Index

Note to the Reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. Italicized page numbers indicate illustrations.

Numbers
2G networks, 364, 365
3DES (Triple-DES), 240
3G networks, 364, 365
4G networks, 364, 365
802.11a standard, 366
802.11ac standard, 366
802.11ad standard, 366
802.11af standard, 366
802.11ax standard, 366
802.11b standard, 366
802.11g standard, 366
802.11n standard, 366
802.11n-2009 standard, 366
802.1x standard, 271

access points, 108–111, 170
antennas, 109–111
cloaking, 172
transitive access, 154–155
evil twin attacks, 174
fat, 110–111
MAC filtering, 109
rogue, 171, 174, 177, 368
stand-alone, 110–111
thin, 110–111
account lockout, 375
account management, 374
least privileges, 375–376
account types, 375–376
least privileges, 376
offboarding, 377–378
onboarding, 377
accountability statements, 18
active backup models, 401
active IDS, 97
active logging, 405
active recon, 387
active responses, 100–102
active vulnerability scanners, 132
configuration, 108
active-active load balancing
ad hoc networking, 374
ad hoc wireless, 59
Ad-Aware, 292
AD-IDS (anomaly-detection IDS), 82, 95–96, 96
Adams, Carlisle, 240
Adaptive Software Development, 216
administrative controls, 316, 349
Advanced Encryption Standard (AES), 239, 240, 242, 252
advanced persistent threats (APTs), 203, 206
adware, 279, 292
AES (Advanced Encryption Standard), 239, 240, 242, 252
agentless solutions, 112
agents, network access control (NAC), 112
aggregation switches, placement, 65
agile development, 203, 216
AH (Authentication Header), 90
air gaps, 336
Aircrack, 130, 130
alarms, 333
ALE (annual loss expectancy), 4, 8–9
all-in-one appliances, 87
alternate sites, 400–402
always-on VPNs, 91
Amazon Web Services, 15
amplification attacks, 304
amplification factor, 304
annual loss expectancy (ALE), 4, 8–9
annualized rate of occurrence (ARO), 4, 8–9
anomalies, 27, 406
anomaly-detection systems, 95–96
ANT, 368
antennas, 109–111
antispoofing protections, 105
antivirus software, 287
Anything as a Service (XaaS), 189
Apache SpamAssassin, 113
appliance operating systems, 69
appliances, 65, 84
all-in-one, 87
WAFs (web application firewalls), 88–89
application attacks
amplification, 304
ARP poisoning, 304
buffer overflows, 299
clickjacking, 306
DDoS (distributed denial-of-service), 280, 293, 297, 297–298
preventing, 298
vs. DoS attacks, 298
zombies, 282, 293, 297
DNS poisoning, 304
domain hijacking, 304–305
DoS (denial-of-service), 279, 293, 296–298
buffer overflows, 279, 297, 299
disassociation, 170, 176
jamming, 171, 174–175, 174–175
preventing, 298
resource exhaustion, 215
driver manipulation, 307–308
injection, 299–302
man-in-the-browser, 305
man-in-the-middle, 280, 298–299, 299
pass the hash, 306
privilege escalation, 303
replay, 305, 306
session hijacking, 30–307
spoofing, 308–309
URL hijacking, 307
XSRF (cross-site request forgery), 302
XSS (cross-site scripting), 302
zero-day exploits, 305
application cells, 192
application control, 370
application-aware devices, 89
application-level proxies, 86
applications
baselining, 219
blacklisting, 73
compiled vs. runtime, 218
database issues, 220–223
development models, 216
patch management, 220
sandboxing, 193, 204, 223
secure configurations, 223–224
vulnerabilities, 214–215
whitelisting, 73, 150
APTs (advanced persistent threats), 203, 206
architectural concepts
device placement, 64–67
IDS vs. IPS, 67
SDN (software-defined networking), 67
VPNs (virtual private networks), 63, 63–64
zones, 57–63
architecture weakness, 212
armored viruses, 279, 285
ARO (annualized rate of occurrence), 4, 8–9
arp command, 138, 139
ARP poisoning, 304
ARP spoofing, 279, 304
asset management, 147
asset tracking, 371
asset value (AV), 4, 8
asymmetric algorithms, 243
Diffie-Hellman, 245, 246
ECC (Elliptic Curve Cryptography), 245–246
ElGamal, 246
Kerckhoff’s principle, 246–247
RSA (Rivest, Shamir, Adleman), 239, 244–245, 246, 261
Atbash cipher, 234–235
attack surface reduction (ASR), 279
attackers. See threat actors
attacks. See also vulnerabilities
application attacks
amplification, 304
ARP poisoning, 304
buffer overflows, 299
clickjacking, 306
DDoS. See DDoS (distributed denial-of-service) attacks
DNS poisoning, 304
domain hijacking, 304–305
DoS. See DoS (denial-of-service) attacks
driver manipulation, 307–308
injection, 299–301
man-in-the-browser, 305
man-in-the-middle, 280, 298–299, 299
pass the hash, 306
privilege escalation, 303
replay, 305, 306
session hijacking, 30–307
spoofing, 308–309
URL hijacking, 307
XSRF (cross-site request forgery), 302
XSS (cross-site scripting), 302
zero-day exploits, 305
social engineering attacks
attack examples, 327
attack motivations, 325
dumpster diving, 322, 322
hoaxes, 323, 324
impersonation, 322
phishing, 320
principles, 326–327
shoulder surfing, 322, 323
tailgating, 320, 321
testing, 328
vishing, 320, 321
watering hole attacks, 282, 324–325
whaling, 320
wireless attacks
bluejacking, 170, 175, 177
bluesnarfing, 170, 175
bluesnarking, 170, 175
dissociation, 170, 176, 367
ever twins, 170, 174, 177
IV (initialization vector) attacks, 171, 173
jamming, 171, 174–175, 177
NFC (near field communications), 171, 176, 368
replay attacks, 172–173, 177
RFID (radio frequency identification), 171, 176
rogue access points, 171, 174, 368
WPS (Wi-Fi Protected Setup), 171, 175
attribute-based access control (ABAC), 161
aups (acceptable use policies), 24–25
authentication, 257. See also digital signatures
biometrics, 153–154
CHAP (Challenge Handshake Authentication Protocol), 124, 156
cryptographic algorithms, 270–271
definitions, 154
digital signatures
biometrics, 153–154
CR (Challenge Response), 124
context-aware, 370
cryptographic algorithms, 270–271
definitions, 154
digital signatures
biometrics, 153–154
context-aware, 370
cryptographic algorithms, 270–271
federations, 154
digital signatures
biometrics, 153–154
context-aware, 370
cryptographic algorithms, 270–271
definitions, 154
differential, 385, 395, 399
digital signatures
federations, 154
context-aware, 370
cryptographic algorithms, 270–271
definitions, 154
differential, 385, 395, 399
digital signatures
out-of-band, 152
PAP (Password Authentication Protocol), 155
RADIUS (Remote Authentication Dial-In User Service), 158, 158–159
SAML (Security Assertion Markup Language), 159
SFA (single-factor authentication), 152, 153
SPAP (Shiva Password Authentication Protocol), 156
TACACS (Terminal Access Controller Access Control System), 158
two-factor authentication, 153
TACACS (Terminal Access Controller Access Control System), 158
authentication Header (AH), 90
authority, social engineering principle, 326
authorization, 152, 153
ABAC (attribute-based access control), 161
Kerberos, 156–157
OAUTH (Open Authorization) standard, 125, 158
RADIUS (Remote Authentication Dial-In User Service), 158, 158–159
SAML (Security Assertion Markup Language), 159
TACACS (Terminal Access Controller Access Control System), 158
automated alerts, 111
autonomous access points, 110
AV (asset value), 4, 8
availability, distributive allocation, 32

