Index

Symbols

0-day attack 295, 323
3-way handshake 138
3DES 69, 269

A

A5/1 75, 206
A5/2 206
A5/3 206
access 48
access control
  for CPU 264–265
  for hardware units 263
  hardware based 260
  in Android 265
  in file system 254–259
  in memory 260–263
access control list *see* ACL
access control matrix (ACM) 252
accountability 355
ack 137, 138
ACL 256, 257
  compressed 255
activation code 115
active attacker 112
active server page 166
ActiveX 316
  security 317
actor 48
actuator 4
Ad hoc Mode 145
ADB 331
address 132
administrator 251
  privileges 255
Advanced Encryption Standard *see* AES
Advanced Persistent Threat *see* APT
AES 72–73, 269
AKA 208
amplification 215
amplifier 215, 217
analysis group 47
Android 266
Android Debug Bridge 331
anomaly detection 196, 294
ANT catalog 228
anti-terror laws 352–353
antivirus system *see* AV system
API 267, 391
App 391
applet 166, 316
  sandbox 316
  security 316
Application layer
  encryption 172, 175–177
application program 391, 393–394
Application Program Interface *see* API
APT 5, 330
arbitrator 102
architecture
  client-server 3, 153
  P2P 3
ARP 141
ARP cache 141
ASCII character set 158
ASP.NET 320
asset 9, 48
  data 9
  equipment 9
  software 9
attack 41, 59, 212
  0-day 295, 323

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2024

R. Sharp, *Introduction to Cybersecurity*, Undergraduate Topics in Computer Science,
https://doi.org/10.1007/978-3-031-41463-3

adaptive chosen plaintext 59
brute-force 59, 101, 203, 241
chosen plaintext 59, 87
ciphertext alone 59
cold boot 269
costs 9
dictionary 241, 243
DoS 199, 211–218
countermeasures 218
distributed 216–217
in Application layer 211–213
in Internet layer 214–215
in Link layer 215
in Physical layer 215
in Transport layer 213–214
permanent 217
risks 218
known cleartext 307
known plaintext 59, 66
length extension 98
man-in-the-middle 29, 111, 112, 187, 199, 203, 209
psychological 18–27
redirection 173, 184
related key 59, 77, 206
ROCA 374
supply-chain 7
virus-based 290–291
worm-based 292
zero-day 272
attribute 299
attribution error, fundamental 24
AuC 149, 204, 207
authentication 107–111, 128
biometric 237–240
face recognition 238
finger pattern recognition 239
fingerprint 237
iris recognition 239
template 240
vein pattern recognition 240
evidence 107
kerberos 248–250
multi-factor 247
one-time password 245–246
password 241–246
pattern lock 246–247
pre-boot 269
protocol 107
server 108, 110, 201, 248
strong 107, 108
three-way 111
through the net 247–250
trends 247
weak 107
with PKCS 110–111
with SKCS 108–109
zero-knowledge 108
authentication code 245
authenticator 108, 249
Authenticode 317
authorisation 250
authoritative DNS-server 218
AV system 293–296
anomaly detection 294
behaviour based 293, 294
in telephone 295
misuse detection 294
signature based 293
availability 10, 12, 171, 211
avalanche effect 98
awareness campaign 342, 343

B

backdoor 19, 289, 374
backup 337
base 400
Base Transceiver Station *see* BTS
base64 encoding 160, 306–307
baseline based analysis 197
basic authentication 305
Basic Service Set *see* WiFi BSS
bastion host 192, 194, 195
BCP 333–341
resource requirements 335
Big Brother society 353
bigram 63
binary data 66
binary digit 401
biometric authentication 237–240
biometric parameter 237
biometric property 388
BIOS 267, 273, 392
birthday paradox 97, 410
bit generator
period 74
pseudo-random 73
random 73
shift register based 74–75
BitLocker 268
Blaise de Vigenère 64
block cipher 101
mode 70–71, 73, 101, 184, 249
Bluebugging 204
Bluejacking 204
Bluesnarfing 204
Bluetooth

authentication 202
encryption key 202
link key 202
pairing 202
security 202–204
SSP 203
BluRay disk 387
boot 392
boot loader 273
boot manager 273
boot sector 273
bootkit 267, 273
botnet 6, 8, 216
brain mode of operation 22
breach of copyright 350
bridge 142, 388
brute-force attack 59, 101, 203, 241
Btrfs 340
BTS 147
false 208–209
buffer overflow 282–284, 292
buffer overread 284–285
bus 381, 388
Business Continuity Planning *see* BCP
BYOD 210
bytecode 265, 316, 320

