

# INDEX

## Symbols

- \* integrity axiom (star integrity axiom), 55
- \* property (star property), 54

## Numbers

- 1Password, 264
- 2FA (two-factor authentication), 33
- 3DES, 82, 83
- 2600 meetings, 279

## A

- AC (attack complexity), 206
- acceptability, 37
- access, 44–45
- access control lists (ACLs), 46–50
- access control models, 51
  - attribute-based, 52–53
  - CAPTCHA illustration, 53
  - discretionary, 51
  - mandatory, 51–52
  - multilevel, 53–56
  - role-based, 52
  - rule-based, 52
- access controls
  - defined, 43
  - finding confused deputies in wild, 59
  - implementing
    - access control lists, 46–50
    - capabilities, 50–51
  - overview, 44–45
  - physical, 56–57
  - review questions, 58
  - sandbox illustration, 45
- accountability
  - in AI systems, 188–189
  - chart, 62
  - defined, 62
  - overview, 62–63
  - review questions, 69
  - security benefits of, 63–65
  - structures for, 211
  - working with audit logs, 69–71
- accountable parties, 211
- accounts, 128–129, 200
- ACLs (access control lists), 46–50
- active discovery, 231
- address space layout randomization (ASLR), 131
- Adleman, Leonard, 84
- administrative accounts, 129
- administrative controls, 214–215
- admissibility of records, 65
- Advanced Encryption Standard (AES), 83
- advanced persistent threat (APT)
  - groups, 26
- adversarial attacks, 180
- adversarial exploits, 181–182
- adversary emulation, 283
- AES (Advanced Encryption Standard), 83
- agented scans, 232
- agents, 142–143, 232
- AI. *See* artificial intelligence
- Aircrack-ng, 119
- air-gapped networks, 146
- airport security, 57
- alert fatigue, 242
- alerts
  - designing, 197–198
  - vs. incidents, 201
  - tuning, 199, 242
- Amazing Fantasy #15* (Lee), 223
- AMD, 131
- analysts in SecOps team, 196
- Android, 142
- anomaly-based IDSs, 115
- anti-malware tools, 131
- Apple, 125, 144
- application layer, 15
- application penetration testing, 236–237

- application scans, 232
- application security
  - database security, 166–169
  - linking CWEs with CVEs, 174–175
  - review questions, 174
  - software development vulnerabilities
    - authentication attacks, 162
    - authorization attacks, 162
    - buffer overflows, 159–160
    - cryptographic attacks, 163
    - input validation attacks, 161
    - overview, 158–159
    - race conditions, 160–161
  - tools, 169–173
  - web security, 163–166
- app permissions, 152–155
- APT (advanced persistent threat)
  - groups, 26
- APT44, 23
- arbitrary code execution, 168–169
- artificial intelligence (AI)
  - and autonomous malware, 24
  - and compliance, 224–225
  - defined, 178–179
  - and impersonation attacks, 259
  - life cycle, 184–186
  - LLMs and generative AI, 180
  - vs. machine learning vs. deep learning, 179–180
  - malicious, 191
  - security
    - AI changing security operations, 189–190
    - designing safer systems, 184–187
    - foundations of, 178–180
    - responsible practices, 187–189
    - review questions, 191
    - risks and vulnerabilities, 180–184
    - slaughterbots and malicious AI, 191
- arXiv, 191
- Ashton, Kevin, 148
- assessments, 67–68, 223–224
- assets, 212
- assume breach security architecture, 102
- asymmetric cryptography, 83–84
- AT (attack requirements), 206
- ATO (authorization to operate), 217
- attack complexity (AC), 206
- attackers, 242–243
- attack requirements (AT), 206
- attacks, 9–12, 187. *See also* social engineering attacks
  - authentication attacks, 162
  - authorization attacks, 162
  - buffer overflow attacks, 131–132, 159–160
  - client-side attacks, 49, 163–164
  - cryptographic attacks, 163
  - denial-of-service (DoS) attacks, 7
  - directory traversal attacks, 165
  - fabrication attacks, 11
  - format string attacks, 161
  - impersonation attacks, 34, 259
  - interception attacks, 9–10
  - interruption attacks, 10
  - man-in-the-middle attacks, 34, 82
  - membership inference attacks, 183
  - MGM resorts attack, 274–275
  - model inversion attacks, 183
  - modification attacks, 10
  - prompt injection attacks, 181
  - quid pro quo attacks, 258–259
  - resource exhaustion attacks, 184
  - server-side attacks, 164–166
  - smishing attacks, 259–260
  - zero-day attacks, 118
- attack surface, 126, 242
- attack vector (AV), 206
- attribute-based access control (ABAC)
  - model, 52–53
- attribution, 25
- auditable models, 186–187
- auditing
  - app permissions, 152–155
  - of cloud environments, 223–224
  - defined, 62
  - in operating system hardening, 130
  - overview, 65–68
  - review questions, 69
  - working with logs, 69–71
- audit logs, 69–71
- authenticated scans, 231–232
- authentication
  - attacks, 162
  - common methods of, 34–38
  - defined, 29

- hashing passwords, 41–42
  - overview, 31–34
  - review questions, 40
  - sending security token to mobile
    - phone, 32
- authenticity, 8
- authorization, 43. *See also* access controls
  - attacks, 162
- authorization to operate (ATO), 217
- Auto-ID Center, 148
- autonomous actors, 23–24
- autonomous malware, 24
- AV (attack vector), 206
- availability, 7
- awareness program, 266–269

## B

- baiting, 258
- baseband operating system, 143–144
- Bell-LaPadula model, 54
- Berkeley Artificial Intelligence Research
  - blog, 191
- bias risks, 188
- Biba access control model, 54–55
- Biography, 28
- biometrics, 32, 35–38
- Bitcoin, 225
- BitLocker, 88
- black-box testing, 235–236
- black hat hackers, 234
- blackholing, 48
- BlackPOS malware, 158
- Bletchley Park, 78
- block mode, 82
- Blowfish cipher, 83
- blue team, 241, 282–283
- bolted-on security, 98–99
- Bombe computer, 78
- botnets, 13, 24
- bounds checking, 159
- box-checking, 99
- breach disclosure laws, 63
- Breachsense, 108
- Brewer and Nash model, 55–56
- bring-your-own-device (BYOD)
  - policy, 143
- browsers, 164
- bruteforcing, 81