B

Back Orifice, 294
backdoor attacks, 279, 294, 295
background checks, 23
backouts, 400
backup generators, 34
Backup Server backup method, 398, 398–399
backup plans, 392–394
Backup Server method, 398, 398–399
backup sites, 400–402
differential, 385, 395, 399
full, 394
Full Archival method, 397–398, 398
Grandfather, Father, Son method, 396–397, 397
HSM (hierarchical storage management), 395
incremental, 386, 394, 395
reasons for, 390
SUSE Linux example, 396
working copies, 390–391
band selection, 109
banner grabbing, 142–143
bare metal hypervisors, 191
barricades, 339
baselines, 145, 219
bastion hosts, 58
BCP (business continuity planning), 389–390, See also business continuity
bcrypt, 249
benchmarks, 64
network infrastructure devices, 56
operating systems, 55–56
web servers, 54–55
beta tests, 353
BGP (Border Gateway Protocol), 106
BIA. See business impact analysis
Big Data, 203, 233
biometrics, 153–154, 338–339
BIOS, secure boot, 68
birthday attacks, 251
BitLocker, 260–270, 269–270
BitLocker to Go, 270
black box testing, 388
blacklisting, 73
Blowfish, 241
bluejacking, 170, 175, 364, 365
bluesnarfing, 170, 175, 364, 365, 365
Bluetooth, 365
bollards, 339
Boonana Trojan, 289
boot, secure, 68
Border Gateway Protocol (BGP), 106
border routers, 105
bot-herders, 293
bots, 279, 293
BPA (business partners agreement), 4, 21
bridge trust model, 258
bridges, 113
brute-force attacks, 234, 250
buffer overflows, 279, 297, 299
burning, 351
business continuity, 389–390
  BIA (business impact analysis), 4, 7,
    28–29, 390
  CBFs (critical business functions), 390
  disaster recovery, 392–403
  incident response, 403–412
  storage mechanisms, 390–391
business impact analysis (BIA), 4, 7,
    28–29, 390
business partners agreement (BPA), 4, 21
business processes, as vulnerability, 212
BYOD (Bring Your Own Device), 364,
    371–373

C

cable locks, 345, 345
CACs (common access cards), 162
Caesar cipher, 234–235
cages, 332
captive portals, 253
carrier unlocking, 374
CAAs (certificate authorities), 257

CASBs (cloud access security brokers), 195
CAST, 240
CBC (cipher-block chaining), 242, 255
CBFs (critical business functions), 390
CCMP (Counter Mode with Cipher Block
  Chaining Message Authentication Code
  Protocol), 253
CCTV (closed-circuit television), 346
CER (crossover error rate), 124, 154
CER certificate format, 262
CERT secure coding standards, 219
certificates
  certificate authorities (CAs), 257
  certificate chaining, 263
  certificate revocation list (CRL), 258
  certificate-signing request (CSR), 264
  RA (registration authority), 258, 264
  revocation, 146
  self-signed, 146
chain of custody, 405
chain of trust, 74
Challenge Handshake Authentication
  Protocol (CHAP), 124, 156
change management, 38, 218
CHAP (Challenge Handshake
  Authentication Protocol), 124, 156
chief privacy officer (CPO), 355
Choose Your Own Device (CYOD), 364,
    372–373
chosen plain-text attacks, 250
cipher-block chaining (CBC), 242, 255
ciphers
  Caesar, 234–235
cipher suites, 266
  Enigma machine, 237
  Feistel, 240
  multi-alphabet substitution, 235
  substitution, 234–235
  transposition, 235–236, 236
  Vernam, 241
  Vigenère, 235
circuit-level proxies, 86
clean desk policy, 23
clickjacking, 279, 306
client operating systems, 69
client-side validation, 219
cloaking, 172
closed-circuit television (CCTV), 346
cloud access security brokers (CASBs), 195
cloud computing. See also virtualization
   CASBs (cloud access security brokers), 195
   cloud platform services, 15
   community cloud, 184, 189–190
   elasticity, 32
   hybrid cloud, 185, 190
   IaaS (Infrastructure as a Service), 188, 188
   laws and regulations, 194
   multitenancy, 194
   PaaS (Platform as a Service), 186–187, 187
   private cloud, 185, 189
   public cloud, 185, 189
   review question answers, 426–427
   review questions, 197–200
   risks, 15–16
   SaaS (Software as a Service), 186, 187
   SECaaS (Security as a Service), 195–196
   XaaS (Anything as a Service), 189
cloud servers, 193
clustering, 33
code
   programming models, 216
   reuse, 224
   signing, 218, 257
   signing certificates, 263
   software testing, 217–218
cold aisles, 316, 340, 340
cold sites, 385, 401, 402
collisions, hashing algorithms, 249
collusion, 22
command injection attacks, 302
command-line tools
   arp, 138, 139
   ifconfig, 138
   ipconfig, 138–139, 139
   netcat, 141–142, 142
   netstat, 136, 136–137
   nmap, 139–141
   nslookup, 137, 138
   ping, 135, 135–136
   traceroute, 137
   tracert, 137, 137
   common access cards (CACs), 162
   community cloud, 184, 189–190
   companion viruses, 279, 285
   Company-Owned and -Provided Equipment (COPE), 364, 373
   compensating controls, 316, 348–349
   competition, as threat actor, 206–207
   compiled programs, 218
   computer certificates, 263
   computer restrictions, 378
   Computer Security Incident Response Team (CSIRT), 403
   confidential classification, 352
   confidentiality, cryptographic algorithms, 254
   configuration issues, 145–147, 210–211, 211
   configuration validation, 31
   consensus, social engineering principle, 326
   containerization, 370
   containers, 192
   content inspection, 88
   context-aware authentication, 370
   contingency plans, 30
   continuing education policies, 23
   continuity of operation planning
      failover, 386, 412
      tabletop exercises, 386, 412
   continuous monitoring, of server operations, 31
   control diversity, 61
   controlled incineration, 351
   controller-based access points, 110–111
   controls, 316
      administrative, 316, 349
      compensating, 316, 348–349
      corrective, 348
      detective, 317, 348
      deterrent, 348
      environmental, 339–345
      location-based, 378
COPE (Company-Owned and -Provided Equipment) – cryptography

