Index

A
Access control
  database security
    mechanisms, 145
    multilevel, 146
    query modification, 146
    stored procedures, 146
    views, 146
  mobile and wireless security, 174
Access Control Lists (ACLs), 56, 59, 63
Address resolution protocol (ARP), 129
Advanced Encryption Standard (AES), 99, 174
Adware
  freeware/shareware, 22
  infected websites, 22
  infinite pop-ups, 21
  man-in-the-middle attacks, 21
  pop-up ads, 20
  slow down device's, 21
  spying, 21
  users, 22
Alternate Data Stream (ADS)
  ADSCheck, 217
  ADSSpy, 217, 218
  CAT tool, Nix Utilities, 217
  feature, 216
  hiding data, 217
  StreamArmor, 218
Anti-Malware detection techniques, 196, 197
Apple iOS security, 170
Apple IPhones™ cloud locks, 164
Apple Mac's FileVault, 109
Applications section
  anti-virus software application, 13
  vulnerability scanning, 13–15
ARP Spoofing attacks, 127–129
Asset value, 9
Attacker
  Malware, 140
  Network, 140
  notice, 144
Attribute-based access control (ABAC), 66
Authentication, Access control and Accountability (AAA), 64

B
Backdoors, 31
BlowFish, 100
Bootkits, 23
Boot-sector viruses, 38
Browser Hijacking, 41

C
Carriage return line feeds (CRLF) Injection attacks, 42
Certificate Authorities (CA), 104, 113
Cipher Block Chaining (CBC), 97
Cipher FeedBack (CFB), 97
Code injection, 41–43
Confidential information, 4
Counter (CTR), 97
Crimeware, 35–37
Cross site request forgery (CSRF), 143, 144
Cross-site Scripting (XSS), 42
Crypto ransomware, 24
Cyber-attacks, 121

I. Alsmadi et al., *Practical Information Security*,
https://doi.org/10.1007/978-3-319-72119-4

D
Data encryption standard (DES), 62
Data modification attacks, 126, 127
Database security
  access control (*see* Access control, database security)
  applications, 155
  attack, SQL injection (*see* SQL injection attack)
  management system, 144
  measures, 145
  privacy
    adding/deleting records, 147
    data perturbation/anonymization, 148
    output perturbation, 148
    query restriction, 148
    statistical database, 146, 147
Denial of Service (DoS) attack, 5–6
Digital Encryption Standard (DES), 96
Disaster Recovery Plan (DRP), 80, 85, 89
Discretionary Access Control (DAC), 56
Disk and computer forensics
  ADS, 216–218
  analysis, 208, 209
  applications
    Kali Linux, 241
    Linux Logs, 241
    Linux Rootkit Checker, 242
    memory analysis with volatility, 240
    Windows registry, 241
  data recovery, 207, 208
  digital investigations, 204
  event viewers, 232, 233
  ext systems (*see* Extended file system (Ext))
  factors, 204
  FAT system, 209, 210, 212, 213
  HFS+ systems, 221–222
  HFS+ volume headers, 222
  image acquisition, 205–207
  Internet usage and traces (*see* Internet traces)
  investigations
    Linux (*see* Linux operating systems)
    MAC operating systems, 236, 237
    Windows operating systems, 227–229
  memory (*see* Memory forensics)
  NTFS systems, 214–216
  operating system, 205
  skills
    Binwalk disk forensic tool, 238
    file carving, 238–240
    foremost forensic tool, 237
    hex-editor program, 238
    raw format image acquisition, 238
  unallocated disk, 214
  web logs, 233
  Windows registry, 229
Distributed denial of service (DDoS) attack, 30
Distribution, Crimeware
  affiliate marketing, 37
  attachment, 36
  hacking, 37
  Internet Worm, 36
  Piggybacking, 36
  Web Browser Exploit, 36
Dynamic link library (DLL) file, 33

E
EICAR test files, 13
Electronic Code Book (ECB), 97
Electronic mail (email) virus, 38
Email (Mail command/SMTP) injection, 42
Encrypted salt-sector initialization vector (ESSIV), 110
Encrypting File System (EFS), 108
Ethernet Network cards (NIC), 251
Extended file system (Ext)
  file recovery, 220, 221
  high level layout, 218
  inode, 219
  journal process, 219
  Linux, 218
  Minix, 219
eXtensible Access Control Markup Language (XACML), 70

