Index

A
Access
- control list, 188, 190–192, 200, 204, 294, 395, 419
- control matrix, 189–190
- mandatory, 193, 200–201, 360
- role-based, 189–192
- rule-based, 189, 192–193

Activism, 114, 445, 451–452
Advocacy, 451–452
Alert notifier, 284, 286
Amplitude, 8, 412
Annualized loss, 162
Anomaly, 276, 279–281, 296
ARPNET, 111
Asynchronous token, 216
Asynchronous transfer mode (ATM), 21, 36, 38, 390, 403
Auditing, 54, 147–148, 168–171, 187, 208, 265, 295, 360, 368
Authentication
- anonymous, 214, 222, 224
- DES, 220, 232
- dial-in, 221, 225
- header, 386
- Kerberos, 218–220, 224, 225, 378–380, 395
- null, 220, 420
- policy, 223–224
- protocols, 324, 394–395
- remote, 220–221, 367–368, 395
- Unix, 220

Authenticator, 207, 210–211, 213, 215, 219, 221
Authority registration, 246
Authorization
- coarse grain, 204
- fine grain, 204
- granularity, 203

Availability, 6, 10, 84, 91, 93, 96, 120, 167, 204, 297, 304, 362, 414, 415, 438, 440, 458, 472, 479, 485, 487–500

B
Bandwidth, 7, 9–12, 24, 38, 84, 133, 283, 285, 335, 403, 409, 414, 416, 418, 431, 468, 479, 485, 525
Base-T, 35
Base-X, 35
Bastion, 252, 253, 255, 267–269
Biometrics, 41, 52, 196–198, 208, 213, 312
Blue box, 111
Bluetooth, 39–40, 399, 401, 417, 423, 425, 435
Bridge, 3, 12, 22, 24, 26–33, 136, 252, 263, 300, 538
Buffer overflow, 61, 65, 77, 86, 108

C
Carrier sense multiple access with collision detection (CSMA), 34, 35
CASPR. *See* Commonly Accepted Security Practices and Regulations (CASPR)
CERT. *See* Computer Emergency Response Team (CERT)
Certificate authority, 217, 239, 241–243, 246, 375, 377, 558
Certification, 147, 148, 154, 166–167, 246, 353, 355, 359, 363, 449, 558
- process, 167
- security, 147, 148, 166–167

Chain of custody, 308, 312, 319
Challenge-response, 208, 215–216, 221, 374
Cipher
- feedback, 229, 370
- specs, 381–383

Cladding, 11, 12

© Springer International Publishing AG 2017

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2

Coaxial cable, 10–11, 152
COBIT. *See* Control Objectives for Information and (Related) Technology (COBIT)
Code Red, 66, 76–77, 96, 113, 337, 339
Common criteria, 355, 358
Commonly Accepted Security Practices and Regulations (CASPR), 54
Communicating element, 4–6, 24, 65, 127, 217, 239–242, 245
Communication
  radio, 12, 408
  satellite, 12
Complacency, 88–89
Complexity, 88, 89, 97, 159, 160, 162, 164, 176, 192, 223, 269, 334, 351, 400, 411, 415, 469, 527, 528
  programming, 142
  software, 89, 487
  system, 97
Compression
  data, 84, 313, 317
  lossless, 310
  lossy, 310
Computer Emergency Response Team (CERT), 55, 61, 87, 90, 96, 112, 142, 143, 145, 333, 544
Confidentiality, 46–47, 61, 91, 107, 128, 227–228, 246, 312, 366, 369, 370, 372, 375, 376, 383, 385–387, 406, 418
  data, 47, 234–236, 272, 439
  information, 56
  message, 442
  PPP, 394
Congestion control, 21, 23, 25, 31, 524
Consolidation, 84
Control Objectives for Information and (Related) Technology (COBIT), 54–55
Cracker, 80, 90, 111–114, 130, 230, 317
CRC. *See* Cyclic redundancy check (CRC)
Cryptanalysis, 46, 229–230
Cryptographic algorithm, 47, 153, 228, 230, 235, 237, 374, 387, 436
CSMA. *See* Carrier sense multiple access with collision detection (CSMA)
Cyber
  crime, 106–130, 177, 327, 328, 447, 450, 451
  cyberspace, 62–64, 66–67, 70, 75, 79, 85, 98, 106, 107, 109, 110, 114, 118, 119, 133, 141, 187, 189, 193, 251, 304, 365, 445–448, 452, 453
  sleuth, 119
Cyclic redundancy check (CRC), 35, 36, 249, 310, 406