physical, 317, 349
preventive, 348
technical, 318, 349
temperature and humidity, 345
COPE (Company-Owned and -Provided Equipment), 364, 373
corporate espionage, 206–207
corrective controls, 348
correlation engines, placement, 64
counter mode, 242
counterintelligence gathering, 405
CPO (chief privacy officer), 355
critical business functions (CBFs), 390
CRL (certificate revocation list), 258
cross-cut shredders, 351
cross-site request forgery (XSRF), 279, 302
cross-site scripting (XSS), 279, 302
crossover error rate (CER), 124, 154
cryptanalysis, 234
  birthday attacks, 251
  brute-force attacks, 234, 250
  chosen plain-text attacks, 250
dictionary attacks, 251
downgrade attacks, 252
frequency analysis, 250
human error, 252
known plain-text attacks, 250
related key attacks, 250
replay attacks, 252
weak key generation, 252
crypto-malware, 288
cryptographic systems, 254
  authentication, 257, 270–271
  confidentiality, 254
digital signatures, 256, 256–257
  integrity, 254–255
  nonrepudiation, 257
  strength, 254
when to encrypt data, 255–256
cryptography
  asymmetric algorithms, 243
    Diffie-Hellman, 245, 246
    ECC (Elliptic Curve Cryptography), 245–246
  ElGamal, 246
  RSA (Rivest, Shamir, Adleman), 239, 244–245, 246, 261
ciphers
  Atbash, 234–235
  Caesar, 234–235
  Feistel, 240
  multi-alphabet substitution, 235
  ROT13, 236–237
  substitution, 234–235
  transposition, 235–236, 236
  Vernam, 241
  Vigenère, 235
Enigma machine, 237
hashing algorithms, 247
  characteristics of hash functions, 247
  collisions, 249
  GOST, 248
  integrity, 254–255
  key stretching, 249
  LANMAN, 248
  MD (Message Digest Algorithm), 248
  NTLM (NT LAN Manager), 249
  rainbow tables, 249
  RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 248
  SHA (Secure Hash Algorithm), 248
historical methods, 234–238
implementation, 269–270
implementation issues, 247
Kerckhoff’s principle, 246–247
PKC (public key cryptography), 243
review questions, 273–276
review questions, answers, 428–429
standards, 258–259
  industry associations, 260–261
  U.S. government agencies, 259–260
  X.509, 261, 262–264
steganography, 143, 237
symmetric algorithms, 239, 239–243
  3DES (Triple-DES), 240
  AES (Advanced Encryption Standard), 239, 240, 242, 252
  Blowfish, 241
CAST, 240
DES (Data Encryption Standard), 240, 242, 250, 252
e execution modes, 242
GOST, 240
high resiliency, 242
IDEA (International Data Encryption Algorithm), 241
key exchange, 242
latency, 241
one-time pads, 241
PRNGs (pseudo-random number generators), 243
RC (Ron’s Cipher), 241
Twofish, 241
Wi-Fi encryption, 252–253
cryptology, 234
Crystal, 216
CSIRT (Computer Security Incident Response Team), 403
CSR (certificate-signing request), 264
CTM (counter mode), 242
CTR (counter mode), 242
custodians, 355
cutover tests, 412
CYOD (Choose Your Own Device), 364, 372–373
data retention policies, 355
data roles, 355
data sanitation tools, 142
data sovereignty, 406
databases
Big Data, 223
cybersecurity, 270
normalization, 204, 223
NoSQL, 204, 222
relational, 220–221
SQL. See SQL
tiered systems model, 221–222
DDoS (distributed denial-of-service) attacks, 280, 293, 297–298
vs. DoS attacks, 298
preventing, 298
zombies, 282, 293, 297
DDoS (distributed DoS) mitigator, placement, 64
deallocated memory, 215
dehatentication attacks, 176
Deep Sound, 143
default accounts/services, disabling, 70–73
defense in depth, 59–61
degaussing, 351
delivery models, cloud
community cloud, 184, 189–190
hybrid cloud, 185, 190
private cloud, 185, 189
public cloud, 185, 189
demilitarized zone. See DMZ
denial-of-service attacks. See DoS (denial-of-service) attacks
DEP (data execution prevention), 124, 151
deprecated algorithms, 252
DER certificate format, 262
DES (Data Encryption Standard), 240, 242, 250, 252
desensitizing, 343, 344
detective controls, 317, 348
deterrent controls, 348
development environment, 73
dial-in privileges, 157
dictionary attacks, 251, 279–280
differential backups, 385, 395, 399
Diffie-Hellman key exchange, 245, 246
DigiCert, 264
digital signatures, 256, 256–257
directory traversal attacks, 301–302
disabling default accounts/services, 70–73
disassociation attacks, 170, 176, 367
disaster recovery, 392
   backout plans, 400
   backup models, 396–399
   backup plans, 392–393
   backup types, 394–395
   recovery sites, 400–402
   review questions, 414–417
   review questions, answers, 432–433
system recovery, 399–400
discretionary access control (DAC), 160
disk duplexing, 35
disk mirroring (RAID 1), 35, 36
disk striping (RAID 0), 35, 36
disk striping with a parity disk (RAID 3),
   35, 36
disk striping with parity (RAID 5),
   35–36, 36
dissolvable agents, network access control
   (NAC), 112
distributed denial-of-service attacks. See
dDoS
distributive allocation, 32
DLL injections, 215
dLP (data loss prevention), 13, 111, 124, 151
dMZ (demilitarized zone), 47, 57–58, 58, 65
dNS poisoning, 304
dNS spoofing, 280, 304
DNS zone transfers, 138
documenting incident responses, 409–410
domain admin accounts, 375
domain hijacking, 304–305
domain name kiting, 304
domain validation certificates, 264
DoS (denial-of-service) attacks, 279, 293, 296–298
   buffer overflows, 279, 297, 299
disassociation, 170, 176
jamming, 171, 174–175
   preventing, 298
   resource exhaustion, 215
downgrade attacks, 252
driver manipulation, 307
   refactoring, 308
   shimming, 281, 307–308
drones, 213
dual-homed firewalls, 67, 86
dumpster diving, 322, 322
duplexing, 35
Dynamic Systems Development Model, 216

E
EAP (Extensible Authentication Protocol),
   270–271
EAP-FAST, 270
EAP-TLS, 270
EAP-TTLS, 270
ECB (Electronic Code Block), 242
ECC (Elliptic Curve Cryptography), 245–246
ECC-DH (Elliptic Curve Diffie Hellman),
   246
ECC-DSA (Elliptic Curve Digital Signature
   Algorithm), 246
EDGE (Enhanced Data Rates for GSM
   Evolution), 365
EF (exposure factor), 4, 8
elasticity, 32
electromagnetic interference (EMI), 60, 343
electromagnetic pulses (EMP), 69
Electronic Code Block (ECB), 242
electronic watermarking, 237
ElGamal, 246
Elliptic Curve Cryptography (ECC), 245–246
Elliptic Curve Diffie Hellman (ECC-DH),
   246
Elliptic Curve Digital Signature Algorithm
   (ECC-DSA), 246
email
   certificates, 264
   personal, 146
embedded systems, 204, 212–214
EMI (electromagnetic interference), 60, 343, 345
EMP (electromagnetic pulses), 69
Encapsulating Security Payload (ESP), 90
encryption. See also cryptographic systems; cryptography
Advanced Encryption Standard (AES), 239, 240, 242, 252
asymmetric algorithms. See asymmetric algorithms
data encryption, 269–270
DES (Data Encryption Standard), 240, 242, 250, 252
FDE (full disk encryption), 68
filesystem encryption, 238
hard drive encryption, 270
hardware-based devices, 269
human error, exploiting, 252
IDEA (International Data Encryption Algorithm), 241
IPSec (IP Security), 82, 90–91
KEK (key encryption key), 68
MEK (media encryption key), 68
Linux filesystems, 238
standards, 258–261
symmetric algorithms. See symmetric algorithms
voice encryption, 370
Wi-Fi encryption, 252–253
end users, as vulnerabilities, 211
end-entity certificates, 262
end-of-life systems, 212
Enhanced Data Rates for GSM Evolution (EDGE), 365
Enigma machine, 237
environmental controls, 339–340
EMI shielding, 343
fire suppression, 340–342
hot and cold aisles, 340, 340
HVAC, 340
temperature and humidity, 345
environmental threats, 8
ephemeral keys, 246
error handling, 214–215
escalation, 406
escalation of privilege, 281, 303, 387
ESP (Encapsulating Security Payload), 90
event deduplication, 111
event duplication, 111
evil twins, 170, 174, 177, 364, 368, 368
exception statements, 18
exit interviews, 23
exploitation frameworks, 135
exposure factor (EF), 4, 8
Extended TACACS (XTACACS), 158
extended validation certificates, 264
Extensible Authentication Protocol (EAP), 270–271
external media, 374
external threats, 8
extranets, 59
Extreme Programming (XP), 216
eye scanners, 153–154

facial recognition, 153–154
failover, 386
Fair Credit Reporting Act, 356
false acceptance rate (FAR), 124, 153–154
false positives, 27, 386, 389, 406
false rejection rate (FRR), 124, 154
familiarity, social engineering principle, 326
Family Educational Rights and Privacy Act (FERPA), 355, 356
FAR (false acceptance rate), 124, 153–154
Faraday cages, 69, 317, 337
fast flux, 304
fat access points, 110–111
fault tolerance, 34
distributive allocation, 32
FDE (full disk encryption), 68
Feature-Driven Development, 216
federation identities, 165
federations, 154
Feistel ciphers, 240
fencing, 332
FERPA (Family Educational Rights and Privacy Act), 355, 356
file integrity checking systems, 150
fingerprint scanners, 153–154
fire extinguishers, 341
fire rated containers, 391
fire suppression, 317, 341, 342, 344
fireproof containers, 391
firewalls, 65–66, 84–85, 85
  content inspection, 88
dual-homed, 67
dual-homed firewalls, 86
  logs, 149–150
NGFW (next generation firewall), 87
  packet filter, 66, 85–86
proxy, 66, 66–67, 86
  stateful packet inspection, 67, 87
  stateful packet inspection (SPI), 47, 67, 87
stateless, 67
URL filtering, 88
UTM (unified threat management)
  appliances, 87
WAFs (web application firewalls), 88–89
firmware, UEFI (Unified Extensible Firmware Interface), 68
first responders, 406
five nines availability, 32
fixed systems, 342
flood guards, 107
FOBs, 339
forced proxy, 107
forensics, 386, 404–405, 411–412
  order of volatility, 411
forward proxy, 107
forward secrecy, 242
frameworks
  ISA/IEC-62443, 53
  ISO (International Organization for Standardization), 48–50
  NERC (North American Electric Reliability Corporation), 50
  NIST (National Institute of Standards and Technology), 51–53
OWASP (Open Web Application Security Project), 54
PCI-DSS (Payment Card Data Industry Security Standard), 53, 53–54
frequency analysis, 250
FRR (false rejection rate), 124, 154
Full Archival backup method, 397–398, 398
  full backups, 386, 394, 395
full disk encryption, 68, 269–270
full distribution classification, 354
full hand scanners, 153–154
full tunnels, 91
fuzzing, 204, 217