F
File allocation table (FAT) system
  corrupted data, 213
  data area, 210
  deleted data, 212
  DOS and Windows operating systems, 209
  extensions, 213
  FAT12 disk sizes, 209, 210
  FAT16, FAT32 and NTFS, 210
  floppy, 209
  fsstat tool, 211
  hidden data, 212
  mmls tool, 211
  primary and backup FAT structures, 210
  reserved area, 210
  unallocated/formatted data, 213
File infectors, 38
File-sharing/peer-to-peer (P2P) worm, 28

Firmware, 24
Flash worm, 28
Foremost tool, 259, 260

G
Global Navigation Satellite Systems (GNSS), 301
GNU Privacy Guard (GnuPG), 105

H
Hardware, 24
Hardware/network security issues in mobile/smart devices, 173
Hardware-based keyloggers
  acoustic keyloggers, 34
  electromagnetic emissions, 34
  firmware-based, 34
  keyboard hardware, 34
  keyboard overlays, 34
  optical surveillance, 34
  physical evidence, 34
  smartphone sensors, 34
  wireless sniffers, 34
Hierarchical file systems (HFS), 221, 222
Host header injection, 42
HTML-Proxies, 29

I
Information hiding and protection
  asymmetric encryption algorithms, 100–104
  commitment schemes, 114
  cryptography applications
    Apple OS/X, 109–111
    browsers, 105–107
    e-commerce, 104, 105
    email communication, 105
    Internet/online communications and e-commerce, 104
    operating systems and disks, 107–109
    telecommunication/networks, 107
  digital time-stamping, 115
  encryption, 92
  experience/ability section, 119, 120
  hashing/steganography, 92
  information authentication, 113
  information concealment, 91, 92
  information concealment/authenticity techniques, 115–117
  information integrity, 91
  information integrity and authentication techniques, 111–113
  information system/website, 92, 93
  knowledge sections
    ciphering/encryption algorithms, 95
    cryptography/encryption, 93–95
    key-based encryption techniques, 95
    methods, 95
  message authentication, 113
  password storage and verification, 114, 115
  skills section
    encryption algorithms, 117
    encryption applications, 118
    information concealment applications, 119
    information integrity algorithms, 118
    information integrity applications, 118
  symmetric encryption algorithms
    block ciphers, 95–100
    BlowFish, 100
    stream ciphers, 100
Information location
  description, 3
  hard and flash drives, 4
  in motion, 4
Information security, 10–12
Information security cases, 12, 13
Information sensitivity
  categories, 4
  confidential information, 4
  private information, 5
  public information, 5
Information state
  creation, 2
  description, 2
  processing, 3
  storage, 3
  transition, 3
Information taxonomy, 2
Internet Bot, 31
Internet DOS, 29
Internet of Things (IoT), 11
Internet Protocol Security (IPSec), 107
Internet Relay Chat (IRC) worm, 28
Internet traces
  applications, 229
  Google Chrome, 230, 232
  Mozilla Firefox, 231
  MS Internet explorer, 230
  OSI layers' perspective, 230
Intrusion Detection/Protection Systems (IDS/IPS), 267–269

J
Jail-breaking, mobile devices, 172

K
Keyloggers, 32–35
Knowledge sections, 1–12, 17–44

L
Lightweight Directory Access Protocol (LDAP) injection attacks, 42
Linux operating systems
  directories, 234
  disk forensics, 233
  forensic investigation, 234
  forensic investigator, 235
  forensic tools, 234
  Linux logon log files, 235
  tools, 235
  versions/flavors, 233
  web browsers, 235
Linux Rootkit Checker, 242
Linux Unified Key Setup (LUKS), 110
Locker ransomware, 24
Logic bombs, 41

