 545–546

Records, in data tables, 732

Recovery  
 disaster preparation and, 600–602  
 business impact analysis, 600  
 strategies for, 600–601  
 from hardware failures, 581  
 from physical disasters, 581

Recovery disks, physical damage, 37–38

Recursive resolvers, 527

Recycled CEK attacks, wrapped keys and, 418–419

Recycle folder, 171

Recycling  
 effectiveness of access control and encryption, 377t  
 securing a volume and, 376

Recycling drive, 409–410

Redacted NSA document, 753f

Redaction problem, 753  
 multilevel security and, 797

Redaction technology, disease testing and, 754

Red/black separation, in crypto device, 778, 778f

Redirected authentication, 592–593

Redirection attacks, ICMP and, 521–522

Red team, 164

Redundant array of independent disks. *See RAID*

Reference monitor, features of, 790

Registered Jack 45. *See RJ-45*

Registration, websites and, 735

Rekeying, 319–321  
 true, encryption key management and, 414

Relational databases, 732

Relativistic security decisions, 3, 4

Religious law, 174

Remediation, 172

Remote Authentication Dial-In User. *See RADIUS*

Removable keys, managing, 416

Removable storage devices, computer viruses and, 8

Replay count, 648

Reputation, companies and, 556–557

Request for Comments, 658

Request to Send, 457

Requirements-based decisions, 3

Resisting website command injection, 740

Resource API, 464

Resource-oriented permissions, 118–119

Resource sharing, 464–465

Retrieve from backup, 233  
 authentication tokens and, 260, 261t

biometric authentication and, 264

Retrieve from backup attack, 227, 228

Return address, 56

Reused keys  
 avoiding, 327–329  
 changing the internal key, 327  
 combining the key with a nonce, 328–329  
 software checklist for internal keys using nonce, 329

Reused key stream, 325, 326f

Reused key stream problem, 325–336

Revision control, software development security and, 582, 584

Revocation list, 594

Revolutions per minute, 184

RFCs. *See Request for Comments*

RFID. *See Radio frequency identification*

Ribbon cables, 53

Rich text format, email in, 661f

Rights, 115

Rijmen, Vincent, 384

Rijndael, 309, 384, 385

Ring topology, 473

Risk assessment, 8–19  
 cybersecurity, 8–19  
 goals and assets, 14–15  
 identifying assets, 15  
 identifying goals, 14  
 large-scale system, 24–25

Proprietor's RMF, 11–14

rule based, 9–11  
 security architecture, 18–19  
 security boundaries, 15–18

Risk identification, 19–32  
 threat agents, 20–26

Risk management framework, 5–8, 6f, 9, 771  
 Continuous Improvement, 8

Risk matrix, 19, 29–32, 31f

Risks  
 analyzing, 37–39  
 authentication and, 225–228  
 client scripting, 727–728  
 identifying, 12f  
 to laptop: example  
 calculating relative significance of attacks, 34

- estimating frequency of individual attacks, 32–33  
estimating impact of attacks, 34t  
estimating the impact of, 33–34  
prioritizing, 32–35
- Ritchie, Dennis, 142, 231
- Rivest, Ron, 235, 298, 344, 349, 385
- Rivest's Cipher 2. *See RC2*
- Rivest's Cipher 4. *See RC4*
- Rivest's Cipher 6. *See RC6*
- Rivest-Shamir-Adleman, 339f, 344–351, 617, 624  
applications with, 345  
bogus primes attacks on, 351  
brute force attacks on, 349–350  
factoring problem, 349  
original challenge, 349  
selecting key size, 349–350  
chosen ciphertext attacks on, 351  
cipher suites in SSL and, 613  
constructing key pair, 348f  
Diffie-Hellman *vs.*, secret key sharing and, 347  
digital signatures and, 344–345  
encapsulating keys with, 345–347  
overview of mathematics, 347–351  
small plaintext attack on, 350  
small private key attack on, 351  
timing attack on, 351  
wrapping secret key with, 626, 626f
- RJ-45, 449–451
- RJ-45 connectors, on Ethernet hub, 450f
- RMF. *See* Risk management framework
- ROM. *See* Read-only memory
- Roman law, 174
- Root certificate authority, 362
- Root directory, 95
- Rootkits, 430–431, 560
- Root zone, 529
- Rotor machines, 289, 291, 291f
- Round, 379, 381
- Routers, 44  
border, 489  
load balancing, 516
- Routine availability, 742
- Routing  
autonomous systems and, 488–489  
Internet, 483, 484, 516  
Internet packets, 485  
Internet protocol layering and, 516f  
mesh network and, 481  
in tree network, 478
- Routing security, 489–490  
international rerouting, 490
- Routing table, 485
- RPM. *See* Revolutions per minute
- RS 232. *See* Recommended Standard 232
- RSA. *See* Rivest-Shamir-Adleman
- RSA Data Security, 385, 386
- RSA digital signature  
constructing, 358f  
verifying, 358f
- RSA Laboratories, 347, 349, 384
- RSA private key, digital signature created with, 357
- RTP. *See* Real-time Transport Protocol
- RTS. *See* Request to Send
- Ruby, 726
- Rule-based access control, multilevel security and, 796
- Rule-based security decisions, 3, 4f
- RW. *See* Read/write (RW) access
- RWX. *See* Read, write, execute access rights
- S
- SA. *See* Security associations
- Safari browser, 462, 703
- Safeguards, 13
- Safeword, 592
- Same origin policy, scripts on the Web and, 728
- Sandboxing, 107  
scripts on the Web and, 728
- SANs. *See* Storage area networks
- SANS Institute, 67, 574
- SAP. *See* Special Access Program
- Sarbanes-Oxley Act, 165
- SATA. *See* Serial ATA
- Satellite communications, bidirectional, 549
- S-boxes, 380, 381, 382
- SC. *See* Security category
- SCADA devices. *See* Supervisory control and data acquisition devices
- SCADA systems, 616
- Schemes, web-oriented, 704
- Schneider, Jerry, 562
- Schneier, Bruce, 4, 384
- Schwartz, Randall, 43
- SCI. *See* Sensitive Compartmented Information
- Scope, 498, 498t
- Screened subnet, 689, 692
- Scripting languages, 103, 107, 725–726
- Script kiddie, 13, 112
- Scripts on the Web, 724–728  
client-side scripts, 726–728  
cross-site scripting, 728  
scripting languages, 725–726  
server-side scripts, 724–725
- SDHC. *See* Secure digital high capacity
- SDNS. *See* Secure Data Network System
- SDXC. *See* Secure digital extra capacity
- Search engines  
crime via, 708–709  
Web directories and, 708–709
- Search space  
active tokens and, 258–259  
passive tokens and, 258–259  
password, 240–242  
for random passwords or passphrases, 242t
- Secrecy  
challenge of, 751–754  
companies and, 557–559  
accountability, 558  
culture of, 558  
managing publicity, 558

