Index

A
abstraction
APIs, 266
black box approach, 69
acceptance testing, 160
access control
ABAC, 277
accountability, 261
administrative, 106
administrator roles, 44–45
attack examples, 98
attribute-based, 222, 277
BibA model, 67, 99
capability tables, 94
captive portals, 185
clearance, 141, 202
constrained interfaces, 96
dependent-context, 110
DAA, 97, 103, 112–113, 253
decentralized, 95, 219, 258
detective, 268
DIgA access codes, 80
discretionary, 97
discretionary, 97
employee termination, 18
implied deny principle, 283
logical, 110
least privilege principle, 140, 147, 207, 279
locks, 113
mandatory. See mandatory
access control (MAC)
meters, 108
need to know, 97, 141, 202, 259
new accounts, 138
privileged, 141
resource-based, 99
role-based, 132, 205
subject/object model, 49, 250
technical, 109
two-person, 141, 143
access control lists, 6, 57
account management
assessment, 242
account reviews, 99
accountability
access control, 261
user IDs, 125
accreditation, DAA, 69
ACID model, 179
ACK, 241
half-open scanning, 241
3-way handshakes, 188, 211–212, 241
Active Directory
for AAA services, 94
Kerberos, 114
trusts, 95–96
Active Directory Domain
Services, 105
active monitoring, 262
active wireless scanning, 118
ad hoc wireless network mode, 72
Address Resolution
Protocol (ARP)
cache poisoning, 80
Layer 2 OSI model, 77
spoofing, 91
administrators
access control, 106
access roles, 44–45
awareness training, 5
admissible evidence, 143
Advanced Encryption Standard
(AES)
BitLocker and EFS, 34
Kerberos, 97
key length, 266
proprietary data, 28
Rijndael block cipher, 265
USB thumb drives, 42
aggregate functions, 162, 175
aggregation
classification, 166
privileges, 151
aggregation attacks, 63, 233
Agile approach, 173, 178, 197, 244
alerts, clipping, 186
algorithmic complexity in TOC/
TOU attacks, 276
annualized loss expectancy (ALE)
flood plains, 188, 242
tornadoes, 24, 216
annualized rate of occurrence
(ARO)
fire, 215
flood plains, 18–19, 150, 242
tornadoes, 24
anomaly-based intrusion
detection, 234
antennas
directional, 214
signal strength, 282
anti-malware software
heuristic-based, 172
hiding viruses from, 169
AppleTalk protocol, 87
application control
blacklisting approach, 213
BYOD environments, 56
whitelisting, 188–189
application firewalls, 259
Application layer in OSI model, 85
application-level gateway firewalls,
89, 247
application logs, 191
application programming interfaces
(APIs)
abstraction, 266
API keys, 179
for code integration, 177
customer integration, 216
testing, 126
artificial intelligence, 178
asset values
business impact analysis, 6
replacement costs, 13
assurance
Common Criteria levels, 56, 202, 260
concept, 50
level of confidence, 165
asymmetric cryptosystem keys, 51–52, 69, 220
asynchronous communication
flags, 184
asynchronous tokens, 111
atomicity in ACID model, 179
attachments, email, 233
attacks. See specific attacks by
name
attribute-based access control
(ABAC) systems, 222, 277
attribute examples, 174
auditors, internal, 249
audits
Service Organizations Control,
10, 245
SSAE-16 Type I reports, 259
third parties, 133
authenticated scans, 132
authentication
biometric. See biometric
authentication systems
captive portals, 262
CCMP, 87
centralized logs, 252
certification process, 111
CHAP, 73
ESP, 227
Google servers, 108
hybrid services, 193
Kerberos. See Kerberos authentication system
knowledge-based, 108
LEAP, 72, 83–84
masquerading, 198
multifactor, 3, 205, 239
off-site users, 103
OpenID Connect, 110
PEAP, 90
port-based, 81
RADIUS, 99
SAML, 112
smartcards, 194
something you have, 198
something you know, 281
ticket-based, 106
tokens, 205, 247
Type 2 authentication factor, 109
user IDs and passwords, 106
voice pattern recognition, 94
authentication, authorization, and accounting (AAA) protocols, 96, 186
authentication headers in IPsec, 275
authorization
access control lists, 6
description, 100
Linux, 267–268
passwords, 257–258
penetration tests, 124
rights, 212
automated recovery, 230, 282
availability
DDoS attacks, 12
fail open configuration, 167
RAID, 11, 15
ransomware attacks, 7
Smurf attacks, 7–8
awareness
description, 23
elements, 247
training, 5, 83

banners, 126
baselines
CIS benchmarks, 29–30
classification labels, 30
configuration, 154
documents, 12
minimum security standard, 26
NIST SP 800-53, 184
purpose, 27
scoping, 42
third parties, 34
bcrypt systems, 38
Bell-LaPadula model
classifications, 287
MAC, 246
* -Security Property, 53
Simple Security Property, 206–207
state machine model, 66–67
benchmarks in CIS, 29–30
beyond a reasonable doubt
standard of proof, 273
Biba model
access control, 67, 99
* -Integrity Property, 55–56
Simple Integrity Property, 50
state machine model, 66–67
bin2hex() function, 178
bind operation in LDAP, 286–287
biometric authentication systems
CER, 111, 268
equal error rate, 193
FRR and FAR, 101–102, 111, 223, 268–269
iris scans, 231
palms scans, 112
passcard users, 106
reference templates, 101
retina scans, 98
throughput rate and enrollment time, 102
Type 1 errors, 243
Type 2 errors, 105
Type 3, 110
BIOS phishing attacks, 64
BitLocker encryption, 31, 34
black-box tests, 117, 121, 166
black boxes
abstraction, 69
phreaking tools, 85
blacklists, 64, 213
blackouts, 68
Blowfish
bcrypt, 38
key strengths, 65–66
blue boxes, 191
bluesnarfing attacks, 81
Bluetooth devices
active scans, 123
bluesnarfing attacks, 81
guidelines, 88–89
botnets
attacks using, 160
social media, 139
bounds, process, 67
bracketing in MAC design, 203
Brewer-Nash model, 48
Bring Your Own Device (BYOD) environments, 56
broadband technologies, 86, 195
brute-force attacks
logs, 187
passwords, 101
buffer overflow attacks
input validation, 163
parameter checking, 57
ping of death, 155
buffer overflow examples, 170
bundled database transactions, 166
Burp Suite tools, 130
bus topology, 79, 246
business associates agreements (BAAs), 265
business continuity planning
approval, 15
CEOs, 15–16
contacts lists, 15
decision-making process, 4
goals, 232
implementation tasks, 214
privacy rights, 11
project scope and planning phase, 15
RAID, 5
risk acceptance strategy, 250
risk assessment, 4
RTO, 232, 263, 283
senior managers, 9
statements of accounts, 12
training, 12–13, 254
business continuity tasks
business impact assessment, 204
electronic vaulting, 12
business impact assessment
asset values, 6
business continuity tasks, 204
identification tools, 22
MTD, 197
qualitative tools, 22
business logic errors, 228, 281
business owners, COBIT for, 26