G

Galois Counter Mode (GCM), 242
gates, 332
gauntlets, 339
GCM (Galois Counter Mode), 242
generator ID, 148
generic accounts, 376
geofencing, 370, 371
Ghost Rat, 293
GNU Privacy Guard (GPG), 265
GoGrid, 15
Good Time virus, 323
Google Code, 15
Google Hack Honeypot, 63
Googlebot, 293
GOST, 240, 242, 248
GPG (GNU Privacy Guard), 265
GPS tracking, 370
Gramm-Leach-Bliley Act, 356
Grandfather, Father, Son backup method, 396–397, 397
grey box testing, 388
group-based control, 160
group-based permissions, 160
GSM (Global System for Mobile Communications), 364, 365
guards, 333
guest accounts, 70, 375
guidelines, 20
HA (high availability), 32
hacktivists, 205
handshakes, SSL, 266–268
hard drive encryption, 270
hardening
applications, 204
  baselining, 219
  open source intelligence, 207–210
  patch management, 220
  programming models, 216
  secure coding standards, 218–219
  software testing, 217–218
operating systems, 55–56
hardware security modules (HSMs), 68, 82, 115, 269
hash-based message authentication code (HMAC), 255
hashing algorithms, 247
  characteristics of hash functions, 247
  collisions, 249
  GOST, 248
  integrity, 254–255
  key stretching, 249
  LANMAN, 248
  MD (Message Digest Algorithm), 248
  NTLM (NT LAN Manager), 249
  rainbow tables, 249
  RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 248
  SHA (Secure Hash Algorithm), 248
 heuristic systems, 96
HIDS (host-based IDS), 82, 102–103, 103, 147–148
hierarchical storage management (HSM), 395
hierarchical trust model, 258
high availability (HA), 32
high resiliency, 242
hijacking, 306
  clickjacking, 279, 306
  domain, 304–305
  session, 306–307
TCP/IP, 280, 299
URL, 281, 307
HIPS (host-based intrusion prevention systems), 147–148
HMAC (hash-based message authentication code), 255
hoaxes, 317, 323, 324
Honeyd, 63
Honeynet Project, 143
honeynets, 47, 62–63
honeypots, 47, 62–63, 143
host health checks, 112
host-based IDS (HIDS), 82, 102–103, 103
hosted servers, 192–193
hot aisles, 317, 340, 340
hot sites, 386, 401
hotfixes, 220
HSM (hierarchical storage management), 395
HSMs (hardware security modules), 68, 82, 115, 269
human error, 252
humidity control, 345
HVAC (heating, ventilation, and air-conditioning) systems, 340
hybrid cloud, 185, 190
hybrid trust model, 258
ehypervisors, 190–192

I

IaaS (Infrastructure as a Service), 188, 188
IaC (Infrastructure as Code), 204, 223
IDEA (International Data Encryption Algorithm), 241
identification, 151–152
IDS (intrusion detection systems), 147–148
  active IDS, 97
  active responses, 100–102
  activities, 93
  AD-IDS (anomaly-detection IDS), 82, 95–96, 96
  administrators, 93
  alerts, 93
analysts, 93–94
anomaly-detection systems, 95–96
behavior-based detection, 94
data source, 94
events, 94
heuristic systems, 96
HIDS (host-based IDS), 82, 102–103, 103, 147–148
vs. intrusion prevention systems, 97
managers, 94
MD-IDS (misuse-detection IDS), 94–95, 95
NIDS (network-based IDS), 97, 97–98
notification, 94
operators, 94
passive responses, 99–100
placement, 64
sensors, 94
signature-based detection, 94–95, 95
IEEE (Institute of Electrical and Electronics Engineers), 261. See also 802.11
standards
PKIX (Public Key Infrastructure X.509), 261
IETF (Internet Engineering Task Force), 260–261
ifconfig command, 138–139
immutable systems, 223
impersonation, 317, 319, 322
implicit deny, 82, 85
in-band key exchange, 242
in-band management, 97
incident response, 404–405
adjusting procedures, 410
chain of custody, 405
documenting/reporting response, 409–410
forensics, 404–405, 411–412
identifying incidents, 405–407
investigating incidents, 407–408
repairing damage, 408–409
review questions, 414–417
review questions, answers, 432–433
incremental backups, 386, 394, 395
indicators of compromise, 96
industry-standard frameworks. See frameworks
information security management system (ISMS), 47, 49
infrared communications, 368–369
infrared detectors, 348
infrastructure
access points, 108–111
bridges, 113
DLP (data loss prevention), 111–112
firewalls, 84–85
content inspection, 88
packet filter, 85–86
proxy, 86
stateful, 87
stateless, 87
URL filtering, 88
UTM (unified threat management) appliances, 87
WAFs (web application firewalls), 88
IDS (intrusion detection systems), 91–93
active responses, 100–102
activities, 93
administrators, 93
alerts, 93
analyzers, 93–94
anomaly-detection systems, 95–96
behavior-based detection, 94
data source, 94
events, 94
heuristic systems, 96
vs. intrusion prevention systems, 97
managers, 94
notification, 94
operators, 94
passive responses, 99–100
sensors, 94
signature-based detection, 94–95, 95
load balancers, 108
mail gateways, 112–113
NAC (network access control), 112
proxies, 107
review questions, 116–119
review questions, answers, 422–423
routers, 104–106
SIEM (security information and event management), 111
SSL accelerators, 113
SSL decryptors, 113
switches, 106–107
TPMs (trusted platform modules), 114–115
VPNs (virtual private networks), 89–91
web security gateways, 114
Infrastructure as a Service (IaaS), 188, 188
Infrastructure as Code (IaC), 204, 223
initial exploitation, 387
initialization vector (IV) attacks, 171, 173
injection attacks, 299–302
  command injection, 302
directory traversal, 301–302
LDAP injection, 301
SQL injection, 300–301
XML injection, 301
inline proxy, 107
input validation, 214
insiders, as threat actors, 206
integer overflows, 280
integration testing, 217
integrity measurement, 74
intercepting proxy, 107
interconnection security agreement (ISA), 4, 21
interference, 170, 172, 177. See also
  jamming
internal threats, 8
International Data Encryption Algorithm
  (IDEA), 241
International Organization for
  Standardization (ISO), 48–50
Internet Engineering Task Force (IETF), 260–261
Internet of Things (IoT), 204, 213
intimidation, social engineering principle, 326
intranets, 58–59
intrusion detection systems. See IDS
intrusion prevention systems. See IPS
intrusive tests, 388
Invisible Secrets, 143, 237
IoT (Internet of Things), 204, 213
IP spoofing, 280, 308–309
ipconfig command, 138–139, 139
IPS (intrusion prevention systems)
  HIPS (host-based intrusion prevention systems), 147–148
  vs. intrusion detection systems, 97
NIPSs (network intrusion prevention systems), 103
IPSec (IP Security), 82, 90–91
Irina virus, 323
ISA (interconnection security agreement), 4, 21
ISA/IEC-62443 standards, 53
island hopping, 387
ISMS (information security management system), 47, 49
ISO (International Organization for
  Standardization), 48–50
IV (initialization vector) attacks, 171, 173

J
Jack, Barnaby, 213
jailbreaking, 373
jamming, 171, 174–175. See also interference
JFS (journaled file system), 391
job rotation policy, 22
journaled file system (JFS), 391

K
KDC (key distribution center), 156–157
Keccak, 248
KEK (key encryption key), 68
Kerberos, 156, 156–157
Kerckhoff’s principle, 246–247
key distribution center (KDC), 156–157
key encryption key (KEK), 68
key escrow, 258
key exchange, 242
key management, 348
key recovery agents, 258
key registration, 258
key stretching, 249
keyloggers, 292
kiosk operating systems, 69
Klex32, 288
known plain-text attacks, 250

