Index

Numbers
3DES (Triple DES), 177, 220, 222–223
802.1X/EAP, 478
802.11 standard, 473

A
AAA services, 8, 11
AACS (Advanced Access Content System), 260
abstraction, 13, 43
acceptable use policies, 28
access abuses, 410–411
access control
administrative control, 583–584
assets, 580–581
attacks, 635–636
access aggregation, 641
asset identification, 637–638
password attacks, 641–648
risk elements, 636
smartcard attacks, 651–652
social engineering attacks, 649–651
spoofing attacks, 648
threat identification, 638–640
vulnerability analysis, 640
authorization
access control matrix, 625
ACL, 625
capability tables, 625
constrained interface, 625–626
content-dependent control, 626
context-dependent control, 626
implicit deny, 625
need to know, 626
principle of lease privilege, 626

separation of duties and responsibilities, 626
CIA Triad and, 581–582
compensating control, 583
corrective control, 583
DAC (Discretionary Access Control), 628, 629
defense-in-depth, 627–628
detectorive control, 582–583
deterrent control, 583
directive control, 583
logical control, 584
nondiscretionary, 630–635
ABAC (Attribute Based Access Control), 629
Attribute Based, 633
MAC (Mandatory Access Control), 629, 633–635
RBAC (Role Based Access Control), 628, 630–632
rule-based access control, 628, 632
permissions, 624
physical control, 584
preventive control, 582
privilege creep, 631
privileges, 625
protection methods
account lockout, 653
electronic access, 652
logon notification, 653
multifactor authentication, 652–653
password hashing, 652
password masking, 652
password policies, 652
password salting, 652
physical access, 652
user education, 653
recovery control, 583
review question answers, 971–973
rights, 624–625
security policies, 626–627
steps, 582
technical control, 584
written lab answers, 996
access control matrix, 286–288, 625
access points, 473–475
ad hoc mode, 475
enterprise extended mode, 475
ESSID, 475
infrastructure mode, 475
rogue access points, 484–485
SSID, 475
stand-alone mode, 475
wired extension mode, 475
access review audits, 785
account lockout, 653
account management reviews, 689
accountability, 11, 43
AAA services, 8
authorization and, 586–587
accreditation, 306–307
CNSS (Committee on National Security Systems), 308
DIACAP (DoD Information Assurance Certification and Accreditation Process), 308
DITSCAP (Defense Information Technology Security Certification and Accreditation Process), 308
NIACAP (National Information Assurance Certification and Accreditation Process), 308
RMF (Risk Management Framework), 308
ACL (access control lists), 625
active website monitoring, 687
ADEPT (Adobe Digital Experience Protection Technology), 261
Adleman, Leonard, 239
administrative access control, 583–584
administrative controls, 78–79
physical, 403
administrative investigations, 846–847
administrative law, 128–129
advisory policies, 27
adware, 928
AES (Advanced Encryption Standard), 220, 224–225
agents, 565
aggregation, 700
Agile development approach, 884–885
ALE (annualized loss expectancy), 70–71, 110
algorithms
asymmetric key, 216–219
hashing algorithms, 219
memorization chart, 246
key spaces, 201
alternate processing sites, 820–821
cloud computing, 824
cold sites, 821–822
hot sites, 822–823
mobile sites, 823–824
service bureaus, 824
warm sites, 823
analytic attacks, 265
AND operation, 202–203
antivirus
heuristic-based detection, 921
Kaspersky Lab, 920–921
signature-based detection, 921
Tripwire, 922
APIPA (Automatic Private IP Addressing), 552–553
application attacks
back doors, 934–935
buffer overflows, 933–934
escalation of privilege, 935
rootkits, 935
TOCTTOU, 934
written lab answers, 1000
Application layer (OSI)
EDI (Electronic Data Interchange), 451
FTP (File Transfer Protocol), 451
HTTP (Hypertext Transfer Protocol), 451
IMAP (Internet Message Access Protocol), 451
LPD (Line Print Daemon), 451
NNTP (Network News Transport Protocol), 451
Application (Process) layer (TCP/IP model) – assurance

cloud-based, 713–714

data classification, 162
  confidential, 162, 164
  defining, 165
  FOIA (Freedom of Information Act), 163
  FOUO (for official use only), 163
  private, 164
  proprietary, 164
  public, 165
  SBU (sensitive but unclassified), 163
  secret, 162
  sensitive, 164
  top secret, 162
  unclassified, 163

data security controls, 165–167

devices, 580

facilities, 580

files, 581

hardware inventories, 710–711

information, 580

media management, 714–715
  flash drives, 715
  lifecycle, 717
  mobile devices, 716–717
  tape media, 716

objects, 581

owners, 179–180

personnel, 580

PHI (protected health information), 161

physical assets, 711–712

PII (personally identifiable information),
  160–161

proprietary data, 161–162

retaining, 175–176

review question answers, 956–958

sensitive
  handling, 170–171
  marking, 169–170

software, licensing, 711

subjects, 581

systems, 580

valuation, 65

virtual assets, 712

written lab answers, 991

assurance, 281

POP3 (Post Office Protocol version 3), 451

SET (Secure Electronic Transaction), 451

SMTP (Simple Mail Transfer Protocol),
  451

SNMP (Simple Network Management
  Protocol), 451

S-RPC (Secure Remote Procedure Call), 451

telnet, 451

TFTP (Trivial File Transfer Protocol), 451

application-level gateway firewalls, 489

APTs (advanced persistent threats), 705, 858,
  917

architecture, 320–321
  distributed, 351
  review question answers, 966–967
  written lab answers, 994–995

ARO (annualized rate of occurrence), 70, 109

ARP (Address Resolution Protocol), 445,
  446–447, 461–462, 567–568

artificial identifiers, 183

ASCII (American Standard Code for
  Information Interchange), 450

asset-focused threats, 31

assets, 64
  access control, 580
asymmetric cryptography
El Gamal, 241
elliptic curve, 242
key length, 240–241
Merkle-Hellman Knapsack, 240–241
private keys, 238–239
public keys, 238–239
RSA algorithm, 239–241
asymmetric cryptosystems, 199
asymmetric key algorithms, 216–219
key management, 253–254
asynchronous dynamic password tokens, 593
ATO (authorization to operate), 63
attacker-focused threats, 31
attacks, 66, 635–636. See also malicious code
access aggregation, 641
access control, 635–636
access aggregation, 641
asset identification, 637–638
password attacks, 641–648
risk elements, 636
smartcard attacks, 651–652
social engineering attacks, 649–651
spoofing attacks, 648
threat identification, 638–640
vulnerability analysis, 640
agents, 565
application attacks
back doors, 934–935
buffer overflows, 933–934
escalation of privilege, 935
rootkits, 935
TOCTTOU, 934
APTs (advanced persistent threats), 858
ARP (Address Resolution Protocol), 567–568
asset identification, 637–638
botnets, 565, 747–748
bots, 565
business, 858
computer architecture
buffer overflow, 386–387
data diddling, 387–388
design-based attacks, 385–388
incremental, 387–388
input checking, 386–387
maintenance hooks and, 387
parameter checking, 386–387
privileged programs, 387
salami attack, 388
state attacks, 389
trusted recovery and, 386
computer crime
APTs, 858
business, 858
corporate espionage, 858
financial, 859
grudge, 859–861
hacktivists, 861
industrial espionage, 858
insider threats, 860
intelligence, 857–858
military, 857–858
script kiddies, 861, 916–917
terrorist, 859
thrill, 861
cryptography
analytic, 265
birthday, 267–268
brute force, 265–266
chosen ciphertext, 267
chosen plaintext, 267
ciphertext only, 266–267
collision attack, 267–268
frequency, 266–267
implementation, 265
known plaintext, 267
man in the middle, 267
meet in the middle, 267
replay, 268
reverse hash matching attack, 267–268
statistical, 265
DDoS (distributed denial of service), 564–565
DNS poisoning, 568
DNS spoofing, 568
DoS (denial of service), 564–565, 748–749
eavesdropping, 565–566
espionage, 755–756
financial, 859
fraggle attacks, 751
grudge, 859–861
hijacking, 568
hyperlink spoofing, 568–569
impersonation, 566–567
insider threats, 860
intelligence, 857–858
land attacks, 752
malicious code, 753–754
drive-by downloads, 753
man-in-the-middle, 754–755
masquerading, 566–567
military, 857–858
modification attacks, 567
password attacks, 641–643
birthday attacks, 645–646
brute-force attacks, 644–645
dictionary attacks, 643
PBKDFw, 646
pepper, 647
rainbow table attacks, 646
sniffer attacks, 647
wireshark capture, 647–648
phishing, 569
ping floods, 751
ping of death, 751–752
replay attacks, 567
review question answers, 968–969
risk elements, 636
sabotage, 755
smartcard attacks, side-channel attacks, 651–652
smurf attacks, 751
social engineering attacks
phishing, 649–650
shoulder surfing, 649
spear phishing, 650
vishing, 651
whaling, 651
spoofing attacks, 648
SYN flood attacks, 749–750
TCP reset, 750
teardrop, 752
terrorist, 859
threat identification
APTs, 639–640
thread modeling, 638–639
thread modeling approaches, 640
thrill, 861
unskilled attackers, 457
VoIP (Voice over Internet Protocol), 525
vulnerability analysis, 640
wireless networking, 482–483
evil twins, 485
IV (initialization vector), 484
replay attacks, 484
rogue access points, 484–485
war chalking, 483
war driving, 483
written lab answers, 995
zero-day exploits, 752–753, 928
zombies, 565
auditing, 42, 783
AAA services, 8, 10–11
access review audits, 785
auditors, 784
change management, 788
COBIT (Control Objectives for
Information and related
Technologies), 667
configuration management, 788
external, 666
inspection audits, 784–785
internal, 665–666
job descriptions, 56
job responsibilities, 56
monitoring, 11
patch management, 787
privileged groups, 786–787
privileges, 56
reporting
distributing, 789
external auditors, 789–790
results protection, 788–789
third-party, 666–667
user entitlement audits, 786
vulnerability management, 788
work tasks, 56
AUP (Agile Unified Process), 885
authentication, 42, 584–585
AAA services, 8–10
authentication factor, 9
biometrics, 588, 595–596
crossover error rate, 598
face scans, 596
false acceptance rate, 598
false rejection rate, 598
fingerprints, 596
hand geometry, 597
heart/pulse patterns, 597
iris scans, 596–597
keystroke patterns, 598
palm scans, 597
registration, 599
retina scans, 596
signature dynamics, 597
voice pattern recognition, 597
challenge-response, 200
context-aware, 588
cryptography and, 200
device, 600–601
identification and, 9–10
multifactor, 599–600
passwords
age, 590–591
cognitive, 592
complexity, 591
history, 591
length, 591
phrases, 591
static, 588–589
review question answers, 969–971
service, 601
smartcards, 592–593
somewhere you are, 588
tokens
asynchronous dynamic password, 593
one-time passwords, 593
synchronous dynamic password, 593
two-factor, 599–600
two-step
HOTP, 594
TOTP, 594–595
Type 1, 587
Type 2, 587
Type 3, 587
written lab answers, 996
authentication protocols
CHAP (Challenge Handshake Authentication Protocol), 524
EAP (Extensible Authentication Protocol), 524
LEAP, 524
PAP (Password Authentication Protocol), 524
PEAP, 524
authorization, 42
AAA services, 8, 10
access control matrix, 10, 625
accountability and, 586–587
ACL, 625
capability tables, 625
constrained interface, 625–626
content-dependent control, 626
context-dependent control, 626
DAC and, 10
implicit deny, 625
MAC and, 10
need to know, 626
principle of lease privilege, 626
privileges, 10
RBAC and, 10
separation of duties and responsibilities, 626
auxiliary station alarm systems, 428
availability, 42
CIA Triad, 2–3, 6–7