B
background checks, 258
backups
data in motion, 45
differential, 273, 275
encryption, 34–35, 157
full, 274
incremental, 275
lost data, 274–275
off-site, 45
reviewing, 128
schedules, 144, 214
shipping, 157
tape rotation schemes, 143

cable modems, 86
cabling
Category 3, 91
Category 5e, 204
Category 6, 204, 277

C
cache poisoning, 80
Caesar ciphers, 58
California Online Privacy Protection Act (OPPA), 45, 230
callbacks
dial-up users, 230
somewhere you are factor, 95
capability tables, 94
capacitance motion detectors, 67
captive portals
access control, 185
email, 262
categorizing and selecting controls, 39–40
Category 3 cable, 91
Category 5e cable, 204
Category 6 cable, 204, 277
cellular 2G technology, 280
cellular networks, 263
Center for Internet Security (CIS), 29–30
centralized logs, 252
Certificate Revocation Lists (CRLs), 69, 222
certificates. See digital certificates
Challenge-Handshake Authentication Protocol (CHAP), 73
challenge/response process, 110–111
change logs, 142
change management
change control, 165, 285
configuration control, 285
release control, 285
request control, 176–177, 285
stakeholders, 17
checking accounts, 3
checklist reviews in disaster recovery, 143
chief executive officers (CEOs), 15–16
chief information officers (CIOs), 9
Children’s Online Privacy Protection Act (COPPA)
consent age, 18
websites, 260
ciphers, 59
civilian classifications, 28
Clark-Wilson integrity model, 213
Class A fire extinguishers, 60
Class B fire extinguishers, 200
Class B network subnet masks, 84, 238
Class C fire extinguishers, 245
classes
examples, 175
variables, 199
classification and classification labels
aggregation, 166
baselines, 30
Bell-LaPadula model, 287
civilian, 28
copyright data, 212
confidential, 27
considerations, 44
costs, 32
data owners, 239
Defense Department, 260–261
DLP detection, 28
highest level, 248–249
HIPAA documents, 33
information, 26
MAC, 107
mapping, 46
military, 282
mixed, 33
multistate systems, 57
new laws, 45
order, 29
purpose, 31
requirements, 35
reuse, 39
screen backgrounds, 41
Secret, 38
security labels, 56
clearance in access control, 202
clearing media, 27
client-side input validation for SQL injection attacks, 171
clipping alerts, 186
logs, 154
clocks in synchronous communications, 277
closed circuit television (CCTV) systems, 48–49
closed head fire suppression systems, 281
cloud computing environments
community, 244
hybrid, 142
IDaaS, 112, 278
OAuth, 109
PaaS, 68
private, 209
public, 144
SaaS, 49
SAML, 193
clusters, failover, 138
code coverage criteria, 125
metrics, 214
race conditions, 129–130
Code of Federal Regulations (CFR), 9
code reviews
description, 160
Fagan inspection, 226, 264
manual, 134, 281
static, 129, 134, 225, 286
codes vs. ciphers, 59
cognitive passwords, 213, 280
cohesion in object-oriented models, 160
cold sites, 15, 149
collisions
collision domains, 72
jam signals, 87
commercial data classification, 212
Common Access Cards, 109
Common Criteria
EAL1 evaluation assurance level, 56
EAL2 evaluation assurance level, 202
EAL7 evaluation assurance level, 260
PPs, 54
security targets, 282
Common Vulnerabilities and Exposures (CVE), 135, 142–143, 282
Common Vulnerability Scoring System (CVSS), 130, 218
Communications Assistance to Law Enforcement Act (CALEA), 16
community clouds, 244
compensation controls, 249
competent evidence, 152
compilers, 168
compliance, Group Policy for, 34
composition theories, feedback, 68
Computer Fraud and Abuse Act (CFAA), 15
Computer Security Act of 1987, 13
crime security incident response team (CSIRT), 144
concentrators, 77
concurrency issues, 175, 181
concurrent tasks, 64
confidential label, 27
confidentiality
cryptography, 283
data breaches, 14
DLP, 33
e-mail, 232, 277
encryption, 53
ESP, 227
keyloggers, 13
NDAs, 16, 24
SLAs, 10
VPNs, 11
Wireshark tool, 20, 221
crossover error rate (CER), 168
biometric devices, 193, 268
description, 111
cryptography. See also encryption
asymmetric, 51
confidentiality, 283
integrity, 209–210
Kerckhoff principle, 54
nonrepudiation, 60
shared secret keys, 228


crystal-box penetration testing, 238
custodians
monitoring security, 44
responsibilities, 27
customer checking accounts, 3
customer confidence, 22
customer integration, 216
cut and paste between virtual machines, 87

cross-site scripting (XSS), 166
cross-site request forgery (CSRF), 116
Customer Integration, 21
Customer Verifiers, 16

database transactions
bundled, 166
durability, 168, 272
lost updates, 170
rollbacks, 173–174
databases
ACID model, 179
concurrency issues, 175, 181
foreign keys, 233, 243
isolation, 187
NoSQL, 173
primary keys, 176, 189
referential integrity, 233–234
table degrees, 164
datacenters, locating, 272
datagrams in OSI model, 259, 266
datagrams in OSI model, 85, 259, 287
decentralized access control, 95, 219, 258
decision-making process in business
continuity planning, 4
declassification, 39
decommissioning DVD-ROMs, 239
decoy, 268
defect recurrence rate, 129
Defense Department classifications, 260–261
defense in depth, 17
defined stage in SW-CMM, 164
degaussing, 35, 225
degrees of database tables, 164
denial of service (DoS) attacks
description, 77
examples, 152, 189
sabotage, 147
teadrop, 89
VoIP phones, 241
Department of Commerce, 3
depth assurance measure, 264
design reviews in SDLC, 165
damage threshold in CFAA, 15
darknets, 142
data at rest
data breaches, 31
description, 29
encryption, 31
Internet connections, 40
symmetric encryption, 44
data breaches
confidentiality, 14
data at rest, 31
laws, 2–3
data centers
humidity, 68
virtualized, 86–87
data classification. See classification
classification labels
data custodian roles, 8–9
data diddling attacks, 244
Data Encryption Standard (DES)
keys, 53
modes of operation, 186
running requirements, 51
3DES, 254
data in motion, 45
data in transit
protecting, 36
TKIP encryption, 204
data in use, 39
Data Link layer, 91–92
data loss prevention (DLP) systems
confidentiality, 33
label detection, 28
network, 209
sensitive information detection, 157–158
data owners
categorization of information systems, 43
classification levels, 239
responsibilities, 37
tasks, 234
data processor roles, 42
Data Protection Directive
actions required, 266
data integrity, 42
GDPR, 42
principles, 38, 41
Safe Harbor. See Safe Harbor third-party organizations, 38
data remanence
description, 28, 278
media reuse, 30–31
sanitization, 39
SSDs, 27–28
data retention policies, 26–27
datacenters, locating, 272
datagrams in OSI model, 259, 266
datagrams in OSI model, 85, 259, 287
de-encapsulation of headers, 202–203
decentralized access control, 95, 219, 258
decision-making process in business
continuity planning, 4
declassification, 39
decommissioning DVD-ROMs, 239
decoy, 268
defect recurrence rate, 129
Defense Department classifications, 260–261
defense in depth, 17
defined stage in SW-CMM, 164
degaussing, 35, 225
degrees of database tables, 164
denial of service (DoS) attacks
description, 77
examples, 152, 189
sabotage, 147
teadrop, 89
VoIP phones, 241
Department of Commerce, 3
depth assurance measure, 264
design reviews in SDLC, 165
cross-site request forgery (CSRF), 116
Customer Integration, 21
Customer Verifiers, 16