C

C 283, 288
cache 141, 383
ARP 141
CPU 328, 383
disk 328
DNS 141, 218
HTTP 167, 168
cache poisoning 219
Caesar code 60
camera 388
canonification 299
capability 253
Capsicum 254
CAPTCHA 27
CBC 70, 101, 184, 185, 249
CCM 101, 185, 201
CD 387
Cellular Network Isolation Card *see* CNIC
Central Processing Unit *see* CPU
CEO fraud 21
certificate 110, 113–116, 175, 176
chain 116
EV 115
OCSP 188
qualified 121
revocation 114, 188
risks 187–188
root 116
self-signed 116, 118, 316
Certificate Authority (CA) 113
Certificate Revocation List *see* CRL
Certificate Signing Policy (CSP) 115
ChaCha20 78, 185
chain of responsibility 330
challenge-response 245
Change Permissions 259
checksum
CRC 200
cryptographic 95, 201
child pornography 350
Chinese remainder theorem 86, 406–407
CIA target 10, 128, 171
definition 10
CIP 226
Cipher Block Chaining *see* CBC
ciphertext 57, 58
CipherText Stealing *see* CTS
CIRP 335
Claude Shannon 66
client 3
client nonce 309
client-server architecture 153
cloud 3, 5, 87, 287, 294, 338, 358
cluster 5
CNIC 331
co-domain 399
COBIT 43
Code Red 293
signature 293
cognitive overload 27
cold site 340, 341
Colonial Pipeline 7
Common Criteria (CC) 275, 321, 375
environment 375
evaluation 276, 375, 377
life cycle 375
Common Name (CN) 114
communication node 125
communication plan 337
communication unit 389–390
community string 225
default 225
computer architecture 381
computer crime 348–353
computer forensics 327
computer system 4
concatenation 96, 100, 103
confidentiality 10, 12, 79, 171
conformance test 341

confusion 66, 68
congruence 80
connection 128
connection oriented 137
connectionless 137
consent 354–356, 366
Content Management System (CMS) 319
control 39
control system 390
cookie 305, 309–312, 367
  domain 310
  expiry 310
  HttpOnly 310
  max-age 310
  path 310
  persistent 310
  risici 311
  secure 310
  store 310
  third-party 312, 367
Copy-on-write (COW) 340
core 382
COSO 43
Council of Europe convention
  Cybercrime 348–352
    extradition 352
    international assistance 352
    jurisdiction 351–352
    procedural criminal law 350–351
    substantive criminal law 349
    substantive criminal law 350
  Personal data 353
  Terrorism 352–353
countermeasure 39, 41–42
Country (C) 114
COW 340
CPU 381
  core 382
  mode 264
critical asset 47
critical infrastructure 7, 226–228
CRL 114, 188
Cross-site scripting *see* XSS
cryptanalysis 59–60
  differential 70
  frequency analytic 61
cryptographic random number generator 67
Cryptolocker 6
cryptosystem 58
  asymmetric 59, 79–88
  broken 60
  ElGamal 104
  malleable 87, 103
  reversible 103
  symmetric 58, 60–78
CTS 249
cursor 387
customer profile 366
CVE system 271
cyberattack 5–9
Cyberincident Recovery Planning *see* CIRP
cyberspace 1
cybersquatting 26
cyberwar 8
cyclic permutation 60

D

DAC 251
Dalvik 265
dark Internet 181
Data Encryption Standard *see* DES
data leakage 360
datamining 365–366
DDoS attack 211, 216–217
decapsulation 131
decryption 57
  function 58
  key 58
Deep Crack 69
DeMilitarized Zone *see* DMZ
deniable encryption 332
DES 68–71
dictionary attack 241
Diffie-Hellman key agreement 112
  attack 112
  in Bluetooth 203
diffusion 66, 68, 71
digest authentication 208, 305
digital signature 273
Digital Signature Standard *see* DSS
directory 253
Directory Information Tree *see* DIT
Disaster Recovery Planning *see* DRP
discoverable 203
Discretionary Access Control *see* DAC
discriminator 197
disk 383–387
  copy 329, 330
    bit-by-bit 329
    file-by-file 329
  forensic acquisition 332
  mounted 329
  sector 384
  track 384
Distinguished Name (DN) 299
DIT 299, 300
divide-and-conquer 394