- BSA (Business Software Alliance), 66
- buffer overflow attack, 131–132, 159–160
- buffer overruns, 159
- bug bounty hunting, 21
- bug bounty programs, 238–239
- Bugcrowd, 239
- builders in security, 283–284
- built-in security, 98–99
- Burp Suite, 172, 232
- Business Software Alliance (BSA), 66

## C

- Caesar cipher, 74, 81
- CAI (confidentiality, integrity, and availability triad), 6–7
- CAN (controller area network) bus, 147
- Canarytokens, 122–123
- capability-based systems, 50–51
- CAPTCHAs, 53
- careers in security, 282–284
- Car Hacker's Handbook, The* (Smith), 147
- Carnegie Mellon University, 158
- cars, 147
- CAST5 cipher, 83
- CBTs (computer-based training), 269–270
- Central Collection Unit of the Intelligence Corps (Unit 8200), 20
- central management, 142
- certificate authority, 86
- certificates, 86–87
- certifications for security professionals, 280–281
- Certified Information Systems Security Professional (CISSP), 280
- chain of custody, 65
- Charge Healthcare, 63
- Children's Internet Protection Act (CIPA), 219
- Children's Online Privacy Protection Act (COPPA), 219
- choke points, 112
- CIA (confidentiality, integrity, and availability triad), 6–7
- ciphers. *See also* cryptography
  - block vs. stream, 82
  - Caesar, 74, 81
  - keyword, 80
  - one-time pads, 80–81

- ciphertext, 73
- circumvention, 37
- Cisco, 31
- CISSP (Certified Information Systems Security Professional), 280
- city planning metaphor, 98–99
- clarity in security architecture, 101
- class A internal network, 230
- class B internal network, 230
- clean desk policies, 266
- clean up after development, 165–166
- cleartext, 73
- clickjacking, 49–50, 164
- client-side attacks, 49, 163–164
- clipping level, 67
- cloud environments
  - and compliance, 222–224
  - penetration testing, 239
  - responsibility of providers, 223
  - scanning for vulnerabilities, 232–233
  - service providers, 218
- Cloud Security Alliance (CSA), 279
- Cobalt Strike, 135
- COBIT (Control Objectives for Information and Related Technologies), 211
- collectability, 37
- collision, 85
- collusion, 100
- Common Vulnerabilities and Exposures (CVEs)
  - calculating vulnerability severity, 204–207
  - confused deputies, 59
  - linking with CWEs, 174–175
  - overview, 11
- Common Vulnerability Scoring System (CVSS), 204–207
- Common Weakness Enumerations (CWEs), 159, 174–175, 204
- communication in security, 284–286, 288
- communication policy, 260
- communications intelligence (COMINT), 255
- company groups, 55
- compensating controls, 215
- complex passwords, 35
- compliance
  - creating cryptocurrency plan for, 226–228
  - defined, 209, 215
  - frameworks for, 220–222
  - industry-specific, 218–220
  - international regulatory environments, 220
  - modern regulatory challenges, 222–226
  - types of, 216–217
  - US government, 217–218
- CompTIA (Computing Technology Industry Association), 280
- CompTIA Advanced Security Practitioner (CASP), 280
- computer-based training (CBTs), 269–270
- Computer Emergency Response Team, 158
- computer science degree, 278
- Computing Technology Industry Association (CompTIA), 280
- Conficker E, 24
- Conficker worm, 24
- confidentiality, 6
- confidentiality, integrity, and availability triad (CIA; CAI), 6–7
- configuration files, 165
- conflict classes, 55
- confused deputy problem, 49, 59
- connections, 89, 114
- consulted parties, 211
- containers, 233
- containment, 203
- containment, eradication, and recovery phase, 203
- Contec patient monitors, 146
- control in Parkerian hexad, 8
- controller area network (CAN) bus, 147
- Control Objectives for Information and Related Technologies (COBIT), 211
- controls for risk mitigation, 214
- COPPA (Children’s Online Privacy Protection Act), 219
- Core Impact, 135
- Cornell University, 23
- corporate-owned business only (COBO) devices, 143

- corporate-owned personally enabled (COPE) devices, 143
- corporations, 21–22
- correlation, 197
- Cotten, Gerald, 225
- credit cards, 216–217
- criminal groups, 22
- critical-risk systems, 106
- cross-site request forgery (CSRF), 49–50, 163–164
- cross-site scripting (XSS), 163
- CrowdStrike security company, 89
- cryptocurrency, 225–228
- cryptographic algorithm, 73
- cryptographic attacks, 163
- cryptographic machines, 75–78
- cryptography
  - defined, 73
  - encrypting and decrypting with PGB, 91–93
  - history of
    - Caesar cipher, 74
    - cryptographic machines, 75–78
    - Kerckhoffs’s principles, 78–79
  - modern cryptographic tools
    - certificates, 86–87
    - digital signatures, 85–86
    - keyword ciphers and one-time pads, 80–81
    - overview, 79–80
    - symmetric and asymmetric cryptography, 81–85
  - overview, 73
  - protecting data, 87–89
  - review questions, 90–91
- CryptoLaw, 227
- CSF (NIST Cybersecurity Framework), 211
- CSRF (cross-site request forgery), 49–50, 163–164
- custom resource definition (CRD), 59
- CVEdetails.com, 59
- CVE Program, 59
- CVEs. *See* Common Vulnerabilities and Exposures
- CVSS (Common Vulnerability Scoring System), 204–207
- CWEs (Common Weakness Enumeration), 159, 174–175, 204
- CyberChef tool
  - generating PGP key pair, 91–92
  - hashing passwords, 41–42
  - testing password entropy, 17–18
- cyber intelligence (CYBINT), 256
- cybersecurity
  - attacks, 9–12
  - college degree in, 278
  - defense in depth, 12–15
  - defined, 4
  - level of security, 4–6
  - models for discussing security issues, 6–9
  - testing password entropy, 17–18
- Cybersecurity Ventures, 108