database transactions
bundled, 166
durability, 168, 272
lost updates, 170
rollbacks, 173–174
databases
ACID model, 179
concurrency issues, 175, 181
foreign keys, 233, 243
isolation, 187
NoSQL, 173
primary keys, 176, 189
referential integrity, 233–234
table degrees, 164
datacenters, locating, 272
datagrams in OSI model, 259, 266
datagrams in OSI model, 85, 259, 287
de-encapsulation of headers, 202–203
decentralized access control, 95, 219, 258
decision-making process in business
continuity planning, 4
declassification, 39
decommissioning DVD-ROMs, 239
decoy, 268
defect recurrence rate, 129
Defense Department classifications, 260–261
defense in depth, 17
defined stage in SW-CMM, 164
degaussing, 35, 225
degrees of database tables, 164
denial of service (DoS) attacks
description, 77
examples, 152, 189
sabotage, 147
teadrop, 89
VoIP phones, 241
Department of Commerce, 3
depth assurance measure, 264
design reviews in SDLC, 165
designated approving authorities (DAAs), 69
destruction of media, 41
detection, fire, 48
detection stage in incident response process, 154, 227–228
detected access controls, 268
deterrence, 230
device fingerprinting, 238–239
DevOps approach, 180, 206, 271
DHCP, 217
dial-up connections, 89–90, 230
Diameter protocol, 113
dictionary attacks, 95
differential backups, 273, 275
Diffie-Hellman algorithm, 54
digital certificates
CRLs, 222
private keys, 220
public keys, 220
self-signed, 70
trusting, 69
X.509 standard, 62–63
Digital Millennium Copyright Act (DMCA)
copyrights, 229
Internet service providers, 2, 247
safe harbor protection, 200
Digital Signature Standard, 49
digital signatures
email, 277
nonrepudiation, 240, 257
private keys, 257
RSA algorithm, 66
Direct Inward System Access (DISA), 80
Direct Sequence Spread Spectrum (DSSS), 73
directional antennas, 214
directives, 200
directory indexing, 208–209
directory traversal attacks, 165
dirty reads, 181
disaster recovery
checklist reviews, 143
cold sites, 15, 149
completion indicators, 150–151
disaster examples, 143
circuit interruption tests, 265
hot sites, 225
MTD, 148
parallel tests, 154, 197, 253
remote journaling, 222
RPO, 238
RTO, 199
structured walk-through tests, 264
 tabletop exercises, 219
tape rotation strategy, 143, 216
warm sites, 229, 266, 273
disasters, manmade, 146
discovery phase in penetration tests, 124, 136, 238
discretionary access control (DAC)
ACLs, 97
description, 253
Linux, 112–113
scalability and flexibility, 103
disintegration of media, 43
disk mirroring, 155, 247
disk striping, 276
disk stripping with parity, 204
disposition guidelines, 35–36
distance-vector protocols, 75
distinguished names (DNs), 101, 113
distributed denial of service (DDoS) attacks
availability attacks, 12
LOIC, 222
risk avoidance, 14
dogs, 101
Domain Keys Identified Mail (DKIM), 92
Domain Name System (DNS)
human-readable addresses, 270
poisoning, 76
ports, 152
DoS attacks. See denial of service (DoS) attacks
Double DES (2DES) encryption algorithm, 64
downgrading media, 41
downgrading systems, 31–32
DSL, 86
due care principle, 5, 195, 273
durability in database transactions, 168, 272
DVDs
decommissioning, 239
secondary storage, 251–252
dynamic testing for software, 162
electrical fires, 245
electromagnetic emanations
Faraday cages, 67–68
fiber-optic cable, 284–285
white noise, 63
Electronic Communications Privacy Act (ECPA), 218
electronic discovery reference model, 202, 248
electronic signatures, 35
electronic vaulting
business continuity tests, 12
description, 150
elevation of privilege threats, 4, 132
email
attachments, 233
captive portals, 262
confidentiality, 232, 277
DKIM, 92
encryption, 41, 267
nonrepudiation, 258
S/MIME, 76
emergency response guidelines
components, 235
contacts lists, 15
immediate response procedures, 254
employees
pre-hire activities, 258
termination, 18
Encapsulating Security Payload (ESP) protocol, 211
functions, 227
IPsec, 52
capsulation
multilayer protocols, 270
OSI model, 223
Encrypting File System, 34
encryption
asymmetric cryptosystems, 51, 220
backups, 34–35, 157
BitLocker and EFS, 34
cellular networks, 263
confidentiality, 53, 283
cordless phones, 84
data at rest, 31, 44
DES, 51
diffie-hellman algorithm, 54
digital signature standard, 49
digital signatures, 257
e-mail, 41, 232, 233
export control laws, 4
FTP and Telnet, 30
full disk, 31
HIPAA documents, 33
integrity, 209–210
Internet connections, 40
IPsec VPNs, 31
Kerberos, 94, 97–98
key retrieval, 49

E
EAL 1 evaluation assurance level, 56
EAL 2 evaluation assurance level, 202
EAL 7 evaluation assurance level, 260
earthquake risk, 21–22
eavesdropping, 103
ECE flag, 216
Economic Espionage Act, 4–5
effectiveness, KPIs for, 262
egress filtering, 153–154, 189
802.1x port-based
authentication, 81
802.11n, 72–73, 77
keys, 51–52, 248, 250
known plaintext attacks, 62
likelihood risk, 249
media, 29
PGP, 45, 267
private keys, 257
public keys, 257
Rijndael block cipher, 265
risk mitigation, 17, 190
RSA, 255
SFTP, 279
shared secret keys, 228
6-bit keys, 189–190
sniffing attacks, 26
SSDs, 62
TACACS+ servers, 279
TKIP, 204
TLS and AES, 28
TPM, 51
USB thumb drives, 42
WEP, 76–77
endpoint security systems, 88
enrollment provisioning process, 217
enrollment time in biometric factors, 102
Enterprise mode in WPA2, 117
entitlement to privileges, 145
ephemeral session keys, 67
equal error rate for biometric devices, 193
erasing media, 32, 35
escape, virtual machines, 87
escrow agents, 49
escrow agreements, 153
establishing phase in IDEAL model, 177
/etc/passwd file, 170, 194–195
/etc/shadow file, 240
European Union
Data Protection Directive. See Data Protection Directive; Safe Harbor
third-party organizations, 38
events
incident response, 152
system logs, 246
evidence
competent, 152
expert opinion, 157
hearsay rule, 243
parol evidence rule, 198–199
preserving, 156
real, 139
tangible, 143
evil twin attacks, 2
examine and test activities, 234
excessive privileges, 104
exclusive or (XOR) operation, 53
expected findings in kickoff meetings, 150
expert opinion evidence, 157
expert systems, 173
export control laws, 4
exposure factor
fire, 215
flood plains, 242
tornados, 23
Extensible Authentication Protocol (EAP), 261

F
Fagan inspection, 130, 226, 264
fail closed approach, 176
fail open configuration, 167
fail secure state in SDL, 161
failover clusters, 138
Fair Cryptosystem approach, 56
false acceptance rate (FAR) and false acceptance rate (FAR) in biometric factors, 101–102, 111, 223, 268–269
Family Educational Rights and Privacy Act (FERPA), 246
Faraday cages, 67–68
fault tolerant systems
failover clusters, 138
RAID. See Redundant Array of Inexpensive Disks (RAID)
fauls, power, 216
fax machines, 85
Federal Information Security Management Act (FISMA), 3, 8
tederal sentencing guidelines for prudent man rule, 3
Federal Trade Commission (FTC), 37
federation
identity integration, 104, 193
SAML, 254
feedback composition theory, 68
fences, 4, 63, 101
Fiber Channel over Ethernet (FCoE), 89
Fiber Distributed Data Interface (FDDI), 82
fiber-optic cable distances, 219
electromagnetic interference, 284–285
file pointers in TOC/TOU attacks, 277
File Transfer Protocol (FTP)
encryption, 30
ports, 73, 120
file transfers
SCP, 230
SFTP, 279
filtering
egress, 153–154, 189
STRIDE, 132
financial statements, 21
fingerprint scans, 3, 110
fingerprinting, device, 238–239
fire
detection, 48
exposure factor, 215
fire extinguishers
Class A, 60
Class B, 200
Class C, 245
fire suppression systems
closed head, 281
Halon, 67
impact reduction, 206
infrastructure hardening, 6
preaction, 52
soda acid, 66
firewalls
application, 259
application-level gateway, 89, 247
log files, 256
rule-based access controls, 106
single-tier, 86
stateful packet inspection, 185
static packet filtering, 84–85, 204
three-tier, 85
two-tier, 75, 88
WAF, 168
first-generation programming languages, 274
first responder guidelines, 235
fixed-length input for hash functions, 54
flash memory cards, 271
flood plains
ALE, 188, 242
ARO, 18–19, 150, 242
exposure factor, 242
flow logging, 118
foreign keys
databases, 233, 243
referential integrity, 164
forensic device controllers, 141, 184, 278
forensic imaging, 147
forensic investigations and analysis
media analysis, 147
netflow data, 154
snapshots, 49–50
software analysis, 157
“Forensic Response Guidelines,” 224
Fortran programming language, 265
Fourth Amendment
privacy rights, 11
searches, 156
fraggle attacks, 156
fragmentation in teardrop attacks, 187
Frame Relay, 72, 245
fraud prevention
mandatory vacations, 12, 153
mechanisms, 142
Frequency Hopping Spread Spectrum (FHSS), 73
full backups, 274
full interruption tests, 265
full mesh topology, 90
functional requirements
SDLC, 161
software, 169
functions, aggregate, 162
fuzzers and fuzzing
bugs, 133
generational, 118
intelligent, 205
web application forms, 116