M
MAC flooding attack, 131, 132
MAC operating systems, 236, 237
Macro viruses, 38
Malware analysis, Software code security
  anti-malware detection techniques, 195
  manual, 197
  NSRL server, 198
  software applications, 194
Malware attacker, 140
Malware threats
  access or intrusion method, 164
  Android platform, 166
  Brain Test, 167
  Dendroid, 166
  Hiddad, 167
  hiding methods, 165
  payload, 164
  Pegasus spyware, 165
  Pretender Applications, 166
  propagation, 164
  RuMMS, 167
  Triada, 167
  ViperRAT, 166
  XcodeGhost, 167
Malwares
  applications section
    dangerous website, 46–47
    Keylogger, 45, 46
    Microsoft safety scanner, 44, 45
    outlook account, 47, 48
    TDSSKiller, 48–50
  knowledge sections
    Adware, 20–22
    backdoors, 31
    browser Hijacking, 41
    classes, 18
    code injection, 41–43
    Crimeware, 35–37
    hardware-based keyloggers, 34, 35
    Internet Bot, 31, 32
    Keylogger, 32, 33
    logic bomb, 41
    pharming, 43
    phishing, 40
    Ransomware, 24–26
    Rogue security software, 31
    Rootkits, 22–24
    Scareware, 37
    software Bugs, 39
    software-based keyloggers, 33
    spamming, 40
    spyware, 18–20
    taxonomy of, 17
    Trojan horses, 29–31
    Viruses, 37–39
    Worms, 26, 28, 29
  skills section, 44
Memory forensics
  analysis with volatility, 240
  BIOS, 223
  computing systems, 223
  data analysis, 223
  information, 223, 224
  ROM, 223
  size, 223
  tools
    analysis, 225
    Dumpit, 225
    FTK Imager memory capture, 226
    Linux, 227
    Redline, 226
    simple/generic, 225
    Volatilitux, 226
    volatility, 225, 226
  virtual, 223
Mobile and wireless security
  access control models, 174
  AES crypto-engine, 174
  age of using mobile phones, 161

anti-malware apps, 168
application code signing, 162
applications, 178
booting process, 173
bring your own device (BYOD), 162, 163
consumer reports, 161
hardware/network, 173
installation, unknown/un-trusted stores, 167
jail-breaking, 172
location-based services and privacy control, 176
malware threats (*see* Malware threats)
operating systems, 170
OSNs, 169
physical thefts, 172
remote wipe feature, 176
Sandboxing, 171
skills
Smart devices operating systems, 177
Software security issues, 177
theft and loss/unauthorized access, 163, 164
TLS/SSL, 175
transmissions, 175
unsecured network connection, 175
updates, operating systems, 172
usage, 161
users/software, 162
Mobile anti-malware systems, 168
Mobile forensics
company to seize, 307
device folders, 305
device information, installed apps, call history, contacts, and messaging, 307
device seize, 301
device states, 300, 305
GPS, 301, 306
hardware and software, 299
mobile device features, 298
operating systems, 299, 300, 304
SIM card, 300, 306
tools, 301, 302
Monte Carlo analysis, 79
Multi-variant virus, 38

N

NAC, *see* Network access control (NAC)
National Institute of Standards and Technology (NIST), 99
Near Field Communication (NFC), 299
Network access control (NAC), 125
Network attacker, 140
Network attacks
address resolution protocol, 129
countermeasures, 129
data modification, 126, 127
denial, service attack, 130
eavesdropping, 125, 126
MAC flooding, 131, 132
Packet sniffers, 134
SMURF, 133
Spoofing
ARP, 127–129
identification, 126
TCP SYN flooding, 132
Network forensics
ARP spoofing, 273
DHCP servers, 250
Ethernet cards promiscuous mode, 251
firewalls, 267
Foremost, 259, 262, 273
IDS/IPS, 267–269, 274, 275, 277, 279, 281
NIC Promisc Mode, 273
packet filtering, 254–257, 261
port mirroring, 264
real time, analysis, 249
routers, 265, 266
SDN switches, 273
static, analysis, 249
switches, 261–264, 274
traffic analysis, 247–249, 272
wire tapping, 250
wireless communication, 269, 270
wireless tapping, 250, 251
Wireshark, 252–255
Network layer, 124
Network security
application layer, 122
applications, 137
attacks (*see* Network attacks)
cyber-attacks, 121
network traffic analysis, 134–137
OSI Model, 121–123
transport Layer (*see* Transport layer)
Non-resident viruses, 38
NTFS systems, disk forensics, 214–216