DKIM 220, 222–224
  signature 222
  tag 223
DMZ 194, 195
  split 194
DNS 119, 139–140, 156, 220
  authentication 219
  cache 141
  confidentiality 220
  integrity 219
  operation 139
  resolver 139, 141, 218
  root server 139
  RR 140
  security 218–220
  server 218
    authoritative 218
    false 219
  zone transfer 140, 220
DNSSEC 219
domain 133–134, 399
Domain Name Service *see* DNS
DomainKeys Identified Mail *see* DKIM
DoS attack 143, 211–218
  fast 211
  slow 212, 213
driver 263, 267, 391
DRP 335–341
  testing 341
DSA 104, 161
DSS 104–105
dual-homed host 192
DVD 387
dynamic analysis 288
dynamic packet filter 190

E

E0 75, 202
EAL 276, 321, 375
EAP 201
eBay 118
ECB 70
ECDSA 104
economy
  underground 9
EDGE 146
EDVAC 381
egress filter 190, 218
eID 119, 247
Electronic Codebook *see* ECB
electronic identity 121
  authentication 121
  quality of credential 121
  quality of issuer 121
Electronic Patient Record 363
electronic signature 102–106, 110, 111, 113, 219
  anonymous 369
  future planning 106
  requirements 102
  verification 102–103
  with appendix 104, 161
  with PKCS 103–105
  with recovery 103
encapsulation 131
encryption 57, 171–178
  asymmetric 79–88
  Full Disk (FDE) 268–270, 332
  function 58
  in Application layer 172, 175–177
  in Internet layer 174
  in Internet layer 173
  in layered architecture 171–172
  in Link layer 174
  in operating system 268–270
  in Physical layer 175
  in Transport layer 173
  key 58
  symmetric 60–66
  transparent 268
end systems 125
end-to-end 130
Enhanced privacy ID (EPID) 369
entertainment device 4
entry point 291
escaping 304
eStream stream cipher 78
Ethernet 143
  switched 144
ethical hacker 295
ethics 364–369
EU Directive 353
EU Regulation 354
Euclid's algorithm 403–404
Euclid's extended algorithm 83, 87, 404–407, 409
Euler's totient function 81, 408
EV certificate 115
Evaluation Assurance Level *see* EAL
Evolved HSPA 146
exclusive or *see* XOR
exfiltration 6
existential forgery 100
exponent 113, 400
Extended Authentication Protocol *see* EAP
Extended Service Set *see* WiFi ESS
Extended Validation (EV) certificate 115

extension 114
extradite-or-prosecute 352, 353

F

face recognition 238
Facebook *Like* 367
Fail-safe Defaults 252
FAIR 43
false acceptance 237
false negative 197, 294
false positive 197, 294
false rejection 237
Faraday cage 329, 331
FDE 268, 332
fear appeal 30
Feistel network 68–69
fence register 260
file
  deletion 329
file descriptor 285
file protection
  Unix 255–257
    group 255, 257
    owner 255, 257
    problems 256
    root 255
    world 255
  Windows 258–259
    group 259
file system 254, 392
FileVault 268
finger pattern 239
fingerprint 237
fingerprint reader 388
FIPS Standard
  140 374
  197 72
  PUB 46 68
firewall 142, 189–196
  application proxy 190
  packet filter (PF) 189
  personal 195–196
  placement 192–194
  residual risks 195
  Stateful Packet Inspection (SPI) 190
  tre-benet 194
Firewire 388
firmware 272, 392
  BIOS 392
flag
  TCP 136
flash drive 385
flight mode 331
FNR 197
forensic acquisition disk 332
Forensic Toolkit (FTK®) 330
forensics 327–333
  encrypted data 332–333
  memory 330
  smartphone 330–331
FPR 197
frame 141
FreeBSD 251, 254, 257, 268
frequency analysis 61–63, 65
  Al-Kindi 61
Friedrich Kasiski 64
Fuchsia 254
Full Control 259
Full Disk Encryption *see* FDE
function 399–400
  co-domain 399
  compression 98
  domain 399
  graph 97, 399
  image 399
  linear 75, 400
  non-linear 75, 98, 400
  one-way 80, 96, 98
  pre-image 96, 400
  total 399
  value 399
fuzz test 287

