Index

A

access control 318–326, 338
  model 345–357
active tracing 368
activity monitoring 358, 362
ADAM 333
advanced encryption standard (AES) 60
aerial photography 300
Al-Jazeera 21
Al-Qaida 8
Al Qaeda 51
amplification attack 265
anomaly detection 327–337, 358
antispam 254–261
association rule mining 359
attacker 165
auditing 210
authentication 130, 189, 258, 338
authenticity 415
authentification 319
authority 194
authorization 318, 319, 356
availability 130, 319

B

barrier
  analysis 245
  design 245
behavioral information security 199–205
bin Laden, Osama 2, 51
bio-cyber nachine gun (BCMG) 338–344
Blaster worm 78–82
bouncing techniques 392–396
business integrity (BI) 67

C

Carnivore 476
charities 141
Chechen rebel 43
chief knowledge officer (CKO) 12
cipher 57
Civil Liberties Monitoring Project (CLMP) 174
civil rights 173–181
Civil War 300
cluster 359
clustering 375
  hamming 379
  unsupervised 375
Code Red 267
COMCRIME study 432–438
command and control warfare (C2W) 441–445
commercial off-the-shelf (COTS) 404
common sense 209
competitive early warning (CEW) 211
computer
  crime 398
  monitoring 175
Computer Misuse Act 308
confidentiality 130, 285, 319, 415
copyright 433–438
corporate security 208
Council of Europe (CoE) 470
counterterrorism 10, 292
counterterrorism program
  crime 4
cracker 307
critical infrastructure 36
critical infrastructure protection (CIP) 84
cryptanalysis 59
cryptography 57–64, 319, 338
cyber
  attack 85, 97, 109, 229, 404, 448
  counterterrorism 291–297
  criminal 121
  exploit 37
  forensics 397–402
  intrusion 374
  planning 9
  security 78–82, 191, 446
    model 228–240
  stalking 216–227
  terrorism 7–16, 36, 42, 83–90, 138, 155, 254, 273, 345, 383
    attack 1–6
  terrorist 43, 113, 184, 241, 392
  war 18
    attack 105–111
    defense 241–253
  warfare 35, 291–297, 327, 439–445
  warrior 241
  weapon 17
cybercrime 431–438, 470
Cybercrime Convention 433–438
cyberspace 7, 36, 91, 421

D

data
  encryption standard (DES) 60
  flow diagram (DFD) 246
  intrusion 470
  mining 358–365
    identification 374
  protection 420–430
  transformation 329
database management system (DBMS) 162
denial-of-service (DoS) 133, 232, 262–272, 273, 328
  attack 421
Department of Defense (DoD) 320, 404, 439–445
digital
  address
    denial-of-service (DoS) 366–373
  security 208
  signature 51, 283

Copyright © 2008, IGI Global, distributing in print or electronic forms without written permission of IGI Global is prohibited.

discretionary access control (DAC) 356
distributed
  attack tool 413
  denial-of-service (DDoS) 262
domain name 122
  server (DNS) 448
  service 94
  system 258
dual criminality 476
dynamic survivability model 408

E

e-
  postage 257
  stamp 257
E-Crime Watch survey 470
eavesdropping 307–317
  software 309
Echelon 453–468
electromagnetic spectrum 299
electronic
  bank 139
  commerce 129, 262
  communication 424
  document interchange (EDI) 285
  government 322
  mail 123, 394–396
    phishing 192
  money management 129–137
  signature 283
  surveillance 173–181
emergency response system 383–391
encryption 59
Environmental Protection Agency (EPA) 294
espionage
  economic 457
  political 458, 459
ethics 105
European Union (EU) 149, 282, 422, 431–438
exploitation 121

F

face-to-face conversation 184
false
  negative 328
  positive 328
Federal Bureau of Investigation (FBI) 4, 177, 254
firewall 100, 311
flood attack 265
Foreign Intelligence Surveillance Court (FISC) 460
fraud 436–438
FS-ISAC 83–90

G

G8 436–438
General Accounting Office (GAO) 85
Geneva Convention 107
geographic information systems (GIS) 291–297
global system for mobile communication (GSM) 148
Google 125
gray market informatics 114
guerilla warfare 12

H

hacker 9, 33, 45, 91, 121
hacking 307–317, 433–438, 469
hacktivism 90
Hammas 9
harassment 217
hashcash 257
Hezbollah 46
hidden pattern 359
hindering 434–438
HIPAA 116
Honeynet Project 99
honeynets 107
honeypot 98, 276
  signature 98
human interaction 207
hybrid system 379

I

information
  extraction (IE) 361
  gathering 120–128
  security 129
  sharing 85
  technology (IT) 2, 65, 86
  warfare 17–25, 44, 403, 441–445
instant messaging (IM) 147
integrity 130, 319, 415
intellectual property 433–438, 436–438
International CybercrimeConvention 469–476
international outsourcing 113
Internet 42–49, 120, 129, 368, 469
  Engineering Task Force (IETF) 449
  growth 200
  protocol (IP) 107, 122, 256, 310, 374, 448
  relay chat (IRC) 152
  service provider (ISP) 393–396, 400, 448
  usage 360
  user 147
interruption 434–438
intrusion detection 268, 274
  system 327, 358, 398