Grant rule, 63
grey-box tests, 118–119, 175, 229, 271
Group Policy
compliance, 34
logging, 120
guards, 101

h
hackers, SQL injection attacks by, 23
half-duplex communications, 229
half open scanning, 128
Halon fire suppression systems, 67
hand geometry scanners, 197
hard disks
data at rest, 29
RAID requirements, 5
sanitization, 251
third-party handling, 44
hardening provisions, 256
hardware MTTF, 60
hashed passwords
rainbow table attacks, 104
salting, 224, 234, 286
hashing
fixed-length input, 54
integrity, 11
keys, 52
MD5 algorithm, 62
TGTs, 98
HAVAL hash function, 49
header flags in TCP, 216
headers
decomapsulation, 202–203
IPsec, 275
TCP, 263
Health Insurance Portability and Accountability Act (HIPAA)
medical records, 265
organizations subject to, 7
PHI, 42, 213, 246
private classification of documents, 33
TLS encryption of documents, 33
hearsay rule, 243
heartbeat sensors, 65
heuristic-based antimalware software, 172
highly privileged account assessments, 242
honey pot systems
decos, 268
description, 193
manual, 139
pseudo laws, 139
host-based intrusion detection systems (HIDSs), 151
host OS attacks, 241
hot sites, 225
hot spots, 79
HTTP
OSI layer, 80
TCP 80, 78–79
human-readable addresses, 270
humidity in data centers, 68
hybrid authentication services, 193
hybrid clouds, 142
hypervisors, 68, 145, 196

I
IDEAL model, 177
identification
process, 101
usernames, 22, 224
identification cards
magnetic stripe cards, 255–256
proximity cards, 196–197
smart cards, 60–61
Identity as a Service (IDaaS), 94, 112, 188, 278
identity integration, 104, 193
identity management registration process, 104
identity proofing
information for, 105, 109
knowledge-based authentication, 108
out-of-band, 192
identity systems
logging, 98
third-party, 94
X.500, 105
IM communication, 78
immediate response procedures, 254
impact
fire suppression systems, 206
qualitative risk assessment, 287
inactivity time-outs, 109
inbound packets in ping flood attacks, 239
incident examples, 153
incident response process
detection stage, 154, 227–228
disaster recovery, 154
incidents, 152
interviews, 149
lessons learned stage, 228
mitigation phase, 151
remediation stage, 228, 232
Reporting phase, 251

G
gaining access phase in penetration tests, 136
Gantt charts, 174–175
gateway firewalls, 89, 247
gateways
IP addresses, 265
proxy, 75–76
General Data Protection Regulation (GDPR), 42
generational fuzzing, 118, 205
generators, 158
geo graphically distributed content distribution, 184
Google Authenticator, 110
Google server authentication, 108
government agents, 138
government contractors, 3
Gramm-Leach-Bliley Act (GLBA)
criminal law, 232
customer checking accounts, 3
privacy notices, 16
response stage, 228
root cause analysis, 228
inconsistent timestamps, 132
incorrect database summaries, 175
incremental backups, 275
industrial processes, 51
inference attacks
from nonsensitive information, 186
polyninstantiation, 177
inference engines in expert systems, 173
inference problems, 167
information, classification, 26
information disclosure
attacks, 24
threat assessment, 275
information flow model, 66–67
information logs, 131
Information Security Continuous Monitoring (ISCM), 128–129, 133
Infrastructure as a Service (IaaS)
environments
examples, 215
hypervisors, 196
object-based storage, 244
patches, 155
shared responsibility model, 243
SOC 2 reports, 245
vendor responsibilities, 59
infrastructure hardening for fire suppression systems, 6
inherence, 162
initial stage in SW-CMM, 163
input validation
buffer overflow attacks, 163
limit checks, 210
SQL injection attacks, 171
user-defined fields, 179
web applications, 255
XSS attacks, 168
insurance, 286
integrity
cryptography, 209–210
data diddling attacks, 244
Data Protection Directive, 42
description, 10
hashing, 11
*Integrity Property in Biba model, 55–56
intellectual property protection
copyrights, 9, 213
Economic Espionage Act, 4–5
logos, 6
patents, 5, 250
trade secrets, 206
watermarking, 149
intelligent fuzzing, 205
interface testing
description, 118, 131
web applications, 205
interfaces
constrained, 96, 199
software testing, 243
interference
description, 264
fiber-optic cable, 284–285
internal auditors, 249
International Information Systems Security Certification Consortium (ISC)³
canons, 146, 224, 254
characteristics, 148
penalties, 287
trademarks, 6
violations, 188
Internet connections, 40
Internet Control Message Protocol (ICMP)
abuses, 195
OSI model, 86
ping utility, 80–81, 239
smurf attacks, 204
Internet service providers, 2, 200, 247
interviews in incident investigation, 149
intrusion detection systems (IDSs)
anomaly-based, 234
event responses, 144–145
heartbeat sensors, 65
intrusion protection systems (IPSs)
cross-site scripting attacks, 75
risk mitigation, 6
inventory control, 147
investigations
operational, 222–223
permissions, 153
IP addresses
gress filtering, 153–154, 189
gateways, 265
gray-box tests, 118–119
land attacks, 258
loopback, 88
NAT, 84, 199
PAT, 252
private, 213, 262
public, 225
spoofing attacks, 169
ipconfig command
DHCP, 217
MAC addresses, 83
IPsec
authentication headers, 275
data in transit, 36
ESP component, 52, 211, 227
L2TP, 90
VPNs, 31, 82
IPX protocol, 87
iris scans, 231
ISAE 3402, 135
iSCSI, 77
ISDN
broadband technology, 86
PRI, 81
ISO 27002 standard, 16
isolation
databases, 187
processes, 60, 196
IT Infrastructure Library (ITIL)
foundation, 145
ITU-T X.509 standards, 260

J
jam signals, 87
Java programming language, 168
JavaScript programming language, 194

K
Kerberos authentication system
Active Directory systems, 114
encryption, 94, 97–98
KDCs, 100
SSO, 113
STs, 280
synchronized time, 113
TGS, 106–107, 184
TGTs, 98, 280
ticket-based authentication, 106
Kerchoff principle, 54
kernel
diagram, 284
ring protection model, 59
Kernel mode, 57
key distribution centers (KDCs), 100
key escrows, 56
key performance indicators (KPIs)
description, 217
effectiveness, 262
example, 125
key risk indicators (KRI)
identifying and tracking, 123
risk exposure, 211
uses, 244
keyboards, 94
keyloggers, 13
keys
AES, 266
API, 179
asymmetric encryption, 51–52, 69, 220
Blowfish, 65–66
databases, 176, 189, 233, 243
dES, 53
Diffie-Hellman algorithm, 54
digital certificates, 220
digital signatures, 257
crystallography, 164
symmetric encryption, 228, 231, 250
TLS, 67
WEP, 76–77, 91
kickoff meetings, 150
knowledge banks in expert systems, 173
knowledge-based authentication, 108
known plaintext attacks, 62
KryptoKnight, 113

