INDEX

Numbers

3DES, 70

A

access controls
  access control lists (ACLs), 38–43
  implementation of, 37–43
  models, 43–48
  overview, 35–37
  physical access controls, 48–50, 124–125
accountability, 52–55
active discovery, 193
address space layout randomization (ASLR), 151–152
Adleman, Leonard, 71
administrative controls, 14, 81, 127
Advanced Encryption Standard (AES), 70, 178
agented scans, 194
air-gapped networks, 165
alerting, 204
AMD, 152
anomaly detection, 138, 151
anti-malware tools, 151
Apple, 163
applications. *See also* software
  mobile devices, 163
  overview, 173–174
  penetration testing (pentesting) of, 198–199
  scanning, 194
  tools for, 184–188
arbitrary code execution, 183
The Art of War (Sun Tzu), 102
Ashton, Kevin, 167
assessments, 57–58
asset identification, 11
associated risk, 10. *See also* risks
asymmetric key cryptography, 70–71. *See also* cryptography
attacks
  attack surfaces, 146
  denial-of-service (DoS) attacks, 5
  types of, 8–10
attribute-based access control (ABAC), 45
auditing, 52, 55–58, 150
authenticated scans, 193–194
authentication
  attacks, 177, 183
  methods of, 25–33
  overview, 7, 23–24, 25–28
authority to operate (ATO), 84
authorization. *See also* access controls
  attacks, 177
  vs. authentication, 25
  overview, 35
automobiles, 165–166
availability
  and confidentiality, integrity, and availability (CIA) triad, 5
  interruption attacks, 9
  Parkerian hexad and, 7

B

baseband operating systems, 162
Bell–LaPadula model, 46
Biba model, 47
biometrics, 26, 29–32
Bitcoin, 92
black-box testing, 197
black hat hackers, 195
blackholing, 40
blockchain, 91–92
block ciphers, 69–70
block mode, 69
blue teams, 203
botnets, 170
bounds checking, 175
breaches, 100
Brewer and Nash Model, 47–48

bring-your-own-device (BYOD) policies, 161
browsers, 179
brute forcing, 68
buffer overflows, 151–152, 175
bug bounty programs, 200–201
Bugcrowd, 201
bugs, 130
Burp Suite, 187–188, 194
business competition, 103
business continuity planning (BCP), 122
Business Software Alliance (BSA), 56

C

Caesar cipher, 62
cameras, 168
Cameroon, 134
capabilities, 42–43
CAPTCHAs, 45
The Car Hacker's Handbook (Smith), 166
cars, 165–166
central management, 159–161
certificate authority, 73
certificates, 73–74
chain of custody, 55
Children's Internet Protection Act (CIPA) (2000), 86
Children's Online Privacy Protection Act (COPPA) (1988), 86
Chinese Wall model, 47–48
choke points, 134, 169, 193
Cisco, 25
class A and class B internal networks, 192
clean desk policies, 119
cleartext, 61
clickjacking, 42, 178–179
client-side attacks, 41, 178–179
cloud computing, 89–91, 194–195, 201
code, 183
collision, 72
compensating controls, 82
competitive intelligence and competitive counterintelligence, 103
Competitive Strategy: Techniques for Analyzing Industries and Competitors (Porter), 103
compliance. *See also* laws and regulations
  controls for achieving, 81–82
  frameworks for, 87–89
  maintaining, 82–83
  overview, 79–81
  technological changes and, 89–92
confidentiality, 5, 7
confidentiality, integrity, and availability (CIA) triad, 4–6, 8
configuration files, 180
confused deputy problem, 41
containers, 195
controller area network (CAN) bus, 165–166
controls, 14
corporate-owned business only (COBO) and corporate-owned personally enabled (COPE) mobile devices, 161
Cotton, Gerald, 92
countermeasures, 98
critical information assets, 96
cross-site request forgery (CSRF), 41–42, 178–179
cross-site scripting (XSS), 178
cryptocurrencies, 92, 163
cryptography
  algorithms, 61–66
  asymmetric key cryptography, 70–71
  attacks, 178
  elliptic curve cryptography (ECC), 71
  history of, 62–66
  keyless cryptography, 71–72
  overview, 61
  symmetric key cryptography, 68–69
  tools for, 67–74
  uses of, 74–77
cyber intelligence/digital network intelligence (CYBINT/DNINT), 114

