

INDEX

- Access checks, Windows security, 726
- Access control, 20, 23, 24, 83, 110–141, 148–153, 692, 693–699, 703–705, 711–717, 724–726, 726–728
 - access right, 115
 - database, 148–153
 - discretionary (DAC), 113, 116–122, 113, 116–122, 692, 693–699
 - Linux security, 692, 693–699, 703–705, 711–717
 - lists (ACLs), 116–117, 125, 724–726
 - mandatory (MAC), 113, 711–717, 726–728
 - network-level, 703–705
 - OSI systems, 23, 24
 - password files, 83
 - policies of, 112–113
 - principles of, 111–114
 - role-based (RBAC), 113, 125–137, 715
 - UNIX file, example of, 122–125
 - Windows security and, 724–726, 726–728
- Access matrix, 116–117, 127–128
- Account defenses, Windows system, 730–732
- Active attacks, 14, 19–20
- Active directory (AD), 721, 722
- Add round key transformation, AES, 606–607
- Address space protection and randomization, 377–378
- Advanced Encryption Standard (AES), 42, 47, 600–607
 - add round key transformation, 606–607
 - algorithm for, 601–607
 - key expansion, 607
 - transformations, 604–607
- Alert Protocol, 654
- Algorithms, correct implementation of, 403–405, 405–406. *See also* Public-key cryptography; Symmetric encryption
- Amplification attacks, 263–265
- Anomaly detection, 183, 185–187, 188, 196–197, 500–501
 - attacks suitable for, 196–197
 - audit trail analysis and , 500–501
 - host-based, 183, 184, 185–187, 188
 - network-based, 196–197
- Answer to reset (ATR) message, 91–92
- Antivirus software, 226–229, 705
- Application-level audit trail, 483–484
- Application-level gateway, 282
- Assets, *see* System resources
- Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct, 583–584
- Association of Information Technology Professionals (AITP) Standard of Conduct, 583, 584–585
- Assurance, 34, 335, 337, 340–343
 - evaluation levels (EALs), 342–343
 - IT security evaluation, 340–343
 - requirements, 335, 337
 - scope of, 341–342
 - target audience, 340–341
- Asymmetric encryption algorithms, 60–61, 641–645. *See also* Public-key encryption
- Atomic operation, software security, 417
- Attacks, 13, 14–16, 19–20, 43–44, 99–101, 196, 249–272. *See also* Malicious software
 - active, 14, 19–20
 - brute-force, 43–44
 - denial-of-service, 19, 101, 196, 249–272
 - network security, 19–20
 - passive, 14, 19–20
 - types of, 14–16
 - user authentication and, 99–101
- Audit and alarms model (X.816), 477–478
- Audit records, host-based intrusion detection and, 184–185, 192
- Audit trails, 481–486
- Audit trail analysis, 497–501
 - anomaly detection and, 500–501
 - audit review, 499
 - baselining, 500–501
 - data analysis, approaches to, 500–501

- Audit trail analysis (continued)
 - log entries, 498
 - preparation for, 497–498
 - timing of, 498–499
- Authenticated boot service, TC, 330–331
- Authentication, 20, 49–63, 111. *See also*
 - Internet authentication; Message authentication; User authentication
 - access control and, 111
 - cryptographic tools and, 49–73
 - digital signatures, 61–64
 - hash functions and, 49–56
 - passwords, 56
 - public-key certificates, 62–63
 - public-key encryption, 56–61
 - symmetric encryption, using, 49
- Authentication Header (AH), 658, 660–661
- Authentication protocol, 90, 92, 97–99, 644
 - biometric, 98–99
 - challenge-response, 90
 - Diffie-Hellman key exchange, 644
 - dynamic password generator, 90
 - passwords, 97–98
 - protocol type selection (PTS), 92
 - static, 90
 - tokens, 90, 92, 98
- Authorization, access control and, 111
- Backdoor (trapdoor), 216–218
- Backscatter traffic, DoS, 254
- Banner grabbing attack, 197
- Baseline approach, 500–501 516
- Base-rate fallacy, 189–190, 211–214
 - Bayes' theorem, 212–213
 - conditional probability and, 211–212
 - demonstration of, 213–214
 - IDS problem of, 189–190
 - independence and, 211–212
- Bastion host, 283–284, 291
- Bayes' theorem, 212–213
- Behavior-blocking software, 229–230
- Bell-Lapadula model (BLP), 304–314
- Biba integrity model, 314–315
- Biometric authentication, 76, 92–97, 101–103
 - accuracy of, 95–97
 - dynamic, 76, 99
 - enrollment in, 93–94
 - iris system, practical application of, 101–103
 - operation of, 93–94
 - physical characteristics used in, 92–92
 - protocol for, 98–99
 - static, 76, 98
 - verification (identification) of, 94
- BitLocker, Windows security, 738–739
- Block ciphers, 44, 47
- Block encryption algorithm, 44–47
- Bloom filter, 87–88
- Boot sector virus, 224
- Bots, 217, 239–242
- Browser defenses, Windows security, 737
- Brute-force attack, 43–44
- Buffer overflow, 350–387, 392–393, 733–737
 - attacks, 351
 - basics of, 352–356
 - compile-time defenses, 373–377
 - function call mechanisms, 356–358
 - head-based detection, 736
 - no-execute (NX), 377, 735
 - program input and software security from, 392–393
 - run-time defenses, 377–378
 - shellcode, 365–372
 - stack, 356–358, 734–735
 - Windows system defenses, 733–737
- Canary value, 376
- Canonicalization, 401
- Capability tickets, 116–117
- Cardinality, RBAC roles, 131
- Cascading authorization, 150–151
- CERT, *see* Computer Emergency Response Team (CERT)
- Certificate authority (CA), 62, 678, 681
- Certificate revocation list (CRL), 680
- Change Cipher Spec Protocol, 654
- Chief Information Officers Council (CIO), 461
- Chinese wall model, 317–319
- Chroot jail, 413, 709–710
- CIA triad, 8–10
- Cipher block chaining (CBC) mode, 612–613