- Need to Know, 558–559  
 obligations, 557  
 trade secrets, 557–558  
 discipline of, 752–753  
 information systems and, 753–754  
 exposure and quarantine, 753–754
- Secrecy in government, 749–756  
 classifications and clearances, 756–770  
 classification levels, 757–758  
 classification levels in practice, 763–764  
 compartments and other special controls, 764–770  
 security clearances, 761–763  
 security labeling, 759–761  
 classified information, 750–751  
 communications security, 775–784  
 data protection, 784–789  
 hostile intelligence services, 750  
 information security and operations, 754–756  
 intelligence and counterintelligence, 754–755  
 military information operations, 755  
 operations security, 755–756  
 national policy issues, 770–775  
 trustworthy systems, 789–799
- Secret classification, 757  
 Secret documents, storing, 763  
 Secret information, color codes for, 759  
 Secret investigations, 762  
 Secret-key building blocks, 621–624  
 key distribution centers, 622–623  
 key wrapping, 621–622  
 shared secret hashing, 621, 623–624
- Secret-key cryptography *vs.* public-key cryptography, 338*t*  
 Secret-key encryption, 340  
 Secret keys  
 protecting, 305–306  
 shared, symmetric cryptography and, 283  
 symmetric encryption and, 283  
 techniques, 617
- Secret-key techniques  
 choosing, 627  
 data integrity verified with, 607
- Secret sharing, Diffie-Hellman and, 340–341
- Sector encryption, with CBC and ESSIV, 405*f*
- Sector keys, on DVD, 335
- Sectors, on hard drive, 182, 185, 185*f*
- Secure Data Network System, 636
- Secure digital (SD) card, 199
- Secure digital extra capacity, 199
- Secure digital high capacity, 199
- Secure email and application security, adoption of, 630
- Secure Hash Algorithms, 235, 354
- Secure MIME (S/MIME), 612, 671
- Secure Multipart Internet Message Extension, 630
- Secure shell protocol, port numbers for, 492
- Secure Sockets Layer, 631–632  
 authenticating web server with, 714  
 cipher suites in, 613  
 socket layer encryption with, 610–611, 611*f*  
 transport layer and, 630–632
- SecurID, 591, 592  
 one-time password token, 257, 257*f*
- Security  
 capability-based, 118  
 I/O devices and, 215–216  
 file access restrictions, 216  
 restricting devices themselves, 215–216  
 restricting parameters in I/O operations, 215
- for operating system, 61  
 on personal computers, 79
- Security analysis, ethical issues in, 41–45
- Security architecture, 18–19
- Security architecture study, 18
- Security associations, 639, 648–649  
 bundling, 642  
 establishing, 648–649  
 establishing keys for, 648–649  
 IKE protocol and, 642
- Security audits, 570–572  
 compliance audits, 571–572  
 security scans, 572
- Security awareness, discipline of secrecy and, 752
- Security boundaries, 15–18
- Security boundary, encryption in hardware and, 411
- Security category, 9–11
- Security checklist, 5
- Security clearances, 757, 761–763  
 access permissions for, 762*f*  
 refusing, 763
- Security controls, 83–86  
 backup procedure, 84–85  
 categories of, 83, 84*f*  
 corrective, 83  
 detective, 83  
 to enforce isolation policy, 123, 123*t*  
 for file-sharing policy, 145, 146*t*  
 preventative, 83  
 for process protection, 90, 90*t*  
 security services and, 86  
 for shared project files, 145*t*
- Security controls for files  
 capabilities, 118  
 in practice, 117  
 resource-oriented permissions, 118–119
- Deny by Default, 116–117, 116*f*
- managing access rights, 117–119
- Security decisions, making, 3–5
- Security Engineering CMM, 565–566