B
back doors, 934–935
backbone distribution system, 407
background checks, 55
backups
differential backups, 830
full backups, 830
incremental backups, 830
verification, 690
badges, 427
baseband cabling, 497–498
baselines, 28
security control baselines, 186–187
scoping, 187
standards, 187
tailoring, 187
BCM (business continuity management), 802
BCP (business continuity planning), 98–99
buildings, 113
continuity goals, 115
documentation, 115
versus DRP (disaster recovery planning), 98–99
emergency response guidelines, 118
exercises, 119
facilities, 113
infrastructure, 113–114
legal requirements, 104–105
likelihood assessment, 108–109
maintenance, 118
organization analysis, 100
people, 112–113
plan approval, 114
plan implementation, 114
regulatory requirements, 104–105
resources, 103–104
review question answers, 952–954
risk acceptance, 117
risk assessment, 116–117
risk identification, 107–108
risk mitigation, 117
senior management and, 102–103
statement of importance, 116
statement of organizational responsibility, 116
statement of priorities, 116
statement of urgency and timing, 116
strategy development, 112
team selection, 101–103
testing, 119
training and education, 115
vital records, 117–118
written lab answers, 989
behavior modification, 86
Bell-LaPadula security model, 288–290
BGP (Border Gateway Protocol), 447
BIA (business impact assessment), 105, 110–111
AV (asset value), 106
cloud and, 108
MTD (maximum tolerable downtime), 106
MTO (maximum tolerable outage), 106
priorities, 106–107
qualitative analysis, 105
quantitative analysis, 105
resource prioritization, 110
RTO (recovery time objective), 107
Biba security model, 290–292
biometrics, 595–596
crossover error rate, 598
face scans, 596
false acceptance rate, 598
false rejection rate, 598
fingerprints, 596
hand geometry, 597
heart/pulse patterns, 597
iris scans, 596–597
keystroke patterns, 598
palm scans, 597
registration, 599
retina scans, 596
signature dynamics, 597
voice pattern recognition, 597
BIOS (basic input/output system), 341–342
birthday attacks, 267–268
bit sizes, 201
black box penetration testing, 681
block ciphers, 213
Blowfish, 177, 220, 223
Bluetooth, 506–507
Boehm, Barry, 883
bombings/explosions, 808
Boolean mathematics, logical operations
AND, 202–203
NOT, 204
OR, 203
XOR (exclusive OR), 204
botnets, 565
bots, 565
bottom-up approach to security, 16
bounds, 279–280
branch coverage analysis, 687
breaches, 66
Brewer and Nash security model, 293
BRI (Basic Rate Interface), 557
bridge routers, 448
broadband cabling, 497–498
broadcast domains, 492
brute force attacks, 265–266
buffer overflows, 933–934
bus topology, 501–502
business attacks, 858
business/mission owners, 180–181
BYOD (bring your own device)
acceptable use policy, 375
antivirus management, 374
architecture/infrastructure and, 375
camera, 375
corporate policies, 374
data ownership and, 373
forensics, 374
legal issues, 375
off-boarding, 374
on-boarding, 374
patch management, 373
privacy, 374
support ownership and, 373
user acceptance, 374
video, 375

C

cable plant management policy
backbone distribution system, 407
entrance facility, 407
equipment room, 407
horizontal distribution system, 407
telecommunications room, 407
cabling
5-4-3 rule, 500
baseband, 497–498
broadband, 497–498
coaxial cable, 496–497

collectors, 499–500
plenum, 499
twisted-pair, 498–499
Caesar cipher, 196–197
CALEA (Communications Assistance for Law Enforcement Act), 142
capabilities, 282
capability tables, 625
capacitance motion detectors, 427
captive portals, 481
CAs (certificate authorities), 250–251
CPS (Certificate Practice Statement), 252
CPV (certificate path validation), 251
CRLs (Certificate Revocation Lists), 253
enrollment, 251
OCSP (Online Certificate Status Protocol), 253
RAs (registration authorities), 250–251
revocation, 252–253
CRLs, 253
OCSP, 253
verification, 252
CRLs, 251
OCSP, 251
CBC (Cipher Block Chaining) mode, 221
CBK (Common Body of Knowledge), 2
CCCA (Comprehensive Crime Control Act), 130
CCE (Common Configuration Enumeration), 668
CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), 478
CCTV (closed-circuit television), 403, 411
CDDI (Copper DDI), 445
CDN (content distribution network), 472
cell phones, 504
ITU-R, 506
mobile service technologies, 505
updates disabled, 740–741
central station alarm systems, 428
centralized access control, 602
certification, 306–307
CNSS (Committee on National Security Systems), 308
DIACAP (DoD Information Assurance Certification and Accreditation Process), 308
DITSCAP (Defense Information Technology Security Certification and Accreditation Process), 308
NIACAP (National Information Assurance Certification and Accreditation Process), 308
RMF (Risk Management Framework), 308
CFAA (Computer Fraud and Abuse Act), 130–131
CFB (Cipher Feedback) mode, 221
challenge-response authentication protocol, 200
change logs, 774–775
change management, 719–721
change approval/rejection, 721–722
change documentation, 722
change implementation, 722
change request, 721
change review, 721
change scheduling, 722
change testing, 722
configuration documentation, 723
goal, 18
reviews, 788
security impact analysis, 721–722
versioning, 722–723
CHAP (Challenge Handshake Authentication Protocol), 524
Chauvaud, Pascal, 245
Chinese Wall security model, 293
chosen ciphertext attacks, 267
chosen plaintext attacks, 267
CIA Triad, 2–3, 42
access controls and, 581–582
availability, 6–7
integrity, 4–5
priority, 7–8
CIDR (Classless Inter-Domain Routing), 460
ciphers, 207–208
block ciphers, 213
*versus* codes, 208
one-time pads, 211–212
running key ciphers, 212–213
stream ciphers, 213
substitution, 209–211
transpositions, 208
ciphertext, 201
ciphertext only attacks, 266–267
circuit encryption
derend-to-end encryption, 262
link encryption, 262
circuit switching, 554
*versus* packet switching, 555
circuit-level gateway firewalls, 489
CISO (chief information security officer), 16
civil investigations, 847
civil law, 128
Clark-Wilson security model, 292
access control triple, 292
CDI (constrained data item), 292
IVP (integrity verification procedure), 293
restricted interface model, 293
TPs (transformation procedures), 293
UDI (unconstrained data item), 292
clearing data, 173
client-based vulnerabilities
applets, 342–344
local caches
ARP cache poisoning, 344
caching DNS server, 345
DNS cache poisoning, 344–345
FQDN, 345
HOSTS file, 345
primary authoritative DNS server, 345
split-DNS systems, 346
temporary Internet files, 346
client-server model, 350–351
cloud computing
CASB, 356
cloud services, 355
cloud shared responsibility model, 357
cloud solution, 354–355
cloud storage, 353
elasticity, 354
hosted solution, 354
hypervisor, 353
IaaS, 354
on-premise solution, 354
PaaS, 354
SaaS, 354
SECaaS, 357
snapshots, 356
VMM (virtual machine monitor), 353
distributed architectures, 351
grid computing, 357–358
P2P (peer-to-peer) technologies, 358
closed systems, 277–278
closed-source solutions, 278
cloud, BIA and, 108
cloud computing
CASB (cloud access security broker), 356
cloud services
community cloud, 355
hybrid cloud, 355
private cloud, 355
public cloud, 355
cloud shared responsibility model, 357
cloud solution, 354–355
cloud storage, 353
elasticity, 354
hosted solution, 354
hypervisor
type I hypervisor, 353
type II hypervisor, 353
IaaS (infrastructure as a service), 354
on-premise solution, 354
PaaS (platform as a service), 354
SaaS (software as a service), 354
SECaaS (security as a service), 357
snapshots, 356
VMM (virtual machine monitor), 353
cloud-based assets
community cloud, 714
hybrid cloud, 714
IaaS (infrastructure as a service), 714
PaaS (platform as a service), 713
private cloud, 714
public cloud, 714
SaaS (software as a service), 713
CNSS (Committee on National Security Systems), 308
COBIT (Control Objectives for Information and Related Technologies), 25, 181, 667
code repositories, 893–894
cognitive passwords, 592
collision attack, 267–268
collision domains, 492
collusion, 52, 54–55
combination locks, 426
commercial business/private classification
ownership, 23
private, 22
public, 23
sensitive, 23
Common Criteria, 296
EALs (Evaluation Assurance Levels), 303, 304
guidelines, 302
Introduction and General Model, 303
Security Assurance, 303
Security Functional Requirements, 303
PPs (protection profiles), 303
STs (security targets), 303
communications
protocols
IPsec, 523
Kerberos, 523
Signal Protocol, 523
S-RPC (Secure Remote Procedure Call), 523
SSH (Secure Shell), 523
SSL (Secure Sockets Layer), 523
TLS (Transport Layer Security), 523
review question answers, 968–969
written lab answers, 995
community cloud, 714
companion viruses, 919
compartmentalized environment, MAC model, 635
compensating access control, 583
compensating controls, 80
compiled languages, 873
compliance
policies, 60–61, 149–150
review question answers, 954–956
written lab answers, 990
composition theories of security models

cascading, 286
feedback, 286
hookup, 286

computer architecture, 320–321

attacks
buffer overflow, 386–387
data diddling, 387–388
incremental, 387–388
input checking, 386–387
maintenance hooks and, 387
parameter checking, 386–387
privileged programs, 387
salami attack, 388
state attacks, 389
trusted recovery and, 386

BIOS (basic input/output system),
341–342
communication disconnects, 389
covert channels, 385
design-based attacks, 385–388
electromagnetic radiation, 389–390
firmware, 341
device firmware, 342
hardware, processor, 321–333
process integration, 389
programming flaws, 388
state changes, 389
technology integration, 389
timing flaws, 389

computer crime, 129–130

attacks
APTs, 858
business, 858
corporate espionage, 858
financial, 859
grudge, 859–861
hacktivists, 861
industrial espionage, 858
insider threats, 860
intelligence, 857–858
military, 857–858
script kiddies, 861, 916–917
terrorist, 859
thrill, 861

CFAA (Computer Fraud and Abuse Act),
130–131
crime, 129–130
cryptoanalysis, 687
confidentiality, 3, 42
CIA Triad, 2–3
concealment, 4
countermeasures, 4
criticality, 4
cryptography and, 198–199
discretion, 4
integrity and, 5–6
isolation, 4
privacy, 4
seclusion, 4
secrecy, 4
sensitivity, 4
violations, 3

configuration documentation, 723
configuration management
baselining, 718–719
reviews, 788
confinement, 279
confusion, cryptography and, 213
constrained interface, authorization and,
625–626
content-dependent control, authorization
and, 626
context-dependent control, authorization
and, 626
contracting, 150–151
control zone, TEMPEST countermeasure,
412
controls, 280
corruption, 129–130
corruption, 129–130
corruption, 129–130
corruption, 129–130
converged protocols, 470
FCoE (Fibre Channel over Ethernet), 471
iSCSI (Internet Small Computer System
Interface), 471
MPLS (Multiprotocol Label Switching),
471
SDN (software-defined networking), 472
VoIP (Voice over IP), 471
COPPA (Children’s Online Privacy
Protection Act), 144
cordless phones, 508

corporate espionage attacks, 858

corporate property, 403

corrective access control, 583

corrective controls, 80

countermeasures
availability, 7
confidentiality and, 4
integrity and, 5
measurement and, 81
monitoring and, 81
review question answers, 963–964
selecting, 77–78
written lab answers, 993

CPE (Common Platform Enumeration), 668

CPTED (Crime Prevention through Environmental Design), 403

CPU (central processing unit), 320–321

criminal investigations, 847

criminal law, 126–128

critical path analysis, 401

criticality, confidentiality and, 4

CRLs (Certificate Revocation Lists), 253

crossover error rate of biometrics, 598

cross-training, 54

cryptanalysis, 201

cryptographic applications
review question answers, 960–961
written lab answers, 992

cryptographic lifecycle, 228–229

cryptographic mathematics
  Boolean mathematics, logical operations, 202–204
ciphers, 207–208
  block ciphers, 213
  \textit{versus} codes, 208
  one-time pads, 211–212
  running key ciphers, 212–213
  stream ciphers, 213
  substitution, 209–211
  transposition, 208–209
confusion, 213
diffusion, 213
modulo function, 205
nonce, 206

one-way functions, 205–206
split knowledge, 207
work function, 207
zero-knowledge proof, 206–207

cryptographic salt, 266

cryptography. \textit{See also} encryption
  AES (Advanced Encryption Standard), 220
  algorithms, 201
  American Civil War, 197
  asymmetric
  El Gamal, 241
ecc, 242
  key length, 240–241
  Merkle-Hellman Knapsack, 240–241
private keys, 238–239
public keys, 238–239
RSA algorithm, 239–241
asymmetric key algorithms, 216–219

attacks
analytic, 265
birthday, 267–268
brute force, 265–266
chosen ciphertext, 267
chosen plaintext, 267
ciphertext only, 266–267
collision, 267–268
frequency, 266–267
implementation, 265
known plaintext, 267
man in the middle, 267
meet in the middle, 267
replay, 268
reverse hash matching, 267–268
statistical, 265

authentication and, 200
Caesar cipher, 196–197
ciphertext, 201
confidentiality and, 198–199
digital signatures, 199–200, 246–247
  DSS, 248–249
  HMAC, 247–248
DRM (digital rights management)
documents, 261–262
e-books, 261
movies, 260
cryptology, 201
cryptosystems, 201
asymmetric, 199
symmetric, 199
cryptovariables, 201
CSO (chief security officer), 16
CTR (Counter) mode, 221
CVE (Common Vulnerabilities and Exposures), 668
CVSS (Common Vulnerability Scoring System), 668
cyber-physical systems, 376
IoT (Internet of Things), 377

D
DAA (designated approving authority), 307
DAC (Discretionary Access Control), 10
damage potential, 37
DARPA model, 441, 451
data
clearing, 173
declustering, 175
degaussing, 174
destruction, 174–175
erasing, 173
overwriting, 173
purging, 174
sensitive
destroying, 172
marking, 169–170
storage, 171–172
data at rest, 168
cryptography and, 199
data breach notification, 143–144
data centers, physical security, 407–409
data classification, 19–20, 44, 162
cryptology, 201
cryptosystems, 201
asymmetric, 199
symmetric, 199
cryptovariables, 201
CSO (chief security officer), 16
CTR (Counter) mode, 221
CVE (Common Vulnerabilities and Exposures), 668
CVSS (Common Vulnerability Scoring System), 668
cyber-physical systems, 376
IoT (Internet of Things), 377