- Cipher block feedback (CFB) mode, 614–615
- Ciphertext, 42, 57, 594
- Circuit-level gateway, 282–283
- Clark-Wolson integrity model, 315–317
- Clear signed data, S/MIME, 664
- Client attacks, 99
- Code, writing safe programs using, 403–407
- Code injection attack, 396–397
- Codes of conduct, 582–586
- Collision resistant hash functions, 55
- Combined approach, security risk assessment, 517–518, 530–534
- Command injection attack, 394, 396
- Common Criteria Evaluation and Validation Scheme (CCEVES), 334
- Communication lines, computer security and, 12, 19–20
- Compile-time defenses, 373–377
- Compression function, 631
- Computer crime, *see* Cybercrime
- Computer Emergency Response Team (CERT), 27–28, 28–31, 179, 460–461, 564, 566
- Computer security, 1–5, 6–39, 303–348, 562–591. *See also* Multilevel security (MLS); Physical security; Trusted computing (TC)
 - breach of levels, 9–10
 - challenges of, 11–12
 - confidentiality of, 7, 8, 10
 - countermeasures, 13, 14, 20–22
 - CSI/FBI Computer Crime and Security Survey, 31–32
 - cybercrime and, 563–567
 - documents for, 37–39
 - integrity of, 8, 10, 21
 - intellectual property and, 567–574
 - legal and ethical aspects of, 562–591
 - model of, 12–14
 - multilevel (MLS), 303–348
 - networks, 12, 19–20, 27–28
 - open systems interconnection, architecture for, 22–27
 - overview of, 6–39
 - privacy and, 574–580
 - reader's guide, 1–5
 - scope of, 27–28
 - standards for, 37–39
 - strategy for, 32–34
 - system resources (assets), 12–14, 14–16, 17–18
 - taxonomy for, 27–28
 - terminology for, 12–14
 - threats to, 13, 14–16, 17–18
 - trends of, 28–32
 - trusted computing (TC), 320–323, 330–334
- Conditional probability of events, 211–212
- Confidentiality, 7, 8, 10, 42–49, 593–624. *See also* Data confidentiality; Privacy
 - computer security and, 7, 8, 10
 - Family Education Rights and Privacy Act (FERPA), 10
 - message, 593–564
 - symmetric encryption and, 42–49, 593–624
- Control Objectives for Information and Related Technology (COBIT), 460
- Copyrights, intellectual property and, 568–569
- Corporate policies, 440–441, 457–459, 464–465, 465–467
- Counter (CTR) mode, 615–62–16
- Cross-site scripting attacks (XSS), 398–400
- Cryptanalysis, 43, 595–596
- Cryptographic services, Windows, 737–739
- Cryptographic tools, 41–73
 - confidentiality, 42–49
 - digital signatures, 61–64
 - encryption of stored data, 67–68
 - hash functions, 49–56
 - key management, 61–64
 - keys, 42, 57–59
 - message authentication, 49–56
 - Pretty Good Privacy (PGP), 67–68
 - pseudorandom numbers, 66–67
 - public-key encryption, 56–61, 61–64
 - random numbers, 65–67
 - symmetric encryption, 42–49, 63
- Cryptography, *see* Public-key encryption; Symmetric encryption
- CSI/FBI Computer Crime and Security Survey, 31–32
- Cybercrime, 563–567
- Cyberslam, DoS, 252

- DAC, *see* Discretionary access control (DAC)
- Data definition language (DDL), 143
- Data Encryption Algorithm (DEA), 44
- Data Encryption Standard (DES), 42, 44–45, 598–600
 - algorithms for, 598–600
 - symmetric encryption use of, 42, 44–45
 - triple (3DES), 45–46, 599–600
- Data manipulation language (DML), 143
- Data perturbation, 164–165
- Data Protection API (DPAPI), 738
- Data surveillance and privacy, 578–580
- Data swapping, 164–165
- Data values, writing correct code for, 406–407
- Database access control, 148–153
 - cascading authorization, 150–151
 - fixed database roles, 152
 - fixed server roles, 152
 - role-based (RBAC), 151–153
 - SQL-based, 149–150
 - user-defined roles, 152–153
- Database management systems (DBMS), 143–144. *See also* Databases
- Databases, 142–175, 325–330
 - access control, 148–153
 - encryption, 166–170
 - inference and, 153–156, 158–159
 - management systems (DBMS), 143–144
 - multilevel security (MLS) of, 325–330
 - queries, 155, 158–159, 159–162
 - query language, 143–144
 - relational, 144–148
 - security of, 142–175
 - statistical (SDB), 156–166
- Deadlock, prevention of, 407
- Decryption algorithm, 42, 57, 594
- Defensive programming, 389–392
- Denial-of-service (DoS), 19, 101, 196, 249–272
 - amplification, 263–265
 - attacks, 250–257
 - classic, 252–253
 - defenses against, 265–268
 - distributed (DDos), 259–260
 - flooding, 257–259
 - reflection, 261–263
 - responding to, 269–270
 - source address spoofing, 253–254
 - SYN spoofing, 254–257
 - Tribe Flood Network (TFN), 259–260
 - user authentication and, 101
- Detailed risk analysis, 517, 518–530
- Diffie-Hellman key exchange, 61, 641–645
- Digital envelopes, 64
- Digital immune system, 228–229
- Digital Millennium Copyright Act (DMCA), 570–571
- Digital Rights Management (DRM), 571–574
- Digital Signature Standard (DSS), 61, 645
- Digital signatures, 61–64
- Discretionary access control (DAC), 113, 116–122, 113, 116–122, 692, 693–699
 - group accounts, 693–694
 - Linux file-system security, 693–699
 - model of, 118–121
 - permissions, 694–699
 - protection domains, 122
 - user accounts, 693–694
- Distributed adaptive intrusion detection, 197–200
- Distributed denial of service (DDos), 259–260
- Distributed detection and interference (DDI), 199, 200
- Distributed firewalls, 289–290, 291
- Distributed host-based intrusion detection, 190–192
- DMZ networks, 286–288
- DNS amplification attacks, 264–265
- Domain accounts, Windows security, 722
- DoS, *see* Denial-of-service (DoS)
- Drones, *see* Bots
- Dynamic binary rewriting, 496–497
- Dynamic biometric authentication, 76, 99
- Dynamic separation of duty (DSD), 134
- Eavesdropping, 100–101
- Electronic codebook (ECB), 47, 611–612
- Electronic Frontier Foundation (EFF), 45
- Elliptic curve cryptography (ECC), 61, 645