D

DARPA. *See* Defense Advanced Research Project Agency (DARPA)
Data circuit-terminating equipment (DCE), 37
Datagram, 20–23, 25, 30–33, 38, 255, 256, 385–388, 417, 527, 556, 557
DCE. *See* Data circuit-terminating equipment (DCE)
Defense Advanced Research Project Agency (DARPA), 19
Demilitarized zone (DMZ), 154, 267–270, 285–287, 291, 292, 553
Denial of Service, 62, 66, 67, 72–74, 76, 105, 107–109, 113, 115, 116, 121, 123, 124, 128, 142, 150, 273, 276, 277, 279, 317, 320, 423, 437, 438, 440, 443, 446, 495, 509, 511, 527, 544, 552, 557
Destroyers, 125, 126, 342
Detection, intrusion, 82, 85, 113, 129, 152, 168, 270, 275–300, 312, 319, 320, 324, 325, 438, 447, 474, 553–558
Deterrence, 41, 154
Disaster
  committee, 181
  human, 176–177
  management, 175–186
  natural, 159, 176
  planning, 180–183
  prevention, 177–178
  recovery, 179–180
  resources, 184–185
  response, 179
Distribution center, 219, 239–240
DMZ. *See* Demilitarized zone (DMZ)
Domain name service (DNS), 20, 50, 114, 137, 151, 169, 259, 267–269, 272, 299, 320, 323, 523–525, 553, 554
Dual-homed, 260, 261
Dumpster diving, 99

E

e-attack, 108
ECBS. *See* European Committee for Banking Standards (ECBS)
ECMA. *See* European Computer Manufacturers Association (ECMA)
Education
  focused, 449–450
  formal, 449
  mass, 448–451, 453
  occasional, 449–450
Effectiveness, 88, 91, 97–98, 166, 167, 179, 208–210, 288, 297, 300, 333, 334, 344, 345, 351, 356, 496, 526

EGP. *See* Exterior gateway protocol (EGP)
Electronic
  codebook, 229
  surveillance, 119, 195–196
Encoding
  analog, 7–8
  digital, 8–9
  scheme, 7, 8
Encryption
  asymmetric, 47, 234, 443
  symmetric, 47, 228, 230–235, 238, 239, 249, 250
End-points, 253, 389
Espionage
  economic, 79–81, 110
  military, 80, 119
Ethernet, 16, 21, 28, 30, 34–36, 40, 252, 290, 294, 537, 543, 558
ETSI. *See* European Telecommunications Standards Institute (ETSI)
European Committee for Banking Standards (ECBS), 49, 50
European Computer Manufacturers Association (ECMA), 49, 50
European Telecommunications Standards Institute (ETSI), 49, 413, 415
Evidence
  analysis of, 313–319
  preserving, 311–312
  recovery, 309–311
Exploits, 63, 64, 66, 78, 108, 114, 127, 149, 300, 438, 507, 509, 552, 554
Exterior gateway protocol (EGP), 31

F

FDDI. *See* Fiber Distributed Data Interface (FDDI)
Federal criteria, 358, 363
Federal Information Processing Standards (FIPS), 50, 359
Fiber Distributed Data Interface (FDDI), 34, 36
File Transfer Protocol (FTP), 20, 53, 151, 154, 205, 222, 246, 256, 257, 259, 261, 267, 268, 272, 299
Filtering
  address, 255–257
  content, 331–349
  exclusion, 331, 333
  keyword, 334
  packet, 251, 255, 258–259, 334, 343
  port, 257–259
  profile, 334–335
  stateful, 255
  stateless, 255
  virus, 336–343
Fingerprint, 45–47, 196–198, 208, 209, 212, 247
FIPS. *See* Federal Information Processing Standards (FIPS)
Firewall
  forensics, 270–271
  limitations, 272
  NAT, 264, 266
  services, 255, 272
  SOHO, 255, 263–264, 266
  VPN, 211, 263, 392
Forensic analysis, 168
Forensics
  computer, 303–327
  network, 303–327
FTP. *See* File Transfer Protocol (FTP)

G

Gateways, 22, 24, 27, 28, 32–34, 44, 128, 135, 251, 252, 255, 335, 336
Globalization, 105, 110, 119, 175, 187, 303, 445
Global System for Mobile Communication (GSM), 399, 400, 408, 413, 416
Goodtimes, 72