D
defining, 165
government/military, 22
  confidential, 21
  FOUO, 21
  secret, 21, 162
  sensitive but classified, 21
  top secret, 21, 162
  unclassified, 21, 163
phases, 20
private, 164
proprietary, 164
public, 165
sensitive, 164
data controller, 181
data emanation, 473
data flow paths, 37
data hiding, 13, 43
data in motion, cryptography and, 199
data in transit, 168
data in use, 168
cryptography and, 199
data integrity, 855–856
Data Link layer (OSI)
  ARP (Address Resolution Protocol), 445, 462–447
  ISDN (Integrated Services Digital Network), 445
  L2F (Layer 2 Forwarding), 445
  L2TP (Layer 2 Tunneling Protocol), 445
  MAC addresses, 445–446
  OUI (Organizationally Unique Identifier), 446
  PPP (Point-to-Point Protocol), 445
  PPTP (Point-to-Point Tunneling Protocol), 445
  SLIP (Serial Line Internet Protocol), 445
data owners, 179
data processors, 181–182
  anonymization, 183–184
  pseudonymization, 182–183
data protection
  symmetric encryption, 176–177
  transport encryption, 177–178
data remanance, 172–175, 339
data retention, 855–856
data security controls, 165–167
data states, 168
data storage
  nonvolatile storage, 905
  primary memory, 905
  random access storage, 905
  secondary storage, 905
  sequential access storage, 905
  threats, 905–906
  virtual memory, 905
  virtual storage, 905
  volatile storage, 905
data stream, 443
databases
  cell suppression, 902–903
  contamination, 901
  multilevel, concurrency and, 901–902
  NoSQL, 904
  ODBC (Open Database Connectivity), 903–904
  polyinstantiation, 903
  recovery, 825
    electronic vaulting, 826
    remote journaling, 826
    remote mirroring, 826–827
security
  aggregation, 347–348
  data analytics, big data, 349
  data dictionary, 348
  data mining, 348–349
  data warehouses, 348
  inference, 348
  parallel computing, 350
  semantic integrity, 902
  time and date stamps, 902
  transactions, 899–900
    ACID model, 900
  views, 901
  vulnerability scans, 677–678
DBMS (database management system), 895
distributed databases, 896
  hierarchical databases, 896
  normalization, 899
DDL (Data Definition Language) – DLP (data loss prevention)

OOP and, 897
RDBMS (relative database management systems), 896
relational databases, 897–899
DDL (Data Definition Language), 899
DDoS (distributed denial-of-service) attacks, 564–565
decentralized access control, 602
declassification, 175
decomposing applications, 36–37
deep packet inspection firewalls, 489
defense in depth, 12–13, 352, 627–628
degaussers, 172
delay controls, physical security, 404
Delta rule, 908
denial, physical security, 404
DES (Data Encryption Standard), 177, 215, 220
CBC (Cipher Block Chaining) mode, 221
CFB (Cipher Feedback) mode, 221
CTR (Counter) mode, 221
ECB (Electronic Code Book) mode, 220–221
OFB (output feedback) mode, 221
detector access control, 582–583
detector controls, 80
physical security, 404
deterrent access control, 583
deterrent alarms, 428
deterrent controls, 79
physical security, 404
device authentication, 600–601
device firmware, 342
DHCP (Dynamic Host Configuration Protocol), 462
DIACAP (DoD Information Assurance Certification and Accreditation Process), 308
diagrams, attack potential, 35–36
dial-up encapsulation protocols
PPP (Point-to-Point), 561
SLIP (Serial Line Internet Protocol), 561
dial-up protocols
PPP (Point-to-Point Protocol), 539
SLIP (Serial Line Internet Protocol), 539–540
differential backups, 830
diffusion, cryptography and, 213
digital certificates, 249–250
digital signatures, 199–200, 246–247
DSS (Digital Signature Standard), 248–249
HMAC (hashed message authentication code), 247–248
directive access control, 583
directive controls, 81
DISA (Direct Inward System Access), 528–529
disasters
man-made
bombings/explosions, 808
fires, 807
hardware failures, 810
infrastructure failures, 809
network failures, 809
NYC blackout, 810
power outages, 808–809
software failures, 810
strikes/picketing, 811
terrorist acts, 807–808
theft, 811–812
utility failures, 809
vandalism, 811–812
natural disasters
earthquakes, 803–804
fires, 806
floods, 804–805
regional events, 806–807
storms, 805–806
discoverability, 38
discretion, confidentiality and, 4
distributed access control, 602
distributed architectures, 351
DITSCAP (Defense Information Technology Security Certification and Accreditation Process), 308
diversity of defense, 352
DKIM (DomainKeys Identified Mail), 533
DLP (data loss prevention)
endpoint-based DLP, 782
network-based DLP, 782
DML (Data Manipulation Language), 899
DMZ (demilitarized zone), 362
DNP3 (Distributed Network Protocol), 465
DNS (Domain Name System), 465
  DNS poisoning, 468–470
  DNSSEC (Domain Name System Security Extensions), 468
  FQDNS (fully qualified domain names), 466–467
  HOSTS file, 468
  permanent addresses, 466
  primary authoritative names server, 467
  resource records, 467
  secondary authoritative names server, 467
  temporary addresses, 466
  TLD (top-level domain), 466–467
  zone files, 467
DNS poisoning, 568
DNS spoofing, 568
Dobbertin, Hans, 245
documentation review, 63
documenting, investigations, 856
DOD model, 451
domain hijacking, 470
DoS (denial-of-service) attacks, 32–33, 564–565
DREAD threat modeling, 33, 37–38
DRM (digital rights management),
  cryptography
  documents, 261–262
  e-books, 261
  movies, 260
  music, 259–260
  video games, 261
DRP (disaster recovery planning), 802
  alternate processing sites, 820–821
    cloud computing, 824
    cold sites, 821–822
    hot sites, 822–823
    mobile sites, 823–824
    service bureaus, 824
    warm sites, 823
  assessment, 829
  backups, 829
    best practices, 832
differential backups, 830
  disk-to-disk, 832
  full backups, 830
  incremental backups, 830
  tapes, 831–833
  using, 830
versus BCP, 98–99
BIA (business impact assessment), 819
checklists and, 828–829
communication and, 828
communications, external, 833–834
crisis management, 819–820
database recovery, 825–827
delayed communications, 820
emergency response, 828
fault tolerance and, 812
hard drive protection, 813–814
logistics, 834
MAAs (mutual assistance agreements), 825
maintenance, 837–838
MTO (maximum tolerable outage), 819
MTTR (mean time to recovery), 819
personnel and, 828
power source protection, 815–816
priorities, 818–819
QoS (quality of service)
  bandwidth and, 817
  interference and, 817
  jitter and, 817
  latency and, 817
  packets and, 817
reciprocal agreements, 825
recovery versus restoration, 834–835
review question answers, 980–981
server protection, 814–815
single point of failure and, 812
software escrow arrangement, 833
supplies, 834
system resilience and, 812
testing
  full-interruption test, 837
  parallel test, 837
  read-through test, 836
  simulation test, 837
  structured walk-through, 837
training and, 835–836
dynamic systems development, 816
firewalls, 816
failure-open systems, 816
manual, 817
utilities, 834
workgroups, 820
written lab answers, 999

DSDM (Dynamic Systems Development Model), 885
DSS (Digital Signature Standard), 248–249
DSSS (Direct Sequence Spread Spectrum), 504
due care, 26, 698
due diligence, 26, 698
duress systems, 708
dynamic NAT, 552

e
EAC (electronic access control) lock, 426
EAP (Extensible Authentication Protocol), 478, 524
earthquakes, 803–804
eavesdropping, 565–566
EBCDICM (Extended Binary-Coded Decimal Interchange Mode), 450
ECB (Electronic Code Book) mode, 220–221
ECC (elliptic curve cryptography), 242
Economic Espionage Act, 142
ECPA (Electronic Communications Privacy Act), 142
EDI (Electronic Data Interchange), 451
EF (exposure factor), 70, 110
egress monitoring
DLP, 782–783
steganography, 783
watermarking, 783
El Gamal, T., 241
electronic discovery, investigations and, 848–849
electronic vaulting database recovery and, 826
elevation of privilege threats, 33
EM (electromagnetic) radiation, 389–390
email attachments, 534
blacklist services, 535
cryptography
PGP, 255–256
S/MIME, 256
DKIM (DomainKeys Identified Mail), 533
IMAP (Internet Message Access Protocol), 530
MOSS (MIME Object Security Services), 533
Opportunistic TLS for SMTP Gateways, 534
PEM (Privacy Enhanced Mail), 533
PGP (Pretty Good Privacy), 533, 534
POP3 (Post Office Protocol version 3), 530
repudiation filtering, 535
security goals, 531–532
security issues, 532–533
sendmail, 531
S/MIME (Secure Multipurpose Internet Mail Extensions), 533
SMTP (Simple Mail Transfer Protocol), 530–531
SPF (Sender Policy Framework), 534
emanation security, 411–412
embedded systems, 375–376
application firewalls, 378
cyber-physical systems, 376–377
diversity control, 379
firmware version control, 379
manual updates, 378
monitoring, 379
network segmentation, 378
redundancy control, 379
security layers, 378
wrappers, 379
emergency management, personnel and, 709–710
EMI (electromagnetic interference), 416
coaxial cabling and, 497
employment agreements, 55–57
encrypted viruses, 923
encryption, 14, 43. See also cryptography
3DES (Triple DES), 177, 220
AES (Advanced Encryption Standard), 177, 220
Blowfish, 177, 220
ciphertext, 201
circuit encryption
end-to-end encryption, 262
link encryption, 262
DES (Data Encryption Standard), 177, 220
FDE (full disk encryption), 254
IDEA (International Data Encryption Algorithm), 220
PKI (public-key infrastructure), 249
plain text and, 201
Skipjack, 220
SSH (Secure Shell), 262
symmetric, 176–177
transport, 177–178
endpoint security, 491–492
endpoint-based DLP, 782
end-to-end encryption, 262
entitlement, 700
entrance facility, 407
environmental security, 400
equipment failure, 404–405
equipment room, 407
erasing data, 173
escalation of privilege attacks, 935
ESSID (extended service set identifier), 475
ethics, 861
IAB (Internet Advisory Board), 862–863
(ISC)² Code of Ethics, 862
review question answers, 981–983
written lab answers, 999–1000
EU Directive 95/46/EC (Data Protection Directive), 62
evidence, 849
admissible, 849
chain of evidence, 850
collection, 851–852
documentary, 849–850
forensic procedures, 851–852
gathering, 853–854
hearsay, 851
real, 849
storage, 413
testimonial, 851
evil twin wireless attack, 485
expert systems, 907
exploitability, 38
exposure, 65
external audits, 666
extranets, 486

F

face scans, 596
facility design, 402. See also physical security
access abuses, 410–411
CPTED (Crime Prevention through Environmental Design), 403
emanation security, 411–412
EMI (electromagnetic interference), 416
equipment failure and, 404–405
evidence storage, 413
fire
damage, 421–422
detection, 419
detection systems, 420
extinguishers, 419
prevention, 417–419
stages, 418–419
suppression, 417–421
humidity, 416–417
HVAC issues, 416–417
IDSs (intrusion detection systems), 410
media storage, 412–413
natural disasters and, 402
noise, 416
restricted areas, 413–414
review question answers, 961–962
RFI (radio-frequency interference), 416
SCIF (Sensitive Compartmented Information Facility), 414
security, 400, 401
site selection, 401–402
smartcards, 409
static, 416–417
temperature, 416–417
utilities
   power issues, 415
   UPS, 414–415
visibility, 402
water issues, 417
wiring closets, 405–407
work areas, 413–414
false acceptance rate of biometrics, 598
false rejection rate of biometrics, 598
Faraday cage, 411
   EM (electromagnetic) radiation, 390
fault tolerance, 310
   leased lines, 557
fax security, 535–536
FCoE (Fibre Channel over Ethernet), 471
FDDI (Fiber Distributed Data Interface), 445
FDE (full disk encryption), 254
FDIM (federated identity management), 605–606
GML (Generalized Markup Language), 606
HTML (Hypertext Markup Language), 606
OAuth, 606–607
OpenID, 607
OpenID Connect, 607
SAML (Security Assertion Markup Language), 606
SGML (Standard Generalized Markup Language), 606
SPML (Service Provisioning Markup Language), 606
Twitter, 607
XML (Extensible Markup Language), 606
Federal Sentencing Guidelines, 131–132
feedback loop, waterfall model, 882
fences, 422–423
FERPA (Family Educational Rights and Privacy Act), 62, 145
FHSS (Frequency Hopping Speed Spectrum), 504
file infector viruses, 919
financial attacks, 859
fingerprints, 596
FIPS (Federal Information Processing Standard), 201
fire, 806, 807
damage, 421–422
detection, 419
detection systems
   fixed-temperature detection, 420
   flame-actuated, 420
   rate-of-rise detection, 420
   smoke-actuated, 420
   extinguisher classes, 419
   prevention, 417–419
   stages, 418–419
   suppression, 417–421
firewall logs, 774
firewalls, 487–488
   application-level gateway, 489
   circuit-level gateway, 489
   deep packet inspection, 489
   deployment architecture, 490–491
   DMZ (demilitarized zone), 490
   multihomed, 490
   Next-Gen, 489
   screening routers, 489
   stateful inspection, 489
   static packet-filtering, 488–489
firmware, 341
device firmware, 342
FISMA (Federal Information Security Management Act), 132–133
FISMA (Federal Information Security Modernization Act), 133–134
flash drives, 715
floods, 804–805
FOIA (Freedom of Information Act), 163
forensic procedures
   hardware/embedded device analysis, 852
   network analysis, 852
   software analysis, 852
fortress mentality, 352
FOUO (for official use only), 163
FTP (File Transfer Protocol), 451, 462
full backups, 830
function coverage analysis, 687
fuzz testing, 31
  bit flipping, 684
generational (intelligent) fuzzing, 684
mutation (dumb) fuzzing, 684
prefuzzing input file, 685
zzuf tool, 685