- E-mail, 219, 225–226, 464–465, 662–665
 - clear signed data, S/MIME, 664
 - enveloped data, S/MIME, 664
 - Internet security protocols, 662–665
 - Multipurpose Internet Mail Extension (MIME), 662–663
 - public-key certificates, 665
 - Secure/Multipurpose Internet Mail Extension (S/MIME), 662–665
 - signed data, S/MIME, 664
 - use policies, 464–465
 - viruses, 219, 225–226
- Employment practices and policies, 461–463
- Encapsulating Security Payload (ESP), 658, 661–662
- Encrypted virus, 224
- Encrypting File System (EFS), 738
- Encryption, 42, 57, 166–170, 331–332, 594, 710. *See also* Symmetric encryption
 - algorithm, 42, 57, 594
 - database, 166–170
 - Linux application security, 710
 - service, TC, 331–332
- End-to-end domain, example of, 723
- Enveloped data, S/MIME, 664
- Environmental threats, 431–434, 436–437
 - chemical, radiological, and biological hazards, 434
 - dust, 434
 - fire and smoke, 432, 433, 436–437
 - humidity, 431–432, 436
 - infestation, 434
 - prevention of, 436–437
 - temperature, 431–432, 436
 - water damage, 432–433, 437
- Environmental variables, software security, 408–411
- Ethics, 580–586
 - Association for Computing Machinery (ACM) Code, 583–584
 - Association of Information Technology Professionals (AITP) Standard, 583, 584–585
 - codes of conduct, 582–586
 - computer and informations systems, 580–582
 - Institute of Electrical and Electronic Engineers (IEEE) Code, 583, 585
 - IS professions and, 580
- European Union Data Protection Directive, 574–575
- Evaluation assurance levels (EALs), 342–343
- Extensible Markup Language (XML), 685
- Factoring problem for RSA algorithms, 638–640
- False negatives, 182
- False positives, 182
- Family Education Rights and Privacy Act (FERPA), 10
- Family, IT security requirements, 335
- Federal Information Processing Standards (FIPS), 5, 8–10, 20–22, 126, 441–446
- Federated identity management, 683–687
- Feistel cipher structure, 596–598
- File access control, 83, 122–125
- File infector, 224
- Files, computer security and, 83, 416–417, 417–419
- FIPS, *see* Federal Information Processing Standards (FIPS)
- Firewalls, 273–302, 704–705, 733
 - application-level gateway, 282
 - basing, 283–286
 - bastion host, 283–284, 291
 - characteristics of, 275–276
 - circuit-level gateway, 282–283
 - distributed, 289–290, 291
 - DMZ networks, 286–288
 - host-based, 284, 291
 - intrusion prevention systems (IPS), 179, 273–302
 - Linux, use of iptables for 704–705
 - location and configurations of, 286–291
 - need for, 274
 - packet filtering, 276–280
 - personal, 284–286
 - screening router, 291
 - stateful inspection, 280–281
 - unified threat management (UTM),
 - example of, 294–298
 - virtual private networks (VPN), 288–289
 - Windows network defenses, 733

Flooding attacks, 257–259
 Function call mechanisms, buffer overflow,
 356–358
 Functional requirements, IT security, 335–336
 Fuzzing software tests, 355, 402–403

Gateways, 282–283
 Generic description (GD), 227–228
 Global data area overflow, 383–385
 Group accounts, Linux security, 693–694
 Guard pages, 378

Hackers, 178–179
 Handshake Protocol, 654–656
 System hardening, 701–709, 729–730
 Hardware, computer security and, 12, 17
 Hash functions, 49–56, 626–632
 MD5 message-digest algorithm, 631
 message authentication and, 49–56
 message authentication using, 626–632
 one-way, 52–54
 requirements for, 54–55
 Secure Hash Algorithm (SHA), 56,
 627–630
 secure, 54–56, 626–632
 whirlpool, 631–632
 Hashed passwords, 78–80
 Heap overflow, 381–383
 Hierarchies, RBAC, 130, 133–134
 HMAC, 632–635
 Honeypots, 202–204
 Host attacks, 99
 Host audit record (HAR), 192
 Host-based firewalls, 284, 291
 Host-based intrusion detection, 181,
 183–190, 190–192
 anomaly detection, 183, 185–187
 audit records and, 184–185, 192
 base-rate fallacy, 189–190
 distributed, 190–192
 rule-based anomaly detection, 187–188
 rule-based penetration identification,
 188–189
 signature detection, 184, 187–189
 Stanford Research Institute (SRI) IDS
 (IDES), 187–188, 189
 tests for limits of, 186–188

Host-based intrusion prevention systems
 (HIPS), 292–293
 Human factors of computer security,
 449–474
 awareness, training and education for,
 452–455
 Control Objectives for Information and
 Related Technology (COBIT), 460
 corporate security policy document,
 example of, 465–467
 e-mail use policies, 464–465
 employment practices and policies,
 461–463
 internet use policies, 464
 policy writers, resources for, 460–461
 security management, standards for,
 469–473
 security policies, 455–461, 473–474
 Human-caused threats, 435