**D**

- DAC (discretionary access control)
  - model, 51
- Dark Angels, 22
- data
  - leakage, 183–184
  - in motion, 10, 87–89
  - poisoning, 182
  - privacy laws, 5
  - protecting over wireless networks, 117
  - at rest, 10, 87–88
  - security, 88
  - in use, 10, 87, 89
- database security, 166–169
- data cleaning and preprocessing
  - phase, 185
- data collection phase, 185
- Data Encryption Standard (DES), 82
- data layer, 15
- Data Life project, 150–151
- data loss prevention (DLP), 102, 261
- data points (transforms), 254
- DDoS (distributed denial-of-service)
  - attacks, 13, 112, 177
- decryption, 73, 91–93
- DEC SEAL, 113
- deep learning, 179–180
- deep packet inspection firewalls, 114
- default accounts, 128–129
- default deny state, 101

DEF CON Groups, 279  
 defenders role in security, 282–283.  
     *See also* blue team  
 defense in depth, 12–15, 102  
 demilitarized zones (DMZs), 114–115  
 denial-of-service (DoS) attack, 7  
 deployment phase, 186  
 deprovisioning accounts, 200  
 DES (Data Encryption Standard), 82  
 detection and analysis phase, 202  
 detection engineering, 198–199  
 deterministic systems, 179  
 deterrence, 64  
 device fingerprints, 134  
 Diffie, Whitfield, 83  
 Diffie-Hellman key exchange, 84  
 digital certificate, 86  
 Digital Equipment Corporation, 113  
 digital network intelligence  
     (DNINT), 256  
 digital signatures, 84–86  
 Digital Signature Standard (DSS), 84  
 directories, 46  
 directory traversal attacks, 165  
 disclosure, alteration, and denial  
     (DAD), 6  
 discovery phase, 235  
 discretionary access control (DAC)  
     model, 51  
 distributed denial-of-service (DDoS)  
     attacks, 13, 112, 177  
 DLP (data loss prevention), 102, 261  
 dm-crypt, 88  
 dongles, 39  
 DoS (denial-of-service) attack, 7  
 DSS (Digital Signature Standard), 84  
 Dyn, 151  
 dynamic analysis, 238

**E**  
 ECC (elliptic curve cryptography), 84  
 education-first path into security  
     profession, 278–279  
 EER (equal error rate), 37  
 electronic intelligence (ELINT), 255  
 electronic protected health information  
     (e-PHI), 218  
 ElGamal, 84  
 ELINT (electronic intelligence), 255  
 elliptic curve cryptography (ECC), 84  
 Elliptic Curve Digital Signature  
     Algorithm (ECDSA), 84  
 email security controls, 260  
 embedded devices  
     defined, 141  
     vs. IOT devices, 150  
     security of, 145–148  
 embedding exploits, 181–182  
 emergent behavior, 178  
 EnCase, 253  
 encryption, 73, 91–93  
 endpoint protection, 260  
 engineers in SecOps team, 196  
 engineers in security, 283–284  
 Enhanced Virus Protection, 131  
 Enigma machine, 77–78  
 Enron scandal, 218  
 enterprise mobility management, 142  
 enterprise security architecture, 107  
 entropy in passwords, 14  
 environmental attributes, 53  
 environmental metrics, 206  
 e-PHI (electronic protected health  
     information), 218  
 Epsimed patient monitors, 146  
 equal error rate (EER), 37  
 eradication in incident life cycle, 203  
 EtherApe, 170  
 Ethereal, 120  
 ethical hacking. *See* penetration testing  
 ethics in AI, 187–188  
 EU AI Act, 188  
 European Commission, 227  
 European Union, 188  
 events, 197–198  
 excessive agency, 181  
 executable space protection, 131–132  
 Execute Disable (XD) bit, 131  
 execute permission, 46  
 ExifTool, 253  
 experience-first path into security  
     profession, 278  
 explainable models, 186  
 exploitability metrics, 206  
 exploitation phase, 235  
 exploit frameworks, 135–136

- exploit maturity, 206
- exploits, 135
- external network layer, 15
- external penetration testing, 236

## F

- fabrication attacks, 11
- factors of authentication, 31–33
- fairness risks, 188
- false acceptance rate (FAR), 37
- false negative, 37
- false positive, 37
- false rejection rate (FRR), 37
- Family Educational Rights and Privacy Act (FERPA), 220
- FAR (false acceptance rate), 37
- Fazio Mechanical, 158
- Federal Information Security Modernization Act (FISMA), 5, 217
- FedRAMP (Federal Risk and Authorization Management Program), 217–218
- FERPA (Family Educational Rights and Privacy Act), 220
- Fighting Computer Crime* (Parker), 7
- file integrity monitoring (FIM) tools, 241–242
- files
  - extraneous, 165–166
  - metadata, 253–254
- filesystem ACLs, 46–47
- File Transfer Protocol (FTP), 49, 117–118
- filetype operator, 252
- FIM (file integrity monitoring) tools, 241–242
- Financial Action Task Force (FATF), 227
- Financial Crimes Enforcement Network, 227
- financial institutions, 219
- financial intelligence (FININT), 256
- findings, 230
- firewalls, 113–115, 121
- FISMA (Federal Information Security Modernization Act), 5, 217
- Fluke Networks, 120
- Food and Drug Administration (FDA), 146

- format string attack, 161
- Fortra, 135
- frameworks
  - for compliance, 220–222
  - for enterprise security architecture, 107
  - for exploits, 135–136
  - for governance, 211
  - Metasploit, 23, 135–136
  - NIST Cybersecurity Framework, 211
  - NIST Risk Management Framework, 221–222
  - STRIDE threat-modeling, 106
  - Zachman Framework, 107
- FraudGPT, 190
- frequency analysis, 80
- FRR (false rejection rate), 37
- FTP (File Transfer Protocol), 49, 117–118
- full-disk encryption, 88
- fuzzers, 172–173
- fuzz testing, 172–173