G
Gantt charts, 887–888
gates, 423
GDPR (General Data Protection Regulation),
  129, 146–148, 178
data processors, 181
pseudonymization, 182–183
GLBA (Gramm-Leach-Bliley Act), 144
Goguen-Meseguer security model, 294
  governance
    review question answers, 950–951
written lab answers, 988
government/military classification, 22
  confidential, 21
  FOOU, 21
  secret, 21
  sensitive but classified, 21
  unclassified, 21
Graham-Denning Model, 294
Gramm-Leach-Bliley Act, 62
gray box penetration testing, 681
grid computing, 357–358
grudge attacks, 859–861
guidelines, 28

H
hacking, threat modeling and, 31
hand geometry scans, 597
hard drive, clearing, 174
hardware
  failures, 810
  input/output devices, 340–341
  inventories, 710–711
  memory, 333–338
  processor, 321–332
  storage, 338–340
hash functions, 242–246
hashing algorithms, 219
HDCP (High-Bandwidth Digital Content
  Protection), 260
HDLC (High-Level Data Link Control), 561
heartbeat sensor, 410
heart/pulse patterns, 597
heat-based motion detectors, 427
hierarchical environment, MAC model,
  635
hijacking, 568
HIPAA (Health Insurance Portability and
  Accountability Act), 62, 142–143, 161
hiring
  background checks, 55
  candidate screening, 55
  employment agreements, 55–57
  job descriptions, 51–52
  position descriptions, 51–52
HITECH (Health Information Technology
  for Economic and Clinical Health)
  Act, 143
HMAC (Hash-based Message
  Authentication Code), 594
HMAC (hashed message authentication
code), 247–248
horizontal distribution system, 407
HOTP (HMAC-based One-Time
  Password), 594
HSM (hardware security module), 310
HSMs (hardware security modules), 254
HTTP (Hypertext Transfer Protocol), 451
HTTP (Hypertext Transport Protocol), 462
HTTPS (Hypertext Transfer Protocol
  Secure), 177, 257
HVAC (heating, ventilation, and air
  conditioning), 403, 416–417
hybrid cloud, 714
hybrid environment, MAC model, 635
hyperlink spoofing, 568–569
Hz (Hertz), 503
IaaS (infrastructure as a service), 714
IAB (Internet Advisory Board), 862–863
IAM (identity and access management) system, 57, 580
IANA (International Assigned Numbers Authority), 454
IC (integrated circuit) cards, 409
ICMP (Internet Control Message Protocol), 447, 460–461
ICS (industrial control system), 359
DCSs (distributed control systems), 359
PLCs (programmable logic controllers), 359
SCADA (supervisory control and data acquisition), 359
IDEA (International Data Encryption Algorithm), 220, 223
IDEAL model, 886
identification, 42, 584–585
AAA services, 8
registration and, 585–586
subject, 9
identity and access provisioning lifecycle, 611
accounts
review, 612–613
revocation, 613–614
creeping privileges, 613
excessive privilege, 612–613
privilege creep, 613
provisioning, 611–612
identity management
AAA protocols, 609
centralized access control, 602
FDIM (federated identity management), 605–607
Kerberos, 603–605
LDAP and, 602–603
PKIs, LDAP and, 603
scripted access, 607
SSO (single-sign on), 602
credential management systems, 607–608
decentralized access control, 602
diameter, 610–611
distributed access control, 602
integrating services, 608
RADIUS (Remote Authentication Dial-in Service), 609–610
review question answers, 969–971
session management, 608–609
TACACS+, 610
written lab answers, 996
Identity Theft and Assumption Deterrence Act, 145
identity tokens, 409
IDF (intermediate distribution facilities), 405
IDSs (intrusion detection systems), 410
IEEE, 802.11 standards, 473
IETF (Internet Engineering Task Force), 177, 263
IGMP (Internet Group Management Protocol), 447, 460, 461
IM (instant messaging), 530
IMAP (Internet Message Access Protocol), 451, 462, 530
impact assessment, 110–111
impersonation attacks, 566–567
implementation attacks, 265
implicit deny, 625
incident response, 738–739
auditing, 783
access review audits, 785
auditors, 784
change management, 788
configuration management, 788
inspection audits, 784–785
patch management, 787
privileged groups, 786–787
reporting, 788–790
user entitlement audits, 786
vulnerability management, 788
cellphone updates, 740–741
computer security incidents, 738
delegation to users, 745
detection
audit log scans, 740
intrusion detection, 740
malware detection, 740
user reports, 740
IDPSs (intrusion detection and prevention systems), 756
IDSSs (intrusion detection systems), 756
anomaly analysis, 758
behavior-based detection, 757–758
host-based, 760–762
knowledge-based detection, 757
network-based, 760–762
response, 759
IPSSs (intrusion prevention systems), 756, 762–763
lessons learned, 744
logging
application logs, 774
change logs, 774–775
data protection, 775–776
Event Viewer, 773–774
firewall logs, 774
proxy logs, 774
security logs, 774
system logs, 774
mitigation, 742
monitoring
accountability and, 777
audit trails, 776
clipping levels, 780
data extraction, 780
egress monitoring, 781–783
investigations and, 778
keystroke monitoring, 781
log analysis, 779
problem identification and, 778
sampling, 780
SEIM, 779–780
traffic analysis, 781
trend analysis, 781
preventive measures, 745–746
anti-malware software, 746, 765–766
applications, 746
attacks, 747–756
blacklisting, 766–767
configuration management, 746
firewalls, 746, 767–768
honeypots/honeynets, 763–764
intrusion detection and prevention, 746
penetration testing, 768–772
protocols, 746
sandboxing, 768
services, 746
system management, 746
systems, 746
third-party security services, 768
warning banners, 764–765
whitelisting, 766–767
recovery, 743
remediation, 744
reporting, 742–743
response, 741–742
review question answers, 977–980
security incidents, 738
SIEM (security information and event management) system, 758–759
written lab answers, 998
incidents
computer security incidents, 738
definition, 738–739
security incidents, 738
incremental backups, 830
industrial espionage attacks, 858
information disclosure threats, 32
information flow security model, 285
information lifecycle management, 706–707
informative policies, 27
InfoSec (information security), 16
infrared motion detectors, 427
infrastructure failures, 809
input points, 37
input/output devices
keyboards, 341
mice, 341
modems, 341
monitors, 340
printers, 340–341
insider threats, 860
inspection audits, 784–785
integrity, 4–5, 42
accountability and, 6
accuracy and, 5
authenticity and, 5
CIA Triad, 2–3
completeness and, 6
comprehensiveness and, 6
confidentiality and, 5–6
cryptography and, 199–200
nonrepudiation and, 6
responsibility and, 6
truthfulness and, 5
validity and, 6
verification, 562
intelligence attacks, 857–858
interface testing, 686
internal audits, 665–666
internal security controls, 425
  badges, 427
  combination locks, 426
  EAC (electronic access control) lock, 426
  intrusion alarms, 428
  keys, 426
  motion detectors, 427
  secondary verification, 428–429
interpreted languages, 873
intranets, 486
intrusion alarms, 428
investigations
  administrative, 846–847
  civil, 847
  conducting, 855
  criminal, 847
data integrity, 855–856
data retention, 855–856
documenting, 856
electronic discovery, 848–849
evidence, 849
  admissible, 849
  chain of evidence, 850
  collection, 851–852
  documentary, 849–850
  forensic procedures, 851–852
  gathering, 853–854
  hearsay, 851
  real, 849
  testimonial, 851
interviews, 855
law enforcement request, 854–855
regulatory, 848
reporting, 856
review question answers, 981–983
search warrant, 853
subpoena, 853
written lab answers, 999–1000
IoT (Internet of Things), 358–359
cyber-physical systems, 377
IP (Internet Protocol), 447, 458
  ARP (Address Resolution Protocol),
    461–462
  CIDR (Classless Inter-Domain Routing),
    460
classes, 459–460
ICMP (Internet Control Message Protocol),
  460–461
IGMP (Internet Group Management Protocol),
  460
loopback address, 460
IP addressing
  APIPA (Automatic Private IP Addressing),
    552–553
loopback address, 553
IP probes, 940
IP spoofing, 942
IPsec (Internet Protocol Security), 178, 263,
  447, 523
  AH (Authentication Header), 544
  ESP (Encapsulating Security Payload),
    544
IPX (Internetwork Packet Exchange), 447
iris scans, 596–597
ISACA (Information Systems Audit and
  Control Association), 25
ISAKMP (Internet Security Association and
  Key Management Protocol), 262, 264
ISC² (International Information Systems
  Security Certification Consortium), 98
Code of Ethics, 862
iSCSI (Internet Small Computer System
  Interface), 471
ISDN (Integrated Services Digital Network),
  445
  BRI (Basic Rate Interface), 557
  PRI (Primary Rate Interface), 557
ISO (information security officer), 16
ISO (International Organization for Standardization), 305–306, 440
ISO/IEC 27002, 25
isolation, 280
confidentiality and, 4
issue-specific security policies, 27
ITIL (Information Technology Infrastructure Library), 25
ITRC (Identify Theft Resource Center), 168
ITSEC (Information Technology Security Evaluation and Criteria), 28, 296
Common Criteria comparison, 305
TCSEC comparison, 301–302, 305
TOE (target of evaluation), 301
IV (initialization vector) wireless attacks, 484

J

jailbreaking, 767
job responsibilities, 53
job rotation, 53–54
JPEG (Joint Photographic Experts Group), 450

K

Kaspersky Lab, 920–921
Kerberos, 523
AES (Advanced Encryption Standard) and, 603
authentication service, 603
database, 604
KDC (key distribution center), 603
ST (service ticket), 604
TGT (Ticket-Granting Ticket), 604
tickets, 604
Kerckhoffs’s principle of cryptography, 201
kernels, 284
key escrow, 207
key spaces, algorithms, 201
keyboards, 341
keys, 426
keystroke patterns, 598
knowledge-based systems, 906–909
known plaintext attacks, 267
Koblitz, Neal, 242
KRACK (Key Reinstallation AttaCKs), 478

L

L2F (Layer 2 Forwarding), 445
L2TP (Layer 2 Tunneling Protocol), 445, 544
labeling sensitive data and assets, 169–170
labels, security labels, 282
LANs (local area networks), 496
CSMA (Carrier-Sense Multiple Access), 512
CSMA/CA (Carrier-Sense Multiple Access with Collision Avoidance), 512
CSMA/CD (Carrier-Sense Multiple Access with Collision Detection), 512
Ethernet, 509
FDDI (Fiber Distributed Data Interface), 510
polling, 513
subtechnologies
analog communications, 510
asynchronous communications, 511
baseband, 511
broadband, 511
broadcast, 511
digital communications, 510
multicast, 511
synchronous communications, 511
unicast, 511
token passing, 513
token ring, 509
lattice-based access controls, 289
classification levels, 289
laws
administrative law, 128–129
civil law, 128
computer crime, 129–131
criminal, 126–128
Economic Espionage Act of 1996, 139
Federal Sentencing Guidelines, 131–132
FISMA (Federal Information Security Management Act), 132–133
GDPR (General Data Protection Regulation), 129
import/export, 140–141
intellectual property, 134–136
licensing, 139–140
National Information Infrastructure Protection Act, 132
patents, 137–138
privacy, 141–148
review question answers, 954–956
trade secrets, 138
trademarks, 136–137
written lab answers, 990
layering, 12–13, 43
multilayered solutions, 12–13
LEAP (Lightweight Extensible Authentication Protocol), 478–479, 524
learning rule, 908
least privilege, 53, 626, 698, 699
legally defensible security, 12
Lenstra, Arjen, 245
lighting, perimeter security and, 424
link encryption, 262
local alarm systems, 428
log reviews, 688
logging
application logs, 774
change logs, 774–775
data protection, 775–776
Event Viewer, 773–774
firewall logs, 774
proxy logs, 774
security logs, 774
system logs, 774
logic bombs, 923–924
logical access control, 584
logical operations (Boolean)
AND, 202–203
NOT, 204
OR, 203
XOR (exclusive OR), 204
logical/technical controls, 78–79
logon notification, 653
loop coverage analysis, 687
loopback address, 460, 553
loss
availability, 582
confidentiality, 581
integrity, 582
LPD (Line Print Daemon), 451, 463