O

Object-based access control (OBAC), 66, 67
Online Social Networks (OSNs), 169
Open Systems Interconnection model (OSI Model)
layers, 121, 122
protocols, 123

Operating systems security issues, mobile/smart devices, 170
Organization's risk tolerance, 73
Output FeedBack (OFB), 97

P
Packet Sniffing attacks, 134
Personal Information Manager (PIM), 299
Pharming, 43
Phishing, 40
Physical security, 126
Physical thefts, mobile phones, 172
Physical-world DOS, 29
Physical-world Reconnaissance, 29
Policy Administration Point (PAP), 67
Policy Decision Point (PDP), 66
Policy Enforcement Point (PEP), 66
Private information, 5
Public information, 5
Public Key Encryption (PKE), 104

R
Radio frequency identification (RFID) virus, 38
Ransomware, 24, 26
Remote wipe feature, 176
Resident viruses, 38
Risk
  definition, 73
  impact of, 73
  metrics, 74
  monitoring, 74
  response, 74
  security, 73
  tracking, 74
Risk management and planning
  applications' section
    assessment/model, 89
    cyber security plan, 89–90
  knowledge sections
    approaches, 76, 82, 83
    assessment and model, 79
    cyber security awareness, 81, 86
    disaster recovery, 80, 81, 85
    DRP sections, 85–86
    forensics resources, 81, 82
    incident response planning, 79, 80, 83, 84
    policies, 77, 78
    security, 75, 76
    self-assessment survey, 84, 85
    tolerance, 76, 77, 83
  skill's section
    development process, 88
    disaster recovery plan, 89
    disaster recovery planning, 87–88
    incident response plan, 88
    metrics, 87
    security incident responses, 87
    tracking, 87
Rivest-Shamir-Adleman (RSA), 101, 102
Rogue security software, 31
Role-based access control (RBAC)
  and OBAC, 66, 67
  in MAC, 64
  permissions, 64
  policies/roles, 65
  policy-based security systems, 64
Rootkits, 22–24, 48–50
RuMMS, 167

S
Sandboxing, 171
Scareware, 37
Script virus, 38
Secunia PSI software, 14
Secure phone booting process, 173
Secure shell (SSH), 107
Secure Socket Tunneling Protocol (SSTP), 107
Secure Sockets Layer (SSL), 104
Security
  mobile and wireless (*see* Mobile and wireless security)
  web (*see* Web security)
Security access controls
  applications sections
    OBAC systems, 70
    RBAC systems, 70
    websites and web-applications, 69
  authentication, 55
  components, 55
  database management systems, 53
  different database management, 54
  different operating systems, 54
  different websites and web-applications, 54
  knowledge sections
    database management systems, 59, 60
    digital certificates, 62–63
    distributed and operating systems, 63, 64
    identity management, 61
    Kerberos, 62
    OBAC and RBAC, 56
    operating and file systems, 56–59
    permissions, 56
    session time-out, 62

SSO methods, 61
websites and web-applications, 60–61
OBAC, 53, 54
operating systems, 53
RBAC, 53, 54 (*see* Role-based access control (RBAC))
skills sections
in Linux, 68, 69
Windows SAM database, 67, 68
websites and web-applications, 53
Security awareness, 10
Security countermeasurement
description, 10
human, 10
legal, 10
organizational, 10
technical, 10
Security education, 10
Security goals
accountability, 6
authentication, 6
authorization, 6
a3vailability, 5
confidentiality, 5
description, 5
identification, 6
integrity, 5
non-repudiation, 7
privacy, 6
Security risks, 7, 8
Security threat, 8
Security training, 10
Single-Sign-On (SSO), 61
Skills section, CIA triad - confidentiality, integrity and availability, 12, 13
Smart devices operating systems and security issues, 177
SMURF attacks, 133
Software Bugs, 39
Software code security
evaluation, software programs, 198
management and control of information, 183
perspectives, 199
skills
Malwares, 198
reviews, 198
testing tools, 197
and vulnerability issues (*see* Vulnerability, Software code security)
Software Defined Networking (SDN) Controllers, 64
Software security issues, smart devices, 177
Software-based keyloggers, 33
API-based, 33
grabbing based, 33
hypervisor-based, 33
Javascript-based, 33
kernel-based, 33
memory injection based, 33
Spamming, 40
Spyware
ActiveX control, 19
anti-spyware, 19
browser add-ons, 19
computer programs, 18
devices, 19
disable active-X, 20
drive-by download, 19
installation, 20
piggybacked software installation, 19
pop-up blocker, 20
type of, 18
"X" icon, 20
SQL GRANT/REVOKE commands, 60
SQL injection (SQLi), 42
SQL injection attack
automated, 149
deleting, updating and inserting data, 154
initiation, 150
input validation vulnerability, 150, 151
mitigation, 152
skills, 152, 153
statements, 149
steal data, 150, 152
Web application, 154
Yahoo Voices, 149
Statistical database, 147
Steal data, 150, 152
Subscriber Identity Module (SIM) card, 300
Swarm worm, 28