Security event log, Microsoft Windows, 160f  
Security fault analysis, 778  
Security flaws  
  exploits and, 127  
  patching, 125–129  
Security goals, 14  
Security label, defined, 585  
Security labeling, 759–761  
  sensitive but unclassified, 761  
Security logs, 160–161  
Security management standards, 564–566  
  evolution of, 565–566  
Security measures, monitoring, 39–41  
Security Parameter Index, ESP packet format and, 639  
Security plan  
  defined, 18  
  for process protection, 86–90  
Security planning, 774–775  
  security system training, 775  
  system life-cycle management, 774–775  
Security policies, 36  
  authentication and, 225  
Security Protocol 3, 638  
Security requirements, 35–41, 40f  
  writing, 36  
Security scans, 572  
Security system training, standards and educational programs for, 775  
Security theater, 4  
Security Through Obscurity, 72, 73, 284, 644  
Seed key, 782  
Seek right, 100  
Seizure, collecting evidence and, 175  
SELECT command  
  example login process and, 735–736, 736f  
  password-oriented injection attacks and, 737  
  in Structured Query Language, 733, 733f  
Self-encrypting drive, 409  
  internal functions of, 410f  
Self-encrypting drive controller

  block diagram of, 411f  
  state diagram of, 412f  
Self-rekeying, 619–620, 619f  
  bootstrap in, 619  
Self-signed certificates, 362, 366–367  
Self-synchronizing ciphers, 397  
Senate website, defaced, 1999, 713f  
Senior management, 567, 568f  
Sensitive but unclassified information, 761  
Sensitive Compartmented Information, 764–767  
  clearances related to, 765  
  example of intelligence agency compartments, 765t  
  processing example for, 765–767  
Separation kernel, 791  
Separation mechanisms, 77–78  
  program modes, 77–78  
  RAM protection, 78  
Separation of Duty, 333–335  
  administrators and, 579  
  compartments and, 765  
  for early nuclear missile, 333, 334f  
  with encryption, 334–335  
  two-person integrity controls and, 779  
Sequence diagram, acknowledgment protocol and, 445, 446f  
Sequence numbers (SEQs), 518  
  ESP packet format and, 639  
  TCP and, 516  
Sequential access, 180  
Serial ATA (SATA), 52  
Serial ATA cables, 53, 53f  
Serial wiring, parallel wiring vs., 52–53  
Serious attacks, handling within enterprises, 598–599  
Serpent, 309, 384  
Server authentication, 714–719  
  expired certificate: possibly bogus, probably not, 719  
  invalid digital signatures: always bogus, 719  
mismatched domain name, 715–717  
revoked certificate: always bogus, 719  
with SSL, 714, 715f  
untrusted certificate authority: difficult to verify, 717–719  
Server masquerades, 719–722  
  bogus certificate authority, 720  
  misleading domain name, 720–722  
  stolen private key, 722  
  tricked certificate authority, 722  
Servers  
  multilevel, 799  
  network services and, 463  
  resource sharing and, 465  
Server Side JavaScript, 726  
Server-side scripts, 724–725  
  executing, 725f  
Service-based authentication, 591–592  
  for 802.11 access, 592f  
Service control, Internet traffic control and, 681  
Service loss attacks, 560  
Service request and reply, client and, 463f  
Session filtering, 683–685, 684f  
Session layer, OSI protocol model, 461  
setuid operation, 140  
SHA. *See Secure Hash Algorithms*  
SHA-0, 235, 235t  
SHA-1, 235, 235t  
SHA-224, 235, 235t  
SHA-256, 235, 235t  
SHA-384, 235, 235t  
SHA-512, 235, 235t  
Shamir, Adi, 344  
Shannon, Claude, 74, 300  
Shannon entropy, 246  
Shannon's maxim, 74, 388, 620  
Shared computer, user isolation policy for, 113–114, 114t  
Shared files, Macintosh ACL for, 147f  
Shared libraries, 103