G

gateway 142
GCC 288
GDPR 353–362, 379
  accountability 355, 361
  authorities 360–362
  certification 361
  code of conduct 361
  consent 354
  controller 354
  data class 356–357
    sensitive 356
  data protection impact assessment 359
  Data Protection Officer (DPO) 360
  European Data Protection Board 361
  European Data Protection Supervisor (EDPS) 361
  legal responsibility 362
  personal data breach 354
  pictures and sounds 357
  processor 354
  profiling 354, 366
  pseudonymisation 354

recipient 354
rights 358–359
erasure 368
objection 366
security of processing 359, 360
security targets 359
standard contractual clause 358
Supervisory Authority 361
third country 358
GEA/3 206
General Data Protection Regulation *see* GDPR
geolocation software 135
GPRS 146
GPU 383, 387
graphic user interface 387
graphics card 387
Graphics Processing Unit *see* GPU
greatest common divisor 403
group 255, 259
GSM 146
authentication 204
encryption 204–206
security 204–206

H

hack 40
half open session 173
Hamming weight 85
Hard Disk Drive *see* HDD
hard problem 82, 83, 88, 106
hardening 192
hardware 381–390
interface 388
hash function
SHA-1 99
hash function 99
collision resistent 96, 100
cryptographic 96–99
MD5 99, 101, 106
non-invertible 96, 100
one-way 96
security strength 97
SHA-1 101, 106
SHA-2 99, 105, 106
SHA-3 99, 105, 106
HDD 384
header 136
health data
access 363–364
protection 363–364
Heartbleed bug 284
hexadecimal digit 401
hibernate state 270
HIDS 198
HMAC 100
Home Location Register (HLR) 148
host 125
hot site 340
household apparatus 4
HSM 220
HTML 165, 210
anchor 166, 210
character code 165
href 166, 210
link 166
webform 313
HTTP 162–169
applications 304–315
architecture 162
authentication 305–309
basic 305–306
digest 307–308
realm 305
vulnerabilities 309
authorisation 167
cache 167, 168
control 167
character set 167
cookie 305, 309–312, 367
non-essential 368
form dataset 314
header field 305
link 162
media type 167
method 166, 304
GET 163, 167, 168, 315
OPTIONS 168
POST 315
operation of 163
request 162, 167–168, 304
response 163, 168, 304
return code 163
script 305
SessionID 312–313
webform 305, 313–315
human rights 351
hyperlink 162
hypertext 162
Hypertext Markup Language *see* HTML
Hypertext Transfer Protocol *see* HTTP
hypervisor 265

I

I/O control hub 388
I/O unit

attachment 388–389
IANA 135, 136
IDE 331
identity module (IM) 148, 330
identity theft 366, 369
IDPS 196
IDS 196–199, 272
anomaly detection 196
in host 198
in network 198
misuse detection 196
IEEE Standard
802 series 144
802.1X 201, 202
802.3 143
802.11 144, 145
802.11i 201
802.15 144
802.16 144
IEEE standard 1394 bus 388
IMAP 153
impact analysis 334
IMSI 148, 208
IMSI catcher 208
Incident Response 325
incomplete mediation 285
industrial espionage 330
Infrastructure Mode 145
ingress filter 190, 218
Initialisation Vector *see* IV
instruction 381
integer 397
integer factorisation
Fermat 84, 401–402
Number Field Sieve 86, 402
Quadratic Sieve 86, 402
integrity 10, 77, 87, 95–101, 171
International Mobile Subscriber Identity *see* IMSI
Internet layer 130
encryption 173–174
Internet name 119, 132–134
Internet of Things *see* IOT
interoperability 144
interpreter 316
Intrusion Detection System *see* IDS
inverse 81, 405, 409
investigation 350
IOT 4, 135, 147, 217, 378
IP address 132
range 221
IP Version 4 (IPv4) 134
IP Version 6 (IPv6) 134
IPsec 180
iris recognition 239
ISO Standard
8859-1 159
9796 103
9798 110
ISO-latin-1 printable 242
ISO/IEC Standard
11889:2009 269
27000 series 44
27005:2011 55
27001 326, 378
27002 11, 43
ISP 142
ITU-T Standard
X.500 series 299
X.520 301
IV 71, 74, 75, 97

J

Java 288, 316, 320
job scheduling 270
John von Neumann 381
jurisdiction 351–352
universal 352