ICMP flood attack, 257–258
 Identification, 20, 75, 89, 94, 188–189
 Identity management, 683–684
 IDS, *see* Intrusion detection systems (IDS)
 Image randomization, Windows system
 defense, 736
 Impersonation, Windows security, 726
 Independent events, 211–212
 Inference, 15, 153–156, 158–159
 channel, 153–154
 compromise, 158–159
 database security and, 153–156
 detection algorithm, 155–156
 statistical databases (SDB), from, 158–159
 Informal approach, security risk assessment,
 516–517
 Information system (IS), 476
 Information technology (IT) security
 evaluation, 334–340, 340–344
 assurance and, 340–343
 assurance requirements, 335, 337
 Common Criteria Evaluation and
 Validation Scheme (CCEVES), 334
 evaluation assurance levels (EALs),
 342–343
 functional requirements, 335–336
 process of, 343–344

- protection profiles (PPs), 336, 338–340
- security targets (STs), 337–338
- target of evaluation (TOE), 335, 340–341, 343–344
- Information technology (IT) security
 - management, 508–537, 538–561. *See also* Security implementation; Security risk assessment
 - case studies of, 530–534, 556–558
 - controls (safeguards), 538–546, 548–550
 - detailed security risk analysis, 517, 518–530
 - implementation of, 538–561
- International Standards Organization (ISO), 509–512, 541–543
- National Institute of Standards and Technology (NIST), 541–546
- organizational context of, 512–515
- overview of, 509–512
- plans, 547–548
- policy development, 513–515
- security risk assessment, 515–518, 515–518, 518–530, 530–534
- Infrastructure security, *see* Physical security
- Infringement, intellectual property and, 568
- Injection attacks, 394–398
- Inside attack, 14
- Institute of Electrical and Electronic Engineers (IEEE) Code of Ethics, 583, 585
- Integrity, *see* Authenticity; Data integrity; System integrity
- Intellectual property, 567–574
 - copyrights, 568–569
 - Digital Millennium Copyright Act (DMCA), 570–571
 - Digital Rights Management (DRM), 571–574
 - infringement, 568
 - patents, 569
 - relevance to network and computer security, 570
 - trademarks, 569–570
 - types of, 568–570
- International Convention on Cybercrime, 564, 565
- International Organization for Standardization (ISO), 5, 37–38, 334–338, 450, 460, 481, 509–512, 541–543, 576–578
- International Telecommunication Union (ITU), 5
- Internet Architecture Board (IAB), 5
- Internet authentication, 671–688
 - federated identity management, 683–687
 - Kerberos, 672–678
 - public-key infrastructure (PKI), 680–683 X.509, 678–680
- Internet Engineering Task Force (IETF), 5
- IETF Public Key Infrastructure X.509 (PKIX) model, 681–683
- Internet protocol security (IPSec), 656–662, 732–733
 - Authentication Header (AH), 658, 660–661
 - benefits of, 657–658
 - Encapsulating Security Payload (ESP), 658, 661–662
 - overview of, 656–657
 - routing applications of, 658
 - scope of, 658
 - security associations (SA), 659
 - Windows network defenses, 732–733
- Internet security protocols, 651–670
 - e-mail, 662–665
 - internet protocol security (IPSec), 656–662
 - Multipurpose Internet Mail Extension (MIME), 662–663
 - radix-64 conversion, 668–670
 - Secure Sockets Layer (SSL), 652–656
 - Secure/Multipurpose Internet Mail Extension (S/MIME), 662–665
 - Transport Layer Security (TLS), 652
- Internet Society (ISOC), 5
- Internet use policies, 464
- Interposable libraries, 493–497
- Intruders, 177–180
- Intrusion detection systems (IDS), 56, 176–214
 - anomaly, 183, 185–187, 196–197
 - base-rate fallacy, 189–190, 211–214
 - distributed adaptive, 197–200

- Intrusion detection systems (IDS)
 - (continued)
 - distributed host-based, 190–192
 - exchange format, 200–202
 - hash functions and, 56
 - honeypots, 202–204
 - host-based, 181, 183–190, 190–192
 - network-based (NIDS), 193–197
 - sensors, 181, 193
 - Snort, example system of, 204–208
 - Stanford Research Institute (SRI) (IDES), 187–188
- Intrusion prevention systems (IPS), 179, 273–302
 - firewalls and, 273–302
 - host-based (HIPS), 292–293
 - network-based (NIPS), 293
 - Snort Inline, 294
 - unified threat management (UTM), example of, 294–298
- IP address spoofing, 280
- IPS, *see* Intrusion prevention systems (IPS)
- IPSec, *see* Internet protocol security (IPSec)
- IT, *see* Information technology (IT)
- ITU, *see* International Telecommunication Union (ITU)
- ITU Telecommunication Standardization Sector (ITU-T), 5, 22–23, 38–39, 477–478
- Kerberos, 672–678
 - internet authentication and, 672–678
 - performance of, 677–678
 - protocol, 672–675
 - realms, 676–677
 - ticket-granting service (TGT), 674–675
 - ticket-granting ticket (TGT), 673
 - versions 4 and 5, 677
- Kernel mode, DAC, 122
- Kernel space, Linux DAC file security, 699
- Key distribution, symmetric encryption, 618–620
- Key exchange, *see* Diffie-Hellman key exchange
- Key expansion, AES, 607
- Key management, 61–64, 166
- Keys, 42, 57–59, 594
- Keystream, 48, 607–608
- Leaky system resources, 12
- Least privileges, 411–413
- Legal aspects of computer security, 562–591.
 - See also* Ethics
 - cybercrime and, 563–567
 - intellectual property and, 567–574
 - privacy and, 574–580
 - ethical issues, 580–586
- Libraries, 375–376, 413–416, 493–497
 - dynamic binary rewriting, 496–497
 - dynamically linked, 493
 - interposable, 493–497
 - safe, compile-time defenses and, 375–376
 - shared, 493
 - standard OS functions, 413–416
 - statically-linked, 493
- Libwrappers, Linux security, 703–704
- Linux, 690–719
 - access controls, 692, 693–699, 703–705, 711–717
 - application security of, 709–710
 - Discretionary Access Controls (DAC), 692, 693–699
 - firewalls, use of iptables for local, 704–405
 - logging, 707–708, 710
 - Mandatory Access Controls (MAC), 711–717
 - network-level access controls, 703–705
 - Novell AppArmor, 716–717
 - OS installation, 702–703
 - root delegation, 706–707
 - security of, 690–719
 - security-enhancing tools for, 708–709
 - SELinux, 711–716
 - system hardening, 701–709
 - user management and, 705–706
 - vulnerabilities of, 699–701
- Loadable modules, 496
- Local accounts, Windows security, 722
- Local security authority (LSA), 721
- Lockfile, software security, 416
- Logging function, 486–497, 707–708, 710
 - application level, at the, 491–492, 710