L
LanHelper, 129, 129
LANMAN protocol, 248
LDAP (Lightweight Directory Access Protocol), 155, 301
LDAPS (secure LDAP), 155
Lean Software Development, 216
LEAP (Lightweight Extensible Authentication Protocol), 270
least functionality, 70
least privileges, 144, 376, 377–378
least significant bit (LSB), 237
legal hold, 405
license compliance violations, 147
lighting, 331
Lightweight Directory Access Protocol (LDAP), 155, 301
Lightweight Extensible Authentication Protocol (LEAP), 270
likelihood assessment scale, 10
limited distribution information, 353
Linux
   backups, 396
   commands, information about, 93
discretionary access control (DAC), 160
filesystem encryption, 238
ifconfig, 138–139
log files, 104
Nessus vulnerability scanner, 132–133, 133
netcat, 141–142, 142
netstat, 136, 136–137
nmap, 139–141
ping, 135, 135–136
root account, 375
security information resources, 92
tcpdump, 125, 126
traceroute, 137
load balancers, 32, 108
placement, 64
location-based controls, 378
lock types, 337–338
lockouts, 369
logic bombs, 280, 293–294, 294
logical subnetwork segments, 60
logs, 347
   active logging, 405
   firewall logs, 149–150
Linux, 104
LSB (least significant bit), 237
LTE (Long-Term Evolution) standard, 364, 365

M
MAC (mandatory access control), 159
MAC (message authentication code), 255, 255
MAC filtering, 109
MAC spoofing, 308–309
machine certificates, 263
machine-based restrictions, 378
macro viruses, 280, 285
mafia, as threat actor, 206
mail gateways, 112–113
malicious code, 280
   antivirus software, 287
   bots, 293
   logic bombs, 280, 293–294, 294
   MSRT (Malicious Software Removal Tool), 88
   Trojan horses, 281, 289
   viruses. See viruses
   worms, 288, 289
malicious insider threats, 280, 325
malware
   adware, 279, 292
   backdoors, 279, 294, 295
bots, 279, 293
crypto-malware, 288
DLL injection, 215
inspection, 88
keyloggers, 292
logic bombs, 280, 293–294, 294
ransomware, 281, 288
RAT (remote administration tool), 293
rootkits, 281, 290
spyware, 281, 292–293
Trojan horses, 281, 289
viruses, 281
antivirus software, 287
armed, 279, 285
companion, 279, 285
macro, 280, 285
multipartite, 280, 285
phage, 281, 285
polymorphic, 281, 285–286
retrovirus attacks, 281, 286
spam, 286–287
spreading of, 283, 283–284, 284
stealth, 281, 286
symptoms of infection, 282–283
worms, 288, 289
Malwarebytes, 148, 148–149
man-hours, tracking, 412
man-in-the-browser attacks, 305
man-in-the-middle attacks, 280, 298–299, 299
mandatory access control (MAC), 159
mandatory vacation policy, 22
manmade threats, 8
mantraps, 317, 336–337, 337
maximum tolerable downtime (MTD), 4
MBSA (Microsoft Baseline Security Analyzer), 133, 133–134
MD (Message Digest Algorithm), 248
MD-IDS (misuse-detection IDS), 94–95, 95
mean time between failures (MTBF), 4, 5, 11
mean time to failure (MTTF), 4, 11
mean time to restore (MTTR), 4, 11
media encryption key (MEK), 68
media sanitation, 350–352
medical devices, 213
MEK (media encryption key), 68
memes, 324
memorandum of agreement (MOA), 4, 21
memorandum of understanding (MOU), 4, 21
memory leaks, 215
memory-related vulnerabilities, 215
mesh trust model, 258
message authentication code (MAC), 255, 255
Message Digest Algorithm (MD), 248
Metasploit, 135
microphones, mobile devices, 374
Microsoft. See also Windows
IIS security guidelines, 55
MBSA (Microsoft Baseline Security Analyzer), 133, 133–134
TechNet, 55
Windows Security page, 55
Microsoft Baseline Security Analyzer (MBSA), 133, 133–134
middle-tier servers, 222
misuse-detection IDS (MD-IDS), 94–95, 95
MITB (man-in-the-browser) attacks, 305
MOA (memorandum of the browser), 4, 21
mobile devices
application control, 370
asset tracking, 371
connection methods, 365
ANT, 368
Bluetooth, 365
cellular, 365
infrared, 368–369
NFC (near field communications), 368
SATCOM (satellite communications), 369
Wi-Fi, 366–368
content management, 371
context-aware authentication, 370
deployment models
BYOD (Bring Your Own Device), 364, 371–373
COPE (Company-Owned and Provided Equipment), 373
CYOD (Choose Your Own Device), 364, 372–373
VDI (Virtual Desktop Infrastructure), 373
device access control, 371
device encryption, 370
enforcement issues, 373–374
geofencing, 370, 371
minimum security measures, 369–371
push notifications, 371
remote wipe, 379
rooting, 373
screen locks, 369
sideloading, 373
storage segmentation, 370
tethering, 374
mobile operating systems, 69
mobile VPNs, 91
model verification, 217
motion detection systems, 347
MOU (memorandum of understanding), 4, 21
MS-CHAP, 156, 270
MSRT (Malicious Software Removal Tool), 88
MTBF (mean time between failures), 4, 5, 11
MTD (maximum tolerable downtime), 4
MTTF (mean time to failure), 4, 11
MTTR (mean time to restore), 4, 11
multi-alphabet substitution ciphers, 235
multifactor authentication, 153
multipartite viruses, 280, 285
multiple barrier systems, 330, 331
multitenancy, 194
multithreaded applications, 215
mutation, 286
mutual authentication, 152
MyDLP, 111
naming conventions, 378
NAT (network address translation), 65
nation-state attacks, 206
National Bureau of Standards (NBS), 260
National Institute of Standards and Technology. See NIST
National Institute of Standards and Technology (NIST), 51–53, 260
National Security Agency (NSA), 259
National Security Agency/Central Security Service (NSA/CSS), 259
National Software Reference Library (NSRL), 411
NBS (National Bureau of Standards), 260
NDAs (nondisclosure agreements), 353
near field communications (NFC), 171, 176, 368, 374
need-to-know basis, 353
NERC (North American Electric Reliability Corporation), 50
Nessus vulnerability scanner, 132–133, 133
NetBus, 294
netcat utility, 141–142, 142
netstat command, 136, 136–137
network access control (NAC), 83, 112
network address translation (NAT), 65
network design
defense in depth, 59–61
firewalls
network segmentation, 59–61, 60
VPNs (virtual private networks), 63, 63–64
wireless segmentation, 59
zones, 57
control diversity, 61
DMZ (demilitarized zone), 57–58, 58
extranets, 59
honeynets, 62–63
honeypots, 62–63
intranets, 58–59
network segmentation, 59–61, 60
vendor diversity, 61–62
wireless, 59
network operating systems, 69

N

N+1 redundancy strategy, 34
NAC (network access control), 83, 112
network scanning, 127
   LanHelper, 129, 129
   SolarWinds, 127, 128
   wireless, 129–130
network segmentation, 59–61, 60
next generation firewall (NGFW), 87
NFC (near field communications), 171, 176, 368, 374
NGFW (next generation firewall), 87
NIDS (network-based IDS), 97, 97–98
NIPSs (network intrusion prevention systems), 103
NIST (National Institute of Standards and Technology), 51–53, 260
   National Software Reference Library (NSRL), 411
nmap command, 139-141
nonce, 243
nondisclosure agreements (NDAs), 353
nonintrusive tests, 388
nonpersistent images, 32
nonrepudiation, 257
nontransitive trusts, 155
NoSQL, 204, 222
Nova Network Security, 143
NSA (National Security Agency), 259
NSA/CSS (National Security Agency/Central Security Service), 259
nslookup command, 138
NSRL (National Software Reference Library), 411
NTLM (NT LAN Manager), 248, 249
one-click attacks, 302
one-tier model, 221
one-time pads, 241
one-time passwords, 158–159
Online Certificate Status Protocol (OCSP), 258
onsite storage, 391
OOV (order of volatility), 411
Open Authorization (OAUTH) standard, 125
Open Shortest Path First (OSPF), 106
open source intelligence, 207–210, 208, 209, 210
Open Stego, 143
Open Web Application Security Project (OWASP), 54, 204, 218–219
OpenPhish, 208, 208
operating systems
   hardening, 55–56
   patch management, 70, 220
   RTOSSs (real-time operating systems), 213
   secure configurations, 70–73
Ophcrack, 131, 132, 249
order of volatility (OOV), 411
organized crime, as threat actors, 206
OSINT Framework, 209, 209
OSPF (Open Shortest Path First), 106
OTA (Over-the-Air) updates, 373
out-of-band authentication, 152
out-of-band key exchange, 242
out-of-band management, 97
Over-the-Air (OTA) updates, 373
overwriting, 352
OWASP (Open Web Application Security Project), 54, 204, 218–219
OWASP ZAP, 134, 134
owners, 355