L
L2F protocol, 82
L2TP protocol
IPsec, 90
VPNs, 82, 253
labels. See classification and
classification labels
land attacks, 258
latency, 145, 205
lattice-based model, 98
laws
CALEA, 16
CFR, 9
classification, 45
criminal, 232
data breaches, 2–3
export control, 4
United States Code, 283
Layer 2 OSI model, 77
Layer 3 OSI model, 86
Layer 6 OSI model, 81–82
Layer 7 OSI model, 80
LDAP. See Lightweight Directory
Access Protocol (LDAP)
least privilege principle, 140, 147, 207, 279
length of passwords, 101–102
Lessons Learned stage in incident
response process, 228
level of confidence in assurance, 165
Lightweight Directory Access
Protocol (LDAP)
Active Directory Domain
Services, 105
bind operation, 286–287
description, 259
DNs, 101, 113
passive monitoring, 255
ports, 104–105, 114
SASL, 112
Lightweight Extensible
Authentication Protocol
(LEAP)
alternates, 72
vs. PEAP, 83–84
likelihood risk, 9, 249
limit checks, 210
link state protocols, 274
links in man-in-the-middle attacks, 253–254
Linux operating system
DAC, 112–113
permissions, 267–268
scanning, 134
locks
compensation controls, 249
description, 113
logic bombs, 178
logical XOR operations, 53
logins
factors, 94
failures, 95
spoofing, 95
workstations, 138
logos, 6
logs
application, 191
brute-force attacks, 187
centralized, 252
change, 142
clipping, 154
directory traversal attacks, 165
events, 246
firewalls, 256
flow, 118
Group Policy, 120
identity systems, 98
inconsistent timestamps, 132
information, 131
NIST Special Publication 800-92, 271
NTP, 120
overwriting, 227
port scans, 163
protecting, 252
SIEM tool, 252
software analysis, 157
sources, 131
SQL injection attacks, 171, 232
statistical sampling, 284
syslog events, 120
Syslog protocol, 116
system disk filled by, 127
user IDs, 125
loopback addresses, 88
lost updates in database
transactions, 170
Low Orbit Ion Cannon (LOIC)
attack tool, 222