- Shared reading, tailored policies and, 113
- Shared secret hashing, 621, 623–624
- Shared secret keys, symmetric cryptography and, 283
- Shared updating, tailored policies and, 113
- access control lists, 146–149
- Sharing dilemma, 134–135
- Sharing files, 111f, 133–167
- controlled sharing, 133–142
  - controls on, 110–112
  - file permission flags, 142–146
  - Microsoft Windows ACLs, 150–159
  - monitoring cyber system security, 159–167
  - objectives for policies related to, 111–112
  - policies for, 112–115
  - risks and, 112
  - Trojan horses, 156–159
- SHA-x.** *See* Secure Hash Algorithms
- Shell,** 57
- Shell script, 107
- Sheymov, Victor, 787
- Shielding, TEMPEST problem and, 787
- Shoplifters, identifying specific attacks by, 28, 28t
- Shopping, online, 631
- Shopping carts, 462, 729
- Shoulder surfing, 226
- SI.** *See* Special Intelligence
- Side channel attacks, 776
- SIM card, 224t
- Simple Mail Transfer Protocol, 664–665
- Simple rekeying, 617
- Simple Security Property, multilevel security and, 795
- Single-firewall topology, 690, 691, 691f
- SKIPJACK, 777
- Skype, 695
- Small networks, wiring, 450–451
- Small plaintext attack, on RSA, 350
- Small private key attack, on RSA, 351
- Smart card, 224t
- Smart networks, “dumb” networks *vs.*, 513–514
- Smart phones, security problems and, 2–3
- S/MIME.** *See* Secure MIME; Secure Multipart Internet Message Extension
- SMTP.** *See* Simple Mail Transfer Protocol
- Smurf attack, ICMP and, 521
- Snake oil products, 301
- Sniff, 226, 228
- Sniff credential
- authentication tokens and, 260, 261t
  - biometric authentication and, 264
- Sniffing, 671
- credentials, 236–237
  - direct authentication and, 589
  - email messages, 664
  - preventing, 650, 650t
- Sniffing protection, deploying cryptography on Internet and scope of, 613, 614
- Snowden, Edward, 759
- Social engineering, 233, 559, 562–563
- examples of, 562
  - thwarting, 563
- Social forgery, laptop risk assessment and, 29
- Socket addresses, 492
- Socket API capabilities, functions of, 492–493
- Socket interface, 491–492
- Socket layer encryption, with SSL/TLS, 610–611, 611f
- Software, 15
- Capability Maturity Model and, 565–566
  - content control, 710
  - database management system, 731
  - domain name resolver, 526
  - Netscape, 631
  - Web server, 703
- Software-based access controls
- encryption, 585
  - integrity checking, 585
  - internal security labels, 585
  - Need-to-Know controls, 585
- Software-based firewalls, 541–542
- application filtering on, 542f
- Software bugs, 77
- Software layers, 210
- abstraction and, 212–213
  - example of, 210–211
  - layering logic, 211–212
- Software patch, 126
- Software security, 575
- enterprises and, 582–585
  - elements of, 582
  - formalized coding activities, 583–585
  - software development security, 582–583
- Software security checklist, 309
- Software updates
- authenticated, 367–369
  - trusted, set of processes for, 368f
  - verifying, 368f
- Solaris operating system, 142
- Sort Merge Generator, 733
- Source routing attack, 522
- Soviet agents, key leakage through spying and, 776–777
- Soviet espionage, one-time pads and, 300, 325
- Soviet Union, nuclear operations during Cold War and, 793
- SOX.** *See* Sarbanes-Oxley Act
- SP3.** *See* Security Protocol 3
- SP 800-30, 9
- SP 800-37, 9
- SP 800-53, 9
- SP 800-60, 9
- Spam, 13, 671, 672–675
- evolution in prevention of, 673–674
  - filtering on spam patterns, 674–675
  - MTA access restriction, 674
  - financial fraud, 672–673
  - phishing and, 676

- SpamAssassin, 675, 685  
Spam score, 675  
Spanish Prisoner fraud, 673  
Special Access Program, 764, 767–768  
Special Intelligence, 764, 768  
Special Publications (SP), 9  
Spreadsheets  
    disclosure of, 35, 38–39  
    physical damage to, 38  
Spread spectrum, 782, 783–784  
Spying  
    corporate *vs.* government, 750  
    key leakage through, 776–777  
Spy tradecraft, 754  
SQL. *See* Structured Query Language  
SSID. *See* Station set identifier  
SSJS. *See* Server Side JavaScript  
SSL. *See* Secure Sockets Layer  
SSL alert protocol, 632  
SSL data packet contents, 634f  
SSL handshake protocol, 632–634, 633f  
    key block of, 632  
SSL keys, constructing through hashing, 633f  
SSL record transmission, 632, 634–636  
    application transparency and end-to-end crypto, 635–636  
    data compression, 635  
    message authentication code, 635  
SSL session, 632  
Stack, 56–57  
Staff, in larger organizations, 568f  
Stallings, William, 460  
Stanford University, 66  
Star network, 472, 474–476, 475f  
    benefits with, 475  
    shortcomings with, 476  
State diagrams, 123, 284–285  
    door's operation shown with, 124f  
    policy illustrated with, 284–285  
    of software vulnerability, 128f  
Stateful packet filter, 684  
Statelessness, 728  
Stateless protocol, 707  
States, 123, 284–285  
    information, 124–125  
Static inheritance, 154  
Static website security, 712–714  
Station set identifier, 644  
Statistical matches, 675  
Stealing, 560  
Stealth aircraft, special access programs and, 767–768  
Steganography, 72, 73, 73f  
STO. *See* Security through Obscurity  
Stock tickers, first, 433  
Stolen authentication database attacks, 234  
Stolen computers, risks to volumes and, 374–375  
Stolen private keys, 722  
Stoll, Clifford, 161, 164, 487  
Storage area networks, 742  
Storage device, lost, risks to volumes and, 374–375  
Storage sizes, 194t  
Storage state, 124  
Storage systems, physical protection of, 581  
Store, boundaries in, 16, 16f  
Storing files, 171–216  
    data stored on hard drive, 179–186  
    digital evidence, 175–179  
FAT: example file system, 195–201  
    incident response and attack, 171–175  
    aftermath of an incident, 173–174  
    legal disputes, 174–175  
input/output and file system software, 207–216  
modern file systems, 201–207  
Stream cipher modes, 392–396  
    ciphertext errors, 392–393  
    OFB in practice, 393–394  
    weaknesses with, 395  
Stream ciphers, 295–298, 295f,  
    381  
Strict layering, 212  
Strong threats, 226f  
    key management and, 318  
    key strength and, 324–325  
policies for  
    passwords alone, 268, 269t  
    passwords plus biometrics, 269, 270t  
    passwords plus tokens, 269, 271t  
Structured Query Language, 733–734  
    SELECT command in, 733, 733f  
Stuxnet, 8, 107, 110, 722  
Subdomains, 524  
Subjects, 115  
Subnets, 483  
Substitution ciphers, 282, 282f, 286, 287  
Substitutions, rounds and, 380  
Subversion, 26, 426  
    file protection policies and, 112  
Subversion attacks, 560  
Suite B, 344  
Sun's Solaris operating system, 57  
Superblock, 203  
Supervisory control and data acquisition devices, 3  
Supreme Court, classified data and, 758  
Surveillance  
    collecting evidence and, 175  
    serious attacks and, 599  
Survey files, policy additions for tailored sharing of, 145t  
Swap files, sniffing keys from, 420  
Switchboards, 472f  
Switches, for wired LANs, 461  
Symmetric encryption, 282, 339f  
    process diagram of, 283f  
SYN/ACK packet, 519  
Synchronized backups, 596–597  
Synchronous links, asynchronous links *vs.*, 441  
SyncToy (Microsoft), 86  
SYN flood attack, 522  
SYN packet, 519