## G

- gamification for security awareness, 270
- GDPR (General Data Protection Regulation), 220
- General Dynamics, 21
- generalists, 281–282
- generative AI, 180
- geographically based authentication factor, 33
- geospatial intelligence (GEOINT), 255
- German Enigma Cipher Machine, The* (Winkel et al.), 78
- GhostGPT, 24
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN), 280
- GIAC Information Security Professional (GISP), 280
- GIAC Penetration Tester (GPEN), 280
- GIAC Security Essentials (GSEC), 280
- GitHub Advisory Database, 59
- GlobeCommerce, 227
- Google, 144
  - Hacking Database, 252–253
  - Scholar, 191
  - search operators, 252–253
- governance, 209, 210–211

- governance, risk, and compliance (GRC)
  - compliance, 215–222
    - frameworks for, 220–222
    - industry-specific, 218–220
    - international regulatory environments, 220
    - types of, 216–217
    - US government, 217–218
  - creating cryptocurrency compliance plan, 226–228
  - defined, 209
  - governance, 209, 210–211
  - modern regulatory challenges, 222–226
  - review questions, 226
  - risk management life cycle, 212–215
  - roles and jobs in, 283
- GPS information, 254
- Gramm–Leach–Bliley Act (GLBA), 219
- gray-box testing, 235–236
- GRC. *See* governance, risk, and compliance
- Greece, 74
- Greenbone graphical interface, 134–135
- grep, 67
- group permissions, 47
- GRU (Russian Main Intelligence Directorate), 20, 23
- Guardian, The*, 28

## H

- HackerOne, 239
- hackers, black hat, 234
- “Hacktivism and the Future of Political Participation” (Samuel), 23
- hacktivists, 23
- hallucination risks, 182
- hardcoded passwords, 162
- hardware testing, 238
- hardware tokens, 39
- hashes, 85
- hash functions, 41, 84–85
- hashing passwords, 41–42
- Health Insurance Portability and Accountability Act (HIPAA), 5, 62, 218–220
- Health Net Federal Services, 216
- Heathrow Airport, 87

- Hellman, Martin, 83
- heuristics, 131
- hidden contexts, 183
- high-risk systems, 106
- HIPAA (Health Insurance Portability and Accountability Act), 5, 62, 218–220
- Honeynet Project, 121
- honeynets, 121
- honeypots, 120–121
- honeytokens, 122–123
- host discovery, 231
- host intrusion detection, 132
- host layer, 15
- HTTP (Hypertext Transfer Protocol), 89
- HUMINT (human intelligence), 250

## I

- IaaS (infrastructure as a service), 222–224, 233
- IAM (identity and access management) life cycle, 200
- ICMP (Internet Control Message Protocol), 121
- IDEA cipher, 83
- identification
  - common methods of, 34–38
  - defined, 29
  - hashing passwords, 41–42
  - overview, 30–31
  - review questions, 40
- identity
  - claim, 30
  - detecting misuse of, 199–201
  - falsification, 31
  - managing, 260
  - theft, 31
  - verification, 30–31
- identity and access management (IAM) life cycle, 200
- IDSs (intrusion detection systems), 65, 115–116, 132
- IGOs (intergovernmental organizations), 20
- IMAP (Internet Message Access Protocol), 49, 89
- impact factor, 12
- impersonation attacks, 34, 259

- incentives in security awareness, 270
- incident responders in SecOps team, 196
- incidents
  - counting number of, 272–273
  - defined, 201
  - life cycle, 201–203
  - reporting policy, 260
  - response to, 201–203
- India, 111–112
- industrial control systems, 146
- industry compliance, 216, 218–220
- information gathering for social engineering attacks
  - human intelligence, 250
  - open source intelligence, 250–255
  - other kinds of intelligence, 255–256
- Information Systems Security Association (ISSA), 279
- informed parties, 211
- InfraGard, 279
- infrastructure as a service (IaaS), 222–224, 233
- injection risks, 183–184
- input manipulation, 181–182
- input validation, 161, 164–165, 180
- instruction leakage, 183
- instructor-led training for security awareness, 269
- integrity, 6–8
- Intel, 131
- intent, 98
- interception attacks, 9–10
- intergovernmental organizations (IGOs), 20
- internal network layer, 15
- internal penetration testing, 236
- Internal Revenue Service, 227
- International Council of Electronic Commerce Consultants (EC-Council), 280
- International Criminal Police Organization (INTERPOL), 20
- International Information System Security Certification Consortium (ISC2), 279
- International Organization for Standardization (ISO), 221
- international regulatory environments, 220
- International Traffic in Arms Regulations (ITAR) law, 84
- Internet Control Message Protocol (ICMP), 121
- Internet Message Access Protocol (IMAP), 49, 89
- Internet of Things (IoT), 141, 148–151
- internet protocol security (IPsec), 89
- internet usage, 66
- INTERPOL (International Criminal Police Organization), 20
- interruption attacks, 10
- intext operator, 252
- Intigriti, 239
- intrusion detection and prevention, 64–65
- intrusion detection systems (IDSs), 65, 115–116
- intrusion prevention systems (IPSs), 65
- inurl operator, 252
- iOS, 142
- IoT (Internet of Things), 141, 148–151
- IP addresses, 48
- IPsec (internet protocol security), 89
- IPSs (intrusion prevention systems), 65
- Iran, 146
- ISACA, 279
- ISC2 (International Information System Security Certification Consortium), 279, 280
- ISO 27k, 221
- ISO 38500, 211

**J**

- jailbreaking, 144
- jailbreak prompt, 184
- Java Virtual Machine (JVM), 45
- Jeep Cherokee, hacking of, 147
- Jefferson disk, 75–76
- Jersey barrier illustration, 57
- job postings, 251
- Joint Test Action Group (JTAG) ports, 238
- Journal des Sciences Militaires*, 78
- JP Morgan, 199