K

KASUMI 206
Keccak 99
kerberos 111, 248–250, 309
Kerckhoff's Principle 58
key agreement 111
Diffie-Hellman 112
in Bluetooth 203
station-to-station 113
key distribution 111–113
Key Exchange Key (KEK) 273
key logger 292
key schedule 69, 72
key transport 111
key wheel 60, 61
Key-Scheduling Algorithm (KSA) 76
keyboard 387
keylogger 274
keyring 269
keystore 269
keystream 73

L

LAN 125, 144
layer
Application 131
Physical 131
LDAP 299

  attribute 299, 301
  DIT 299, 300
  escaping 304
  injection 299–304
  input control 304
  metacharacters 304
  object class 300
    device 299
    organization 299
    organizationalUnit 299
    person 299
  search 302–304
    base 302, 303
    filter 303
    scope 302
  type control 304
  URI 302
Least Privilege 251, 257
legal person 348
LFSR 74
  period 74, 75
lifecycle 375
lifetime 111
Lightweight Directory Access Protocol *see* LDAP
Linear Feedback Shift Register *see* LFSR
link 162, 166, 210
link key 202, 203
Link layer 130
  encryption 174
Lithium-ion (LiON) 390
Local Area Network *see* LAN
log file 327, 392
logic bomb 289
long-term key 76
LPC bus 389
LTE Advanced 147

M

MAC 100, 251, 275
  hash-based 100
MAC address 132
MAC key 100
MAC protocol 143
mail relay 156–157
Mail Transfer Agent *see* MTA
Mail User Agent *see* MUA
mailbox 153, 156
mainframe 5, 268
malicious code 289–296
malleable 77, 87, 103, 124
malware 2, 40, 267, 281, 289–296
  backdoor 289, 374
  logic bomb 289
  rabbit 289
  ransomware 289
  spyware 289, 374
  trojan horse 289
  virus 289
  worm 289
MAN 125, 144
Man-machine interface 387
Management Information Base (MIB) 225
Mandatory Access Control *see* MAC
Master Boot Record 267, 329
MBR 273
MD5 99, 101, 106, 168, 176, 309
Media Access protocol 143
mediation 285
memory 383
  control hub 388
  paging 261
  physical 328
  segmented 260
  volatile 392
memory card 385, 386
memory leak 288
Memory Management Unit *see* MMU
memory unit 381
Merkle-Damgaard construction 98
message
  corruption 128
  forgery 128, 199
  loss 128
Message Authentication Code *see* MAC
message digest 96, 104
  function 96
message format 129
message key 105
metacharacters 298
metadata 268, 360
method 162
Metropolitan Area Network *see* MAN
Michael cryptographic checksum 201
Microsoft Exchange data breach 7
Milgram's eksperiment 21
MIME 158–162
  entity 159
    body 159
    composed 161
    content type 159
    encoding type 159
    header 159
  header field 159
  subtype 160, 176, 178
  type 160, 176, 178
    application 160, 176, 178

message 162
multipart 161, 176, 178
MISTY1 206
misuse detection 196, 294
MLS 275
MMI code 210
MMI unit 387
MMU 260
mobile code 316–317
mobile device security 209–211
Mobile Station International Subscriber Directory Number *see* MSISDN
mobile telephone network 146–149
2G 146
3G 146
4G 147
5G 147, 374
AuC 149
authentication centre *see* AuC
core network 147
GPRS 146
GSM 146, 147
HLR 148
security 204–211
surveillance 208–209
UMTS 146, 207–208
VLR 148
mobile unit 148, 330
modular arithmetic 80–82
modular exponentiation 81, 82, 105
modular squaring 82
modulus 104, 113
monitoring
passive 199
monoalphabetic cipher 61
motivation 342
motive 48
mouse 387
MSISDN 148
MTA 156
MUA 156
multi-factor authentication 247
Multi-Level Security *see* MLS
multiprogramming 391
Multipurpose Internet Mail Extensions *see* MIME
MX record 156

N

name administrator 133
native code 265, 317
natural person 348
NEED 217
network 3–4
Network access layer 131
Network Enabled Embedded Device *see* NEED
Network technology 141–149
neural network 197
NIDS 198
non-repudiation 102, 128
nonce 71, 74, 76, 77, 96, 107, 110, 111, 200, 208, 307, 309
definition 71
nonce counter 309
NotPetya 6
NSA 228
NTP 249
number system 400
binary 401
hexadecimal 401
positional 401