M
m of n control systems, 49
machine languages, 274
macro viruses, 164
magnetic stripe cards, 255–256
magnetic tape remnant data, 157
maintenance hooks, 50
malicious insiders, 130
malware
blacklisting approach, 64
hiding anti-malware software
from, 169
polymorphic viruses, 167
ransomware, 177–178
signature detection, 179
worms, 167, 187, 244
man-in-the-middle attacks
ARP spoofing, 91
description, 158
preventative measures, 253–254
managed stage in SW-CMM, 164
mandatory access control (MAC)
Bell-LaPadula, 246
Biba, 99
description, 100–101, 278
environments, 203
labels, 107
lattice-based model, 98
secret data, 110
mandatory vacations, 12, 153
manmade disasters, 146
mantraps, 54–55, 235, 258
manual code reviews, 134, 281
manual recovery, 139
mapping classifications, 46
markup languages, 203
masquerading, 198
master boot record (MBR) viruses, 181
matrices
access control, 108
risk, 17–18
segregation of duties, 140
maximum tolerable downtime (MTD)
business continuity planning, 232
business impact assessment, 197
disaster recovery plans, 148
verification, 119
MD5 hash algorithm, 62
mean time to failure (MTTF), 60
media
classification labels, 26
clearing, 27
data remanence, 30–31
destruction, 41
dowgrading, 41
cryptography, 29
erasing, 32, 35
forensic analysis, 147
Media Access Control (MAC)
addresses
displaying, 83
OSI layer, 91–92
spoofing, 80
medical records, 265
meet in the middle attacks, 64
memory
data in use, 39
primary storage, 162
process isolation, 196
volatile, 209
mesh topology
description, 82
node connections, 90
Metasploit tool, 128, 203, 260
methods
element, 162
object-oriented programming, 169
military classification scheme, 282
mission owner roles, 217
misuse case diagrams, 134
misuse case testing, 121, 281
mitigation phase in incident response, 151
Mobile Device Management (MDM), 60, 188
modems, 89
modulo (MOD) function, 192
monitoring
active, 262
custodian role, 44
ISCM, 128–129, 133
LDAP servers, 255
passive, 123, 214–215
proactive, 196
RUM, 122
synthetic, 121, 123
user session, 131
VMware environment,
256–257
monitors, reference, 230–231
motion detectors
capacitance, 67
wave pattern, 185
multifactor authentication, 3, 205, 239
multilayer protocols
drawbacks, 78–79
encapsulation, 270
SCADA systems, 76
multipartite viruses, 169, 181
multistate systems, 57
multitasking, 248
mutithreading, 64
mutation testing, 116
security controls
assessments, 14
NIST Special Publication 800-18
system security plan updates, 200
tasks, 41
NIST Special Publication 800-53
baselines, 184
depth, 264
NIST Special Publication 800-53A
examine and test assessments, 234
mechanism assessment
objects, 117
security and privacy controls, 127
specifications, 270
NIST Special Publication 800-60,
39–40
NIST Special Publication 800-88,
35–36, 39
NIST Special Publication 800-92, 271
NIST Special Publication 800-115, 136
NIST Special Publication 800-122, 31
NIST Special Publication 800-137,
128–129, 133
nmap tool
penetration tests, 124
port scanner, 135
port status, 131
non-disclosure agreements (NDAs)
confidentiality, 16, 24
personnel retention, 231
proprietary information, 33–34
purpose, 223
trade secrets, 248
non-IP protocols
elements, 87
issues, 90
nonrepudiation
cryptography, 60
description, 17
digital signatures, 240, 257
e-mail, 258
RSA, 221
nontransitive trusts, 225
NoSQL databases, 173
Notice principle, 2
OASIS standard markup
language, 251
OAuth tool, 109, 110
object-based storage, 244
object examples, 212
object-oriented programming
abstraction, 69
class variables, 199
coupling and cohesion, 160
inheritance, 162
language examples, 265
methods, 169
off-site backups, 45
office productivity documents,
micro viruses in, 164
offsite user authentication, 103
on-premise third-party identity
services, 94
one-way nontransitive trusts, 225
Online Certificate Status Protocol
(OCS), 286
Online Privacy Protection Act
(OPPA), 45, 230
open networks, 185
open relays, 252
open services, 120
Open Shortest Path First (OSPF)
protocol, 274
open-source software, 57
Open Web Application Security
Project (OWASP), 66, 169
OpenID
phishing attacks, 112
website integration, 219
OpenID Connect, 110
OpenLDAP, 105
OpenVAS, 116
operational investigations, 222–223
Optimizing stage in SW-CMM, 240
Orthogonal Frequency-Division
Multiplexing (OFDM), 73
OSI model
datastreams, 85, 259, 287
encapsulation, 223
Layer 2, 77
Layer 3, 86
Layer 6, 81–82
Layer 7, 80
layer order, 89
MAC addresses, 91–92
Physical layer, 83, 195
TCP/IP model matches, 80
Transport layer, 83, 229–230, 259, 266
out-of-band identity proofing, 192
over-the-shoulder reviews, 223
overlapping security controls, 17
overwriting
flash memory cards, 271
logs, 227
media, 27
P
P7S format, 233
packet filtering firewalls, 84–85, 185, 204
packet source addresses, 240
palm scans, 112
parallel tests in disaster recovery, 154, 197, 253
parameter checking for buffer
overflow attacks, 57
parol evidence rule, 198–199
passive monitoring
description, 214–215
LDAP servers, 255
vs. synthetic, 123
passive scanning, 123
passwords
authentication, 106
authorization, 257–258
cognitive, 213, 280
credential management systems,
215–217
dictionary attacks, 95
history, 251
length, 101–102
rainbow table attacks, 104, 249
salt values, 52
salting, 224, 234, 286
screensavers, 109
self-service password reset, 108
shadowed, 170, 194–195, 240
SSO, 221
web applications, 107–108
WPA2 Enterprise mode, 117
patches
IaaS, 155
regression testing, 123, 165, 224
service packs, 141
vulnerabilities, 122
zero-day attacks, 256
patents
duration, 250
intellectual property
protection, 5
requirements, 13
path disclosure, 121
Payment Card Industry Data
Security Standard (PCI DSS), 8, 29, 43
PEAP
authentication, 90
EAP, 261
vs. LEAP, 83–84
penetration tests
black-box, 117, 121, 166
Bluetooth active scans, 123
crystal-box, 238
discovery phase, 124, 136, 238
gaining access phase, 136
gray-box, 118–119, 229, 271
hazards, 127
Metasploit, 128, 260
misuse cases, 281
open services, 120
permissions, 134
planning phase, 124
ports, 133–134
reporting phase, 124
reviews, 124, 136
social engineering, 195
web-based applications, 180
Whois tool, 208
Xmas scans, 135
permissions
examples, 215
investigations, 153
least privilege, 140
Linux, 267–268
penetration tests, 134
Take-Grant model, 186
persistent XSS attacks, 172
Personal Health Information (PHI),
213
personally identifiable information
(PII)
data breach laws, 2–3
description, 31
examples, 189, 269
Notice principle, 2
personnel retention, 35, 231
PERT charts, 171
phishing attacks, 100, 112
phishing tool, 64
PHP applications, 178
phreaking tools
black boxes, 85
blue boxes, 191
physical controls, 101
physical infrastructure hardening, 6
Physical layer in OSI model, 83,
195
ping flood attacks
ICMP, 195
inbound packets, 239
Ping of Death attacks, 155, 195
ping utility
function, 212
ICMP, 80–81
plaintext attacks, 62
planning phase in penetration tests,
124
Platform as a Service (PaaS)
environments
application code, 156
description, 68
Point-to-Point Protocol (PPP) authentication, 73
dial-up connections, 89–90
polymorphic viruses, 167
POODLE attacks, 34
Port Address Translation (PAT), 252
port-based authentication, 81
private clouds, 209
private IP addresses, 213, 262
private keys
digital certificates, 220
digital signatures, 257
encryption, 51–52, 257
privilege creep, 100, 201
privilege escalation, 4, 132
privilege escalation attacks, 151
privileged mode
Kernel mode, 57
ring protection model, 276
privileged
access reviews, 141
aggregation, 151
authorization, 212
entitlement, 145
excessive, 104
proactive monitoring, 196
probability in qualitative risk assessment, 287
processes
bounds, 67
isolation, 60, 196
multitasking, 248
Waiting state, 222
productivity documents, macro viruses in, 164
program reviews, 129
project scope and planning phase in business continuity plans, 15
proprietary information, NDAs for, 33–34
Protected Health Information (PHI) examples, 281
HIPAA, 42, 246
Protection Profiles (PPs), 54
provisioning
enrollment, 217
roles, 201–202
signature-based detection, 103–104
workflow-based account, 201
proximity cards, 196–197
proxy gateways, 75–76
prudent man rule, 3
pseudo flaws in honeypot systems, 139
PSH flag, 226
public clouds, 144
public domain software, 158
public IP addresses, 225
public keys
digital certificates, 220
encryption, 51–52, 257
pulverizing DVD-ROMs, 239
purging, 225
Pretty Good Privacy (PGP), 45, 267
Presentation layer in OSI model, 8
Presentation layer in OSI model, 133–134
preset questions for cognitive passwords, 213
Pretty Good Privacy (PGP), 45, 267
preventative measures, 147
primary database keys, 176, 189
Primary Rate Interface (PRI), 81
primary storage, 162
printer discovery, 130
privacy
California Online Privacy Protection Act, 45, 230
FERPA, 246
Fourth Amendment rights, 11
GLBA notices, 16
OPPA, 45
reasonable expectation of, 218–219
Safe Harbor principles, 190
private branch exchange (PBX) systems, 84
private classification, 33
private clouds, 209
private IP addresses, 213, 262
private keys
digital certificates, 220
digital signatures, 257
encryption, 51–52, 257
privilege creep, 100, 201
privilege escalation, 4, 132
privilege escalation attacks, 151
privileged mode
Kernel mode, 57
ring protection model, 276
privileged
access reviews, 141
aggregation, 151
authorization, 212
entitlement, 145
excessive, 104
proactive monitoring, 196
probability in qualitative risk assessment, 287
processes
bounds, 67
isolation, 60, 196
multitasking, 248
Waiting state, 222
productivity documents, macro viruses in, 164
program reviews, 129
project scope and planning phase in business continuity plans, 15
proprietary information, NDAs for, 33–34
Protected Health Information (PHI) examples, 281
HIPAA, 42, 246
Protection Profiles (PPs), 54
provisioning
enrollment, 217
roles, 201–202
signature-based detection, 103–104
workflow-based account, 201
proximity cards, 196–197
proxy gateways, 75–76
prudent man rule, 3
pseudo flaws in honeypot systems, 139
PSH flag, 226
public clouds, 144
public domain software, 158
public IP addresses, 225
public keys
digital certificates, 220
encryption, 51–52, 257
pulverizing DVD-ROMs, 239
purging, 225
quantitative risk assessment
probability and impact, 287
risk matrices, 17–18
tools, 203
quantitative tools for business impact assessment, 22
quantitative risk assessment, 2
R
race conditions
code coverage testing, 129–130
description, 100
TOC/TOU attacks, 170
Radio Frequency IDentification (RFID) technology, 147
RADIUS
AAA servers, 186
description, 99
Diameter replacement for, 113
TACACS+, 241
UDP, 99
RADIUS over TCP, 108–109
RAID. See Redundant Array of Inexpensive Disks (RAID)
rainbow tables
attacks, 104, 249
salting, 193
RAM
data in use, 39
volatile memory, 209
random sampling, 190
random values, 52
ransomware, 7, 177–178
ready state for schedulers, 56
real evidence, 139
real user monitoring (RUM), 122
realm trusts, 95–96
reasonable expectation of privacy, 218–219
reconnaissance attacks, 168, 276
record retention
description, 44
policies, 34, 232, 275
records, sampling, 158
recovery
automated, 230, 282
electronic vaulting, 150
manual, 139
RAID-5, 112
recovery point objective (RPO), 238
recovery time objective (RTO)
business continuity planning, 232, 263, 283
disaster recovery, 199
reduction analysis, 20–21
Redundant Array of Inexpensive
Disks (RAID)
availability, 11, 15
business continuity planning, 5
purpose, 209
RAID 0, 276, 277
RAID-1, 155, 157, 184, 247
RAID-5, 5, 112, 195, 204
reference monitors, 230–231
reference templates, 101
referential integrity
databases, 233–234
foreign keys, 164
reflected input in XSS attacks, 171
registration process, 104
regression testing
defect recurrence rate, 129
patches, 123, 165, 224
software changes, 171
regulatory investigations, 138
relative distinguished names
(RDNs), 113
release control
change management, 285
software acceptance testing, 160
remediation
incident response process, 228, 232
vulnerabilities, 130
remnant data
description, 253
magnetic tapes, 157
remote access
screen scrapers, 76
VPNs, 75
remote journaling, 222
remote server administration, 35
remote wiping, 188, 263
repeatable stage in SW-CMM, 164, 178, 211
repeaters, 77
replacement costs, 13
reporting phase
incident response process, 251
penetration tests, 136
repudiation in STRIDE, 10, 132, 221
request control in change
management, 176–177, 285
resource-based access controls, 99
response stage in incident response
process, 228
RESTful API, 110
retention, personnel, 35, 231
retention requirement for electronic
signatures, 35
retina scans, 98
reuse
classification labels, 39
declassification, 39
downgrading systems, 31–32
Reverse Address Resolution
Protocol (RARP), 77
RFC 1918 addresses, 254–255
rights
account reviews, 99
authorization, 212
Rijndael block cipher, 265
ring protection model
kernel, 59
privileged mode, 276
user programs and applications, 218
risk topology, 74, 246
risk mitigation
encryption, 17, 190
intrusion prevention system, 6
risks
ALE, 188
ARO, 215
business continuity planning, 4
DDoS attacks, 14
earthquakes, 21–22
exposure factor, 215
formula, 13
KRIs, 211
malicious insiders, 150
matrices, 17–18
qualitative assessment, 17–18, 203, 287
risk acceptance strategy, 18, 219, 250
risk transference strategy, 224, 286
SLE, 251
unpatched web applications, 225
Rivest, Shamir, Adleman (RSA)
algorithmdigital signatures, 66
key requirements, 255
nonrepudiation, 221
gerogue devices, 123
role-based access controls (RBACs), 132, 205
rollbacks of database transactions, 173–174
root cause analysis, 228
routers
effective protocols, 221
purpose, 238
Routing Information Protocol
(RIP), 86
RST flag, 72
rule-based access controls, 106
S
S/MIME, 76
sabotage, 147
Safe Harbor
Data Protection Directive. See
Data Protection Directive
Department of Commerce, 3
DMCA, 200
European Union, 27
FTC, 37
principles, 190, 200, 265, 270
saliency
passwords, 52, 234, 286
rainbow tables, 193, 249
table applications, 107–108, 224
sampling
logs, 284
random, 190
records, 158
sandboxing
purpose, 50
virtualized environments, 155
sanitization
data remanence, 39
description, 38
hard drives, 251
NIST Special Publication
800-88 guidelines, 35–36
SSDs, 43
workstations, 29, 270–271
Sarbanes-Oxley Act (SOX), 21
SAS 70 reports, 246
SCADA systems, 76
scanners and scanning
authenticated, 132
half open, 128
nmap tool, 135
gerogue devices, 123
SSH, 155
vulnerabilities, 117, 121
scheduler ready state, 56
schedules, backup, 144, 214
scoping
baseline security controls, 42
CIS benchmarks, 30
description, 248
SCP (Secure Copy), 230
screen backgrounds, 41
screen scrapers, 76
screensaver passwords, 109
searches, Fourth Amendment
protection, 156
second-generation firewalls, 89
secondary storage, 251–252
Secret classification, 38, 110, 220
Secure cookies, 278
Secure File Transfer Protocol (SFTP), 279
Secure Shell (SSH)
remote server administration, 35
scanning, 155
Secure Sockets Layer (SSL) in OSI layer, 34, 83
Security Assertion Markup Language (SAML)
cloud computing environments, 193
federation, 254
secure mode, 103
Security Content Automation Protocol (SCAP), 126, 206
Security Information and Event Management (SIEM) tool, 252, 271
security labels, 56
*Security Property, 53
security targets (STs), 282
segmentation, network, 86
segregation of duties, 140
self-service password reset, 108
self-signed digital certificates, 70
senior managers in business continuity planning, 9
separation of duties, 8, 150, 198, 235, 240
serial numbers for CRLs, 69
service-level agreements (SLAs) confidentiality, 10
description, 145
Service Organization Control (SOC) reports, 117–118
audits, 10
SOC 1, 117, 128, 245
SOC 2, 223, 245
SOC 3, 118
service packs, 141
Service Provisioning Markup Language (SPML) description, 203
OASIS, 251
provisioning, 104
service tickets (STs), 280
SESAME SSO systems, 113
session hijacking attacks
cookies, 179–180
TLS, 170
Session layer in OSI model, 85
session monitoring, 131
session time-outs, 109
severity levels, syslog, 247
shadowed passwords, 170, 194–195, 240
shared responsibility model, 243
shared secret keys, 228
sharing identity information, 193
shift ciphers, 58
signal strength in wireless networks, 282
signature-based detection, 103–104, 179
Simple Authentication and Security Layer (SASL), 112
Simple Integrity Property, 50
Simple Mail Transfer Protocol
open relays, 252
OSI layer, 80
Simple Network Management Protocol (SNMP), 80
Simple Security Property, 206–207
Single Loss Expectancy (SLE), 251
single sign-on (SSO)
 implementations
examples, 96, 113
passwords, 221
third-party control, 103
single-tier firewalls, 86
site surveys, 79–80
smart cards
Common Access Cards, 109
identification cards, 60–61
something you have, 198
type 2 authentication, 194
X.509 standard, 260
Smurf attacks
DoS, 7–8
ICMP, 195, 204
sniffing attacks
TLS, 26
VPNs for, 262
social engineering
examples, 126, 160, 191
penetration testing, 195
preventative measures, 253
social media, 139
soda acid fire suppression systems, 66
software
acceptance tests, 160
assurance, 165
dynamic tests, 162
disclosure agreements, 153
forensic investigation analysis, 157
functional requirements, 169
grey-box tests, 175
interface tests, 243
mutation tests, 116
open-source, 57
public domain, 158
regression tests, 171
spiral development model, 176
static tests, 174
test coverage analyses, 121
threat coverage analyses, 20
threat modeling, 161
trademarks, 10
UAT tests, 169
unit tests, 173
use case tests, 212
white-box tests, 172, 190
whitelists, 242
Software as a Service (SaaS)
environments, 49, 63, 142
Software Capability Maturity Model (SW-CMM)
Optimizing stage, 240
Repeatable stage, 178, 211
software-defined networks (SDNs), 85, 139, 239
software development life-cycle (SDLC) model
design reviews, 165
functional requirements determination, 161
waterfall, 234, 269, 287
WBS, 207
software tokens, 205
something you have
authentication, 198
something you know
authentication, 281
somewhere you are factor, 95
source addresses in packets, 240
Spam over Internet Telephony (SPIT) attacks, 81
specifications, 270
spikes, power, 273
spiral software development model, 176
spoofing
ARP, 91
blocking packets, 169
evil twin attacks, 2
login, 95
MAC addresses, 80
spread spectrum techniques, 73
SQL injection attacks
description, 23
indication, 171, 232, 272
input validation, 171, 255
SQL server ports, 116
sqlmap tool, 123
SSAE-16, 135, 199, 259
SSDs
data remanence, 27–28
cryptography, 62
erasing, 190
physical destruction, 282–283
sanitization, 43
SSID broadcasts
- disabling, 75
- enabling, 73
SSID/WTLS, 185
SSL/HTLS, 104–105