## K

- Kahn, David, 78
- Kali Linux, 118
- Kerckhoffs, Auguste, 78
- Kerckhoffs's principles, 78–79
- key controls, 215
- key exchange, 81
- keyless cryptography, 84–85
- keys for cryptographic algorithms, 73
- keyword ciphers, 80
- Kia, 147
- Kismet, 117, 119, 120

## L

- “La cryptographie militaire”  
(Kerckhoffs), 78
- LAN (local area network), 88
- large language models (LLMs), 180
- LastPass, 264
- layered design, 102
- leads in SecOps team, 196
- Lee, Stan, 223
- liblzma library, 131
- limiting access, 44
- Linux operating systems, 46–47, 74,  
118, 129
- LLMs (large language models), 180
- local area network (LAN), 88
- Lockheed Martin, 21
- logging, 66–67, 70–71, 130
  - audit logs, 69–71
  - log aggregation, 197
- logical controls, 214
- London, 87
- low-risk systems, 106

## M

- MAC (mandatory access control)
  - model, 51–52
- MAC address filtering, 48
- machine learning, 179–180
- malicious apps, 144–145
- Maltego, 254–255
- malware
  - authors of, 22–23
  - autonomous, 24
  - BlackPOS malware, 158
  - creation kits, 22

- protecting against, 130–132
- in security awareness, 266

- managed security service providers  
(MSSPs), 281

- managers
  - in SecOps team, 196
  - and security awareness,  
268–269
- mandatory access control (MAC)
  - model, 51–52
- man-in-the-middle attack, 34, 82
- Manipur, 111–112
- mapping environments, 230–231
- Marktechpost, 191
- Marsh, Stephen Paul, 101
- measurement and signature
  - intelligence (MASINT), 255
- measure twice, cut once, 127
- medical devices, 146–147
- medium-risk systems, 106
- membership inference attacks, 183
- Message-Digest (MD) algorithm, 85
- messaging for security awareness,  
270–271
- metadata, 253–254
- Metasploit Framework, 23, 135–136
- metrics
  - for security awareness program,  
271–272
  - of strings, 206
- MFA (multifactor authentication), 33
- MGM resorts attack, 274–275
- Microsoft operating systems, 129
- Miller, Barton, 173
- Miller, Charlie, 147
- minutiae, 36
- Mirai malware, 151
- misinformation risks, 182
- mitmproxy, 150
- MITRE, 174
- MK-1 eyeball, 189
- mobile device security
  - auditing app permissions,  
152–155
  - overview, 142–145
- model behavior exploits, 181–182
- model integrity risks, 182–183
- model inversion attacks, 183

- model poisoning, 182
- model training phase, 185–186
- model training risks, 182–183
- modification attacks, 10
- monitoring, 67, 196–199
  - and maintenance phase, 186
- Morris, Robert, 23
- Morris worm, 23
- Morse code, 77
- multifactor authentication (MFA), 33
- multilevel access control models, 53–56
- mutual authentication, 34

## N

- National Institute of Standards and Technology (NIST), 173, 217
- National Security Agency (NSA), 12, 20, 26, 28
- National Vulnerability Database, 59
- Nessus, 229–230
- NETSCOUT, 119
- netstat, 127
- network ACLs, 48–49
- network analyzer, 119–120
- Network Mapper (Nmap)
  - features, 133–134
  - listening on network ports, 127–128
  - mapping environments, 230
  - scanner capabilities, 119
- network penetration testing, 236
- network perimeter layer, 15
- network ports, 127–128
- networks
  - defined, 111
  - neural, 179
  - protecting, 112–116
  - protecting traffic on, 116–118
  - security, 112–118
    - awareness, 265
    - experimenting with honeytokens, 122–123
    - review questions, 122
    - tools, 118–121
  - segmentation, 112
- “New Directions in Cryptography” (Hellman and Diffie), 83
- New York Times rule, 285

- NIST (National Institute of Standards and Technology), 173, 217
  - Cybersecurity Framework, 211
  - Risk Management Framework (RMF), 221–222
  - Special Publications, 217, 221–222
- Nmap. *See* Network Mapper
- noise in data, 181
- nondeterministic systems, 179
- nonrepudiation, 8, 64
- non-state actors, 21–23
- nonverbal communication, 285
- no read down rule, 55
- no read up property, 54
- North Atlantic Treaty Organization (NATO), 20
- North Korea, 20, 89
- Northrup Grumman, 21
- no write down property, 54
- no write up rule, 55
- NSA (National Security Agency), 12, 20, 26, 28

## O

- objects resource, 55
- offensive security, 283. *See also* red team
- Office of Foreign Assets Control, 227
- OffSec Certified Expert 3 (OSCE<sup>3</sup>), 280
- OffSec Certified Professional (OSCP), 280
- one-time pads, 80–81
- one-way problems, 79
- Open Group Architecture Framework, The (TOGAF), 107
- open source intelligence (OSINT), 250–255
- OpenText Forensic, 253
- OPENVAS, 134–135
- Open Web Application Security Project (OWASP), 279
- operating systems, 125, 169
  - security
    - hardening, 125–130
    - protecting against malware, 130–132
    - review questions, 137
  - scanning with Zenmap, 138–139
  - tools, 133–136

- OptiView Integrated Network Analyzer, 120
- ORYX cipher, 83
- OSCE<sup>3</sup> (OffSec Certified Expert 3), 280
- OSCP (OffSec Certified Professional), 280
- OSINT (open source intelligence), 250–255
- outdated devices, 151
- output processing, 183–184
- overfitting, 186
- OWASP (Open Web Application Security Project), 173, 174, 279