M
MAC (Mandatory Access Control), 10
compartmentalized environment, 635
hierarchical environment, 635
hybrid environment, 635
MAC addresses, 445–446
MAC filter, 479
machine language, 873
machine learning techniques, 908
macro viruses, 919–920
masquerading attacks, 941–942
IP spoofing, 942
session hijacking, 942
password attacks
countermeasures, 932–933
dictionary attacks, 930–931
guessing, 929–930
social engineering, 931–932
reconnaissance attacks
IP probes, 940
port scans, 940–941
vulnerability scans, 941
review question answers, 984–986
sources, 916–917
spyware, 928
Trojan horses, 924–925
viruses, 917–918
anti-virus, 920–922
companion viruses, 919
encrypted, 923
file infector viruses, 919
hoaxes, 923
macro viruses, 919–920
multipartite, 922
polymorphic, 923
service injection viruses, 920
stealth, 922–923
vulnerable platforms, 920
web applications
dynamic Web applications, 937–938
SQL injection, 937, 938–940
XSRF/CSRF, 936–937
XSS attacks, 935–936
worms, 925
Code Red, 926–927
RTM, 926–927
Stuxnet, 927–928
written lab answers, 1000
zero-day vulnerabilities, 928
Zeus Trojan horse, 917
man in the middle attacks, 267
man-made disasters
bombings/explosions, 808
fires, 807
hardware failures, 810
infrastructure failures, 809
network failures, 809
NYC blackout, 810
power outages, 808–809
software failures, 810
strikes/picketing, 811
terrorist acts, 807–808
theft, 811–812
utility failures, 809
vandalism, 811–812
mantraps, 423–424
masked data, 184
masquerading attacks, 410, 566–567, 941
IP spoofing, 942
session hijacking, 942
MBR viruses, 918–919
MD2 (Message Digest 2), 244–245
MD4 (Message Digest 4), 245
MD5 (Message Digest 5), 245–246
media, zeroization, 412
media management, 714–715
flash drives, 715
lifecycle, 717
mobile devices, 716–717
tape media, 716
media storage, 412–413
meet in the middle attacks, 267
Meltdown, 309
memory
memory addressing
base-offset addressing, 336
direct addressing, 336
immediate addressing, 336
indirect addressing, 336
register addressing, 336
primary, 905
RAM (random access memory), 334–335
registers, 336
ROM (read-only)
EEPROM, 334
EPROM, 334
flash, 334
PROM, 333–334
secondary addressing, 337
security issues, 337–338
virtual, 905
memory cards, 409
memory protection, 309
constrained interface, 310
fault tolerance, 310
HSM (hardware security module), 310
Meltdown, 309
restricted interface, 310
Spectre, 309
TPM (Trusted Platform Module), 310
virtualization, 310
Merkle-Hellman Knapsack algorithm, 240
mesh topology, 503
metacharacters, 362
Metasploit, 679–680
mice, 341
Microsoft Hyper-V, 310
MIDI (Musical Instrument Digital Interface), 450
military attacks, 857–858
mobile devices, 365, 508–509
    Android, 366
    application security, 371–372
    BYOD (bring your own device), 372–373, 716–717
    acceptable use policy, 375
    antivirus management, 374
    architecture/infrastructure and, 375
    camera, 375
    corporate policies, 374
    data ownership and, 373
    forensics, 374
    legal issues, 375
    off-boarding, 374
    on-boarding, 374
    patch management, 373
    privacy, 374
    support ownership and, 373
    user acceptance, 374
    video, 375
    COPE (company-owned personally
        enabled), 372
    corporate-owned mobile strategy, 372
    CYOD (choose your own device), 372, 716–717
    device security
        access control, 369–370
        application control, 368
        asset tracking, 369
        disabling features, 370
        full device encryption, 367
        GPS, 368
        inventory control, 369
        lockout, 367
        MDM (mobile device management), 369
        remote wiping, 367
        removable storage, 370
        screen locks, 367–368
        storage segmentation, 369
    iOS, 366
    PEDs (portable electronic devices), 366–367
    VDI (virtual desktop infrastructure), 372
    VMI (virtual mobile infrastructure), 373
    modems, 341
    modification attacks, 567
    modulo function, 205
    monitoring, 11
        accountability and, 777
        audit trails, 776
        clipping levels, 780
        data extraction, 780
        egress monitoring, 781–782
        DLP, 782–783
        steganography, 783
        watermarking, 783
        investigations and, 778
        keystroke monitoring, 781
        log analysis, 779
        problem identification and, 778
        sampling, 780
        SEIM (Security Information and Event
            Management), 779
        SIM (Security Information Management), 779
        traffic analysis, 781
        trend analysis, 781
    monitors, 340
    monolithic security stance, 352
    MOSS (MIME Object Security Services), 533
    motion detectors, 427
    MPEG (Moving Picture Experts Group), 450
    MPLS (Multiprotocol Label Switching), 471
    MTBF (mean time between failures), 105
    equipment, 405
    MTD (maximum tolerable downtime), 106
    MTO (maximum tolerable outage), 106
    MTTF (mean time to failure), equipment, 405
    MTTR (mean time to repair), equipment, 405
    multifactor authentication, 599–600,
        652–653
    multihomed, 490
    multilayered defense, 352
    multilayered protocols, 463–465
    multilayered solutions, 12–13
    multimedia collaboration, 529–530
    multipartite viruses, 922
NAC (network access control), 487
NAT (Network Address Translation), 447, 549–550
APIPA (Automatic Private IP Addressing), 552–553
dynamic, 552
IP addresses, private, 550–551
PAT (port address translation), 551–552
stateful, 551–552
static, 552
National Information Infrastructure Protection Act, 132
natural disasters
earthquakes, 803–804
fires, 806
floods, 804–805
regional events, 806–807
site design and, 402
storms, 805–806
NCA (noncompete agreement), 56
NCSC (National Computer Security Center), 296
NDAs (nondisclosure agreements), 56
need to know, 626, 698, 699
NetFlow logs, 688
network discovery scans
nmap, 670–673
TCP ACK scanning, 669
TCP connect scanning, 669
TCP SYN scanning, 669
Xmas scanning, 669
network failures, 809
Network layer (OSI)
BGP (Border Gateway Protocol), 447
bridge routers, 448
ICMP (Internet Control Message Protocol), 447
IGMP (Internet Group Management Protocol), 447
IP (Internet Protocol), 447
IPSec (Internet Protocol Security), 447
IPX (Internetwork Packet Exchange), 447
NAT (Network Address Translation), 447
non-IP protocols, 447–448
OSPF (Open Shortest Path First), 447
RIP (Routing Information Protocol), 447
routers, 448
SKIP (Simple Key Management for Internet Protocols), 447
network vulnerability scan
authenticated scans, 674
false negative reports, 673
false positive reports, 673
Nessus, 675
TCP ports, 675
network-based DLP, 782
networking, cryptography
circuit encryption, 262
IPsec, 263–264
ISAKMP, 264
wireless networking, 264–265
networks
amplifiers, 493
bridges, 493
broadcast domains, 492
brouters, 494
cabling
baseband, 497–498
broadband, 497–498
coaxial cable, 496–497
conductors, 499–500
twisted-pair, 498–499
collision domains, 492
communication, 486
concentrators, 493
circuit-level gateway, 489
deployment architecture, 490–491
multihomed, 490
Next-Gen, 489
screening routers, 489
stateful inspection, 489
static packet-filtering, 488–489
gateways, 494
hubs, 493
LANs (local area networks)
  Ethernet, 509
  Extenders, 495
  FDDI, 510
  subtechnologies, 510–513
  token ring, 509
  modems, 493
  NAC (network access control), 487
  performance boosts, 486
  proxies, 494–495
  repeaters, 493
  routers, 494
  security, 486
  segments, 486
  switches, 493–494
  topologies
    bus, 501–502
    mesh, 503
    ring, 500–501
    star, 502
  transmission media, 496–500
  wireless communications
    Bluetooth, 506–507
    cell phones, 504
      ITU-R, 506
      mobile service technologies, 505
    cordless phones, 508
    DSSS (Direct Sequence Spread Spectrum), 504
    FHSS (Frequency Hopping Speed Spectrum), 504
    Hz (Hertz), 503
    mobile devices, 508–509
    NFC (near-field communication), 507
    OFDM (Orthogonal Frequency-Division Multiplexing), 504
    PANs (personal area networks), 506–507
    RFID (radio-frequency identification), 507
    neural networks, 908
  Next-Gen firewalls, 489
  NFC (near-field communication), 507
  NFS (Network File System), 449, 463

NIACAP (National Information Assurance Certification and Accreditation Process), 308
NIST (National Institute of Standards and Technology), 28
  assessments, 664
  FISMA and, 132–133
  NNTP (Network News Transport Protocol), 451
  nonces, 206
  noninterference security model, 285–286
  nonrepudiation, 43
cryptography and, 200
  nonvolatile storage, 905
  NoSQL, 904
  NOT operation, 204
  notification alarms, 428
  NYC blackout, 810

O
objects, 277
OCSP (Online Certificate Status Protocol), 253
ODBC (Open Database Connectivity), 903–904
OFB (output feedback) mode, 221
OFDM (Orthogonal Frequency-Division Multiplexing), 504
offboarding employees, 57
onboarding employees, 57
one-time pad substitution cipher, 211–212
one-way functions, 205–206
OOP (object-oriented programming), 874–875, 897
open systems, 277–278
open-source solutions, 278
operational plans, 16, 17
Opportunistic TLS for SMTP Gateways, 534
OR operation, 203
Oracle VirtualBox, 310
Orange Book, 296
organizational processes, 17–18
  change management, 18–19
data classification, 19–23
  commercial business/private, 22–23
declassification, 20
government/military, 21–22
  phases, 20
organizational security policies, 27
OSA (open system authentication), 476
OSI (Open Systems Interconnection)
  Model, 440
  Application layer, 443, 450
data stream, 443
  protocols, 451
  layers, 441–442
  Network layer
    bridge routers, 448
    non-IP protocols, 447–448
  physical layer, 444–445
  bits, 443
  Presentation layer, format standards, 450
  Session layer, protocols, 449
  TCP/IP model and, 441, 452
  Transport layer
    datagrams, 443
    protocols, 449
    segments, 443
OSPF (Open Shortest Path First), 447
OSSTMM (Open Source Security Testing Methodology Manual), 25
OUI (Organizationally Unique Identifier), 446

output devices
  keyboards, 341
  mice, 341
  modems, 341
  monitors, 340
  printers, 340–341
OVAL (Open Vulnerability and Assessment Language), 668
overwriting data, 173
ownership of data, 178
  administrators, 184
  asset owners, 179–180
  business/mission owners, 180–181
  custodians, 184–185
  data owners, 179
  data processors, 181–184
  protecting privacy, 185–186
  users, 185

P

PaaS (platform as a service), 713
packet switching, 554–555
palm scans, 597
PANs (personal area networks), 506–507
PAP (Password Authentication Protocol), 524
parallel configurations, 13
Parallels Desktop for Mac, 310
passive audio motion detectors, 427
passive website monitoring, 687
password attacks
  common passwords, 929–930
  countermeasures, 932–933
dictionary attacks, 930–931
guessing, 929–930
rainbow tables, 931
social engineering
  dumpster diving, 932
  phishing, 931–932
password hashing, 652
password masking, 652
password policies, 652
password salting, 652
PASTA (Process for Attack Simulation and Threat Analysis), 33
PAT (port address translation), 551–552
patch management
  embedded systems, 723–724
  program steps, 724–725
  reviews, 787
  systems to manage, 723–724
PBX (private branch exchange), 525, 536
fraud/abuse, 527–529
PCI DSS (Payment Card Industry Data Security Standard), 62, 305–306
PDU (protocol data unit), 443
PEAP (Protected Extensible Authentication Protocol), 478, 524
PEDs (portable electronic devices), 366
war driving and, 483
PEM (Privacy Enhanced Mail), 533
penetration testing
  black box, 681
  ethical hacking, 772
  exploitation, 679–680
  full-knowledge team, 771
  gray box, 681
  information gathering and discovery, 679–680
  Metasploit, 679–680
  partial-knowledge team, 771
  permission, 770
  planning, 679–680
  report protection, 772
  reporting, 679–680
  risks, 769–770
  threat modeling and, 31
  vulnerability scanning, 679–680
  white box, 681
  zero-knowledge team, 770–771
perimeter security controls, 422
fences, 422–423
gates, 423
lighting, 424
mantraps, 423–424
security bollards, 424
security dogs, 424–425
security guards, 424–425
turnstiles, 423
permissions, 624
personal property, 403
personnel
  candidate screening, 55
  collusion, 52, 54–55
  cross-training, 54
  employment agreements, 55–57
  hiring, 51–52, 55
  job responsibilities, 53
  job rotation, 53–54
  offboarding, 57
  onboarding, 57
  separation of duties, 52, 53
  termination, 57–59
personnel security/safety
duress systems, 708
emergency management, 709–710
review question answers, 951–952
training, 710
travelling, 709
written lab answers, 988–989
PERT (Program Evaluation Review Technique), 887–888
PGP (Pretty Good Privacy), 255–256, 533, 534
PHI (protected health information), 161
phishing, 569, 931–932
spear phishing, 931
vishing, 931
whaling, 931
photoelectric motion detectors, 427
phreakers, 527
physical access control, 584
physical assets, 711–712
physical controls, 78–79
physical security, 403
regulatory requirements, 431
physical security, 400. See also
  environmental security; facility design;
  site design
  access abuses, 410–411
  CCTV, 411
data centers, 407–409
delay, 404
piggybacking – port scans