O

object 250, 252
owner 251, 252
OCSP 188
responder 188
response 188
stapling 188
OCTAVE 43, 45–53
Phase 1 46–53
threat analysis 49–53
threat classes 48
definition 48
threat profile 48
access 48
actor 48
asset 48
motive 48
outcome 48
threat tree 48
Office of Public Management (OPM) 5
One-Time Pad 67–68
one-time password 245–247
one-way function 80
OpenSSL 284
operating system *see* OS
oracle 100
Organisation (O) 114
Organizational Unit (OU) 114
Orion 7
OS 390–393
module 267
security 235–279
trusted 275

updating 271–272
OTP *see* one-time password
OTP device 245
outcome 48
owner 255

P

padding 66, 87
page 261
page table 261
pairing 202
PAN 125, 144
passive attacker 112
passkey 247
password 241–246
choice 243–245
protection 242–243
strength 241–242
password tiredness 249
pattern lock 246–247
payload 136
PCI Expressbus 388
PDCA process 53, 54, 334
PDoS 217
peer-to-peer (P2P) 3, 216
Pegasus 296
pentest 287
permissions 258
person 347
Personal Area Network *see* PAN
personal data 354
protection 353–362
personal firewall 195–196
PGP 118, 175, 177
type 178
phishing 25–27, 367
bait 25
e-mail 25, 26, 155
social media 25
PHP 288, 320
Physical layer 130, 131
encryption 175
physical security 274
pigpen cipher 63
PKCS 59, 79–88
PKCS#1 87, 104
PKCS#7 161, 176
PKCS#10 115
PKCS#12 115, 121
PKI system 113, 117
plaintext 57, 58
Platform Key (PK) 273
point-to-point 143
polyalphabetic cipher 64–65
POP3 153
port
allocated 135
freely available 136
registered 136
TCP 135–136
UDP 135–136
port number 132
Post-Quantum Cryptography *see* PQC
power supply 390
PQC 106
competition 106
pre-boot authentication 269, 332
preimage resistance 96
prime factor 397
prime number 397
mutual 403
priming 23
primitive polynomial 75
Privacy-Enhancing Technology (PET) 368
private key 79, 103, 104, 110
privilege escalation 266, 296
proactive control 244
process hollowing 292, 294
processor 381
program 381
program analysis
dynamic 288
static 288
program vulnerability 281
protection 391
protection ring 264
protocol 107
ARP 141
DNS 139–140
HTTP 162–169, 304–315
ICMP 215
IMAP 153
LDAP 299–304
POP3 153
SMTP 153–162, 220–224
SNMP 224–225
station-to-station 113
TCP 136–139, 213–214
Protocol Control Information (PCI) 129
proxy 192
public key 103, 110
Public Key Cryptosystem *see* PKCS
Public Key Infrastructure *see* PKI

Q

qop 308

qualified certificate 121
quality of protection 307
quantum computer 88
query 319

R

rabbit 289
race condition 286
Radio Network Controller *see* RNC
Rainbow Series 1
random permutation 61
ransomware 6, 289, 338
RC4 76–78, 200
  keystream generator 76
  vulnerabilities 185
  weakness 76–78
reactive control 244
recovery
  data 337–340
  system functionality 340–341
Recovery Point Objective *see* RPO
recovery target 334
Recovery Time Objective *see* RTO
redirection attack 173, 184
Redline 330
redundancy 226, 335
Reference Monitor (RM) 236, 267–268, 376
reference number 95
register
  CPU 383
Registration Authority (RA) 115
Registry 263
  key 263
  subkey 263
remote wipe 331
replaying 199
request 162
residual risk 39, 52
  matrix 39, 53
resolver 139, 141, 218
resource 304
Resource Record (RR) 140, 156
response 163
return code 163
RFC 150
right 250, 358–359
right to be forgotten 368
Rijndael 72
risk 37, 38
  analysis 45
  avoidance 42
  management 42
  matrix 38, 52
  mitigation 42
    strategy 42
  objective 37
  reduction 42
  residual 39
  retention 42
  sharing 42
  subjective 37
  transfer 42
RNC 207
roaming 148
Robust Security Network *see* RSN
robustness 288
ROCA attack 374
role 251
Role Based Access Control (RBAC) 251
root 251
  privileges 255
root certificate 116, 118
root keys 263
root server 139
rootkit 266–267
  BIOS 267
  bootkit 267
  kernel mode 267
  user mode 266
round key 72, 269
router 132, 142–143
RPO 334, 337–341
RR 140, 156
RSA 82–88, 103, 113, 161, 407–409
  key generation 83, 374
  modulus 82
  private exponent 82
  private key 82
  public exponent 82
  public key 82
  vulnerabilities 86–87
RSA number 85, 402
RSN 201
RTO 334, 337–341
rule of procedure 129