## P

- P2P file-sharing, 116
- PaaS (platform as a service), 222–223, 233
- packet filtering firewalls, 113
- packets, 113
- packet sniffers, 119–120
- Parker, Donn, 7–8
- Parkerian hexad, 7–9, 212–213
- partnerships for security awareness, 266–267
- passive scanning, 231
- password entropy
  - CyberChef showing Shannon entropy, 18
  - project testing, 17–18
- passwords
  - auditing, 65–66
  - best practices, 13–14
  - hashing, 41–42
  - for identification and authentication, 35
  - managers, 35, 264
  - preventing authentication attacks, 162
  - in security awareness, 264–265
  - strong, 35
- PASTA (Process for Attack Simulation and Threat Analysis), 106
- patches, 130
- paths into security profession, 277–279
- patriot hackers, 23
- patterns, 98
- PCI DSS (Payment Card Industry Data Security Standard), 5, 216
- penetration testing. *See also* vulnerability assessments
  - vs. assessments, 68
  - bug bounty programs, 238–239
  - detecting own attacks, 241–242
  - for different layers, 14
  - fixing security holes, 243
  - process, 233–235
  - realistic, 240
  - review questions, 229–233
  - scanning system for vulnerabilities, 245
  - security evolution, 242–243
  - targets, 236–239
  - technological challenges, 239
  - types of, 235–236
- pentesting. *See* penetration testing
- Pen Test Partners, 149
- performance measurement of biometrics, 37–38
- permanence, 37
- permissions, 165
- personal identification number (PIN), 29
- personally identifiable information (PII), 3
- PGP (Pretty Good Privacy), 84, 91–93
- PHI (protected health information), 218
- phishing
  - overview, 256–257
  - and security awareness, 265
- physical access controls, 56–57, 214
- physical penetration testing, 237
- physical security, 88, 149–150, 266
- piggybacking. *See* tailgating
- PII (personally identifiable information), 3
- PIN (personal identification number), 29
- PKI (public key infrastructure), 87
- plaintext, 73
- platform as a service (PaaS), 222–223, 233
- point-of-sale (POS) systems, 158
- policies
  - for AI, 187–188
  - bring-your-own-device, 143
  - clean desk, 266
  - communicating to team, 268–269
  - in governance, 210
  - against social engineering, 260
- POP (Post Office Protocol), 89, 117–118

- ports, 48–49
  - port scanners, 119
  - POS (point-of-sale) systems, 158
  - possession, 8
  - post-incident activity phase, 203
  - post-mortem, 203
  - Post Office Protocol (POP), 89, 117–118
  - post-quantum cryptographic algorithms, 79
  - PR (privileges required), 206
  - preparation phase, 202
  - pretexting, 250, 256
  - Pretty Good Privacy (PGP), 84, 91–93
  - principle of least privilege, 52, 99–100
  - printers, 149
  - PRISM program, 28
  - private key cryptography, 81
  - privilege escalation, 169
  - privileges, 129
  - privileges required (PR), 206
  - procedures in governance, 210
  - Process for Attack Simulation and Threat Analysis (PASTA), 106
  - projects
    - assessing real security architecture, 108–109
    - auditing app permissions, 152–155
    - calculating vulnerability severity, 204–207
    - classifying Edward Snowden, 27–28
    - creating cryptocurrency compliance plan, 226–228
    - designing own Shodan, 262
    - encrypting and decrypting with PGB, 91–93
    - experimenting with honeytokens, 122–123
    - exploring 2023 MGM resorts attack, 274–275
    - exploring slaughterbots and malicious AI, 191
    - finding confused deputies in wild, 59
    - hashing passwords, 41–42
    - knowing audience, 288
    - linking CWEs with CVEs, 174–175
    - scanning system for vulnerabilities, 245
    - scanning with Zenmap, 138–139
    - testing password entropy, 17–18
    - working with audit logs, 69–71
  - prompt injection attacks, 181
  - prompt leakage during inference, 184
  - protected health information (PHI), 218
  - protections for mobile devices, 142–143
  - protocols
    - analyzers, 119–120
    - based on asymmetric cryptography, 84
    - File Transfer Protocol, 49, 117–118
    - Hypertext Transfer Protocol, 89
    - Internet Control Message Protocol, 121
    - Internet Message Access Protocol, 49, 89
    - internet protocol security, 89
    - issues for databases, 167–168
    - Post Office Protocol, 89, 117–118
    - Secure File Transfer Protocol, 118
    - Secure Sockets Layer, 84, 88–89
    - Signaling System No. 7, 144
    - SSH, 118
    - Telnet, 117–118
    - using secure, 117–118
  - provisioning accounts, 200
  - proxy servers, 114
  - public key cryptography, 83
  - public key infrastructure (PKI), 87
  - public records, 251
  - purple team, 241
- ## Q
- Quadriga, 225
  - Qualys tool, 67–68, 229–230
  - quantum computing, 79
  - Queen Elizabeth II, 87
  - quid pro quo attacks, 258–259
- ## R
- RACE algorithm, 85
  - race conditions, 160–161
  - RACI matrix, 211
  - radio-frequency identification (RFID), 44
  - ransomware, 22
  - Rapid7, 135
  - Raspberry Pi, 142
  - Raytheon, 21
  - RBAC (role-based access control)
    - model, 52

- RC4 cipher, 83
- RC6 cipher, 83
- reactive tool, 66
- read permission, 46
- real-time operating systems (RTOSs), 146
- reconnaissance in penetration testing process, 234
- records, admissibility of, 65
- recovery in incident life cycle, 203
- red team, 234, 283
- redundancies for network connection, 112
- regulations, 268–269
- regulatory compliance, 216
- remote code execution, 168
- reporting phase, 235
- resource attributes, 53
- resource exhaustion attacks, 184
- responsibility in cloud models, 223
- responsible parties, 211
- résumés, 251
- review questions
  - application security, 174
  - artificial intelligence security, 191
  - auditing and accountability, 69
  - authorization and access controls, 58
  - cryptography, 90–91
  - cybersecurity, 16–17
  - governance, risk, and compliance, 226
  - identification and authentication, 40
  - mobile, embedded, and IoT security, 152
  - network security, 122
  - operating system security, 137
  - security architecture, 108
  - security awareness, 274
  - security operations, 204
  - security profession, 287
  - social engineering attacks, 261–262
  - threat landscape, 27
  - vulnerability assessments and penetration testing, 244
- RFID (radio-frequency identification), 44
- risk-based approach, 217
- risk-driven architecture, 105–107
- risk management, 209, 212–215.
  - See also* risks
  - NIST Risk Management Framework, 221–222
- risks
  - assessing in management life cycle, 214
  - communicating effectively, 285, 288
  - defined, 12
  - mitigating in management life cycle, 214–215
  - mitigating user types of, 264–266
  - scoring, 105–106
  - tiers, 106
- Rivest, Ron, 84
- rogue access points, 117
- Roku, 219
- role-based access control (RBAC) model, 52
- roles in security, 282–284
- Rome, 74
- Roomba Home app, 152–155
- root, 129
- rootkits, 22
- ROT13 cipher, 74
- RSA algorithm, 84
- RTOSs (real-time operating systems), 146
- rule-based access control (RuBAC) model, 52
- rules of engagement, 234, 240
- Russia, 20, 23
- Russian Foreign Intelligence Service, 267
- Russian Main Intelligence Directorate (GRU), 20, 23
- Russia Today, 251