denial, 404
detection, 404
deterrence, 404
eMAN (emanation security), 411–412
EMI (electromagnetic interference), 416
environment safety, 429–430
evidence storage, 413
fire
damage, 421–422
detection, 419–420
extinguishers, 419
prevention, 417
stages, 418–419
suppression, 417–421
functional order of use, 404
humidity, 416–417
HVAC issues, 416–417
IDSs (intrusion detection systems), 410
internal security controls, 425
badges, 427
combination locks, 426
EAC (electronic access control) lock, 426
intrusion alarms, 428
keys, 426
motion detectors, 427
secondary verification, 428–429
legal requirements, 430
life safety, 429–430
masquerading, 410
media storage, 412–413
memory cards, 409
noise, 416
perimeter security controls, 422
fences, 422–423
gates, 423
lighting, 424
mantraps, 423–424
security bollards, 424
security dogs, 424–425
security guards, 424–425
turnstiles, 423
piggybacking, 410
privacy and, 430
proximity readers, 409–410
restricted areas, 413–414
review question answers, 965–966
RFI (radio-frequency interference), 416
RFID (radio-frequency identification), 410
SCIF (Sensitive Compartmented Information Facility), 414
secure facility plan, 401
server rooms, 407–409
server vaults, 407–409
smartcards, 409
static, 416–417
temperature, 416–417
utilities, 414–415
water issues, 417
work areas, 413–414
written lab answers, 994
PII (personally identifiable information), 61, 160–161
PKI (public-key infrastructure), 249
asymmetric key management, 253–254
CAs (certificate authorities), 250–253
digital certificates, 249–250
review question answers, 960–961
written lab answers, 992
plaintext, cryptography and, 200–201
plenum cable, 499
policies
security
acceptable use, 28
advisory, 27
component relationships, 30
individuals and, 27
informative, 27
issue-specific, 27
organizational, 27
regulatory, 27
system-specific, 27
security policies, 15, 26
polymorphic viruses, 923
POODLE (Padding Oracle On Downgraded Legacy Encryption) attack, 177
POP3 (Post Office Protocol version 3), 451, 462, 530
port scans, 940–941
POTS (plain old telephone service), 536, 537–538
POTS/PSTN, 525
power outages, 808–809
PPP (Point-to-Point Protocol), 445
PPTP (Point-to-Point Tunneling Protocol), 445, 543
premises wire distribution room, 405
Presentation layer (OSI)
   ASCII (American Standard Code for Information Interchange), 450
   EBCDICM (Extended Binary-Coded Decimal Interchange Mode), 450
   JPEG (Joint Photographic Experts Group), 450
   MIDI (Musical Instrument Digital Interface), 450
   MPEG (Moving Picture Experts Group), 450
   TIFF (Tagged Image File Format), 450
preventive access control, 582
preventive controls, 80
preventive measures, 745–746
   anti-malware software, 746, 765–766
   applications, 746
attacks
   botnets, 747–748
   DoS (denial of service), 748–749
   espionage, 755–756
   fraggle attacks, 751
   land attacks, 752
   malicious code, 753–754
   man-in-the-middle, 754–755
   ping floods, 751
   ping of death, 751–752
   sabotage, 755
   smurf attacks, 751
   SYN flood attacks, 749–750
   TCP reset, 750
   teardrop, 752
   zero-day exploits, 752–753
blacklisting, 766–767
configuration management, 746
firewalls, 746
   circuit-level gateway firewalls, 767
IANA, 767
next-generation firewall, 767
stateful inspection firewalls, 767
UTM (unified threat management), 767
honeypots/honeynets, 763
   padded cells, 764
   pseudo flaws, 764
   intrusion detection and prevention, 746
   penetration testing, 768
   ethical hacking, 772
   permission, 770
   report protection, 772
   risks, 769–770
   techniques, 770–771
protocols, 746
sandboxing, 768
services, 746
system management, 746
systems, 746
third-party security services, 768
warning banners, 764–765
whitelisting, 766–767
PRI (Primary Rate Interface), 557
primary memory, 905
principle of least privilege. See least privilege
printers, 340–341
privacy
   confidentiality and, 4
   employees’ rights, 146
   European Union, 146–148
Privacy Act of 1974, 142
privacy laws, U.S.
   CALEA, 142
   COPPA, 144
   data breach notification, 143–144
   Economic Espionage Act, 142
   ECPA, 142
   FERPA, 145
   Fourth amendment, 141–142
   GLBA, 144
   HIPAA, 142–143
   HITECH, 143
   Identity Theft and Assumption Deterrence Act, 145
   Privacy Act of 1974, 142
   USA PATRIOT Act, 145
privacy policies, 61–62
private cloud, 714
private key cryptography, 215–216
privileged operations, 37
privileges
access control and, 624
escalation, 935
least privilege, 53, 626, 698, 699–700
privilege creep, 631
separation of privilege, 701
proactive approach to threat modeling, 30
procedures, 28–29. See also SOP (standard operation procedures)
processor, 321
execution types
MPP, 322–323
multicore, 322
multiprocessing, 322
multiprogramming, 323
multitasking, 322
multithreading, 323–324
SMP, 322
microprocessor, 321
operating modes
privileged mode, 332–333
user mode, 332
processing types
multi-state, 324
single-state, 324
protection mechanisms
process states, 327–332
protection rings, 325–327
procurement, 150–151
programming flaws, 388
programming languages, 872–873
compiled languages, 873
interpreted languages, 873
machine language, 873
protection mechanisms, 12, 379–380
CMWs (compartmented mode workstations), 331
compartmented mode, 330
computer architecture, 383
dedicated mode, 330
multilevel mode, 331
operating states, 327
policy mechanisms
accountability, 384
principle of least privilege, 383
separation of privilege, 384
problem state, 327
process scheduler, 328–329
process states, 327
program executive, 328
protection rings, 325
kernel, 325
kernel mode, 326
mediated-access model, 326
privileged mode, 326
system call, 327
user mode, 326
ready state, 327
running state, 328
security modes, 329
comparison, 332
stopped state, 328
supervisor state, 327
supervisory state, 328
system hide mode, 330
technical mechanisms
abstraction, 381–382
data hiding, 382
hardware segmentation, 382–383
layering, 380–381
process isolation, 382
waiting state, 327–328
protocols, 440
authentication
CHAP, 524
EAP, 524
PAP, 524
communications
IPsec, 523
Kerberos, 523
Signal Protocol, 523
S-RPC, 523
SSH, 523
SSL, 523
TLS, 523
converged protocols, 470–471
proximity readers – remote access

FCoE (Fibre Channel over Ethernet), 471
iSCSI (Internet Small Computer System Interface), 471
MPLS (Multiprotocol Label Switching), 471
SDN (software-defined networking), 472
VoIP (Voice over IP), 471
discovery, 457–458
proximity readers, 409–410
proxy logs, 774
PSTN (public switched telephone network), 536, 537–538, 554
public cloud, 714
public key algorithms, 216–219
PVCs (permanent virtual circuits), 555

Q

qualitative risk analysis, 68, 75
quantitative risk analysis, 68–69, 75
  ALE (annualized loss expectancy), 70–71
  ARO (annualized rate of occurrence), 70, 109
  EF (exposure factor), 70
  formulas, 73
  safeguard cost/benefit, 72
  safeguard costs, 71–72
  SLE (single loss expectancy), 70

R

RADIUS (Remote Authentication Dial-In User Service), 540
RAID (redundant array of inexpensive disks), 310
rainbow series, 296, 299–300
  Green Book, 299
  Orange Book, 298
  Red Book, 299
random access storage, 905
ransomware, WannaCry, 167
RBAC (Role Based Access Control), 10
RC5 (Rivest Cipher 5), 224
reactive approach to threat modeling, 31
reconnaissance attacks
  IP probes, 940
  port scans, 940–941
  vulnerability scans, 941
record retention, 175–176
recovery access control, 583
recovery controls, 80
reduction analysis, threat modeling, 36–37
reference monitors, 284
regional disasters, 806–807
registration, 585–586
  biometrics, 599
regulatory investigations, 848
regulatory policies, 27
  compliance, 149–150
  review question answers, 954–956
  written lab answers, 990
relational databases
  candidate keys, 898
  cardinality, 897
  degrees, 897
  domains, 897
  fields, 897
  foreign keys, 898
  primary keys, 898
  referential integrity, 898
  SQL, 898–899
  tuples, 897
remote access, 536
  authentication protection, 538
  authentication services, 540
dial-up protocols
  PPP, 539
  SLIP, 539–540
RADIUS (Remote Authentication Dial-In User Service), 540
remote connectivity technology, 538
remote control, 537
remote node operation, 537
remote user assistance, 538–539
scraping, 537
screen scraper, 537
security plan, 538–539
remote journaling database recovery and – risk management

incident response, 977–980
investigations, 981–983
laws, 954–956
malicious code, 984–986
network architecture, 966–967
network attacks, 968–969
network components, 966–967
personnel security, 951–952
physical security, 965–966
PKI (public-key infrastructure), 960–961
regulations, 954–956
risk management, 951–952
security assessment, 973–974
security capabilities, 961–962
security design, 961–962
security models, 961–962
security operations, 975–977
software development security, 983–984
symmetric key algorithms, 958–959
testing, 973–974
threats, 963–964
vulnerabilities, 963–964

reviews
account management reviews, 689
backup verification, 689
key performance indicators, 690
log reviews
GPOs (Group Policy Objects), 688
NetFlow logs, 688
NTP (Network Time Protocol), 688
SIEM (security incident and event management) packages, 688
risk indicators, 690
RFI (radio-frequency interference), 416
RFID (radio-frequency identification), 410, 507
ID tags, 414
rights, access control and, 624
ring topology, 500–501
RIP (Routing Information Protocol), 447
risk, 65
risk framework. See RMF (Risk Management Framework)
risk management, 63–64
asset valuation, 65, 82
assets, 64
attacks, 66
breaches, 66
countermeasures, selecting, 77–78
exposure, 65
qualitative risk analysis, 68, 75
   Delphi technique, 75
   scenarios, 74–75
quantitative risk analysis, 68–69, 75
   ALE (annualized loss expectancy), 70–71
   ARO (annualized rate of occurrence), 70, 109
   EF (exposure factor), 70
   formulas, 73
   safeguard cost/benefit, 72
   safeguard costs, 71–72
   SLE (single loss expectancy), 70
residual risk, 77
review question answers, 951–952
risk, 65
risk acceptance, 76
risk assignment, 76
risk avoidance, 77
risk deterrence, 77
risk mitigation, 76
risk rejection, 77
risk reporting, 83
safeguards, 66
security controls
   administrative, 78–79
   compensating controls, 80
   corrective controls, 80
   detective controls, 80
   deterrent controls, 79
   directive controls, 81
   logical/technical, 78–79
   measurement and, 81
   monitoring and, 81
   physical, 78–79
   preventive controls, 80
   recovery controls, 80
   SCA (security control assessment), 81
threat actors, 65–66
threat agents, 65–66
threat events, 65–66
threat identification, 67–68
threats, 65
total risk, 77
vulnerability, 65
written lab answers, 988–989
risk-based management, 38–40
Rivest, Ronald, 239, 244
RMF (Risk Management Framework), 83–84, 308
Rogier, Nathalie, 245
rogue access points, 484–485
ROI (return on investment), 17
ROM (read-only memory)
   EEPROM (Electrically Erasable Programmable Read-Only Memory), 334
   EPROM (Erasable Programmable Read-Only Memory), 334
   flash, 334
   PROM (programmable read-only memory), 333–334
rootkits and, 935
ROT3 (Rotate 3), 197
routers, 448
   screening routers, 489
Royce, Winston, 882
RPC (Remote Procedure Call), 449
RSA public key algorithm, 239–241
RTO (recovery time objective), 107
running key ciphers, 212–213