O
OAUTH (Open Authorization) standard, 125, 158
OCSP (Online Certificate Status Protocol), 258
offboarding, 377–378
offsite storage, 391
omnidirectional antennas, 110
on-premise servers, 192–193
onboarding, 23, 377
P
P12 certificate format, 262
PaaS (Platform as a Service), 186–187, 187
packet filter firewalls, 66, 85–86
Pan, Tilt, and Zoom (PTZ) cameras, 318, 346
PAP (Password Authentication Protocol), 155
parallel tests, 412
parity information, 35
PASS (Pull, Aim, Squeeze, and Sweep)
method, 317, 341
pass the hash attacks, 306
passive reconnaissance, 387
passive responses, 99–100
passive vulnerability scanners, 132
Password Authentication Protocol (PAP), 155
Password-Based Key Derivation Function 2
(PBKDF2), 249
passwords
age, 375
complexity, 375
crackers, 130–131
history, 375
for mobile devices, 369–370
one-time, 158–159
patch management, 70, 150, 220
Payment Card Data Industry Security
Standard (PCI-DSS), 53, 53–54
PBKDF2 (Password-Based Key Derivation
Function 2), 249
PCI-DSS (Payment Card Data Industry
Security Standard), 53, 53–54
PDS (protected distribution system), 335–336
PEAP (Protected Extensible Authentication
Protocol), 270
PEM certificate format, 262
penetration testing, 12, 387–389
perfect forward secrecy, 242
perimeter security, 317, 330, 331, 332
peripherals, 73
permanent agents, network access control
(NAC), 112
permissions
DAC (discretionary access control), 160
least privileges, 144, 376, 377–378
smartcards, 161–162
persistence, 387
personal email, 146
personal health information (PHI), 355
personal identity verification (PIV),
162, 317
personally identifiable information (PII), 12,
47, 50, 317, 354–355
personnel issues, 146
personnel policies, 22–25
PFX certificate format, 262
PGP (Pretty Good Privacy), 264–265, 265
phage viruses, 281, 285
PHI (personal health information), 355
phishing, 318, 320
spear phishing, 318, 320
vishing, 318, 320, 321
whaling, 318, 320
physical barriers, 330, 331
physical controls, 317, 349
physical security
air gaps, 336
alarms, 333
biometric systems, 338–339
cable locks, 345, 345
cold aisles, 340, 340
environmental controls, 339–340
Faraday cages, 317, 337
fire extinguishers, 341
tions, 342
salars, 333
hot aisles, 340, 340
HVAC (heating, ventilation, and air-
conditioning) systems, 340
infrared detectors, 348
key management, 348
lighting, 331
lock types, 337–338
log files, 347
mantraps, 336–337, 337
motion detection systems, 347
PDS (protected distribution system),
335–336
perimeter security, 332
protected cabling, 336
safes, 334
screen filters, 346
signs, 331–332
temperature and humidity controls, 345
video surveillance, 346
physical tokens, 339
PIA (privacy impact assessment), 12
PII (personally identifiable information), 12, 47, 50, 317, 354–355
ping of death, 297
ping utility, 135, 135–136
pinning, 263
PIV (personal identity verification), 162, 317
PKC (public key cryptography), 243
PKI (public key infrastructure), 264
data encryption, 269–270
hardware-based encryption, 269
HSM (hardware security module), 82, 115
PGP (Pretty Good Privacy), 264–265, 265
SSL (Secure Sockets Layer), 266–268, 267
TLS (Transport Layer Security), 266, 268, 268–269
PKIX (Public Key Infrastructure X.509), 261
Platform as a Service (PaaS), 186–187, 187
pod slurping, 24
point-to-point connections, 270–271
Point-to-Point Tunneling Protocol (PPTP, 88, 89
pointer dereferencing, 215
policies
accountability statements, 19
application policies, 25
exception statements, 19
v.s. guidelines, 18
for personnel, 22–25
network policies, 25
policy overview statements, 18
policy statements, 18
scope statement, 17–18
social media policies, 25
standards, 18–19
vendor policies, 21
polymorphic malware, 285–286
polymorphic viruses, 281, 285–286
pons, 135
port mirroring, 64, 98
port spanning, 98
post-mortems, 411
power level controls, 110
PPTP (Point-to-Point Tunneling Protocol), 88, 89
Pretty Good Privacy (PGP), 264–265, 265
preventive controls, 317, 348
printers, 213
privacy filters, 318, 346
privacy impact assessment (PIA), 12
privacy issues, 12
privacy officer, 355
privacy threshold assessment (PTA), 12
private cloud, 185, 189
private information, 352
privileged accounts, 375
privilege audits, 377
privilege escalation, 281, 303, 387
PRNGs (pseudo-random number generators), 233, 243
programming models, 216
proprietary classification, 354
protected cabling, 336
protected distribution system (PDS), 335–336
Protected Extensible Authentication Protocol (PEAP), 270
protected health information, 355
protocol analyzers, 125
tcpdump, 125, 126
Wireshark, 126, 126–127, 127
prototyping, 204, 216, 216
proxies, 107
proximity cards, 330
proximity readers, 330
proxy firewalls, 66, 66–67, 86
pseudo-random number generators (PRNGs), 243
PTA (privacy threshold assessment), 12
PTZ (Pan, Tilt, and Zoom) cameras, 318, 346
public cloud, 185, 189
public information, 353–354
pulping, 351
pulverizing, 351
purging data, 352
push notifications, 371
pwdump, 130–131
qualitative risk assessment, 9–10
quantitative risk assessment, 9–10
QuickStego, 237

RA (registration authority), 258, 264
race conditions, 215
RACE Integrity Primitives Evaluation
Message Digest (RIPEMD), 248
radio frequency identification (RFID), 171, 176
radio frequency interference (RFI), 343, 344
RADIUS (Remote Authentication Dial-In
User Service), 158, 158–159
RAID (Redundant Array of Independent
Disks), 35–38, 36
rainbow tables, 233, 249, 249, 252
ransomware, 281, 288
RAT (remote administration tool), 293
RBAC (role-based access control), 160–161
RBAC (rule-based access control), 160–161
RC (Ron’s Cipher), 241
RC4, 241
RDS (Reference Data Set), 411
real-time operating systems (RTOSs), 213
recertification, 377
reciprocal agreements, 401
recovery point objective (RPO), 4, 11
recovery sites, 400–402
recovery time objective (RTO), 5, 11
redundancy, 33
distributive allocation, 32
refactoring, 308
reference architectures
ISA/IEC-62443, 53
ISO (International Organization for
Standardization), 48–50
NERC (North American Electric
Reliability Corporation), 50
NIST (National Institute of Standards
and Technology), 51–53
OWASP (Open Web Application Security
Project), 54
PCI-DSS (Payment Card Data Industry
Security Standard), 53, 53–54
Reference Data Set (RDS), 411
registration authority (RA), 258, 264
regression testing, 218
related key attacks, 250
relational databases, 220–221
remote access, 89
remote administration tool (RAT), 293
remote attestation, 68
remote wipes, 370
replay attacks, 171, 172–173, 252, 305, 306
request for comments (RFC), 260
residual risk, 3
resiliency, 33
resource exhaustion, 215
restricted information, 352–353
retrovirus attacks, 281, 286
reverse proxy, 107
revert to known state, 32
revision ID, 148
RFC (request for comments), 260
RFI (radio frequency interference),
343, 344
RFID (radio frequency identification),
171, 176
Rijmen, Vincent, 240
Rijndael algorithm, 240
RIP (Routing Information Protocol), 106
RIPEMD (RACE Integrity Primitives
Evaluation Message Digest), 248
risks
acceptance, 13–14
appetite, 14
assessment, 6
calculations, 8–9
measurements, 10–12
privacy issues, 12
process components, 6–7
quantitative vs. qualitative, 9–10
avoidance, 12–13
with cloud computing, 15–16
management
best practices, 28–38
change management, 38
threat assessment, 6
mitigation, 13
policies. See policies
residual, 3
resiliency, 33
review questions, 40–43
review questions, answers, 420–421
transference, 13
with virtualization, 16–17
Rivest, Ron, 241
rogue access points, 171, 174, 177, 368
disassociation attacks, 170, 176
evil twins, 170, 174, 177, 368
rogue detection systems, 127. See also
network scanning
role-base awareness training, 23–24
role-based access control (RBAC), 160–161
roll back to a known configuration, 32
root certificates, 263
root of trust (RoT), 68–69
rooting mobile devices, 373
rootkits, 281, 290
RoT (root of trust), 68–69
ROT13 cipher, 236–237
round-robin load balancing, 108
routers, 104–106
Routing Information Protocol (RIP), 106
RPO (recovery point objective), 4, 11
RSA (Rivest, Shamir, Adleman) algorithm,
239, 244–245, 246, 261
RTO (recovery time objective), 5, 11
RTOSs (real-time operating systems), 213
runtime programs, 218