H

Hacktivist, 114–116, 128
Half open, 64, 108, 139
Hash function, 47, 215, 246–248, 313, 371, 375, 383, 442
Hashing algorithm, 47
Hidden files, 311, 315–316
Honeypot, 291–292, 422
Hotlines, 452
HTTPS. *See* Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)
Humanware, 93, 159, 161, 163, 165
Hybrid, 16, 238, 279, 289, 290, 390, 392, 423
Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), 365, 367, 375, 553

I

ICMP. *See* Internet Control Message Protocol (ICMP)
Ignorance, 82, 119, 120
Impersonation, 100, 127

Incident response, 156, 292, 293, 321–323
Information quality, 84
Information Sharing and Analysis Center (ISAC), 105
Infrared, 12, 39, 198, 435, 510
Initial sequence numbers, 258–259
Integrated services digital network (ISDN), 36–37, 221
Integrity, 34, 44, 47, 50, 51, 61, 80, 91, 106, 107, 109, 153, 154, 167, 193, 210, 217, 227, 228, 234–237, 239, 241, 242, 246–248, 272, 307, 308, 311–313, 326, 341, 360, 362, 372, 375–377, 380, 381, 383–387, 390, 438, 439, 442, 463, 536, 541, 545
Interface, 18, 19, 28, 30–34, 44, 48, 63, 91–93, 101, 138, 140, 141, 144, 158, 161, 164, 183, 189, 193, 211, 254, 289, 352, 353, 360, 401, 404, 407, 430, 469, 480–482, 485, 486, 489, 497, 527, 556, 557
Internet Control Message Protocol (ICMP), 20, 21, 29, 31, 65, 66, 108, 153, 255, 256, 385, 522, 552, 557
Internetworking, 4, 28–34, 110
Intruder, 41, 42, 64, 65, 76, 79, 82, 87, 88, 94, 95, 107–109, 125–127, 152, 153, 161, 164, 165, 194, 196, 204, 209, 213, 215, 216, 230, 237, 253, 258, 259, 262, 267–269, 276–278, 280, 281, 286, 288, 290, 291, 308, 320, 345, 369, 376, 419, 421–423, 441, 491, 496, 497, 507, 511, 536, 543, 544
Intrusion detection, 82, 113, 129, 152, 168, 270, 271, 275–300, 312, 319, 320, 324, 325, 438, 447, 474, 553–558
IPsec, 50, 51, 263, 272, 365, 385–389, 392–393, 474, 553, 554
IPv4, 21, 346, 385, 388, IPv6, 21, 346, 385, 388
Iris, 45, 198, 208, 209, 212, 213
ISAC. *See* Information Sharing and Analysis Center (ISAC)
ISDN. *See* Integrated services digital network (ISDN)

J

Jamming, 35, 114, 421, 423, 440
Javascript, 134, 136, 138, 143–144, 340
JPEG, 74, 75, 371

K

Kerberos, 50, 212, 217–219, 224–225, 312, 365, 367, 373, 377–380, 392, 395, 424, 426, 554
Key
- distribution, 219, 233, 239–240, 245, 370, 554
- encryption, 230, 374, 424
- escrow, 243–245
- exchange, 215, 237–239, 373–374, 392, 424, 441
- infrastructure, 217, 222, 240, 245, 372, 558
- management, 50–52, 238–245, 405, 420–421, 440–442, 554
- private, 47, 216–218, 222, 228, 234–236, 248, 370, 377, 378, 382
- public, 47, 49–51, 214, 216–218, 222, 224–225, 228, 231, 234–250, 369–371, 373–374, 376, 381–382, 392, 495, 558

L

LAN. *See* Local area network (LAN)
Land.c attack, 108
Least privilege, 203
Legislation, 129–130, 304, 349, 445–447
Load balance, 280–282
Local area network (LAN), 5, 6, 12, 14–16, 20, 26–40, 107, 120, 155, 252, 399, 401, 405, 416, 420–421, 425

M

MAC, 36, 50, 193, 247–248, 256, 319, 369, 383, 384, 401–404, 406, 419, 424, 432, 442
MAN. *See* Metropolitan area network (MAN)
Manchester, 8
MD-5, 51
Metropolitan area network (MAN), 6, 13, 40, 539
Mobile IP, 408–409
Modes
- transport, 388, 392, 395
- tunnel, 388–389, 395