S

SA (security association), 264
SaaS (software as a service), 713
safeguards, 66
sandboxing, 279
SBU (sensitive but unclassified), 163
SCA (security control assessment), 81
Schneier, Bruce, 177, 223
SCIF (Sensitive Compartmented Information Facility), 414
scoping, security baselines, 187
SCP (Secure Copy), 178
screening routers, 489
script kiddies, 916–917
Scrum, 885
SD3+C, 30
SDH (Synchronous Digital Hierarchy), 559–560
SDL (Security Development Lifecycle), 30
SDLC (Synchronous Data Link Control), 560
SDN (software-defined networking), 472, 548
SDNs (software-defined networks), 712
seclusion, confidentiality and, 4
secondary data storage, 905
secondary verification mechanisms, 428–429
secrecy, confidentiality and, 4
secret key cryptography, 215–216
Secure by Design, Secure by Default, Secure in Deployment and Communication. See SD3+C
secure facility plan, 401
security. See also physical security
abstraction, 13
awareness, 86
behavior modification, 86
bottom-up approach, 16
business cases, 15
CISO (chief information security officer), 16
corporate property, 403
CSO (chief security officer), 16
data hiding, 13
due care, 25
due diligence, 25
education, 87
encryption, 14
ISO (information security officer), 16
layering, 12–13
legally defensible security, 12
operational plans, 16, 17
organizational processes, 17–18
change management, 18–19
data classification, 19–23
parallel configurations, 13
personal property, 403
policies, 15, 26, 43
acceptable use, 28
advisory, 27
component relationships, 30
individuals and, 27
informative, 27
issue-specific, 27
organizational, 27
regulatory, 27
system-specific, 27
protection mechanisms, 12
senior management and, 16
serial configurations, 16
strategic plans, 16, 17
tactical plans, 16, 17
top-down approach, 15
training, 86–87
security applications, 909
security assessment, 664
review question answers, 973–974
written lab answers, 997
security audits
auditing standards, COBIT, 667
external, 666
internal, 665–666
third-party, 666–667
security awareness training, 43
security bollards, 424
security boundaries, 563–564
security capabilities
review question answers, 961–962
written lab answers, 992–993
security controls, 12
administrative, 78–79
administrative physical controls, 403
baselines, 186–187
scoping, 187
standards, 187
tailoring, 187
compensating controls, 80
corrective controls, 80
data, 165–167
detective controls, 80
deterrent controls, 79
security dogs – security operations

directive controls, 81
frameworks, 25
logical/technical, 78–79
measurement and, 81
monitoring and, 81
physical, 78–79, 403
preventive controls, 80
recovery controls, 80
SCA (security control assessment), 81
technical physical controls, 403
security dogs, 424–425
security governance, 14–15, 42, 62
ATO (authorization to operate), 63
compliance policies, 61–62
contracting and, 150–151
documentation review, 63
procurement and, 150–151
third-party governance, 62–63
security guards, 424–425
security incidents, 738
security labels, 282
security logs, 774
security models, 281–282
access control matrix, 286, 288
ACLs, 287
capabilities list, 287
mandatory, 287
rule-based, 287
Bell-LaPadula model, 288
* (star) Security Property, 289
classification levels, 289
Discretionary Security Property, 289
Simple Security Property, 289
trusted subject, 290
Biba model, 290
* (star) Integrity Property, 290
drawbacks, 291–292
Simple Integrity Property, 290
Brewer and Nash model, 293
Chinese Wall model, 293
Clark-Wilson model, 292
access control triple, 292
CDI (constrained data item), 292
IVP (integrity verification procedure), 293
restricted interface model, 293
TPs (transformation procedures), 293
UDI (unconstrained data item), 292
composition theories
cascading, 286
feedback, 286
hookup, 286
Goguen-Meseguer model, 294
Graham-Denninger Model, 294
information flow model, 285
kernels, 284
lattice-based access controls, 289
classification levels, 289
noninterference model, 285–286
reference monitors, 284
review question answers, 961–962
security perimeter, 283
state machine models
FSM, 284
secure state machine, 285
state transition, 284–285
states, 284
Sutherland Model, 294
Take-Grant model, 286
directed graph, 287
TCB (trusted computing base), 282–283
written lab answers, 992–993
security operations
aggregation, 700
due care, 698
due diligence, 698
entitlement, 700
information lifecycle management
archive, 707
capture, 706
classification, 706
creation, 706
destruction, 707
purging, 707
storage, 707
usage, 707
job rotation, 703
least privilege, 698, 699–700
mandatory vacations, 703–704
need to know, 698, 699
personnel security/safety
  duress systems, 708
emergency management, 709–710
training, 710
travelling, 709
privileged account management, 704–706
review question answers, 975–977
segregation of duties, 701–703
separation of duties and responsibilities, 700–701
separation of privilege, 701
SLAs (service-level agreements), 707–708
transitive trust, 700
two-person control, 703
written lab answers, 997–998
security perimeter, 283
security policies, 626–627
security roles
  auditor, 24
  CIRT (computer incident response team), 24
data custodian, 24
data owner, 24
InfoSec (information security) officer, 24
security professional, 24
senior manager, 23
user, 24
security testing, 662–663
penetration testing
  black box, 681
  exploitation, 679–680
  gray box, 681
  information gathering and discovery, 679–680
  Metasploit, 679–680
  planning, 679–680
  reporting, 679–680
  vulnerability scanning, 679–680
  white box, 681
software, 681–682
  code review, 682–683
dynamic testing, 683–684
fuzz testing, 684–685
interface testing, 686
misuse case testing, 686
static testing, 683
test coverage analysis, 686–687
website monitoring, 687
security through obscurity, 13
segregation of duties, 701
control matrix, 702
sendmail, 531
sensitivity, confidentiality and, 4
separation of duties and responsibilities, 52, 53, 626, 700–701
sequential access storage, 905
serial configurations, 13
server rooms, physical security, 407–409
server-based vulnerabilities, 346–347
service authentication, 601
session hijacking, 942
Session layer (OSI)
  NFS (Network File System), 449
  RPC (Remote Procedure Call), 449
  SQL (Structured Query Language), 449
SET (Secure Electronic Transaction), 451
SFTP (Secure File Transfer Protocol), 178
SHA (Secure Hash Algorithms), 244
Shamir, Adi, 239
SHS (Secure Hash Standard), 244
SIEM (security incident and event management) packages, 688
Signal Protocol, 523
signature dynamics, 597
site design. See also physical security
  access abuses, 410–411
  emanation security, 411–412
  EMI (electromagnetic interference), 416
evidence storage, 413
fire damage, 421–422
fire detection, 419, 420
fire extinguishers, 419
fire prevention, 417–419
fire stages, 418–419
fire suppression, 417–418
gas discharge systems, 421
water, 420–421
humidity, 416–417
HVAC issues, 416–417
IDSs (intrusion detection systems), 410
SKA (shared key authentication) – software development

media storage, 412–413
natural disasters and, 402
noise, 416
restricted areas, 413–414
review question answers, 961–962
RFI (radio-frequency interference), 416
SCIF (Sensitive Compartmented Information Facility), 414
security, 400
site selection, 401–402
smartcards, 409
static, 416–417
temperature, 416–417
utilities
  power issues, 415
  UPS, 414–415
visibility, 402
water issues, 417
work areas, 413–414
written lab answers, 992–993
SKA (shared key authentication), 476
SKIP (Simple Key Management for Internet Protocols), 447
Skipjack, 220, 223–224
SLAs (service-level agreements), 40, 60, 707–708
  equipment failure and, 405
  software development, 894
SLE (single loss expectancy), 70, 110
SLIP (Serial Line Internet Protocol), 445
smart devices, 358
  PIV (Personal Identity Verification) cards, 593
smartcards, 409
  CACs (Common Access Cards), 593
S/MIME (Secure Multipurpose Internet Mail Extensions), 256, 533
SMTP (Simple Mail Transfer Protocol), 451, 462, 530–531
sniffers, 565–566
SNMP (Simple Network Management Protocol), 451, 463
SOA (service-oriented architecture), 389
social engineering, 526–527
  phreakers, 527
software
  ConfigMgr, 711
  licensing, 711
  SCCM (System Center Configuration Manager), 711
software development
  APIs (application programming interfaces), 890–891
  assurance, 875
  change management, 888–889
  code repositories, 893–894
  configuration management, 888–889
  development lifecycle, 878–879
    Agile model, 884–885
    change management, 881
    code review, 881
    control specifications, 880
    design review, 880–881
    functional requirements, 879–880
    Gantt charts, 887–888
    IDEAL model, 886–887
    maintenance, 881
    PERT, 887–888
    software capability maturity model, 885
    spiral model, 883
    user acceptance testing, 881
    waterfall model, 882–883
DevOps approach, 889–890
OOP (object-oriented programming)
  behaviors, 874
  classes, 874
  cohesion, 875
  coupling, 875
  delegation, 875
  inheritance, 875
  instances, 874
  messages, 874
  methods, 874
  objects, 874
  polymorphism, 875
programming languages, 872–873
  compiled languages, 873
  interpreted languages, 873
  machine language, 873
review question answers, 983–984
SLAs (service-level agreements), 894
software acquisition, 894–895
system failure
  avoiding, 875–878
  mitigating, 875–878
testing
  black-box testing, 892
dynamic testing, 892
gray-box testing, 892
  reasonableness check, 891–892
  static testing, 892
  white-box testing, 892
written lab answers, 1000
software failures, 810
software focused threats, 31
software security testing, 681–682
  black box, 681
code review, 682–683
dynamic testing, 683–684
ethical hacking, 772
exploitation, 679–680
full-knowledge team, 771
fuzz testing, 684
  bit flipping, 684
  generational (intelligent) fuzzing, 684
  mutation (dumb) fuzzing, 684
  prefuzzing input file, 685
  zzuf tool, 685
gray box, 681
information gathering and discovery, 679–680
interface testing
  APIs, 686
  physical interfaces, 686
  UIs, 686
Metasploit, 679–680
misuse case testing, 686
partial-knowledge team, 771
permission, 770
planning, 679–680
report protection, 772
reporting, 679–680
risks, 769–770
static testing, 683
test coverage analysis, 686
  branch coverage, 687
  condition coverage, 687
  function coverage, 687
  loop coverage, 687
  statement coverage, 687
threat modeling and, 31
vulnerability scanning, 679–680
website monitoring
  active monitoring, 687
  passive monitoring, 687
  synthetic monitoring, 687
white box, 681
zero-knowledge team, 770–771
SONET (Synchronous Optical Networking), 559–560
SOP (standard operation procedures), 28–29
source code review, threat modeling and, 31
SOX (Sarbanes-Oxley Act of 2002), 62
Spectre, 309
SPF (Sender Policy Framework), 534
spiral lifecycle model, 883
split knowledge, 207
spoofing, 32
SPX (Sequenced Packet Exchange), 449
spyware, 928
SQL (Structured Query Language), 449
SQL injection attacks, 937, 938–939
  account privilege limits, 940
  dynamic Web applications, 937–938
  input validation and, 939–940
  prepared statements and, 939
S-RPC (Secure Remote Procedure Call), 451, 523
SSAA (System Security Authorization Agreement), 308
SSDs (solid state drives), 173
SSH (Secure Shell), 262, 523
SSID (service set identifier), 475–476
  beacon frame, 475
  disabling broadcast, 476
SSL (Secure Sockets Layer), 177, 257, 449, 462, 523
standards, 28
  security baselines, 187
star topology, 502
state attacks, 389
state machine security models
  FSM (finite state machine), 284
  secure state machine, 285
  state transition, 284–285
  states, 284
stateful inspection firewalls, 489
statement coverage analysis, 687
static NAT, 552
static packet-filtering firewalls, 488–489
static passwords, 588–589
static systems, 376–377
  application firewalls, 378
  diversity control, 379
  firmware version control, 379
  manual updates, 378
  monitoring, 379
  network segmentation, 378
  redundancy control, 379
  security layers, 378
  wrappers, 379
statistical attacks, 265
stealth viruses, 922–923
steganography, 257–259, 783
storage
  evidence, 413
  media storage, physical, 412–413
  sensitive data, 171–172
storms, 805–806
STP (shielded twisted-pair) cabling, 498
strategic plans, 17
stream ciphers, 213
STRIDE threat modeling, 32–33
strikes/picketing, 811
subjects, 277, 624
substitution ciphers, 209–211
supply chain, risk-based management and, 38–40
Sutherland Model, 294
SVCs (switched virtual circuits), 555
SW-CMM (Software Capability Maturity Model), 885
switching technologies, 553
  circuit switching, 554
packet switching, 554–555
  virtual circuits, 555–556
symmetric cryptography
  Diffie-Hellman, 226–227
  escrow encryption standard, 228
  fair cryptosystems, 228
  key management
    creation, 226–227
    destruction, 227
    distribution, 226–227
    key escrow, 228
    recovery, 228
    storage, 227
  offline distribution, 226
  public key encryption, 226
  split-knowledge, 227
symmetric cryptosystems, 199
symmetric encryption, 176–177
symmetric key algorithms, 215
  review question answers, 958–959
  weaknesses, 216
  written lab answers, 991–992
synchronous dynamic password tokens, 593
synthetic website monitoring, 687
system failure
  authentication, 876
  error handling, 876
  fail-open failure state, 877–878
  fail-secure failure state, 877–878
  input validation and, 875–876
    limit checks, 875
  logging, 877
    OWASP guidelines, 877
  session management, 876
system logs, 774
system-specific security policies, 27