salami attacks, 23
Salesforce.com, 15
Salt, 233, 249
SAML (Security Assertion Markup
Language), 159
SAN (Subject Alternative Name), 263
sandboxing, 74, 193, 204, 223
Sarbanes-Oxley, 15
SATCOM, 369
SCADA (Supervisor Control and Data
Acquisition) systems, 213
scalability, 32
scarcity, social engineering principle, 326
scheduling load balancing, 108
Scherbius, Arthur, 237
scope statements, 17–18
screen filters, 346
screen locks, 369
script kiddies, 204–205
Scrum, 216
SDKs (software development kits), 224
SDN (software-defined networking), 47, 67, 67
SECaaS (Security as a Service), 195–196
secure baselines, 74
secure boot, 68
secure coding, 218–219
Secure Hash Algorithm (SHA), 248
secure LDAP (LDAPS), 155
Secure Multipurpose Internet Mail
Extensions (S/MIME), 263
Secure Sockets Layer. See SSL
SecurID, 339
Security as a Service (SECaaS), 195–196
Security Assertion Markup Language
(SAML), 159
security baseline, 145
security cameras, 214, 346
security guards, 333
security information and event management
(SIEM), 83, 111
security through obscurity, 247
security tokens, 162
security topology, 84

S

S/MIME (Secure Multipurpose Internet Mail
Extensions), 263
SaaS (Software as a Service), 185, 186, 187
safes, 334
SEDs (self-encrypting drives), 68
segmentation
mobile devices, 370
network segmentation, 59–61, 60
wireless segmentation, 59
self-encrypting drives (SEDs), 68
self-signed certificates, 146, 263
sending them to the honeypot, 101
separation of duties policies, 22
server operating systems, 69
server-side validation, 219
service models
IaaS (Infrastructure as a Service), 188
PaaS (Platform as a Service), 186–187, 187
SaaS (Software as a Service), 186, 187
service packs, 220
session hijacking, 306–307
session riding, 302
SFA (single-factor authentication), 152, 153
SHA (Secure Hash Algorithm), 248
shadow copies, 390
Shibboleth, 159
shielding, 337
EMI (electromagnetic interference), 343
Faraday cages, 337
TEMPEST shielding protection, 344
shimming, 281, 307–308
Shiva Password Authentication Protocol
(SPAP), 156
Shodan, 209, 210
shoulder surfing, 318, 322–323, 323
shredding, 351
shunning, 99
sideloading, 373
SIEM (security information and event
management), 83, 111
Signature ID, 148
signature-based detection, 94–95, 95
signs, 331–332
simulations, 412
model verification, 217
single loss expectancy (SLE), 5, 8–9
single point of failure (SPOF), 5, 30
single-factor authentication (SFA), 152, 153
single-tier environment, 221
tsit surveys, 172
SLE (single loss expectancy), 5, 8–9
smart technology, 213
smartcards, 161–162
Snort ID, 148
SNORT IDS/IPS, 148
SoC (system-on-a-chip), 213
social engineering, 146, 318–320
attack examples, 327
attack motivations, 325
dumpster diving, 322, 322
hoaxes, 323, 324
impersonation, 322
phishing, 320
principles, 326–327
review questions, 358–361
review questions, answers, 430–431
shoulder surfing, 322, 323
tailgating, 320, 321
testing, 328
vishing, 320, 321
watering hole attacks, 282, 324–325
whaling, 320
social media, 25, 146
software
development models, 216
exploitation, 288
Software as a Service (SaaS), 185, 186, 187
software-defined networking (SDN), 47, 67, 67
testing, 217–218
unauthorized, 146–147
SolarWinds, 127, 128
SOP (standard operating procedure), 21
spam, 286–287
spam over instant messaging (SPIM), 287
spam over Internet telephony (SPIT), 287
SPAP (Shiva Password Authentication
Protocol), 156
spear phising, 318, 320
SPI (stateful packet inspection), 47, 67, 87
SPIM (spam over instant messaging), 287
SPIT (spam over Internet telephony), 287
split tunnels, 91
SPOF (single point of failure), 5, 30
spoofing, 281, 308, 308–309
antispoofing protections, 105
ARP spoofing, 279, 304
DNS spoofing, 280
IP spoofing, 280, 308–309
MAC spoofing, 308–309
Spybot, 292
spyware, 281, 292–293
Spyware Doctor, 292
SQL (Structured Query Language), 204, 220–222

vs. NoSQL, 222
SQL injection attacks, 214, 300–301
stored procedures, 204, 223
validation, 219
SSID (Service Set Identifier), 171–172
SSL (Secure Sockets Layer), 266–268, 267
accelerators, 113
decryptors, 113
handshakes, 266–268
RC4, 241
staging, 73–74
stand-alone access points, 110–111
standard operating procedure (SOP), 21
standards
ISA/IEC-62443, 53
ISO (International Organization for Standardization), 48–50
NERC (North American Electric Reliability Corporation), 50
NIST (National Institute of Standards and Technology), 51–53
OWASP (Open Web Application Security Project), 54
PCI-DSS (Payment Card Data Industry Security Standard), 53, 53–54
secure coding, 218–219
stapling, 258
stateful inspection, 67
stateful packet inspection (SPI), 47, 67
stateful packet inspection firewalls, 67, 87
stateless firewalls, 67
static
code analyzers, 215
firewalls, 85–86
password tokens, 162
stealth viruses, 281, 286
steganography, 143, 237
stewards, 355
storage mechanisms, 390–391
stored procedures, 204, 223
strategic intelligence, 405
strength, of cryptographic system, 254
stress testing, 204, 217
Stuxnet, 305
Subject Alternative Name (SAN), 263
substitution ciphers, 234–235
Atbash cipher, 234–235
Caesar cipher, 234–235
Enigma machine, 237
multi-alphabet ciphers, 235
ROT13 cipher, 236–237
Vigenère cipher, 235
Super Wi-Fi, 366
supply chain, 11, 69
surrogate proxy, 107
switches, 106–107
Symantec Decoy systems, 63
symmetric algorithms, 239, 239–243
3DES (Triple-DES), 240
AES (Advanced Encryption Standard), 239, 240, 242, 252
Blowfish, 241
CAST, 240
DES (Data Encryption Standard), 240, 242, 250, 252
execution modes, 242
GOST, 240
high resiliency, 242
IDEA (International Data Encryption Algorithm), 241
system images – trigger criteria

Kerckhoff’s principle, 246–247
key exchange, 242
latency, 241
one-time pads, 241
PRNGs (pseudo-random number generators), 243
Ron’s Cipher, 241
Twofish, 241
system images, 411
System Restore, 395
system sprawl, 212
system testing, 217
system-on-a-chip (SoC), 213
systems design
hardware, 68–69
operating systems, 69–73
peripherals, 73
staging deployments, 73–74