- interposable libraries, 493–497
- Linux security, 707–708, 710
- security auditing implementation of, 486–497
- syslog (UNIX), 489–491, 707–708
- system levels of, 486–491
- Windows event log, 486–489
- Logic bomb, 217, 218
- Logical security, 428, 441–446
- Macro virus, 224, 225
- Maintenance hook, 216
- Malicious software, 215–248
 - backdoor (trapdoor), 216–218
 - bots (zombies), 217, 239–242
 - logic bomb, 217, 218
 - mobile code, 217, 219
 - multiple-threat malware, 219–220
 - rootkits, 217, 242–244
 - Trojan horse, 217, 218–219
 - types of, 216–220
 - viruses, 217, 220–226, 226–230
 - worms, 217, 231–239
- Malware, 219–220
- Man-in-the-middle-attack, 644–645
- Mandatory Access Controls (MAC), 113, 711–717, 726–728
- Markov model, 85–87, 187
- Masquerade, security threats by, 15, 16, 19, 117
- MD5 message-digest algorithm, 631
- Mean and standard deviation, 187, 188
- Memory cards, 89
- Memory leak, 407
- Memory management unit (MMU), 377
- Message authentication, 49–56, 625–650
 - code (MAC), 50–52
 - compression function, 631
 - Diffie-Hellman exchange, 641–645
 - hash functions and, 49–56, 626–627
 - HMAC, 632–635
 - MD5 message-digest algorithm, 631
 - public-key cryptography and, 625–650
 - public-key encryption and, 635–641, 641–645
 - RSA algorithm, 635–341
 - secure hash algorithm (SHA), 56, 627–631
 - symmetric encryption, using, 49
 - Whirlpool, 631–632
 - without message encryption, 49–50
- Message confidentiality, symmetric encryption and, 593–624
- Metamorphic virus, 224
- Misfeasors, 177
- Mix column transformation, AES, 606
- MLS, *see* Multilevel security (MLS)
- Mobile code, 217, 219
- Mobile phone worms, 235
- Modes of operation, symmetric encryption, 47, 610–616
- Modification of messages, 19
- Modularity, Linux application security, 710
- Monitoring, Analysis, and Response System (MARS), 503–504
- Morris worm, 232
- Multilevel security (MLS), 303–348. *See also*
 - Information technology (IT) security evaluation; Trusted computing (TC)
 - application of, 323–330
 - Bell-Lapadula model (BLP), 304–314
 - Biba integrity model, 314–315
 - Chinese wall model, 317–319
 - Clark-Wolson integrity model, 315–317
 - database security and, 325–330
 - information technology security evaluation, 334–340, 340–344
 - role-based access control (RBAC), for, 324–325
 - trusted computing (TC), 320–323, 330–334, 334–340
- Multipartite virus, 219
- Multiple-threat malware, 219–220
- Multipurpose Internet Mail Extension (MIME), 662–663
- Multivariate model, 187
- Mutually exclusive roles, RBAC, 131
- National Institute of Standards and Technology (NIST), 5, 7, 34, 38, 44–45, 47, 61, 452, 453, 541–546. *See also* Federal Information Processing Standards (FIPS)
- National Security Agency (NSA), 39

- Natural disasters as threats to physical security, 430–431, 437–438
- Network-based intrusion detection (NIDS), 193–197
 - alerts, logging, 197
 - anomaly detection, 196–197
 - banner grabbing, 197
 - sensor deployment, 193–196
 - signature detection, 196
- Network-based intrusion prevention systems (NIPS), 293
- Network-based worm defense, 238–239
- Network defenses, Windows system, 732–733
- Network interface card (NIC), 193
- Network-level access controls, 703–705
- Networks, computer security and, 12, 19–20, 27–28
- NIST, *see* National Institute of Standards and Technology (NIST)
- No-execute bit, 377
- Noise as a physical interference, 435
- NOP sled, 369
- Novell AppArmor, 716–717
- Numeric modes, Linux DAC file security, 698–699
- Objects of access control, 115
- Off-by-one attacks, 379–380
- One-way hash functions, 52–54
- Open Shortest Path First (OSPF), 658
- Open systems interconnection (OSI), 22–27
- Operating systems (OS), 408–419, 702–703
 - environmental variables, 408–411
 - interacting with other programs, 408–419
 - least privileges, 411–413
 - Linux security and installation of, 702–703
 - privilege escalation, 411
 - race conditions, prevention of, 416–417
 - software security and, 408–419
 - standard library functions, 413–416
 - systems calls and, 413–416
 - temporary files, safe use of, 417–419
- Organizational security policy, 455–461
- OS, *see* Operating systems (OS)
- OSI, *see* Open systems interconnection
- Output perturbation, 165
- Outside attack, 14
- Overflows, 350–387
 - buffer, 350–387
 - global data area, 383–385
 - heap, 381–383
 - off-by-one attacks, 379–380
 - replacement stack frame, 379–380
 - return to system call, 380–381
 - stack, 352–372
- Overrun, *see* Overflows
- Overvoltage, 434
- Packet filtering firewalls, 276–280
- Parasitic software, 216
- Partitioning, 162–163
- Passive attack, 14, 19–20
- Passwords, 56, 75, 76–88, 97–98, 706
 - aging, Linux, 706
 - authentication protocol, 97–98
 - Bloom filter, 87–88
 - choices of, 81–82
 - computer-generated, 84
 - cracking approaches, 80, 85
 - dictionary compilation, 85
 - file access control, 83
 - hash functions as, 56
 - hashed, 78–80
 - Markov model, 85–87
 - proactive checker, 84–85
 - reactive checking strategy, 84
 - selection strategies, 83–85
 - user authentication and, 75, 76–88
 - use of, 78–80
 - vulnerability of, 76–78
- Patch management, Linux security and, 703
- Patents, intellectual property and, 569
- Permission, computer security and, 128, 132, 694–699
- Personal firewall, 284–286
- Personal identification number (PIN), 89
- Personal identity verification (PIV), 441–446
- Perturbation, 164–166
 - data swapping, 164–165
 - limitations of, 165–166