Monitoring remote, 45
Multiplexing, 9, 32, 407, 412, 432
Multi-ported, 27–29

N

Narrowband, 39
US National Infrastructure Protection Center (NIPC), 106
National Institute of Standards and Technology (NIST), 49, 50

Network
  centralized, 4–5, 362
  civic, 6, 209
  distributed, 4–5, 43
  extended, 12, 252
  mobile, 12, 223, 414
  packet, 25, 30, 63, 106, 211, 249–250, 252–253, 256, 258–260, 264, 272, 346, 387, 398, 420–421
  public, 37, 255, 322, 561
  wireless, 11, 39, 40, 223, 397–424
Next-hop, 31–32, 127, 323
NIPC. *See* US National Infrastructure Protection Center (NIPC)
NIST. *See* National Institute of Standards and Technology (NIST)
Nmap, 554, 558
Nonrepudiation, 228, 234, 237, 246, 438
Nonreturn to zero (NRZ), 8
Nonreturn to zero, invert on ones (NRZ-I), 8
Nonreturn to zero level (NRZ-L), 8
Normalizer, 296
Notoriety, 82, 109, 120
NRZ. *See* Nonreturn to zero (NRZ)
NRZ-I. *See* Nonreturn to zero, invert on ones (NRZ-I)
NRZ-L. *See* Nonreturn to zero level (NRZ-L)

O
Open architecture, 17, 63, 165, 415
OpenSSL, 51–52
Orange Book, 53, 354, 355, 359, 362
Open systems interconnection (OSI), 17–20, 29, 30, 32, 37
  model, 17–20, 28, 37, 402, 537

P
Packet
  filtering, 255, 258–259, 334
  inspection, 254–256, 260
Password
  cracking, 194, 317
  one-time, 214–215, 554
  token, 215
Pathogen, 70
PGP. *See* Pretty Good Privacy (PGP)
Phase shift, 8
Phreaking, 111, 117
Ping-of-death, 277
PKCS. *See* Public Key Cryptography Standards (PKCS)
PKI. *See* Public key infrastructure (PKI)
PKZip, 310
Point-to-Point Protocol (PPP)
  authentication, 221, 394
  confidentiality, 394
Prank, 118
Precedence, 188–189
Pretty Good Privacy (PGP), 51, 53, 236, 239, 311, 324, 369–372, 395–396, 553, 554, 559
Prevention, 41, 44, 107, 128–129, 152, 176–179, 275–300, 554
Protocol
  alert, 383
  SSL record, 383–384
Proxy server, 254, 260–263, 271, 335–336, 344–345
Public Key Cryptography Standards (PKCS), 49–51, 373–375
Public key infrastructure (PKI), 51, 56, 217–218, 222, 225, 240, 245–246, 249–250, 369, 558

R
RADIUS. *See* Remote Authentication Dial-In User Service (RADIUS)
Regulation, 54, 129, 304, 445, 446
Remote Authentication Dial-In User Service (RADIUS), 220, 221, 299, 367–368, 395, 424, 425
Repeater, 8, 26–27, 37
Replication, 125, 169, 224, 342, 440
Risk assessment, 184
Rivest, Shamir, and Adleman (RSA), 49–52, 56, 213, 237, 244, 247, 369–371, 373

S
SATAN, 554
Scanning
  content, 332
  heuristic, 332
Scripts
  CGI, 134, 138–142, 340, 417
  hostile, 89, 127, 133, 142, 177, 316
  Perl, 134–136
  server-side, 135, 140, 143, 145
Secure/Multipurpose Internet Mail Extensions (S/MIME), 49–53, 365, 367, 371, 396, 553, 554