- Syntax, misleading or obfuscating, 721
- SysAdmin, Audit, Network, Security Institute. *See* SANS Institute
- SySS, 415
- System-high mode, computer modes of operation and, 797, 798
- System life-cycle management, 774–775
- acquisition policy, 774
  - enterprise architecture, 774
  - risk management, 774
- System logs, 160–161
- System rights
- permission flags and, 121, 121f
  - in practice, 122
- System Security Engineering CMM, 565–566
- Systems engineering process, 7–8
- SYSTEM user identity**, 122
- 
- T**
- Tags, HTML, 701–703
- Tailored file security policies, 134
- Tailored policies, 112, 113
- Tailored sharing of survey files, policy additions for, 145t
- Tapes, erasure or destruction of, 785
- Target, hypertext links, 702
- Tavares, Stafford, 309
- TCB. *See* Trusted computing base
- TCP. *See* Transmission Control Protocol
- TCP connections, stateful filters and, 684
- TCP flags, Wireshark display, 519f
- TCP/IP, 516
- TCP/IP attacks, 522–523
- IP spoofing attacks, 522–523
  - source routing attacks, 522
  - SYN flood attacks, 522
- TCSEC. *See* Trusted Computer System Evaluation Criteria
- Technical surveillance countermeasures, 754–755.
- TEK. *See* Traffic encrypting key
- Telecom, 488
- Telegrams, 435
- from New York to Fargo, 433–434, 433f
  - sending, 433–434, 433f
- Telegraph, 432–434, 543–544
- Telegraph codes, 612
- Telephone networks, 545
- network topology: evolution of, 472–473
  - telegrams *vs.*, 434
- Telephones, 434
- Telephone system
- circuit switching and, 435, 437
  - evolution of, 481
  - as “smart” network with “dumb” end-points, 513
- Teletype machines, Unix
- developers working on, 231f, 232
- Teletype networks, message switching and, 434
- Teletypes, 293, 433, 434f, 436f
- link encryption for, 612
- Television, 443, 545
- cable, 548–549
  - satellite, 549
- TEMPEST attacks, 237
- TEMPEST problem, 776, 784
- countermeasures relative to, 787–788
  - crosstalk, PDS and, 786
  - history behind, 787
- TEMPEST protection, 772
- TEMPEST red/black problem, 788
- TEMPEST separation, between red and black components, 789
- TEMPEST zones, 788
- Temporary permissions, for administrative powers, 139
- 10-, 100-, 1000-baseT, 52
- Terrorist organizations, 750
- Text, using for encryption keys, 321–323
- Textual keys, binary keys *vs.*, 321
- TFC Padding, ESP packet format and, 640
- Theft, 426
- effectiveness of access control and encryption, 377t
  - of laptops, 418
  - risks to volumes and, 375
  - securing a volume and, 376
  - stolen private keys, 722
  - workplace, 560
- The Tale of Peter Rabbit* (book), 280
- Thieves, 19, 28
- risk assessment and, 12
- Third-party assessments, 571
- Thompson, Ken, 142, 231
- Threat agents, 12, 17, 20–26
- categories of, 21
  - five-level scale, 23
  - hostile intelligence service, 750
  - identification of, 20–23
  - identifying specific attacks by, 28, 28t
  - major elements of, 24
  - potential attacks, 26–29
  - profiling of, 23–26
- Threats, authentication and, 225
- 3DES. *See* Triple Data
- Encryption Standard
- Three-factor authentication, 225
- Three-legged firewall, 690, 691–692, 692f
- Three-way handshake, 519
- Thunderbird, 630, 663
- Thunderbolt, 52
- Ticker tape, 433
- Ticket, 591
- Ticket-based authentication, 591
  - by Kerberos, 591f
- Timeouts, 447, 516
- Timesharing, 795
- Time to live, 485
- Timing attack, on RSA, 351
- Titan II nuclear missile, Separation of Duty for, 333, 334f
- Titan missile launch control center, no lone zone and, 780f
- Titan timesharing system (University of Cambridge), 232
- Title tags, HTML, 701

