Index

A
abstract state machine language (AsmL) 296
access
   control list (ACL) 5, 81
   point (AP) 3, 76, 83
advanced encryption standard (AES) 88, 306
anti-phishing
   Act 236
   defenses 235
   scheme 232
   Working Group (APWG) 211, 227
anti-virus
   and firewall software 54
   scanners 190
   tools 190
API snippets 202
application
   -based IDS (AIDS) 94, 95
   program interface (API) 190, 199
architectural component (AC) 112, 114, 115
armoring 244
attribute
   -based trust negotiation language (ATNL) 129
   authority (AA) 155, 157
   query message (AQM) 157
   response message (ARM) 157
authentication
   and key agreement (AKA) 52
   authorisation and accounting (AAA) 23, 86
   service 41
   solutions 54
   technique 235
authorization certificate 154
autonomic communication 120
autonomy 244
B
basic security module (BSM) 292
boot sector 243
broadband access server (BAS) 3
business continuity plan (BCP) 272
C
California social worker license (CCSW L) 123
card issuing system (CIS) 110
certificate
   authority (CA) 4, 107, 116
directory (DIR) 110
chief compliance officer (CCO) 175
Ciphering algorithm 89
commercial virus scanners 198
common
 algebraic specification language (CASL) 288
development and distribution license (CDDL) 178
intrusion specification language (CISL) 292
compliance officer (CCO) 183
Computer Emergency Response Team (CERT) 286
Confidentiality, Integrity, Availability (CIA) 23
content segment license (CSL) 176
control model 155
CORAS 311
 approach 311
risk
 analysis 311
 management method 313
correlated attack modeling language (CAML) 294
counter-phishing measure 223
countermeasures 263, 267
Cross Site Scripting (CSS) 213
cryptographic software module 31
cryptography provider manager (CPM) 56
custom attack simulation language (CASL) 294

D

data
 caging 38
 items (DI) 112
synchronization services (OMA) 35
defence mechanism 244
deleagatable authorization program (DAP) 159
delegation model 155
DeleteCriticalSection function 207
demilitarized zone (DMZ) 5, 81
denial of service (DoS) 77, 196
detection languages 294
device access control 31
differentially fed artificial neural network (DANN) 304
digital
 enabled usages (DEU) 179
 media business models (DMBM) 179

dependent
 data caging (DC) 110

policy management (DPM) 169, 185
property rights language (DPRL) 174
rights management (DRM)
 37, 57, 169, 177, 330
DIR directory service 111
directed acyclic graph (DAG) 27
directory service authority 110
direct phishing attacks 229
disaster recovery plan (DRP) 272
discretionary access control (DAC) 111
distributed program execution monitor (DPEM) 294
distribution rules 112, 117
DLV system 136
DMZ 14, 15
DNSSEC server 26
domain
 authority cookies 156
 name system (DNS) 3
term list 112
dynamically linked libraries (DLL) 199
dynamic host configuration protocol (DHCP) 3

E

EAP
 -transport layer security (EAP-TLS) 49
 -tunneled transport layer security (EAP-TTLS) 49
elected component complexes (SCC) 112
electronic
 healthcare record (EHCR) 104
 patient record (EPR) 104
 serial number (ESN) 56
elements 12, 14, 18
encryption software 54
enhanced message service (EMS) 35
EnterCriticalSection function 207
enterprise GRID alliance (EGA) 24
event languages 292
extended architecture 112
extreme programming (XP) 282
extensible rights markup language (XrML) 175

F

fault tolerance 23
file infector virus 243
Index

firewall 8, 12
forensic analysis software 54

G
general
  packet radio service (GPRS) 33
  purpose SSL (GPL) 289
geo-location information 235
GetKeyboardType function 207
Global GRID Forum (GGF) 24
Good Electronic Health Record (GEHR) project 113
graphical user interface (GUI) framework 35
graphics device interface (GDI) 36
GRID
  particle physics (GRIDPP) 25
  Research Integration Development and Support Center (GRIDS) 24
technologies 20
GSM networks (GPRS) 52

H
handle service (HS) 157
Hipocrates's oath 106
HiPoP Dynamic Sandbox (HDS) 27
host-based IDS (HIDS) 94
hypertext transfer protocol (HTTP) 99

I
IDWG transport protocol (IDP) 99
image conversion library (ICL) 36
incident object description exchange format (IODEF) 93
infection mechanisms 244
information
  rights management (IRM) 172
technology (IT) 246
infrared data association (IrDA) 33
initialization vector (IV) 84
input/output (I/O) circuits 43
instant messenger (IM) 255
intellectual property
  rights (IPR) 313
  property (IP) 312
interface definition language (IDL) 290
internal 6
Internet
  engineering task force (IETF) 93, 99
  protocol (IP) 97
interoperable DRM platform (IDP) 179
interpretation of attack specification 292
intranet worm 193
intrusion
  alert protocol (IAP) 99
detection
  exchange protocol (IDXP) 92, 93, 98, 99
  in our time (IDIOT) 294
  message exchange format (IDMEF) 93, 98, 292
  systems (IDS) 3, 78, 80, 92, 93, 290, 307
  prevention system (IPS) 3
Intrusion Detection Working Group (IDWG) 93, 99

J
Jackson structured design (JSD) 287

K
key
  generation instance 110
  loggers 224, 229
knowledge query and manipulation language (KQML) 290

L
language
  class 292
  of temporal order specification (LOTOS) 288
LeaveCriticalSection function 207
life cycle 244
  phase 277
lightweight directory access protocol (LDAP) 3, 111
link items (LI) 112
local
  area network (LAN) 32, 94, 193
  or a central key generator (LKG) 110