K

Kazaa 311
key
  logger 310
  logging 185
keystroke 185
  recording 176
kill files 220
knowledge 8
  discovery in databases (KDD) 359
  management 7–16
    system (KMS) 247
  society 7
  worker 8

L

Land Information Warfare Activity (LIWA) 441–445
light detection and ranging (LIDAR) 294
link analysis 360
load balancing 268
local area network (LAN) 310
logs 275

M

Magic Lantern software 309
malware 37, 154–160
mandatory access control (MAC) 321
Massachusetts Institue of Technology (MIT) 61
measurers of performance (MOP) 407
micropayment 269
military
  classification 349
  history 97
MINARET 459
mobile payment 138, 142
money laundering 138–145, 436–438
Morris worm 273

N

naïve Bayes (NB) 377
National Security Agency (NSA) 453–468
NetWar 7, 11
network

effect 79–82
monitoring 273
security 274, 281–290
sniffer 275

O

Office of Emergency Preparedness (OEP) 386
offshoring 113
outsourcing 113
over-criminalization 434–438
overloading 193

P

pacifism 106
packet sniffing 37, 312
passive attack 400
password 309
cracking 313
PayPal 129
penetration test 415
perception war 21
personal
computer (PC) 469
data 432–438
digital assistant (PDA) 398
identification
card (PID) 210
number (PIN) 310
information 112
privacy 173
personality disorder 219
personnel anomaly detection 206–215
phishing 22, 93, 255
pingsweep 368
Polybius 58
port address translation (PAT) 369
portscan 368
port scanning 121
predictive modeling 359
prepaid card 142
privacy 50, 66, 175, 207, 216, 4 32–438
protection 422
Privacy Rights Clearinghouse 178
privilege escalation 93
propaganda 43
public
-key certificate 284
key
cryptography 61, 282
infrastructure 281–290

Q

quality of service (QoS) 268

R

rank 209
reciprocation 193
reliability 66, 130
remailer approach 256
remote
-to-local (R2L) attack 328
sensing 298
reverse firewall 100
risk
analysis 244
identification 243
role-based access control (RBAC) 322
root key 284
rootkit 313
round-trip time (RTT) 369

S

security 19, 57, 66, 129, 187, 208, 345, 413, 421
monitoring 274
national 347, 449
needs 243
scan 415
system 2
vulnerability 92
self-awareness 209
sender authentication 258
September 11 3, 36, 183, 293, 443–445, 446
short messaging service (SMS) 147
signature 98
simple
mail transfer protocol (SMTP) 123
public key infrastructure (SPKI) 287
smart identification (ID) card 211
sniffer 99, 267, 275
social
awareness 206
engineering 121, 182–190, 191–198, 415
network analysis 11
software
security 78–82
survivability 406
vendor 80–82
spam 146–153, 254
trafficking 147
SpamMimic 52
spim 146–153
spoofing 92
spyware 101, 311
SQL
code poisoning 161–172
SQL injection attack 161
stalker
off-line 219
stalking
computer 217
e-mail 217
Internet 217
static survivability model 408
steganography 50–56, 62
strong affect 193
surveillance 174, 221, 309, 456, 476
survivability 404
Syracuse Information Systems Evaluation (SISE) 201

T

terrorism 1, 7–16, 42–49, 345, 420–430
financing 140
terrorist
attack 293, 443–445, 449
crime 3
group 345
groups 301
organization 360
Terrorist Detection System (TDS) 362
threat analysis 244
time
-to-live (TTL) 368
between attacks 230
timestamps 275
traceroute 368
transfers 140
Tribe Flood Network (TFN) 266
Trojan horse 94, 154–160, 190, 415
trust 75, 193
trustworthiness 68
Tupac Amaru Revolutionary Movement (MRTA) 43

U

U.S. Defense Advanced Research Projects Agency (DARPA) 367
ultra high frequency (UHF) 455
user
datagram protocol (UDP) 264
profile 350

V

VeriSign 131
very high frequency (VHF) 455
virtual
  gold currencies 141
  private network (VPN) 282
virus 6, 34, 37, 108, 314, 433–438
  attachment 308
  detection 275
visual
  data mining 359
  evoked potential (VEP) signal 339

W

warfare 26–34
watch lists 459
watermark 51, 284
weapons of mass destruction (WMD) 16, 26
Web
  content mining 358
  crawling 124
  hacking 165
  information agents 358
  mining 358
  server hacking 313
workplace privacy 175
worms 37, 260, 273, 309
  attack 331

X

XACML standard 349
xenophobic 476

Y

Y2K 386