TLDs. *See* Top-level domains  
TLS. *See* Transport Layer Security  
To: header, for Internet email, 660  
T1 connections, 548  
Top-level domains, 524  
DNS redundancy and, 530–531  
types of, 524  
Topology, 472  
Top Secret classification, 757, 758  
Top Secret clearances, 762  
Top Secret documents, storing, 763  
Top Secret information  
color codes for, 759  
compartmented or partitioned mode of operation and, 798  
greater restrictions and, 764  
Top Secret keying materials, two-person integrity controls and, 780  
Tornadoes, 595  
Track, 182, 182f  
Trade-off analysis, security process and, 7  
Trade secrets, 385  
companies, secrecy, and, 557–558  
theft of, 559  
Traffic analysis, 614  
Traffic blocking, 710  
Traffic encrypting key, 621  
Traffic filtering, deploying cryptography on Internet and, 613, 614  
Traffic-filtering mechanisms, 683–685  
application filtering, 683, 685, 685f  
packet filtering, 683, 683f  
session filtering, 683–685, 684f  
Traffic flow confidentiality, TFC Padding and, 640  
Training, information security, 573  
TRANSEC. *See* Transmission security

Transitive Trust, 159  
cryptonets and, 318  
disclosure and, 751  
Internet access and, 487  
leakage threat and, 795  
routing security and, 490  
secrecy and, 559  
web of trust and, 365  
Transmission Control Protocol, 445, 447, 515, 516–519, 694  
connections, 518–519  
connection timeout, 519  
as end-to-end protocol, 516  
header displayed in Wireshark, 517f  
packet fields, 516, 517f  
sequence and acknowledgment numbers and, 518  
TCP flags displayed in Wireshark, 519f  
window size, 518  
Transmission security, 776, 782–784  
electronic warfare and, 782–783  
jamming and, 782  
spread spectrum, 783–784  
traffic analysis, 782  
Transmission state, 124  
Transport layer, OSI protocol model, 461  
Transport Layer Security, 631–632  
socket layer encryption with, 610–611  
transport layer and, 630–632  
Transport mode, Encapsulating Security Payload and, 639, 641  
Transport protocol, 457  
Transposition cipher, 282, 282f  
Trash folder, 171  
Treason, Espionage Act and, 749–750  
Tree network, 473, 477–480, 478  
benefits and shortcomings with, 479  
Tricked certificate authority, 722  
Triple Data Encryption Standard, 310, 389, 408  
encryption, 382–383, 383f

Trojan crypto  
effectiveness of access control and encryption, 377t  
securing a volume and, 376  
Trojan horses, 156–159, 367, 430  
access rights applied to files, 158t  
effectiveness of access control and encryption, 377t  
preventing access by, file encryption and, 302  
securing a volume and, 376  
Trojan game copies secret files, 158f  
Trojan infection, 108  
Truly random numbers, 243  
Trunks, on phone network, 472  
Trust, but Verify maxim, 711  
*Trusted Computer System Evaluation Criteria* (Orange Book), 165  
Trusted computing base, 790  
Trusted systems, today, 791  
Trusted third party, 361  
Trustworthy systems  
government, national defense and, 789–799  
computer modes of operation, 797–799  
integrity of operations, 792–795  
multilevel security, 795–797  
T3 connections, 548  
TTL. *See* Time to live  
Tunneling, 694  
HTTP, dilemma of, 711–712  
Tunnel mode  
Encapsulating Security Payload and, 639, 640–641  
IPsec, packet layout in, 641f  
TV. *See* Television  
Tweakable cipher, 400  
Tweakable encryption mode, 406–407  
Two-factor authentication, 224–225  
Twofish, 309, 384  
Two-person integrity controls, Top Secret keying materials and, 780  
Two-way radio bands, 443