M
macro-viruses 191, 243
malicious
  code 191, 239
Index

programs 203
software 191
malware 191, 239
signature 191
mandatory access control (MAC) 111
mass-mailing worm 193
master boot
record (MBR) 197
sector 243
media support library (MSL) 36
MEDIS
architecture 114
project 114
message integrity code (MIC) 87
metacomputer 21
metamorphic 193, 207, 244
metropolitan area networks (MANs) 32
mobile
access number (MAN) 56
station (MS) 44
switching centre (MSC) 44
model-based security risk analysis 311
Moving Picture Experts Group (MPEG) 176
multifactor authentication 210
multifunctional software 54
multilayered security 256
multimedia framework (MMF) 36
Multimedia Hypermedia Experts Group (MHEG-5) 290
multipartite virus 243
multiple-input multiple output (MIMO) 57

N
naming authority (NA) 110
Nessus attack specification language (NASL) 294
network
-based IDS (NIDS) 94
access
control 31
server (NAS) 3
address translation (NAT) 3, 308
intrusions 239
monitoring/management (snmp) 32
service access control 31
nonfunctional requirements (NFR) 295

O
object management group (OMG) 290
one-way authentication 108
online certificate status protocol (OCSP) 38
open
digital rights language (ODRL) 176
mobile alliance (OMA) 176
operationally critical threat, asset, and vulnerability evaluation (OCTAVE) 268
method 268
original component complexes (OCCs) 112
orthogonal frequency division multiplexing (OFDM) 57
outgoing traffic 5
over-the-air (OTA) 55

P
Palo Alto Research Center (PARC) 175
parallel virtual machine (PVM) 21
participant cookies 156
passport unique identifier (PUID) 156
peer-to-peer (P2P) 22, 120, 193
architecture 172
performance evaluation 292
personal
area networks (PANs) 32
digital assistant (PDA) 32
information management (PIM) 35
personalized architecture 7
phishing-resistant schemes 233
physical protection 31
Planet-Lab hierarchy model 123
platform security 38
polymorphic 193, 207, 244
pre-shared key (PSK) 47, 87, 88
pretty good privacy (PGP) protocols 3
primary care provider (PCP) 112
privilege management infrastructure (PMI) 154
product design database (PDD) 317, 320
professional
authentication authority (PAA) 110
certification authority (PCA) 110
registration authority (PRA) 110
Project DIR 111
proxy 12, 15, 16, 17, 24
public key
certification authority (PKCA) 110
infrastructure (PKI) 4, 42, 154
registration authority (PKRA) 110

Q
qualification authentication authority (QAA) 110
quality
  of service (QoS) 302
  of service modeling language (QML) 290

R
radio waves 77
random early prediction (REP) 308
registration authority 110
RegQueryValueEx function 207
regular expression over events (REE) 294
release-of-information credential (CRoI) 123
remote authentication dial in user service (RA-DIUS) 4, 86, 306
reporting languages 292
reproduction 244
response languages 292
return
  on investment (ROI) 263
  on security investment (ROSI) 7, 18
rights
  delegation 23
  management services (RMS) 175
risk
  management 261
role
  -based access control (RBAC) 111
  based trust management framework (RT) 159
  model 155
root
  component 112, 114
  rootkits 239

S
scanners 207
script-viruses 243
secondary care provider (SCP) 112
secure
  electronic transactions (SET) 51
  socket layer (SSL) 4, 214
  video processor (SVP) 176
security
  architecture 2, 7, 15, 19
  constraints 1, 19
  education training and awareness (SETA) 247
  identifier (SID) 39
  policy 5, 7
sensitive servers 9, 10, 17
service level agreements (SLAs) 321
Shibboleth
  attribute requester (SHAR) 157
  Indexical Reference Establisher (SHIRE) 157
short message service (SMS) 35
simple
  hierarchical event description language (SHEDEL) 294
  mail transfer protocol (SMTP) 3
single
  sign-in (SSI) 156
  sign on (SSO) 24, 28
social engineering 211
software
  development life cycle (SDLC) 286
  key loggers 224
  specification languages (SSL) 286, 287
  usage monitor (SUM) 174
source of authorization (SOA) 155
SSH server 26
SSL protocol 24
stealth 244
storage protection 31
structured query language (SQL) 290
subscriber identity module (SIM) 42
Symbian
  -based mobile computing devices 31
  application 54
  based mobile devices 32
  devices 31
  OS 31, 35
    architecture 31
    platforms 33
    security 36
    root certificate 38
    security 32
  synchronized random dynamic (SRD) 214
system integrator (SI) 317

T
temporal key integrity protocol (TKIP) 86
three-way authentication 108
traditional rights usages (TRUs) 179
transmission control protocol (TCP) 99
transport layer security (TLS) 50, 82
trojans 192
TrustCoM risk analysis 315
trusted
computing base (TCB) 38
computing environment (TCE) 38
third party (TTP) 107
TrustHealth Project 110
tunnelling 244
two-way authentication 108

U
Universal SIM (USIM) 42
user interface (UI) 35

V
viral capacity 244
virtual
LAN (VLAN) 3, 81
organisation (VO) 312
private network (VPN) 4, 19, 34, 82, 94
viruses 239
virus writer 194
VOIP traffic 303
VPN 11
module 26
software 54

W
WAP identity module (WIM) 51
Web services security (WS-Security) 118
weighted
graphs 163
trust graph (WTG) 163
Where are you from? (WAYF) 157
wide area networks (Satellite-based WANs) 32
WiFi protected access (WPA) 86
wired equivalent privacy (WEP) 46, 83
wireless
application protocol (WAP) 50
equivalent privacy (WEP) 306
local area network (WLAN) 33, 42, 75
public key infrastructure (WPKI) 51
security software 54
transport layer security (WTLS) protocol 50
worms 192, 239