D

data
  protection of, 127–129
  at rest and in motion, 9, 74–77
  storage of, 7, 128–129
databases, 181–184
Data-Life project, 169
deep packet inspection firewalls, 136
default accounts, 148–149
defense in depth strategy, 17–20
demilitarized zones (DMZs), 137
denial-of-service (DoS) attacks, 5
DES, 69–70
detective controls, 123–124
deterrence, 54

deterrent controls, 123
Diffie, Whitfield, 70
digital certificates, 73–74
digital network intelligence (DNINT), 114
digital signatures, 72–73
directory traversal attacks, 180
disaster recovery planning (DRP), 122
disclosure, alteration, and denial (DAD), 5. *See also* confidentiality, integrity, and availability (CIA) triad
discretionary access control (DAC) model, 43
distributed denial-of-service (DDoS) attacks, 170
DMZs (demilitarized zones), 137
dongles, 32
dynamic analysis, 199

E

Ecole de Guerre Economique (Economic Warfare School), 103
electronic intelligence (ELINT), 114
electronic protected health information (e-PHI), 85
elliptic curve cryptography (ECC), 71
embedded devices, 164–167, 169
encryption, 61, 70, 178
energy anomalies, 125
Enhanced Virus Protection, 152
Enigma machine, 64–65
enterprise mobility management, 161
environmental attributes, 45
equal error rates (EERs), 31
Equifax, 53
equipment, 129–132
EtherApe, 185
Ethereal, 142
ethical hacking, 195–200
evacuations, 126–127
executable space protection, 151–152
Execute Disable (XD) bit, 152
EXIF data, 111–112
exploit frameworks, 156

F

fabrication attacks, 10
Facebook, 109
factors, 26–27
false acceptance rates (FARs) and false rejection rates (FRRs), 31
falsified information, 25
Family Educational Rights and Privacy Act (FERPA) (1974), 86
Fazio Mechanical, 174
Federal Information Security Management Act (FISMA) (2002), 4, 84
Federal Risk and Authorization Management Program (FedRAMP), 85
Fighting Computer Crime (Parker), 6, 122
file metadata, 111
file system ACLs, 38–39
FIM (file integrity monitoring) tools, 203–204
financial intelligence (FININT), 114
fingerprints, 29–30. *See also* biometrics
firewalls, 135–137, 143–144, 152–153
flash media, 128
forensic investigations, 111
format string attacks, 176
frequency analysis, 67
FTP (File Transfer Protocol), 140
full disk encryption, 75
fuzzers, 188

G

General Data Protection Regulation (GDPR) (2018), 87
geospatial intelligence (GEOINT), 113
GitHub, 169
Global Positioning System (GPS) information, 112
Google, 110–111, 163, 200
Gramm–Leach–Bliley Act (GLBA) (1999), 86
gray-box testing, 198
Greenbone, 155
group permissions, 39

H

Haase, Kurt, 99
HackerOne, 201
hard-coded passwords, 177
hardware devices, 200
hardware tokens, 32–33
hash functions, 71–72

Health Insurance Portability and Accountability Act (HIPAA) (1996), 4, 52, 85
Hellman, Martin, 70
heuristics, 151
honeypots and honeynets, 143
hosts, 193
human intelligence (HUMINT), 108

I

IaaS (infrastructure as a service) environments, 89–91, 195
identification, 23–33
identity thieves, 25
impact, 11
impersonation attacks, 27–28
incident response process, 15–17
industrial control systems, 164–165
industrial espionage, 103
industry compliance, 80–81. *See also* compliance
information security policies, 81–82
infrastructure as a service (IaaS) environments, 89–91, 195
input validation attacks, 176, 180
integrity, 5, 7
Intel, 152
Interagency OPSEC Support Staff (IOSS), 104
interception attacks, 8
International Organization for Standardization (ISO), 88
Internet of Things (IoT) devices, 159, 167–170
Internet Protocol (IP) addresses, 40
Internet Protocol Security (IPsec), 76
interruption attacks, 9
intrusion detection systems (IDSs)
  accountability and, 54–55
  implementation of, 138
  operating systems and, 152–153
intrusion prevention systems (IPSs), 54–55
IOSS (Interagency OPSEC Support Staff), 104
IP addresses, 40

J

jailbreaking, 162–163
Java Virtual Machine (JVM), 37
Jefferson Disk, 62–64
job listings, 109
Joint Test Action Group (JTAG) debug ports, 200

K

Kali, 141
Kerckhoffs, Auguste, 66
key controls, 82
key exchange, 68
keyless cryptography, 71–72
keys, 61
keyword ciphers, 67
Kismet, 141, 143
KRACK vulnerability, 168