- U**
- UAC. *See* User account control
- UCL. *See* University College (London)
- UDP. *See* User Datagram Protocol
- UFS. *See* Unix file systems
- Unclassified indicators, 756
- Undelete program, 172
- Undeleting files, FAT directories and, 201
- Underlying system policy, for shared computers, 113, 113t
- Unencrypted volumes, policy for, 378, 378t
- Uniform Resource Identifiers, 704, 704f
- Uniform Resource Locators, 703 email, 704 format of, 704f
- Uninterruptible power systems, 580
- United States, nuclear operations during Cold War and, 793
- Universal plug and play (UPnP), 541
- Universal Serial Bus, 52
- University College (London), 482
- University of California (Berkeley), 66
- Unix, 142–143, 462 commands for adjusting file's rights, 143 denying access on, 151
- Unix-based systems, 57 root directories for, 95
- Unix directory listing command “ls,” 143, 143f
- Unix file permissions, for typical file, 142
- Unix file systems, 201, 203–204 directories, 204 inodes, 203–204 local authentication and, 589
- Unix-like systems, file and directory name formats, 97t
- Unix ps command, partial list of processes displayed by, 59, 60f
- Unix “root” account, 140
- Unix timesharing system, developers of, 231
- Unix volume format, classic, 203f
- Unpatched flaws, time line for attacking, 127f
- Unsafe functions, do not use, 584
- Untrustworthy encryption, 408
- Uplinks, 451
- Upper bound, 240
- UPS. *See* Uninterruptible power systems
- URIs. *See* Uniform Resource Identifiers
- URLs. *See* Uniform Resource Locators
- U.S. Army, 749 TEMPEST zones and, 788
- U.S. Army Security Agency, 325, 326
- USB. *See* Universal Serial Bus
- USB direct connect challenge-response tokens, 256–257, 256f
- USB drives, 8
- USB password token, 224t
- US-CERT, 67
- U.S. Defense Security Service, 751
- User account control pop-up window, 141f on Windows, 141–142
- User Datagram Protocol, 515–516 as end-to-end protocol, 516 header displayed in Wireshark, 515f packet fields, 515f
- User file-sharing policy, 115t
- User groups, basic file sharing on Windows and, 136–139
- User identities (user IDs), 78, 221, 577
- UserID field, in User tables, 732
- User interface, I/O system and, 61
- User isolation policy, for shared computers, 113–114, 114t
- User mode, 77
- User rights, 142
- U.S. Navy, 749
- U.S. State Department, 749
- V**
- Vandalism, workplace, 560
- Vandals, 19
- Vaults, 71, 72, 117
- VENONA project (NSA), declassified intercepts from, 768f
- Verification, security process and, 7
- Verified by Visa service, 592
- Verisign, 716
- Vernam, Gilbert, 293, 294, 295, 325, 612
- Vernam cipher, 779
- VGA. *See* Video Graphics Array
- Vice president, 567, 568f
- Video card, 51
- Video displays, 51
- Video Graphics Array, 52
- Vignère cipher, 287–289
- Virtual address extension, 487
- Virtual private networks, 610, 637–638
- bundling security associations, 642
- implementing, 641–642
- IPsec gateways and, 642
- private IP addressing and, 642
- small, 637f
- Viruses, 75, 430 biological, 105 computer, 103–107 diskette infected with, 106f email, 671, 677–680 infection by, 103–106 macro, 106–107 malicious, 105–106
- Virus hoaxes, 679–680
- Virus infection, in executable program file, 104f
- Visicalc, 103
- Visual Basic, 103, 106, 725
- Voice over IP (VoIP), 695
- Volume layout, FAT formatted, 195f
- Volumes. *See also* Encrypting volumes risks and policy trade-offs, 376–379 identifying critical data, 377–378

policy for encrypted volumes, 378–379  
policy for unencrypted volumes, 378  
risks to, 374–376  
discarded hard drives, 375–376  
eavesdropping, 375  
securing, 373–379  
VP. *See* Vice president  
VPNs. *See* Virtual private networks  
Vulnerabilities, 228  
of authentication tokens, 260–261, 261*f*, 261*t*  
of biometric authentication, 264–265  
for DVD CSS arrangement, 312  
searching for, 42–43  
sharing or publishing, 43–45  
Vulnerability, 13  
Vulnerability scan, 571

**W**

W3C. *See* World Wide Web Consortium  
Wagner, David, 384  
Waledac, 107, 108  
Walker, John A., 777  
Walker spy ring, preventing repetition of, 781  
WANs. *See* Wide area networks  
Ward, James B., 279–280  
Wardriving, 644  
*WarGames* (film), 62  
Wavelength, 442, 442*f*  
Weak threats, 226*f*  
key management and, 318  
key strength and, 324  
Web availability categories  
continuous availability, 742, 743  
continuous operation, 742  
routine availability, 742  
same origin policy, 742  
Web browsers, 657, 703  
Web content management system, 731*f*  
Web crawlers, 708

Web directories, search engines and, 708–709  
Web forms, POST command and, 723–724, 723*f*  
Web integrity, 741  
Web of trust, 364–366, 366*f*  
Web pages, 463  
addressing, 703–706  
default, 706  
simple, 700*f*  
static, retrieving, 706–709  
building a page from multiple files, 707  
crime via search engines, 708–709  
with HTTP, 706*f*  
web crawlers, 708  
Web directories and search engines, 708–709  
Web servers and statelessness, 707–708  
Web privacy, 743–745  
client anonymity, 743–744  
anonymous proxies, 744  
private browsing, 744–745  
Web-security issues, 709–722  
client policy issues, 709  
policy motivations and objectives, 709–710  
server authentication, 714–719  
server masquerades, 719–722  
static website security, 712–714  
tunneling dilemma, 711–712  
Web-use strategies, 710–711