Security
  analysis, 361
  assessment, 147–171, 354, 547
  associations, 386–387
  assurance, 147–171, 353, 360
  awareness, 84, 92, 102, 155, 450, 453, 506
  certification, 147, 148, 166–167
  model, 262–263, 515, 527, 553
  policy, 57, 91, 128–129, 147–155, 165–167, 191, 223, 251, 255, 265, 284, 287, 293, 296, 332, 360, 555, 561
  requirements, 147–148, 157–158, 167, 354, 356, 359, 391, 392, 438, 447, 506, 512
  threat, 53, 61–85, 105, 136, 142–145, 158–171, 421, 450, 465, 474, 494, 505, 506, 526, 560, 561
  vulnerability, 76, 87–88, 163
Self-regulation, 129, 447–448, 452
Sensor Networks
  design features, 431
  growth, 430–431
  routing in, 432
  securing, 438
  vulnerability of, 436–437
Service set identifier (SSID), 419, 422–424, 546, 547
Shadow, 68, 495
Signature
  chameleon, 213
  digital, 47–48, 51, 52, 213, 216, 222, 228, 242–243, 247–249, 369–371, 374–376, 378
Simple Network Management Protocol (SNMP), 20, 61, 151, 284, 422, 553, 554
S/Key, 215
Slack space, 316
S/MIME. *See* Secure/Multipurpose Internet Mail Extensions (S/MIME)
Sniffer, 46, 124, 127, 195, 260, 291, 312, 543, 553
Sniffing, 65, 119, 128
SNMP. *See* Simple Network Management Protocol (SNMP)
Snort, 298, 327, 554–556
Social engineering, 62, 79, 85, 88, 98–100, 102, 119, 127, 155, 165, 170, 422, 510, 511, 544
Software
  application, 44, 52, 94, 153, 164, 276, 309, 560
  controls, 165
  security, 102
Spam laws, 348–349
Spread spectrum, 12, 39
SSID. *See* Service set identifier (SSID)
Steganography, 313, 316–317
Surrogate, 4–5, 46, 71, 74, 115, 125–126, 336–339
Switching
  circuit, 24
  data, 24
  packet, 20, 24–25
SYN flooding, 64, 108

T

TACAS/TACAS+. *See* Terminal Access Controller Access Control System (TACAS/TACAS+)
TCPDump, 90, 127, 327, 555–557
TCP/IP. *See* Transmission Control Protocol/Internet Protocol (TCP/IP)
TDM. *See* Time-division multiplexing (TDM)
TDMA. *See* Time division multiple access (TDMA)
Teardrop, 108–109
Terminal Access Controller Access Control System (TACAS/TACAS+), 368
Terrorism, 79–80, 106, 118, 123–124, 176, 181, 347
Third generation, 413–414
Three-way handshake, 22, 64–65, 85, 108, 127, 139–140, 221, 258, 381
Time
  bomb, 125–126, 342
  response, 82, 96, 485
  turnaround, 83, 85, 96–98
Time division multiple access (TDMA) 412–413, 416
Time-division multiplexing (TDM), 9
Toolkit, 170, 291, 305, 309, 318
Topology
  bus, 14–15
  ring, 16
  star, 15–16
Transmission Control Protocol/Internet Protocol (TCP/IP), 18–20, 32, 38–40, 51, 64, 254, 256, 264, 299, 375, 389, 410, 418, 432, 520, 522–525, 527
Trapdoor, 125–126, 280
Trust model, 210, 211

U

Unauthorized access, 44, 62, 107, 144, 150, 203, 204, 215, 275, 279, 385, 496
User Datagram Protocol (UDP), 20–23, 64, 65, 153, 255–260, 270, 272, 385, 552, 557

V
VBScript, 136, 138, 143–144, 340
Vendetta, 79, 81, 88, 117–118, 121, 122
Verifier, 211, 290
Victim computer, 77, 107, 109
Virtual private network (VPN)
  hybrid, 392
  secure, 391
  trusted, 390–391
Virtual sit-in, 114–116
Virus
  boot, 339
  Code Red, 96, 113, 337, 339
  multipartite, 341
  palm, 74–75
  polymorphic, 340–341, 343
  retro, 341
  stealth, 341
  Trojan horse, 340
VPN. *See* Virtual private network (VPN)
Vulnerability assessment, 100–102, 147, 170, 276, 277

W
WAN. *See* Wide area network (WAN)
War
  chalking, 421
  driving, 421
  fare, 116, 118
  flying, 421
  games, 421
  walking, 421
Wide area network (WAN), 5–7, 13, 20, 26, 34, 36–39, 107, 300, 392
WI-FI, 223, 399, 401, 404, 405, 414, 416, 421, 423, 424
WildList, 343
WinNuke, 277
WinZip, 310
Wireless
  LAN, 39, 50, 399, 405, 418–424
  loop, 405 please check
Wiretap, 81, 128, 293
Workload, 159
World Wide Web Consortium (W3C), 49, 50, 52, 354

X
X.25, 36–38
xDirect service line (xDSL), 38
XML, 50–52, 416

Y
Y2K
  bug, 71–72
  crisis, 72

Z
ZDNeT, 73