- output, 164, 165
- random-sample queries, 165
- Physical security, 427–448
 - corporate policy, example of, 440–441
 - environmental threats to, 431–434, 436–437
 - human-caused threats to, 435
 - logical security and, integration of, 441–446
 - natural disasters and, 430–431, 437–438
 - personal identity verification (PIV), 441–446
 - planning and implementation for, 439–440
 - prevention and mitigation of attacks, 435–738
 - security breaches, recovery from, 438
 - technical threats to, 434–435, 437
 - threat assessment, 439–440
 - threats to, 429–435
- Ping of death, DoS, 252
- Plaintext, 42, 57, 594
- Poison packet, DoS, 251
- Policy enforcement points (PEPs), 199, 200
- Policy writers, resources for, 460–461
- Polymorphic virus, 224
- Preimage resistant hash functions, 54
- Premises security, 428
- Pretty Good Privacy (PGP), 67–68
- Privacy, 574–580
 - computer usage, 576–578
 - data surveillance and, 578–580
 - European Union Data Protection Directive, 574–575
 - laws and regulations of, 574–576
 - organizational response to, 576
 - United States Privacy Act, 575–576
- Private keys, 57–59
- Privileges, 411–413, 724, 731–732
 - escalation, 411
 - least, 411–413
 - low privilege service accounts, 731
 - operating systems (OS), 411–413
 - stripping, 731–732
 - Trusted Computing Base (TCB), 724
 - Windows security and, 724, 731–732
- Proactive worm containment (PWC), 237–238
- Profile-based anomaly detection, 183, 186
- Program input, 392–403
 - buffer overflow, 392–393
 - cross-site scripting attacks (XSS), 398–400
 - fuzzing, 402–403
 - injection attacks, 394–398
 - interpretation of, 393–394
 - size of, 392–393
 - validating syntax, 400–402
- Program output, 419–422
- Protected storage, TC, 333–334
- Protection domains, DAC, 122
- Protection profiles (PPs), 336, 338–340
- Protocol type selection (PTS), 92
- Protocol, *see* Authentication protocol; Internet security protocols
- Proxy, *see* Gateways
- Pseudorandom numbers, 66–67
- Public-key certificates, 62–63, 665
- Public-key encryption, 56–61, 61–64, 635–641, 641–645
 - asymmetric encryption algorithms, 60–61, 645
 - asymmetric process of, 57–59
 - certificates, 62–63
 - cryptosystems, applications for, 59
 - Diffie-Hellman exchange, 61, 641–645
 - Digital Signature Standard (DSS), 61, 645
 - digital signatures, 61–64
 - elliptic curve cryptography (ECC), 61, 645
 - key management, 61–64
 - keys for, 57–59
 - message authentication and, 635–641, 641–645
 - requirements for, 60
 - RSA algorithm, 60, 635–341
 - structure of, 56–59
 - symmetric key exchange using, 63
- Public-key infrastructure (PKI), 680–683
 - IETF Public Key Infrastructure X.509 (PKIX) model, 681–683
 - internet authentication and, 680–683
 - management functions and protocols, 682–683
- Public keys, 57–59

- Queries, 155, 158–159, 159–162
 - denial and information leakage, 163
 - inference from, 155, 158–159
 - partitioning, 162–163
 - random-sample, 165
 - restriction, 159–162
 - set overlap control, 162
- Query language, 143–144. *See also* Structural Query Language (SQL)
- Race conditions, prevention of, 407, 416–417
- Radix-64 conversion, 668–670
- Rainbow table, 80
- Random (selective) drop of an entry, 268
- Random numbers, 65–67
 - independence of, 65
 - pseudorandom numbers versus, 66–67
 - true generator (TRNG), 66–67
 - uniform distribution, 65
 - unpredictability of, 66
- Random-sample queries, 165
- Raw socket interface, DoS, 253
- RBAC, *see* Role-based access control (RBAC)
- RC4 algorithm, 607, 609–610
- Realms, Kerberos, 676–677
- Reference monitors, TC, 320–322
- Reflection attacks, 261–263
- Registration authority (RA), 681
- Relational databases, 144–148
- Release of message contents, 19
- Remote code injection attack, 397–398
- Remote user authentication, *see* Authentication protocol
- Replacement stack frame, 379–380
- Replay attacks, 19, 101
- Requests for Comments (RFCs), 5, 12–14, 39, 266, 491–491
- Return address defender (RAD), 337
- Return to system call, 380–381
- RFCs, *see* Requests for Comments (RFCs)
- Risk, 13, 21, 521–528. *See also* Security risk assessment
 - analyzing, 524–528
 - appetite, 521
 - consequences and impact of threats, 525–526, 529
 - evaluation of, 528
 - existing controls, 524
 - identification of, 522–524
 - likelihood of threat, 524–525, 529
 - register for documentation of, 527–528
 - system resources and, 13, 21, 521–522
 - treatment of, 528–529
- Role-based access control (RBAC), 113, 125–137, 151–153, 324–325
 - access control matrix, 127–128
 - base model, RBAC₀, 128–130
 - case study of, 134–137
 - constraints, RBAC₂, 130–131
 - core, 132–133
 - database management systems (DBMS), 151–153
 - dynamic separation of duty (DSD), 134
 - hierarchical, 133–134
 - multilevel security (MLS) for, 324–325
 - NIST model, 131–134
 - reference models, 128–131
 - role hierarchies, RBAC₁, 130
 - roles of, 126–128
- Roles, 126–128, 130, 133–134, 152–153
 - DBMS access control, 152–153
 - fixed database, 152
 - fixed server, 152
 - hierarchies, 130, 133–134
 - RBAC, 126–128, 131
 - user-defined, 152–153
- Rootkit attacks, 217, 242–244, 701
 - countermeasures for, 243–244
 - installation of, 243
 - Linux vulnerability to, 701
 - system-level call attacks, 243
- Routing applications of IPSec, 658
- RSA algorithm, 60, 635–641
 - description of, 636–638
 - factoring problem for, 638–640
 - message authentication and, 635–641
 - timing attacks and, 640–641
 - security of, 638–641
- Rule-based anomaly detection, 187–188
- Rule-based penetration identification, 188–189
- Run-time defenses, 377–378