Web security properties  
ensuring, 740–745  
Web confidentiality, 740–741  
Web integrity, 741  
Web availability, 741–743  
Web privacy, 743–745  
Web servers, statelessness and, 707–708  
Web server software, 703  
Website aliases, 526  
Website command injection, resisting, input validation and, 740  
Websites. *See also* Content management systems

dynamic, 723–730  
phishing and, 677  
registration and, 735  
Website whitelist, 710  
Web software, 462  
Web standards, 700  
Web traffic scanning, 710  
Web use strategies, 710–711  
monitoring, 711  
traffic blocking, 710  
training, 711  
WEP. *See* Wired Equivalent Privacy  
Wesley, Charles, encrypted diary of, 280, 284  
Western Union, 544  
Western Union telegram, 433*f*  
White-hat hackers, 14, 562  
White hats, windows of vulnerability and, 127  
Whitelists, 674, 710  
Whiting, Doug, 384  
whois database, 531  
whois response for stthomas.edu, 531

Whole-system backups, 596  
Wide area networks, 483, 485  
Wi-Fi, 450  
Wi-Fi Alliance, 450, 645  
Wi-Fi Protected Access, 645  
Wikipedia, 744  
Wilson, Woodrow, 749  
Wily Hacker, 161, 164  
Window of vulnerability, 127–129  
defined, 128  
state diagram of, 128*f*  
Windows. *See* Microsoft Windows  
Windows 8.1, 135–136, 136*f*  
Windows-based systems, 57  
Windows Internet Name Service, 540  
Window size, TCP and, 518  
Windows NT operating system, 206  
Windows system drive, root directory folder for, 96*f*  
Windows Vista, user account control on, 141

- Windows XP Pro, editing  
“Survey” user group on, 137f
- Winer, David, 292
- WINS. *See* Windows Internet Name Service
- Wired Equivalent Privacy, 645
- Wired Ethernet networks, 449
- Wired mechanisms, for communicating information, 544
- Wired network connections, popularity of, 425–426
- Wireless collisions, handling, 456–457
- Wireless connections, 425–426
- Wireless defenses, 644–645
- Wireless LAN encryption, cipher suites for, 613
- Wireless network technology, 449
- Wireless packet protection, 645–647  
decryption and validation, 647  
encryption processing, 646–647  
integrity processing, 647
- Wireless Protected Access, version 2, 609, 645  
encrypted packet contents, 646f
- Wireless retransmission, 457
- Wireless systems, categories of, 442
- Wireless transmission, 442–444, 544  
AM and FM radio, 443–444  
frequency, wavelength, and bandwidth, 442–443  
frequency sharing, 443–444  
radio propagation and security, 444
- Wireshark, 502–505, 707  
ARP request displayed in, 504f  
ARP response displayed in, 505f  
DNS response display on, 529f  
Ethernet header displayed in, 503f  
examples, 503–505  
features of, 503
- IP header displayed in, 505f  
ping packet shown in, 521f
- TCP connection summarized by, 518f
- TCP flags displayed by, 519f
- TCP header displayed in, 517f
- UDP header displayed in, 515f
- window for layout of, 502f  
sections of, 502–503
- WordPress, 731
- Word-processor program, execution access rights and, 102
- Work factor, 241
- Working key storage, 414
- Working storage, persistent storage *vs.*, 53–54
- Workplace security policy  
passwords and tokens, 268  
passwords only, 268
- World rights  
permission flags and, 121, 121f
- Unix file permissions, 142, 142f
- World War I, 749  
security classification systems during, 756
- World War II, 750  
British spying network in Germany during, 324
- German Enigma cipher machine used during, 289, 291f  
special intelligence and, 768
- TEMPEST problem and, 787
- World Wide Web, 487, 525, 630–631, 680, 699–745.  
*See also* Internet  
basic Web security, 709–722  
content management systems, 730–740  
dynamic websites, 723–730  
ensuring Web security properties, 740–745  
hypertext fundamentals, 699–709  
information security investments for, 569  
port numbers for, 492
- World Wide Web Consortium, 700
- Worm propagation, 108
- Worms, 2, 62, 77  
Morris worm, 62–71, 487, 488, 571
- network, 430
- Stuxnet, 8, 722
- WPA. *See* Wi-Fi Protected Access
- WPA2. *See* Wireless Protected Access, version 2
- Wrapped keys  
cryptoperiods and, 332  
key splitting and, 332–333  
multiple recipients and, 331–332  
recycled CEK attacks and, 418–419  
risks and benefits with, 416  
with RSA, 626, 626f  
software checklist for, 333
- Write right, 100
- WWW. *See* World Wide Web
- X
- Xerox Alto, 425, 426f
- Xerox Corporation, 425, 448
- XML. *See* Extensible Markup Language
- XML tunnels, 711
- xor. *See* Exclusive or (xor) cipher
- Xor-Encrypt-Xor, 406
- XSS. *See* Cross-site scripting
- XTS  
cipher mode and, evolution of, 406  
encrypting data on a disk sector and, 406f  
two parts to, 406
- Y
- Yahoo!, 708
- Z
- Zbot malware, 109
- Zero-day exploit, 127, 128
- Zeroize, 779
- Zeus, 107, 109, 237, 431
- Zimmerman, Phil, 308, 364
- Zone of control, 788
- Zones, 529
- Zoning, TEMPEST problem and, 788