T

TACAC5+ (Terminal Access Controller
  Access-Control System), 540
tactical plans, 17
tailoring, security baselines, 187
Take-Grant security model, 286
directed graph, 287
tampering threats, 32
tape backups, 831
  best practices, 832
disk-to-disk, 832
rotating
  GFS strategy, 832
  HSM (hierarchical storage management), 833
  Six Cartridge Weekly Backup strategy, 832
  Tower of Hanoi strategy, 832
tape media, 716
TATO (temporary ATO), 63
TCB (trusted computing base), 282–283
TCP (Transmission Control Protocol), 449
  headers, 455–457
  port scans, 675
two-way handshake, 454
TCP wrappers, 453
TCP/IP model, 441, 451
  Application (Process) layer, 451
  protocols, 462–463
DNS (Domain Name System), 465
  DNS poisoning, 468–470
  DNSSEC, 468
  FQDNs, 466–467
  HOSTS file, 468
  permanent addresses, 466
  primary authoritative names server, 467
  resource records, 467
  secondary authoritative names server, 467
  temporary addresses, 466
  TLD, 466–467
  zone files, 467
dynamic ports, 454
ephemeral ports, 454
IP (Internet Protocol), 458
  ARP, 461–462
  CIDR, 460
  classes, 459–460
  ICMP, 460–461
  IGMP, 461
  loopback address, 460
Link layer, 451
  multilayer protocols, 463–465
  Network layer, 458–459
OSI model comparison, 452
random ports, 454
registered software ports, 454
service ports, 453
TCP (Transmission Control Protocol), 453
Transport (Host-to-Host) layer, 451
UDP (User Datagram Protocol), 453, 458
VPN links, 453
vulnerabilities, 463–465
well-known ports, 453
TCSEC (Trusted Computer System Evaluation Criteria), 28, 297
Common Criteria, 295
  comparison, 305
ITSEC comparison, 301–302, 305
  mandatory protection
    labeled security, 298
    security domains, 298
    structured protection, 298
  minimal protection, 297
rainbow series, 296, 299–300
  verified protection, 298
technical access control, 584
  technical physical security controls, 403
technology convergence, 401
telecommunications room, 407
telecommuting, 536. See also remote access telephony, 536
Telnet, 451, 462
TEMPEST countermeasures, 411
termination of employees, 57–58
  complexities, 59
  exit interviews, 58
terrorist acts, 807–808
terrorist attacks, 859
test coverage analysis
  branch coverage, 687
  condition coverage, 687
  function coverage, 687
loop coverage, 687
statement coverage, 687
testing, 662–663
  DRP (disaster recovery and planning)
    full-interruption test, 837
    parallel test, 837
    read-through test, 836
    simulation test, 837
    structured walk-through, 837
penetration testing
  black box, 681
  ethical hacking, 772
  exploitation, 679–680
  gray box, 681
  information gathering and discovery, 679–680
    Metasploit, 679–680
    permission, 770
    planning, 679–680
    report protection, 772
    reporting, 679–680
    risks, 769–770
    techniques, 770–771
    vulnerability scanning, 679–680
white box, 681
review question answers, 973–974
software, 681–682
  code review, 682–683
  dynamic testing, 683–684
  fuzz testing, 684–685
  interface testing, 686
  misuse case testing, 686
  static testing, 683
  test coverage analysis, 686–687
  website monitoring, 687
software development
  black-box testing, 892
  dynamic testing, 892
  gray-box testing, 892
  reasonableness check, 891–892
  static testing, 892
  white-box testing, 892
written lab answers, 997
TFTP (Trivial File Transfer Protocol), 451, 462

theft, 811–812
third-party audits, 39–40, 666
third-party governance, 62–63
threat actors, 65–66
threat agents, 65–66
threat events, 65–66
threat identification
  DoS (denial of service), 32–33
  DREAD, 33
  elevation of privilege, 33
  ethical hacking and, 31
  fuzz testing and, 31
  individuals, 34–35
  risk management and, 67–68
threat modeling, 30, 44
  asset focus, 31
  attacker focus, 31
  decomposition, 36–37
  diagramming potential attacks, 35–36
  information disclosure, 32
  PASTA (Process for Attack Simulation and Threat Analysis), 33
  penetration testing and, 31
  prioritization, 37–38
  proactive approach, 30
  reactive approach, 31
  reduction analysis, 36–37
  repudiation, 32
  responses, 37–38
  software focus, 31
  source code review and, 31
  spoofing, 32
  STRIDE, 32–33
  tampering, 32
  trike, 33
  VAST (visual, agile, and Simple Threat), 34
threats, 65
  review question answers, 963–964
  written lab answers, 993
three dumb routers, 359
thrill attacks, 861
TIFF (Tagged Image File Format), 450
TKIP (Temporal Key Integrity Protocol), 479
TLS (Transport Layer Security), 257, 449, 523
TOC (time of check), 389
TOCTTOU (time of check to time of use), 389, 934
tokenization, 183
tokens, 282
asynchronous dynamic password, 593
synchronous dynamic password, 593
top-down approach to security, 15
topologies
bus, 501–502
mesh, 503
ring, 500–501
star, 502
TOTP (Time-based One-Time Password), 594
TOU (time of use), 389
TPM (Trusted Platform Module), 254, 255, 310
training, personnel, 710
transitive trust, 277, 700
transmission mechanisms, 562–563
transparency, 561
transport encryption, 177–178
Transport layer (OSI)
SPX (Sequenced Packet Exchange), 449
SSL (Secure Sockets Layer), 449
TCP (Transmission Control Protocol), 449
TLS (Transport Layer Security), 449
UDP (User Datagram Protocol), 449
transposition ciphers, 208
travelling personnel, 709
Trojan horses, 924–925
botnets, 925
trust boundaries, 37
trusted systems, 281
tunneling, VPNs, 541–542
Turing, Alan, 198
turnstile, 423
twisted-pair cabling
STP (shielded twisted-pair), 498
UTP (unshielded twisted-pair), 498
two-factor authentication, 599–600

U
UDP (User Datagram Protocol), 449, 458
USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism), 145
user education, 653
user entitlement audits, 786
utilities
failures, 809
power issues, 415
UPS (uninterruptible power supply), 414–415
UTP (unshielded twisted-pair) cabling, 498

V
vandalism, 811–812
VDIs (virtual desktop infrastructures), 712
VENOM (Virtualized Environment Neglected Operations Manipulations), 547
versioning, 722–723
virtual assets
SDNs (software-defined networks), 712
VDIs (virtual desktop infrastructures), 712
VMs (virtual machines), 712
VSANs (virtual storage area networks), 712
virtual circuits, 555–556
PVCs (permanent virtual circuits), 555
SVCs (switched virtual circuits), 555
virtual memory, 905
virtual storage, 905
virtualization, 310, 546
virtual networking, SDN (software-defined networking), 548
VM escaping, 547
viruses, 917–918
antivirus, 920
heuristic-based detection, 921
Kaspersky Lab, 920–921
VLANs (virtual local area networks) – vulnerability scans

signature-based detection, 921
Tripwire, 922
companion viruses, 919
encrypted, 923
file infect virus, 919
hoaxes, 923
Kaspersky Lab and, 920–921
macro viruses, 919–920
MBR viruses, 918–919
multipartite, 922
polymorphic, 923
service injection viruses, 920
stealth, 922–923
vulnerable platforms, 920
VLANs (virtual local area networks), 545–546
virtual applications, desktops, 547–548
VMs (virtual machines), 712
VMware Fusion for Mac, 310
VMware vSphere, 310
VMware vSphere Hypervisor, 310
VMware Workstation Pro, 310
voice communications
abuse, 527–529
fraud, 527–529
PBX (private branch exchange), 525
POTS/PSTN, 525
social engineering, 526–527
DISA (Direct Inward System Access), 528–529
phreakers, 527
VoIP (Voice over Internet Protocol), 525–526
SRTP, 526
voice pattern recognition, 597
VoIP (Voice over IP), 471, 525–526, 536
SRTP (Secure Real-Time Transport Protocol), 526
volatile storage, 905
VPNs (virtual private networks), 178, 536, 540–541
IPSec, 453
L2TP (Layer 2 Tunneling Protocol), 453
OpenVPN, 453
overview, 542–543
PPTP (Point-to-Point Tunneling Protocol), 453
protocols
IPsec, 544–545
L2TP, 544
PPTP, 543
SSH (Secure Shell), 453
tunneling, 541–542
VSANs (virtual storage area networks), 712
vulnerabilities
client-based
applets, 342–344
local caches, 344–346
review question answers, 963–964
server-based, data flow control, 346–347
written lab answers, 993
vulnerability, 65
vulnerability assessments, 726–727
descriptions, 668
CCE, 668
CPE, 668
CVE, 668
CVSS, 668
OVAL, 668
XCCDF, 668
scans, 668–669, 726–727
database vulnerability scans, 677–678
network discovery scans, 669–673
network vulnerability scans, 673–675
vulnerability management workflow, 678–679
web vulnerability scans, 676–677
vulnerability management, 725–726
CVE (Common Vulnerability and Exposures) dictionary, 728
reviews, 788
systems to manage, 723–724
vulnerability assessments, 727–728
vulnerability scans, 726–727
workflow
detection, 678
remediation, 679
validation, 678
vulnerability scans, 941
WannaCry ransomware, 167
WANs (wide area networks), 496
  ATM (asynchronous transfer mode), 559
  CIR (committed information rate), 559
dedicated lines, 556
dial-up encapsulation protocols
  PPP, 561
  SLIP, 561
DSL (digital subscriber line), 557
Frame Relay connections, 558–559
HDLC (High-Level Data Link Control), 561
ISDN (Integrated Services Digital Network), 557
leased lines, 556
  fault tolerance, 557
nondedicated lines, 556
point-to-point links, 556
SDH (Synchronous Digital Hierarchy), 559–560
SDLC (Synchronous Data Link Control), 560
SMDS (Switched Multimegabit Data Service), 559
SONET (Synchronous Optical Networking), 559–560
X.25 connections, 558
WAPs (wireless access points), 474
SSID (service set identifier), 474
war chalking, 483
war driving, 483
waterfall lifecycle model, 882–883
watermarking, 257–259, 783
wave pattern motion detectors, 427
web applications
  cryptography, 256–257
  steganography, 257–259
  watermarking, 257–259
security
  dynamic Web applications, 937–938
  SQL injection, 937, 938–940
  XSRF/CSRF, 936–937
  XSS attacks, 935–936
  web vulnerability scanning, 676–677
web-based systems
  directory traversal attack, 363
directory traversal attack, 363
  DMZ (demilitarized zone), 362
  injection attacks, 361–363
  account privileges limiting, 362
  input validation, 362
  LDAP injection, 363
  XML injection, 363
OWASP (Open Web Application Security Project), 360–361
XML exploitation, 363–364
XSS (cross-site scripting), 364
website monitoring
  active monitoring, 687
  passive monitoring, 687
  synthetic monitoring, 687
WEP (Wired Equivalent Privacy), 264, 476–477
white box penetration testing, 681
white noise, 411
wireless communications
  Bluetooth, 506–507
cell phones, 504
  ITU-R, 506
  mobile service technologies, 505
cordless phones, 508
DSSS (Direct Sequence Spread Spectrum), 504
FHSS (Frequency Hopping Speed Spectrum), 504
NFC (near-field communication), 507
OFDM (Orthogonal Frequency-Division Multiplexing), 504
PANs (personal area networks), 506–507
RFID (radio-frequency identification), 507
wireless networking, 472–473
  802.1X/EAP, 478
access points, 473
  ad hoc mode, 475
  enterprise extended mode, 475
  ESSID, 475
infrastructure mode, 475
power level controls, 480
SSID, 475
stand-alone mode, 475
wired extension mode, 475
antennas
placement, 479–480
types, 480
attacks, 482–483
evil twins, 485
IV (initialization vector), 484
replay attacks, 484
rogue access points, 484–485
war chalking, 483
war driving, 483
captive portals, 481
CCMP, 478, 479
channels, 475
data emanation and, 473
EAP (Extensible Authentication Protocol), 478
encryption protocols, 476
KRACK (Key Reinstallation AttaCKs), 478
LEAP (Lightweight Extensible Authentication Protocol), 478–479
MAC filter, 479
OSA (open system authentication), 476
PEAP (Protected Extensible Authentication Protocol), 478
site surveys, 476
SKA (shared key authentication), 476
SSID (service set identifier), 475–476
TKIP (Temporal Key Integrity Protocol), 265, 479
WEP (Wired Equivalent Privacy), 264, 476–477
WPA (WiFi Protected Access), 265, 477–478
WPA2 (Wi-Fi Protected Access 2), 478
as security feature, 482
WPS (WiFi Protected Setup), 481
wiring closets, 407
IDF (intermediate distribution facilities), 405
premises wire distribution room, 405
work area security, 413–414
work functions, 207
worms, 925
Code Red, 926–927
RTM, 926–927
Stuxnet, 927–928
WPA (WiFi Protected Access), 265, 477–478
WPA2 (Wi-Fi Protected Access 2), 478
WPS (WiFi Protected Setup), 481
written lab answers
access control, 996
application attacks, 1000
asset security, 991
authentication, 996
BCP (business continuity planning), 989
communications, 995
countermeasures, 993
cryptographic applications, 992
cryptography, 991–992
DRP (disaster recovery planning), 999
effects, 999–1000
governance, 988
identity management, 996
incident response, 998
investigations, 999–1000
laws, 990
malicious code, 1000
network architecture, 994–995
network attacks, 995
network components, 994–995
personnel security, 988–989
physical security, 994
PKI (public-key infrastructure), 992
regulations, 990
risk management, 988–989
security assessment, 997
security capabilities, 992–993
security design, 992–993
security models, 992–993
security operations, 997–998
software development security, 1000
symmetric key algorithms, 991–992
testing, 997
threats, 993
vulnerabilities, 993
X

X Window, 463
XCCDF (Extensible Configuration checklist Description Format), 668
XenServer, 310
XOR (exclusive OR) operation, 204
XP (Extreme Programming), 885
XSRF (cross-site request forgery), 364
XSRF/CSRF (cross-site request forgery) attacks, 936–937

XSS (cross-site scripting), 364
XSS (cross-site scripting) attacks, 935–936

Z

zero-day attacks, 928
zeroization of media, 412
zero-knowledge proofs, 206–207
Zimmerman, Phil, 255
zombies, 565