- Salt value, 79
- Scanning attacks, 197
- Screening router, 291
- SDB, *see* Statistical databases (SDB)
- Second preimage resistant hash functions, 54
- Secret key, 42, 57, 594
- Secure hash algorithm (SHA), 56, 627–631
- Secure hash functions, *see* Hash functions
- Secure programming, *see* Defensive programming
- Secure Sockets Layer (SSL), 652–656
 - architecture of, 652
 - Record Protocol, 653–654
 - Change Cipher Spec Protocol, 654
 - Alert Protocol, 654
 - Handshake Protocol, 654–656
- Secure/Multipurpose Internet Mail Extension (S/MIME), 662–665
- Security account manager (SAM), 721, 722
- Security Assertion Markup Language (SAML), 685
- Security associations (SA), 659
- Security auditing, 475–507
 - architecture of, 475–481
 - audit and alarms model (X.816), 477–478
 - audit trails, 481–486, 497–501
 - functions of, 479–480
 - implementation guidelines for, 481
 - integrated approach, example of, 501–504
 - interposable libraries for, 493–497
 - logging function, 486–497
 - Monitoring, Analysis, and Response System (MARS), 503–504
 - requirements for, 480–481
 - security information and event management system (SIEM), 501–502
- Security defenses, 729–737
- Security ID (SID), Windows, 723
- Security implementation, 538–561
 - case study of, 556–558
 - change and configuration management, 551–552
 - compliance, 551
 - controls (safeguards), 538–546, 548–550
 - detection of incidents, 553–554
 - documentation of incidents, 556
 - follow-up, 550–556
 - handling of incidents, 552–553
 - incident response, 554–555
 - ISO security controls, 541–543
 - IT security management, 508–537, 538–561
 - maintenance, 550
 - NIST security controls, 541–546
 - plans, 547–548
- Security information and event management system (SIEM), 501–502
- Security information management system (SIM), 501
- Security management, standards for, 469–473
- Security Parameters Index (SPI), 659
- Security policy, standards for, 473–474
- Security reference monitor (SRM), 721
- Security risk assessment, 21, 515–518, 518–530, 530–534. *See also* Risk
 - asset identification, 521–522
 - baseline approach, 516
 - case study of, 530–534
 - combined approach, 517–518, 530–534
 - context establishment, 520–524
 - detailed risk analysis, 517, 518–530
 - identification of threats, risks, and vulnerabilities, 522–523
 - informal approach, 516–517
 - risk analysis and evaluation, 524–528
 - treatment of identified risks, 528–529
- Security targets (STs), 337–338
- SELinux, 711–716
- Sensors, 181, 193–196
- Service restart policy, Windows system defense, 736–737
- setgid, Linux DAC file security, 697–698
- setuid, Linux DAC file security, 697–698
- Shadow password file, 83
- Shared files, locking for software security, 416–417
- Shellcode, 365–372
- Shift row transformation, AES, 604, 606
- Signature detection, 184, 187–189, 196
- Signed data, S/MIME, 664
- Simple Object Access Protocol (SOAP), 685

- Smart cards, 89–92
- Snort, 204–208, 294
- Software, 12, 17–18, 215–248
 - behavior-blocking, 229–230
 - malicious, 215–248
 - multiple-threat malware, 219–220
 - threats to, 17–18
- Software security, 388–425
 - defensive programming and, 389–392
 - operating systems, interaction of, 408–419
 - program input, 392–403
 - program output, 419–422
 - writing safe program code, 403–407
- Source routing attacks, 280
- Spoofing, 253–354, 254–257, 280
- SQL injection attack, 396, 397
- SSL Record Protocol, 653–654
- Stack buffer overflow, 356–358
- Stack frame, 356–357
- Stack overflow, 352–372
- Stack randomization, Windows system
 - defense, 736
- Stack smashing, 356
- Standard library functions, 413–416
- Stanford Research Institute (SRI) IDS (IDES), 187–188, 189
- Stateful inspection firewalls, 280–281
- Static biometric authentication, 76, 98
- Static separation of duty (SSD), 134
- Statistical databases (SDB), 156–166
 - characteristic formula, 156, 158
 - inference from, 158–159
 - partitioning, 162–163
 - perturbation, 164–166
 - queries and, 155, 158–159, 159–162
- Stealth virus, 224
- Sticky bit, Linux DAC file security, 696–697
- Stream ciphers, 47–49, 607–610
- Structured Query Language (SQL), 147–148, 149–150
- Subjects of access control, 115
- Substitute bytes transformation, AES, 604
- Symmetric encryption, 42–49, 63, 593–624
 - Advanced Encryption Standard (AES), 42, 47, 600–607
 - block encryption algorithms, 44–47
 - cipher block chaining (CBC), 612–613
 - cipher block feedback (CFB), 614–615
 - counter (CTR) mode, 615–616
 - cryptanalysis and, 595–596
 - cryptography and, 594–595
 - Data Encryption Algorithm (DEA), 44
 - Data Encryption Standard (DES), 42, 44–45, 598–600
 - devices, location of, 616–618
 - electronic codebook (ECB), 47, 611–612
 - Electronic Frontier Foundation (EFF), 45
 - Feistel cipher structure, 596–598
 - key distribution, 618–620
 - key exchange using public-key encryption, 63
 - message authentication using, 49
 - message confidentiality and, 42–49, 593–624
 - modes of operation, 47, 610–616
 - principles of, 594–598
 - RC4 algorithm, 607, 609–610
 - secret key, 42, 594
 - stream ciphers, 47–49, 607–610
 - triple DES (3DES), 45–46, 599–600
- Syslog (UNIX), 489–491
- Syslogd (Linux), 707–708
- Systems calls, software security, 413–416
- System-level audit trail, 483
- System resources (assets), 12–14, 14–16, 17–18, 521–522
 - attacks on, 14–16, 19–20
 - categories of, 12–13
 - communication line threats, 19–20
 - data threats, 18
 - hardware threats, 17
 - identification of for security risk assessment, 521–522
 - network security attacks, 19–20
 - software threats, 17–18
 - threats to, 14–16, 19–20
 - vulnerabilities of, 12–13
- Target of evaluation (TOE), 335, 343–344
- TC, *see* Trusted computing (TC)
- TCP SYN flood attack, 258–259
- TCP wrappers, Linux security, 703–704
- Teardrop attack, DoS, 252