L

laws and regulations. *See also* compliance
  Children's Internet Protection Act (CIPA) (2000), 86
  Children's Online Privacy Protection Act (COPPA) (1988), 86
  familiarity with, 119
  Family Educational Rights and Privacy Act (FERPA) (1974), 86
  Federal Information Security Management Act (FISMA) (2002), 4
  General Data Protection Regulation (GDPR) (2018), 87
  Gramm–Leach–Bliley Act (GLBA) (1999), 86
  Health Insurance Portability and Accountability Act (HIPAA) (1996), 4, 52, 85
  international, 87
  overview, 4
  Sarbanes–Oxley Act (SOX) (2002), 52, 55, 85
Linux operating systems, 141, 149, 185
logging, 56–57, 150
logical controls, 14

M

magnetic media, 127–129
malicious apps, 163
Maltego, 113

malware, 118, 151–153, 170
mandatory access control (MAC) model, 43
man-in-the-middle attacks, 27–28
mapping environments, 192
measurement and signature intelligence (MASINT), 113
Media Access Control addresses, 40
medical devices, 165
metadata, 111
Metasploit framework, 155
Microsoft, 149
Miller, Barton, 188
Miller, Charlie, 166
minutiae, 29–30
Mirai botnet, 170
mitmproxy, 169
mobile devices, 160–164
modification attacks, 9
Mogul, Jeffrey, 135
monitoring, 57
multifactor authentication, 27
multilevel access control models, 45–48
mutual authentication, 27

N

National Institute of Standards and Technology (NIST), 84, 88
National Security Agency (NSA), 11
Nessus, 191
networks
  access control lists (ACLs), 39–41
  air-gapped networks, 165
  class A and class B internal networks, 192
  Internet of Things (IoT) devices on, 167–168
  overview, 133–134
  penetration testing of, 198
  protection of, 134–138
  security tools, 140–144
  segmentation, 134
  tools for, 140–144
  usage, 117–118
  virtual private network (VPN) connections, 76, 118, 139
  wireless networks, 139–141
NIST (National Institute of Standards and Technology), 84, 88
Nmap, 141, 147–148, 153–155, 192
noncompliance, 81. *See also* compliance
nonmobile devices, 161
nonrepudiation, 7, 54, 73
NoScript, 179

O

one-time pads, 67–68
one-way problems, 66
open source intelligence (OSINT), 108–113
OpenVAS, 155–156
operating systems
  malware and, 151–153
  operating system hardening, 146–150
  overview, 145–146
  tools for, 153–156
operations security (OPSEC)
  laws of, 99–100
  origins of, 101–104
  overview, 95–98
  personal data and, 100–101
optical media, 128
OWASP Zed Attack Proxy (ZAP), 186

P

PaaS (platform as a service) environments, 89–91, 195
packets, 135–136, 138
packet sniffers, 142–143
Parker, Donn, 6–8, 122
Parkerian hexad, 6–8, 12
passive scanning, 193
passwords
  authentication attacks and, 177
  defense in depth strategy, 18
  overview, 28–29
  password managers, 29
  security training programs and, 116–117
Payment Card Industry Data Security Standard (PCI DSS), 4, 80
penetration testing (pentesting), 19, 58, 195–201
people, protection of, 125–127
permissions, 38–40
personal equipment, 118
phishing, 114–115
physical controls
  compliance and, 81
  overview, 14, 48–50
  types of, 122–125

physical penetration testing, 199
physical security
data, 75, 127–129
devices, 168
equipment, 129–132
overview, 121–122
people, 125–127
threats, 122
plaintext, 61
platform as a service (PaaS) environments, 89–91, 195
Porter, Michael E., 103
ports, 40–41
port scanners, 141, 147–148, 153–155
possession, 7
Post Office Protocol (POP), 140
pretexting, 114
Pretty Good Privacy (PGP), 71
preventive controls, 124
principle of least privilege, 43–44, 149
printers, 167
Privacy Rights Clearinghouse, 100
privilege escalation attacks, 183–184
protected health information (PHI), 85
protocols
FTP (File Transfer Protocol), 140
Internet Protocol (IP) addresses, 40
Internet Protocol Security (IPsec), 76
Post Office Protocol (POP), 140
Secure File Transfer Protocol (SFTP), 140
Secure Sockets Layer (SSL) protocol, 71
Signaling System No. 7 (SS7) protocol, 162
vulnerabilities and, 182
proxy servers, 137
public key infrastructure (PKI), 74
public records, 109–110
public wireless networks, 139–141
Purple Dragon, 103
purple teams, 203