T

TCP SYN flooding, 132
TDSSKiller, 48, 49
Theft and loss/unauthorized access, mobile devices, 163, 164
Time Stamping Authority (TSA), 115
Transmission Control Protocol (TCP), 122
Transport layer
Network layer, 124
routing and translation, addresses, 125
types of addresses, Internet, 124, 125
UDP, 123
TCP, 122
Transport Layer Security (TLS), 105

Transport Layer Security (TLS) or Secure Socket Layer (SSL), 175
Triada, 167
Trojan horses, 29–31
TrueCrypt, 110
Trusted Third Party (TTP), 104

U
Ubuntu shadow content, 114
Unsecured wireless network connection, 175
User Datagram Protocol (UDP), 123
User-mode/kernel-mode hybrid Rootkit, 23
Users/software security, mobile/smart devices, 162

V
VeraCrypt, 110
Vetting, 162
Virtual Private Networks (VPNs), 105
Virus detection pop-up window, 14
Virus life cycle
  dormant phase, 39
  execution phase, 39
  propagation phase, 39
  triggering phase, 39
Viruses, 37–39
Vulnerability, 9
Vulnerability threats, 74
Vulnerability, Software code security
  anti-malware detection techniques, 195–197
  buffer and stack overflows, 184
  design flaws
    changes, 193
    control modules and APIs, 193
    encryption, 193
    sensitive data, 193
    validate user inputs, 192, 193
  design principles and practices, 190–192
  exception handling, 194
  feedback exceptions, 194
  malware analysis, 195
  manual malware analysis, 197
  memory leak and violation issues, 185
  race conditions, 187, 188
  SQL injection and XSS, 185–187
  static and dynamic security analysis, 188–190
  techniques and tools, 188

W
Warhol worm, 28
Web application code, 140
Web browser, 140
Web forensics
  artifacts for investigation, 294
  criminal and civil cases, 295
  criminal cases with web, 291
  email
    and browsers information, 292
    clients, 285
    file reports, 291
    files, 289, 290
    forensics tools, 286, 287
    headers, 287–289
    headers review, 293
    mail servers, 285
    protocols, 285
  scan for archived files, 293
  software, 295
  steps, 284
  web browsers, 291, 292
  web browsing history, 294, 295
Web logs, 233
Web security
  and database (*see* Database security)
  applications, 139, 155
  Cloud, 139
  online transactions, 139
  threat models, 140–144
Web threat models
  cross site scripting
    Cookie encryption, 143
    Cookies associated with a web page, 142
    impacts, 143
    sever response, 142
    techniques, 141
    textbox and text area, 141, 142
    URL, 141
  CSRF, 143, 144
  malware attacker, 140
  network attacker, 140
  web attacker, 140
Wide Area Networks (WAN), 265
Windows operating systems
  event viewers, 232, 233
  forensic investigations
    artifacts, 229
    backdoors/Rootkits, 228
    disk, 228
    keyword searches, 227
    malicious processes, 228

review, 227
unauthorized user accounts/groups, 228
versions of, 228
Windows registry, 229, 241
Wire tapping, 250
Wireless security, *see* Mobile and wireless security
Wireless tapping, 250, 251
Worms
activation, 27
malicious code, 26
payloads, 28
propagation techniques, 28
scanning, 27
types of, 27, 28

X
XcodeGhost, 167
XML injection, 42
XPath injection, 42