stakeholders in change
management, 17

standards of care, 5

star topology, 210, 246

start flags, 184

state machine models, 66–67

state tokens, 108

stateful packet inspection firewalls, 185

statements of accounts, 12

static code analyses, 129, 134, 225, 26

static packet filtering firewalls, 84–85, 204

static software testing, 174

statistical sampling
- logs, 154, 284
- records, 158

stealth viruses, 172

steganography, 58, 146, 194

stop flags, 184

storage
- covert channels, 166
- object-based, 244
- primary, 162
- secondary, 251–252

storage-centric converged protocols, 89

strategic plans, 8

STRIDE model
- elevation of privilege threats, 4, 132
- filtering, 132
- information disclosure, 24, 275
- repudiation, 10, 132, 221
- tampering, 221, 275
- threat categorization, 122

string conversions, 178

structural coverage, 207–208

structured walk-through tests, 264

student records, 246

subject/object model
- access control, 49, 250
- documents, 202

subjects in web applications, 273

subnet masks for Class B networks, 84, 238

supervisory control and data acquisition (SCADA) systems, 51

SW-CMM
- defined stage, 164
- initial stage, 163

managed stage, 164

repeatable stage, 164

symmetric encryption
- data at rest, 44
- keys, 228, 231, 250

SYN flood attacks, 148

synchronized time, 113

synchronous communications, 277

synchronous tokens, 110

synthetic monitoring, 121, 123, 131, 262

synthetic, use case testing, 122

syslog events
- severity levels, 247
- Windows desktop systems, 120

Syslog protocol
- logs, 116
- UDP ports, 226

system administrators, 37

System High mode, 57–58

system logs, 246

system owner responsibilities, 210–211, 281

system security plan updates, 200

TCP
- common ports, 73
- connect scans for open services, 120
- header flags, 216
- headers, 263
- HTTP, 78–79
- OSI model, 229–230
- ports, 282
- reconnaissance attacks, 276
- SYN scans, 128
- TACACS+ servers, 279
- 3-way handshakes, 188, 211–212, 241, 286
- TCP/IP model, 80