Q

Quadriga, 92
Qualys, 58, 191

R

race conditions, 175–176
RAID arrays, 128
reactive tools, 56–57
Reagan, Ronald, 104
real-time operating systems (RTOSs), 164–165
red teams, 196
redundant arrays of inexpensive disks (RAID), 128
regulations. *See* laws and regulations
regulatory compliance, 80–81. *See also* compliance
remote code executions (RCEs), 53, 183
residual data, 129
resource attributes, 45
résumés, 109
risk-based approach, 84
risks. *See also* operations security (OPSEC)
assessment of, 13, 98
management processes, 11
mitigation of, 14
overview, 10
Rivest, Ron, 71
Rivest-Shamir-Adleman (RSA) algorithm, 71, 178
rogue access points, 139–140
role-based access control (RBAC) model, 44
ROT13 cipher, 62
rule-based access control, 44
rules of engagement, 196, 201

S

SaaS (software as a service) environments, 89–91
safety of people, 126
sandboxes, 37
Sarbanes–Oxley Act (SOX) (2002), 52, 55, 85
SaverSpy, 100
scanners, 141, 153–155, 193–194. *See also* vulnerabilities
Scapy, 143
SCIP (Strategic and Competitive Intelligence Professionals), 103
scoping, 196
Secure File Transfer Protocol (SFTP), 140
secure protocols, 140
Secure Shell (SSH), 140
Secure Sockets Layer (SSL) protocol, 71
security through obscurity strategy, 65

segmentation, 134
server-side attacks, 179–181
services, 147–148
SFTP (Secure File Transfer Protocol), 140
Shamir, Adi, 71
Shannon, Claude, 66
shifts, 67–68
Shodan, 100, 112
Signaling System No. 7 (SS7) protocol, 162
signals intelligence (SIGINT), 114
signature-based IDS, 138
"Simple and Flexible Datagram Access Controls" (Mogul), 135
smart devices, 159, 167–170
smart locks, 168
sniffers, 142–143, 184–185
Snowden, Edward, 76
social engineering attacks
  information for, 108–114
  overview, 107–108
  penetration testing (pentesting) and, 199–200
  security training programs and, 117
  types of, 114–116
social media, 101, 109
sockets, 41
software. *See also* applications
  databases, 181–184
  extraneous, 146–147, 181
  licenses, 56
  vulnerabilities, 174–178
  web applications, 178–181
software as a service (SaaS) environments, 89–91
Spafford, Eugene, 2
spear phishing, 115
Special Publications (SPs), 84, 88
spidering, 186
SQL injection, 184
SSH (Secure Shell), 140
stateful packet inspection firewalls, 136
static analysis, 199
Strategic and Competitive Intelligence Professionals (SCIP), 103
stream ciphers, 69
StrongVPN, 139
Stuxnet virus, 164
subject attributes, 45
subnets, 134
substitution ciphers, 62
Sun Tzu, 102
supervisory control and data acquisition systems, 164
surveillance cameras, 168
symmetric key cryptography, 68–69. *See also* cryptography
Synack, 201

T

tailgating, 48–49, 116, 200
Talos Intelligence Group, 25
Tapplock, 168
Target Corporation, 173–174
Tcpdump, 142
technical controls, 14, 82
technical intelligence (TECHINT), 114
technological changes
  compliance and, 89–92
  data storage and, 128
  Internet of Things (IoT) devices and, 170
  vulnerability assessments and, 204–205
threats. *See also* operations security (OPSEC)
  analysis of, 97
  identification of, 12, 122
  overview, 10
tokens, 42–43
Triton, 151, 164
trust but verify, 117, 187
two-factor authentication, 27

U

unauthenticated scans, 193
unified endpoint management, 161
Universal Asynchronous Receiver/Transmitter (UART) debug ports, 200
UNIX operating systems, 149
updates
  browsers, 179
  embedded devices, 166
  mobile devices, 163–164
  operating systems, 150
user interface redressing, 42
US National Institute of Standards and Technology (NIST), 84
US National Security Agency (NSA), 11
utility, 7

V

Valasek, Chris, 166
validation, 176, 180
vehicles, 165–166
Vietnam War, 103
VPN (virtual private network) connections, 76, 118, 139
vulnerabilities. *See also* operations security (OPSEC)
  assessment of, 12–13, 58, 97, 155–156, 191–195
  overview, 10
  protocols and, 182
  scanners, 141, 153–155, 193–194
  software development, 174–178

W

Washington, George, 102
web applications, 178–181
white-box testing, 197–198
Wi-Fi Protected Access (WPA, WPA2, and WPA3), 140
Wired Equivalent Privacy (WEP), 140
wireless networks, 139–140, 141
Wireshark, 142, 184–185

X

XD bit, 152
XSS (cross-site scripting), 178

Z

ZAP (Zed Attack Proxy), 186
zero-day attacks, 141