- Technical threats, 434–435, 437
 - electrical power, 434–435
 - electromagnetic interference (EMI), 435
 - prevention of, 437
- Temporary files, safe use of, 417–419
- The Standard of Good Practice for Information Security* (ISF05), 460, 469–473, 473–474, 576
- Threat source, 522–523
- Threats, 13, 14–16, 17–20, 429–435, 522–523
 - communication lines and, 19–20
 - data and, 18
 - environmental, 431–434
 - hardware and, 17
 - human-caused, 435
 - identification of for security risk
 - assessment, 522–523
 - natural disasters, 430–431
 - networks and, 19–20
 - physical security, 429–435
 - software and, 17–18
 - technical, 434–435
 - types of, 14–16
- Threshold detection, 183, 186, 501
- Ticket-granting service (TGT), 674–675
- Ticket-granting ticket (TGT), 673
- Time series model, 187
- Timing attacks and RSA algorithms, 640–641
- Tiny fragment attacks, 280
- Tokens, 75, 88–92, 100–101
 - authentication protocol, 90, 98
 - automatic teller machine (ATM), 89
 - memory cards, 89
 - personal identification number (PIN), 89
 - smart cards, 89–92
 - theft of, 100–101
 - USB dongle, 92
 - user authentication and, 75, 88–92
- Trademarks, intellectual property and, 569–570
- Traffic analysis, 19
- Transport Layer Security (TLS), 652
- Tribe Flood Network (TFN), 259–260
- Triple DES (3DES), 45–46, 599–600
- Trojan horse, 101, 217, 218–219, 322–323
- True random number generator (TRNG), 66–67
- Trusted computing (TC), 320–323, 330–334, 334–340. *See also* Information technology security evaluation
 - authenticated boot service, 330–331
 - certification service, 331
 - concept of, 320–323
 - encryption service, 331–332
 - information technology security evaluation, 334–340, 340–344
 - platform module (TPM), 330, 332–333
 - protected storage, 333–334
 - reference monitors, 320–322
 - Trojan horse defense, 322–323
- Trusted platform module (TPM), 330, 332–333, 739
- Tuples, relational databases, 146
- UDP flood attack, 258
- Undervoltage, 434
- Unified threat management (UTM),
 - example of, 294–298
- Uninterruptible power supply, 437
- United States Privacy Act, 575–576
- UNIX, 79–80, 122–125, 489–491
 - access control lists in, 125
 - file access control, example of, 122–125
 - hashed passwords, implementations of, 79–80
 - syslog, 489–491
- USB dongle, 92
- USENET newsgroups, 4
- User accounts, Linux security, 693–694
- User authentication, 74–109. *See also* Authentication protocol
 - authentication protocol, 90, 97–99
 - biometric, 76, 92–97, 101–103
 - case study of, 103–105
 - means of, 75–76
 - passwords, 75, 76–88
 - remote, 97–99
 - tokens, 75, 88–92, 100–101
 - Trojan horse attacks, 101
- User Principal Name (UPN), Windows, 723
- USTAT, state-transition model, 189–190

View, relational databases, 146–147
 Virtual private networks (VPN), 288–289
 Viruses, 219–239
 antivirus approaches, 226–229
 behavior-blocking software, 229–230
 classification of, 223–224
 countermeasures for, 226–230, 235–239, 242, 243–244
 e-mail and, 219, 225–226
 kits for, 224
 macro, 225
 nature of, 220–223
 structure of, 221–223
 Vulnerability, 12–13, 76–78, 523, 699–701, 728–729
 identification of for security risk
 assessment, 523
 Linux security, 699–701
 loadable kernel modules (LKMs), 701
 passwords, 76–78
 rootkit attacks, 701
 setuid root program, 700
 system resources, 12–13
 Web application, 700–701
 Windows security, 728–729

Web clients and servers, 220
 Web sites, 3–4.
 Whirlpool, 631–632
 Windowing, audit trail analysis, 501
 Windows, 219, 486–489, 720–741
 access control lists (ACL), 724–726
 active directory (AD), 721, 722

Common Criteria EAL4+Flaw
 Remediation status, 739
 cryptographic services of, 737–739
 discretionary ACL (DACL), 724–726
 end-to-end domain, example of, 723
 event log, 486–489
 local security authority (LSA), 721
 mandatory access control (MAC), 726–728
 security account manager (SAM), 721, 722
 security architecture, 721–728
 security defenses, 729–737
 security reference monitor (SRM), 721
 vulnerabilities of, 728–729
 Worms, 197, 217, 231–239
 attacks by, 197, 233–234
 countermeasures for, 235–239
 mobile phones and, 235
 Morris, 232
 network-based defense, 238–239
 proactive containment (PWC), 237–238
 propagation model, 232–233
 state-of-the-art technology of, 234
 Writing safe program code, 403–407
 WS-Security, 685

X.509, 62, 678–680
 XSS reflection vulnerability, 398

Yahoo newsgroups, 4

Zero-day vulnerabilities, 703
 Zombies, *see* Bots