**S**

- SaaS (software as a service), 222–224
- SABSA (Sherwood Applied Business Security Architecture), 107
- salt value, 42
- Samuel, Alexandra, 23
- sandboxes, 45
- Sandworm, 23
- SANS (SysAdmin, Audit, Network, and Security) Institute, 148, 280

- Sarbanes–Oxley Act (SOX), 62, 65, 218
- scanners, 119, 133–134
- scanning in vulnerability assessments, 231–232
- Scapy, 121
- Scherbius, Arthur, 77
- Schneier, Bruce, 28
- scope in penetration testing, 234, 240
- script kiddies, 23
- SEAL cipher, 83
- SecOps. *See* security operations
- secure defaults, 100–101
- Secure File Transfer Protocol (SFTP), 118
- Secure Hash Algorithm (SHA), 41, 84, 85
- Secure Shell (SSH), 49, 118
- Secure Sockets Layer (SSL) protocol, 84, 88–89
- Securities and Exchange Commission (SEC), 267
- security
  - and CIA triad, 7
  - vs. compliance, 216
  - defined, 4
  - evolution of, 242–243
  - fixing holes in, 243
  - level of, 4–6
  - monitoring in SOC, 196–199
  - oversight mechanisms, 210
- Security+ certification, 280
- security architecture
  - assessing real examples, 108–109
  - city planning metaphor, 98–99
  - defined, 97
  - foundational architectural principles, 99–102
  - frameworks for enterprise security architecture, 107
  - review questions, 108
  - risk-driven architecture, 105–107
  - trust boundaries, 102–104
- security awareness
  - communicating to team, 269–271
  - designing program for, 266–269
  - evaluating training effectiveness, 271–273
  - MGM resorts attack case, 274–275
  - mitigating user risks, 264–266
  - review questions, 274
- security communities, 279
- security information and event management (SIEM), 197
- security issues
  - with embedded devices, 147–148
  - with IoT devices, 150–151
  - with mobile devices, 143–145
  - models for discussing, 6–9
- Security Live CD distributions, 118
- Security Onion, 241
- security operations (SecOps)
  - AI changing, 189–190
  - calculating vulnerability severity, 204–207
  - defined, 195
  - detecting identity misuse, 199–201
  - incident response, 201–203
  - review questions, 204
  - role of SecOps team, 196
  - in SOC, 196–199
- security operations center (SOC), 195, 196–199
- security policies, 260
- security profession
  - careers and roles, 282–284
  - generalist vs. specialist, 281–282
  - knowing audience, 288
  - paths into, 277–279
  - review questions, 287
  - soft skills in, 284–286
  - training and certifications, 280–281
- security researchers, 21
- security teams, working with, 286
- security through obscurity, 78
- security zones, 103–104
- Seizing the Enigma* (Kahn), 78
- separation of duties, 100
- Serpent cipher, 83
- server-side attacks, 164–166
- services, removing unessential, 127–128
- SHA (Secure Hash Algorithm), 41, 84, 85
- Shadow Brokers, The, 26
- Shamir, Adi, 84
- Shannon, Claude, 17, 79
- Shannon entropy, 17
- shared responsibility models, 224

- Sherwood Applied Business Security Architecture (SABSA), 107
- shift left, 199
- shifts, 80
- Shodan, 254, 262
- SIEM (security information and event management), 197
- SIGINT (signals intelligence), 255
- Signaling System No. 7 (SS7)
  - protocol, 144
- signature-based IDSs, 115
- “Simple and Flexible Datagram Access Controls for Unix-Based Gateways” (Mogul), 113
- simple integrity axiom, 55
- simple security property, 54
- simplicity in security architecture, 101
- site operator, 252
- slaughterbots, 191
- smishing attacks, 259–260
- Smith, Craig, 147
- Sniffer (NETSCOUT), 119
- sniffers, 119, 169–171
- Snowden, Edward, 27–28
- SOC (security operations center), 195, 196–199
- social engineering attacks
  - defined, 249
  - designing own Shodan, 262
  - gathering information for
    - human intelligence, 250
    - open source intelligence, 250–255
    - other kinds of intelligence, 255–256
  - preventing and mitigating, 260–261
  - review questions, 261–262
  - and security awareness, 265
  - types of
    - other common attacks, 258–260
    - phishing and spear phishing, 256–257
    - pretexting, 256
    - tailgating, 257–258
- social engineering testing, 237–238
- social media, 251
- sockets, 49
- soft skills in security, 284–286
- software, unnecessary, 126–127
- software as a service (SaaS), 222–224
- software development vulnerabilities
  - authentication attacks, 162
  - authorization attacks, 162
  - buffer overflows, 159–160
  - cryptographic attacks, 163
  - input validation attacks, 161
  - overview, 158–159
  - race conditions, 160–161
- software firewalls, 132
- software licenses, 66
- SolarWinds, 267
- “something you are,” 32
- “something you do,” 33
- “something you have,” 32
- “something you know,” 32
- SOX (Sarbanes–Oxley Act), 62, 65, 218
- SP 800-37, 221–222
- SP 800-53, 221–222
- Spafford, Eugene, 4
- spear phishing, 256–257
- specialists, 281–282
- spidering, 171
- SQL (Structured Query Language), 168
  - injection, 169
- SS7 protocol, 144
- SSH protocol, 49, 118
- SSL protocol, 84, 88–89
- standards in governance, 210
- star (\*) integrity axiom, 55
- star (\*) property, 54
- state actors, 20
- stateful firewalls, 113–114
- stateful packet inspection firewalls, 113–114
- state-sponsored actors, 20
- static analysis, 237–238
- stream ciphers, 83
- STRIDE threat-modeling frameworks, 106
- StrongVPN, 116
- Structured Query Language (SQL), 168
- structure in security architecture, 98
- Stuxnet virus, 146
- subject attributes, 53
- subnets, 112
- substitution cipher, 74
- supervisory control and data acquisition system, 146