TCP packets
- PSH and URG flags, 226
- RST flag, 72

teardrop attacks, 89, 98, 187

technical access control, 16, 109

telnet
- encryption, 30
- ports, 120
- remote server administration, 35

TEMPEST program, 61

Temporal Key Integrity Protocol (TKIP)
- encryption, 204
- WPA, 221

Terminal Access Controller Access-Control System (TACACS), 241

termination of employees, 18

test coverage
- analyses, 121
- computing, 229
- reports, 129

test directories, 208

tests. See penetration tests

third parties
- baselines, 34
- Data Protection Directive, 38
- drive handling, 44
- identity services, 94
- security audits, 133
- SSO directs, 103

verification process, 59–60

1000Base-T 1 gigabit network, 81

threat modeling
- examples, 2
- goals, 161

threats
- repudiation, 10
- risk formula, 13

STRIDE categorization, 122

three-tier firewalls, 85

3-way handshakes in TCP, 188, 211–212, 241, 286

throughput rate in biometric factors, 102

ticket-based authentication, 106

Ticket-Granting Service (TGS), 184

ticket-granting tickets (TGTs), 106–107

hashes, 98

sending, 280

validating, 280

time-based controls, 110

Time of Check to Time of Use (TOC/TOU) attacks

algorithmic complexity, 276

description, 62

file pointers, 277
race conditions, 170
symlinks, 198
timing conditions, 175, 223
timestamps, inconsistent, 132
timing covert channels, 166
TLS. See Transport Layer Security (TLS)
tokens
asynchronous, 111
dynamic passwords, 247
FDDI networks, 82
multifactor authentication, 205
synchronous, 110
Top Secret classification, 282
tornadoes
ALE, 24, 216
ARO, 24
exposure factor, 23
trace coverage, 207–208
trade secrets
Economic Espionage Act, 4–5
intellectual property protection, 206
NDAs, 248
trademarks
intellectual property protection, 6
software protection, 10
USPTO, 8
traffic sniffing
TLS, 26
VPNs for, 262
training
awareness, 5, 83
business continuity plans, 12–13, 254
purpose, 23
transformation procedures (TPs) in
Clark-Wilson integrity model, 213
transformer failures, 146
transitive trusts, 156
Transport layer in OSI model, 83,
229–230, 259, 266
Transport Layer Security (TLS)
data in transit, 36
ephemeral session keys, 67
HIPAA documents, 33
Internet connections, 40
OSI layer, 83
proprietary data, 28
RADIUS over TCP, 108–109
SAML eavesdropping, 103
session hijacking attacks, 170
sniffing attacks, 26
transport mode in ESP, 211
transposition ciphers, 64
Triple DES, 254
Trusted Computing Base (TCB),
61–62
translated paths for login spoofing, 95
Trusted Platform Module (TPM),
51
trusted recovery processes, 282
trusts
Active Directory, 95–96
CSRF attacks, 160
man-in-the-middle attacks,
253–254
one-way nontransitive, 225
transitive, 156
turnstiles, 261
two-person control, 141, 143, 235
two-tier firewalls, 75–88
2G cellular technology, 280
Type 1 authentication factor, 281
Type 1 errors, 243
Type 2 authentication factor, 109,
194, 247
Type 2 errors, 105
Type 3 authentication factor, 94,
110, 112–113

U
UDP
fragile attacks, 156
OSI model, 83, 229–230
ports, 282
RADIUS, 99
syslog service ports, 226
unauthorized vulnerability scans, 147
unencrypted open networks, 185
uninterruptible power supplies
(UPSs), 68, 250
unit testing, 173
United States Code (USC), 283
United States Patent and
Trademark Office (USPTO), 8
unpatched web applications, 225
updates for system security plans,
200
URG flag, 226
URL encoding attacks, 172
US government classification labels
Confidential, 27
mapping, 46
mixed, 33
order, 29
Secret, 38, 220
USB thumb drives, 42
use case testing, 212
user acceptance testing (UAT), 169
user accounts provisioning
process, 217
user awareness, 83
user-defined fields input validation, 179
user IDs
authentication, 106
logging, 125
user interfaces, constrained, 96, 199
user perspective in black-box tests, 166
user programs and applications in
ring protection model, 218
user session monitoring, 131
usernames
credential management systems,
216–217
identification, 22, 224
userPassword attribute, 105

V
vacations, mandatory, 12, 153
validating TGTs, 280
Van Eck radiation, 61
vendor responsibilities
IaaS environments, 59
SaaS environments, 63, 142
verification process, 59–60
virtual machines
cut and paste between, 87
description, 155
escape, 87
virtual private networks (VPNs)
common protocols, 82
confidentiality, 11
data in transit, 36
hopping, 84
L2TP, 253
remote PCs, 75
traffic sniffing, 262
virtual span ports, 256–257
virtualized data centers, 86–87
virtualized environments
hyperlivers, 68, 145
sandboxing, 155
SDN, 139
viruses
hiding antimalware software
from, 169
macro, 164
MBR, 181
multipartite, 169, 181
polymorphic, 167
stealth, 172
vital records programs, 22–23
VLANs, 91
VMware environment, 256–257
voice communication, PBX systems, 84
voice pattern recognition, 94
VoIP systems
  attack examples, 278–279
  DoS and host OS attacks, 241
  SPIT attacks, 81
  VPN hopping, 84
  volatile memory, 209
VPNs. See virtual private networks (VPNs)
Vulnerabilities
  causes, 126
  CVE, 135, 142–143, 282
  CVSS, 130
  maintenance hooks, 30
  nessus tool, 180
  NVD, 282
  OpenVAS for, 116
  patches, 122
  path disclosure, 121
  remediation, 130
  risk formula, 13
  scanners, 117, 121
  SCAP, 126
  zero-day, 135, 148
Vulnerability scans and scanners
  examples, 202
  unauthorized, 147
  web applications, 130

W
Waiting process state, 222
Wapiti tool, 130
warm sites, 229, 266, 273
waterfall model, 179, 234, 269, 287
watermarks
  description, 28
  example, 149
owner identification, 44
purpose, 272
wave pattern motion detectors, 185
wear leveling in SSDs, 62
web application firewalls (WAFs), 168
web applications
  cross-site scripting attacks, 264
  forms, 116
  input validation, 255
  interface testing, 205
  OWASP, 66
  passwords, 107–108
  penetration tests, 180
  Secure cookies, 278
  subjects, 273
  unpached, 225
  vulnerability scanners, 130
  web defacement, 284
web-based attack vectors, 169
web defacement, 284
websites
  COPPA regulations, 260
  OpenID integration, 219
  white-box tests, 129, 172, 190
  white noise, 63
  whitelisters, 188–189, 242
  Whois tool, 208
  Windows desktop system syslog events, 120
  Windows SQL server ports, 116
  Wired Equivalent Privacy (WEP) keys, 76–77, 91
wireless networks
  ad hoc mode, 72
  signal strength, 282
  site surveys, 79–80
  SSID broadcasts, 73
  SSIDs, 185
wireless scanning, 118
Wireshark tool, 20, 221
wiring closets, 55
work breakdown structure (WBS), 207
workflow-based account provisioning, 201
workstations
  logging into, 138
  sanitization, 29, 270–271
worms, 167, 187, 244
WPA, 221
WPA2, 83
CCMP, 87
Enterprise mode, 117
SSIDs, 185
write blockers, 278
written works, 9

X
X.25 standard, 72, 245
X.500 standard, 105
X.509 standard
  digital certificates, 62–63
  smartcards, 260
Xmas scans, 135
XOR operation, 53
XSRF (cross-site request forgery)
  attacks
    state tokens, 108
    trust relationships, 160

Z
zero-day attacks
  detecting, 234
  heuristic-based antimalware software, 172
NAC systems, 207
patches, 256
vulnerabilities, 135, 148
zero-knowledge proof technique, 65
zzuf tool, 122