T
tabletop exercises, 412
TACACS (Terminal Access Controller Access Control System), 158
TACACS+, 158
tailgating, 318, 320, 321
Tavares, Stafford, 240
TCP SYN flood DoS attacks, 297
TCP/IP hijacking, 280, 299
tcfdump, 125, 126
technical controls, 318, 349, 350
temperature and humidity controls, 345
TEMPEST shielding protection, 344
Temporal Key Integrity Protocol (TKIP), 173, 253
Terminal Access Controller Access Control System (TACACS), 158
test environment, 73
tethering, 374
TGT (ticket granting ticket), 157
thin access points, 110–111
third-party libraries, code reuse, 224
ThreatCrowd, 207, 208
threats
environmental, 8
external, 8
internal, 8
manmade, 8
open source intelligence, 207–210
threat actors, 203–204
competitors, 206–207
hacktivists, 205
insiders, 206
nation states, 206
organized crime, 206
script kiddies, 204–205
vectors, 11
three-tier model, 222
ticket granting ticket (TGT), 157
tiered systems database model, 221–222
time synchronization, 111
time-of-day restrictions, 377
TKIP (Temporal Key Integrity Protocol), 173, 253
TLS (Transport Layer Security), 91, 266, 268, 268–269
accelerators, 113
domain validation certificates, 264
downgrade attacks, 252
EAP (Extensible Authentication Protocol) versions, 270
RC4, 241
tokens, 162
TOTP (time-based one-time password), 158
Tower of Hanoi backup method, 397
TPMs (trusted platform modules), 68, 114–115, 269
tracert command, 137, 137
transitive access, 154–155
transitive trust, 154–155
transparent proxy, 107
Transport Layer Security. See TLS
Transport mode, IPSec, 91
transposition ciphers, 235–236, 236
trigger criteria, 111
Triple-DES (3DES), 240
Tripwire, 112, 150
Trojan horses, 281, 289
TrueCrypt, 115
trust models, 258
trust, social engineering principle, 326
Trusted Computing Group, 269
trusted platform modules (TPMs), 68, 114–115, 269
Tunneling mode, IPSec, 91
tunneling protocols, 63–64
two-factor authentication, 153
two-tier model, 222
Twofish, 241
Type I errors, 27
Type I hypervisors, 185, 190–192, 191
Type II errors, 27
Type II hypervisors, 185, 190–192, 191
Type III errors, 27
typo squatting, 281, 307

URL hijacking, 281, 307
usage audits, 377
USB OTG (On the Go), 374
use policies, 24
user acceptance testing, 218
user accounts, 375
user certificates, 263
user training, 62
USM (unified security management) systems, 151
UTM (unified threat management), 87, 151

U

UAVs (unmanned aerial vehicles), 213
UEFI (Unified Extensible Firmware Interface), 68
UMTS (Universal Mobile Telecommunications Systems), 364, 365
unauthorized software, 146–147
undocumented assets, 212
unified security management) systems (USMs), 151
unified threat management (UTM), 87, 151
uninterruptible power supply (UPS), 34
unit testing, 217
Universal Mobile Telecommunications Systems (UMTS), 364, 365
Unix, discretionary access control (DAC), 160
unmanned aerial vehicles (UAVs), 213
UPS (uninterruptible power supply), 34
urgency, social engineering principle, 327
URL filtering, 88

V

Van Eck phreaking, 343
VDE (virtual desktop environment), 185, 192
VDI (virtual desktop infrastructure), 185, 192, 373
vendor diversity, 61–62
VeraCrypt, 270
Verisign, 264
Vernam cipher, 241
version control, 218
video surveillance, 346
Vigenère cipher, 235
VIP (virtual IP), 108
virtual datacenters, 32
virtual desktop environment (VDE), 185, 192
virtual desktop infrastructure (VDI), 185, 192, 373
virtual IP (VIP), 108
virtual local area networks (VLANs), 60
virtualization, 61. See also cloud computing
application cells, 192
containers, 192
hypervisors, 190–192
IaaS (Infrastructure as a Service), 188, 188
SDNs (software-defined networks), 67
server models, 192–193
VDE (virtual desktop environment), 185, 192
VDI (virtual desktop infrastructure), 185, 192
VM escape, 185, 193
VM sprawl, 185, 193
viruses, 281, 282
antivirus software, 287
armored, 279, 285
companion, 279, 285
macro, 280, 285
multipartite, 280, 285
phage, 281, 285
polymorphic, 281, 285–286
retrovirus attacks, 281, 286
spam, 286–287
spreading of, 283, 283–284, 284
stealth, 281, 286
symptoms of infection, 282–283
vishing, 318, 320, 321
VLANs (virtual local area networks), 60
VM escape, 185, 193
VM sprawl, 185, 193
voice encryption, 370
voice recognition, 153–154
VPNs (virtual private networks), 63, 63–64, 89–91
always-on VPNs, 91
concentrators, 64, 65
mobile VPNs, 91
vulnerabilities. See also attacks
account configuration, 211
architecture weakness, 212
business processes, 212
configuration issues, 210–211, 211
DLL injections, 215
dead-on systems, 212
disk handling, 214–215
input-related, 214–215
memory-related, 215
pointer dereferencing, 215
race conditions, 215
resource exhaustion, 215
system sprawl, 212
undocumented assets, 212
untrained users, 211
user issues, 211
weak configuration, 210–211
zero-day exploits, 204, 211–212
vulnerabilities, wireless
bluejacking, 170, 175, 177
bluesnarfing, 170, 175
bluesnarking, 170, 175
disassociation, 170, 176, 367
evil twins, 170, 174, 177
IV (initialization vector) attacks, 171, 173
jamming, 171, 174–175, 177
NFC (near field communication), 171, 175, 368
replay attacks, 172–173, 177
RFID (radio frequency identification), 171, 176
rogue access points, 171, 174, 368
WPS (Wi-Fi Protected Setup), 171, 175
vulnerability scanning, 131–132, 386, 388
active scanners, 132
credentialled vs. non-credentialled, 388–389
exploitation frameworks, 135
false positives, 386, 389, 406
MBSA (Microsoft Baseline Security Analyzer), 133, 133–134
Nessus, 132–133, 133
OWASP ZAP, 134, 134
passive scanners, 132
vulnerability testing, 12

W

W-Fi Protected Setup (WPS), 171, 175, 253
W32/Klez virus, 288
WAFs (web application firewalls), 88–89
walkthroughs, 412
warm sites, 386, 401
waterfall software development model, 204, 216
watering hole attacks, 282, 318, 324–325
weak algorithms, 252
weak configuration, 210–211
weak key generation, 252
web application firewalls (WAFs), 88–89
Web Application Security Project, 143
web applications
   OWASP (Open Web Application Security Project), 54
   WAFs (web application firewalls), 88–89
web security gateways, 114
WEP (Wired Equivalent Privacy), 171, 173, 253, 367
wireless access points, 170
cloaking, 172
evil twin attacks, 174
misconfigured, 145
rogue, 171, 174, 177
SSIDs, 109
wireless attacks
   bluejacking, 170, 175, 177
   bluesnarking, 170, 175
disassociation, 170, 176, 367
evil twins, 170, 174, 177
   IV (initialization vector) attacks, 171, 173
jamming, 171, 174–175, 177
NFC (near field communications), 171, 176, 368
replay attacks, 172–173, 177
RFID (radio frequency identification), 171, 176
rogue access points, 171, 174. 368
WPS (Wi-Fi Protected Setup), 171, 175
wireless networks
   ad hoc wireless, 59
   password cracking, 129–130
review questions, answers, 425–426
review questions, answers, 179–182
scanning tools, 129–130
segmentation, 59
Wireshark, 126, 126–127, 127
WLANs (wireless LANs), 108–109
WordPress vulnerability, 224
work factor, cryptographic algorithms, 254
working copy backups, 390–391
worms, 288, 289
WPA (Wi-Fi Protected Access), 253, 367
WPA2, 367
WPS (Wi-Fi Protected Setup), 171, 175, 253

x

X.509 standard, 233, 261, 262–264
XaaS (Anything as a Service), 189
Xmas attacks, 282
XML injection attacks, 301
XP (Extreme Programming), 216
XPath, 301
XSRF (cross-site request forgery), 279, 302
XSS (cross-site scripting), 279, 302
XTACACS (Extended TACACS), 158

Z

zero-day exploits, 204, 211–212, 305
zombies, 282, 293, 297

zone transfers, DNS, 138
zones, 57
control diversity, 61
DMZ (demilitarized zone), 57–58, 58
extranets, 59
honeynets, 62–63
honeypots, 62–63
intranets, 58–59
network segmentation, 59–61, 60
vendor diversity, 61–62
wireless, 59