- supply chain risks, 182
- surveillance cameras, 149
- symmetric block ciphers, 83
- symmetric cryptography, 81–83
- SysAdmin, Audit, Network, and Security (SANS) Institute, 148, 280
- system impact metrics, 206
- system prompts, 183
- Systems Security Certified Practitioner (SSCP), 280

## T

- tailgating, 56, 237, 257–258
- Talos Intelligence Group, 31
- Tapplock smart padlock, 149
- Target Corporation, 157
- targets of penetration testing, 236–239
- tcpdump, 119
- teams, working with, 286
- TECHINT (technical intelligence), 255
- technical controls, 214, 260–261
- Telnet protocol, 117–118
- Tenent Media, 251
- testers, finding, 239
- testing. *See* penetration testing
- test set, 179
- text messages, 259
- third-party model risks, 182
- threat actors, 19, 25–26
- threat landscape
  - attribution, 25
  - autonomous actors, 23–24
  - classifying Edward Snowden, 27–28
  - non-state actors, 21–23
  - review questions, 27
  - state actors, 20
  - threat actor skill levels, 25–26
- threat metrics, 206
- threat modeling, 106–107
- threats, 11, 212–213
- TLS (Transport Layer Security), 84, 88–89
- TOGAF (The Open Group Architecture Framework), 107
- tokens, 50
- tools
  - anti-malware, 131
  - for application security, 169–173

- for catching penetration testers, 241–242
- for network security, 118–121
- for operating system security, 133–136
- for vulnerability assessment, 134–135
- web application analysis, 171–173
- “Towards a Common Enumeration of Vulnerabilities” (MITRE), 11
- training
  - evaluating effectiveness of security awareness, 271–273
  - for security awareness, 267–268
  - for security professionals, 280–281
- training set, 179
- transformers, 180
- transforms (data points), 254
- transparency, 150–151, 188–189
- transparent models, 186
- Transport Layer Security (TLS), 84, 88–89
- Trending Papers, 191
- trigger, 182
- trust boundaries, 102–104
- tunnel, 116
- two-factor authentication (2FA), 33
- Twofish cipher, 83

## U

- UART (universal asynchronous receiver/transmitter) ports, 238
- uBlock Origin, 164
- UI (user interaction), 206
- Ukraine, 23, 191
- unauthenticated scans, 231
- understandable models, 186–187
- unified endpoint management, 142
- uniqueness, 36–37
- Unit 8200 (Central Collection Unit of the Intelligence Corps), 20
- United Nations (UN), 20
- universal asynchronous receiver/transmitter (UART) ports, 238
- universality, 36
- Unix operating systems, 47, 74, 129
- Unshorten.me, 266
- updates
  - to mobile devices, 145
  - performing, 129–130
  - to technology, 243

- upgrading embedded devices, 147–148
- USB drives, 258
- US Computer Emergency Readiness Team (US-CERT), 173
- US Department of Defense, 86
- US Department of Health and Human Services Office for Civil Rights Breach Portal, 108
- user interaction (UI), 206
- user interface redressing, 50
- user permissions, 47
- users
  - and security awareness, 264–266
  - testing regarding security awareness, 273
- US Government Accountability Office, 63
- US government compliance, 217–218
- US Office of Personnel Management, 38
- US presidential election, 251
- utility, 8–9

**V**

- Valasek, Chris, 147
- validation, 161, 179, 186
- VAST (Visual, Agile and Simple Threat), 106–107
- vector string, 205–207
- vehicles, 57
- VeraCrypt, 88
- verbal communication, 285
- verification policy, 260
- Verisign, 86
- Vernam cipher, 80
- virtual private networks (VPNs), 116, 265
- visitor policy, 260
- Visual, Agile and Simple Threat (VAST), 106–107
- visuals for security awareness, 270–271
- VoIP (voice over IP), 84, 89
- VPN concentrator, 116
- VPNs (virtual private networks), 116, 265
- vulnerabilities
  - assessing in risk management life cycle, 213–214
  - calculating severity of, 204–207

- defined, 11
- examples of, 5
- scanners, 119
- vulnerability assessments.
  - See also* penetration testing
  - auditing with, 67–68
  - overview, 229–233
  - review questions, 229–233
  - scanning system for
    - vulnerabilities, 245
  - tools for, 134–135

## **W**

- WAN (wide area network), 88
- web application analysis tools, 171–173
- web application scanners, 232
- web security, 163–166
- Website Vulnerability Scanner, 244
- WEP (Wired Equivalent Privacy), 117
  - “where you are,” 33
- white-box testing, 235–236
- wide area network (WAN), 88
- Wi-Fi Protected Access (WPA) 1–4, 117
- Wifite, 119
- WinDump, 119
- Winkel, Brain J., 78
- Wired*, 28, 147
- Wired Equivalent Privacy (WEP), 117
- wireless access points, 101
- wireless networks, 117
- wireless protection tools, 118
- Wireshark, 120, 169–170
- Women in Cybersecurity (WiCyS), 279
- Women in Tech, 279
- workflow enforcement, 261
- WormGPT, 190
- Wormhole, 238
- worms, 23
- WPA (Wi-Fi Protected Access) 1–4, 117
- write permission, 46
- written communication, 284

## **X**

- XD bit, 131
- XKeyscore program, 28
- XSS (cross-site scripting), 163
- XZ Utils backdoor, 131