S

S/MIME 161, 175, 177
  type 176
safe harbour 358, 365
safe library 283
salt 243
sandbox 265
scheme 163, 164, 210
Schrems II 366
screen 387

screened host 193
screened subnet 194
screening router 192
script 305
second-preimage resistance 96
secret key 102, 108, 111
Secret Key Cryptosystem *see* SKCS
sector 384
Secure Boot 272
Secure Digital (SD) 386
Secure Hash Algorithm (SHA) 176
Secure Shell (SSH) 247
security
  breach 325
    conditions 17
  failure 281
  incident 325
  policy 11–12
  strength
    DSA signature 104
    hash function 97, 106
  target 9–10, 128
security analysis
  systematic 43–54
security awareness 32, 342, 377
security device 387
security in depth 194
security parameter 184
security zone 317
segment 260
segment table 260, 261
self-efficacy 31
SELinux 251, 267, 376
Semalt 6
Sender Policy Frmamework *see* SPF
sensor 4
separation 250
seq 136, 137
sequence number 136
server 3
server script 166
service 127
  complex 2
  connection-oriented 128
  connectionless 128
  cybercriminal 8
  error-free 128
  secure 128
  sequence preserving 127
  SMS 146
  stream-oriented 129
service extension 154
servlet 319–320
session key 175, 176, 205, 248, 249
session theft 173
SessionID 312–313
  risici 312
set 398
  cardinality 398
  containment 398
  difference 398
  intersection 398
  membership 398
  subset 398
  union 398
Set Groupid 257
Set Userid 257
setgid 257
setuid 257
SHA-1 99, 101, 106
SHA-2 99, 105, 106, 309
SHA-3 99, 105, 106
shared medium 130, 143
  cable-based 143–144
  wireless 144–149
side effect 315
sidetabel 262
signature 196, 293
signature based analysis 196
SIM card 148, 204
Simple Mail Transfer Protocol *see* SMTP
Simple Network Management Protocol *see* SNMP
single sign-on (SSO) 249
SKCS 59–78
Slowloris 212
smartcard 115, 121, 148, 236, 269
  UICC 207, 331
smartphone
  forensics 330–331
SMTP 153–162
  command 153
  error code 222
  header line 157–158, 222
  mailbox 153, 156
  Message-ID 157
  operation 154
  response 153
  risks 155
  security 220–224
  service extension 186
  spoofing 155, 220
  tracking 157
Smurf attack 215
snapshot 339
sniffer 132, 143, 174
SNMP 224
  security 224–225

social engineering 18, 241, 292
social media 25, 367
soft certificate 121
software 390–394
  application 393–394
  flaw
    buffer overflow 282–283, 292
    buffer overread 284–285
    detection 286
    incomplete mediation 285
    malicious 281
    non-malicious 281
    stack overflow 282
    TOCTTOU 285
  injection 285
  operating system 391–393
  system utility 393
  test 286
  vulnerability 283, 292
Solid State Drive *see* SSD
sound card 387
spam mail 155
spearphishing 26
special permissions 258
SPF 220–222
  mechanism 221
  policy 221
  qualifier 221
spoofing 220
  DNS 217
  e-mail 26, 155
  ICMP 215
  IP 173, 189
  TCP SYN 213
spyware 289, 296, 312, 374
SQL injection 296–299
square-and-multiply method 85
SS code 210
SSD 385
  wear levelling 385
SSID 145, 200
SSL 180, 182–187, 318
  Alert protocol 183
  Change Cipher Spec protocol 183
  Handshake protocol 183–185
  Record protocol 183
  securing application protocols 185–187
  security parameter set 184–185
stack 282
stack overflow 282
Standard Contractual Clause (SCC) 366
standby state 269
Stanley Milgram 21
STARTTLS 185–187
state machine 97
static analysis 288, 289
StingRay 209
storage unit 381
stream cipher 73
STRIDE 47
Stuxnet 6, 266
stylus 387
subject 250–252, 259
Subscriber Identity Module 148
substitution cipher 60–65
swap area 262, 268
switch 144, 174
symmetric stream cipher 73–78
  eStream 78
  RC4 76–78
SYN flood 213
SYN spoof 213
System 1 22
System 2 22
system history 327
system of systems 5
system program 390, 393
system state 327
  volatile 328
system utility 393

T

tag 100
Take Ownership 259
TCP
  flag 136, 137
  operation 137–139
  port 135–136
telephone modem 389
template 240
Temporal Key Integrity Protocol *see* TKIP
test
  blackbox 287
  fuzz 287
  penetration 287
  whitebox 287
texting 419
TGT 248
The Sleuth Kit (TSK) 330
threat 37
  data related 41
  hardware related 40
  in IT system 40–41
  liveware related 41
  software related 40
threat analysis 49–53, 334
threat profile 47

threat tree 48
Ticket Granting Server (TGS) 248
Ticket Granting Ticket *see* TGT
tickets 248
tiered architecture 394
time stamp 95
Time-of-check to Time-of-use *see* TOCTTOU
timeout time 213
TKIP 201
TLS 78, 180, 182–187, 318
  Heartbleed 284
TOCTTOU flaw 285
Tor 181–182, 368
touch sensitive 387
tracking 366–368
transaction 367
transparent encryption 268
Transport layer 130
  encryption 173
transposition cipher 65–66
trapdoor function 79–80
trigram 63
Triple-DES (3DES) 69, 176
trojan horse 28, 289
TrueCrypt 268
trust 158
trust model 117
  hierarchical 117–118
  reputation-based 117–119
  web-of-trust 117–118
Trust Service Provider *see* TSP
Trusted Platform Module (TPM) 269
TrustedBSD 251
TSP 120
tunneling 178–180
type control 304

U

UDP 139, 219
  port 135–136
UEFI 273, 392
  boot loader 273
  boot manager 273
  KEK 273
  PK 273
  trust 273
UMTS 146
  AKA 208
  authentication vector 207
  security 207–208
Unified Extensible Firmware Interface *see* UEFI
Uniform Resource Identifier *see* URI
Universal Serial Bus *see* USB
URI 162–164, 305
  password 163
  path 164
  port number 164
  query 164
  scheme 163, 164, 210
  userid 163
usability 178
USB 388
  hub 388
  key 386
  port 385
user control 392
user interface 392
utility program 393

V

vein pattern 240
Vigenère cipher 64–65
  encoding table 65
virtual machine *see* VM
virtual memory 262
Virtual Private Network *see* VPN
virus 289
  attack 290–291
  code 291
  concealment 290
  execution 290
  placement 290, 291
Visitor Location Register (VLR) 148
VM 265, 329
  guest 265
  host 265
Volatility 330
von Neumann architecture 382
VPN 178–182
vulnerability 37
  psychological 38
    affect 25
    anchoring 23
    attribution 24
    belief in authority 20–22
    curiosity 19
    framing 24–25
    helpfulness 19–20
    sympathy and hate 20
    uncertainity in decision making 23–25
  technical 37

W

walkthrough 341

- WAN 125, 144
- WannaCry 271
- warm site 340, 341
- weakness 37
- wear levelling 385
- Web-of-trust 117
- webform 305, 313–315
  - BUTTON element 313
  - checkbox 314
  - file 314
  - hidden field 314
  - INPUT element 313
  - menu 314
  - password 314
  - radio button 314
  - reset 313
  - risks 315
  - SELECT element 314
  - submit 313
  - TEXTAREA element 314
- webserver
  - vulnerability 317–318
- WEP 77, 200
- whois 134
- Wi-Fi Protected Access *see* WPA
- Wide Area Network *see* WAN
- WiFi 144–145
  - Access Point (AP) 145
  - authentication
    - 802.1X 201, 202
    - Open System 200
    - Shared Key 200
  - BSS 145
  - ESS 145
  - integrity
    - CCM 201
    - CRC 200
    - Michael checksum 201
  - mode
    - ad hoc 145, 146
    - infrastructure 145–147
  - RSN 201
  - SSID 145, 200
  - WEP 200
  - WPA 201
  - WPA2 201
- WiMAX 147
- Windows
  - VSS 340
  - XP 268, 376
- wireless network 144–149
  - security 199–211
- worm 289
  - attack 292
  - payload 292
  - propagator 292
- WPA 201
- WPA2 201

X

- X-as-a-service 8
- X.500 Directory 116, 299
- X.500 name 114, 301
- X.509v3 certificate 113
- XOR function 67, 68, 73
- XSS 318–319

Z

- zero-day attack 272
- ZFS 340
- zombie 216
- zone transfer 140, 220
- Zone Walking 220