Index

*  
*-property • 74

A

A1 (Verified Design) • 151
abstraction • 311
level of • 126–33
access control • 45–93, 187–89, 323
decision facility • See ADF
enforcement facility • See AEF
granularity • 627
list • 63, 168
policy • 49–95, 49
access matrix • 178
access mode • 50, 52–64
accountability • 64, 142, 165, 177, 324
accreditation • 298–303, 347
accreditor • 348
accuracy • 326
ACL • See access control list
active attack • 357
ADF • 188–94
adjudication • 188
administration • 67
administrator • 165, 166
Advanced Secure DBMS • See ASD
advisory marking • 69
AEF • 188–89
American National Standards Institute • See ANSI
ANSI • 244–61, 260
architecture • 263
artifices • 33
ASD • 553–57, 580
assurance • 143–58, 145, 270, 306, 313, 327
balanced • 154
uniform • 154
assured pipelines • See LDV
asymmetric cryptosystem • See public key
atomicity • 536
attack
active • 357
authenticity • 357
integrity • 357
masquerade • 358
ordering • 358
passive • 357
scenario • 35
attribute • 188–92, 419
policy decision • 166–69
polyinstantiation • 495
propagation • 177
audit • 324, 585–95
policy • 65
record • 34, 49, 52, 120
requirements • 586
authentication • 65, 145–52, 288, 319
authenticity attack • 357
authority • 165, 177
availability • 42, 164, 177, 312, 401, 422

B

B1 (Labeled Security Protection) • 146
B2 (Structured Protection) • 147
B3 (Security Domains) • 149
balanced assurance • 154
Bell-LaPadula • 74, 173
Biba • 74
block
  cipher • 353
  encryption • 362
bridge • 394
bundling • 314
bus interface unit • See NIU
business activity • 426

C

C1 (Discretionary Security Protection) • 145
C2 (Controlled Access Protection) • 145
CA • 377, 417–21, 432
CAE • 244–47
Canadian Trusted Computer Product Evaluation Criteria • See CTCPEC
CBEMA • 261
CC • 243–62, 297–317
CCITT • See ITU-T
CEN • 257
CENELEC • 257
centralized authority • 177
certificate • 408–22
certificate-based key management • 377
certification • 300–304, 302, 339, 347
Certification Authority • See CA
certification body • 304
CESG • 304
checkfunction • 122, 323
cipher
  block • 353
  product • 353
  substitution • 353
ciphertext • 92, 351–83, 351. Compare plaintext
Clark-Wilson • 75, 180, 189–94
class • See evaluation class
clearance • 167
cleartext • See plaintext
CLEF • 300–304
CMW • 179
Comité European de Normalization • See CEN
Comité European de Normalization Electrotechnique • See CENELEC
commercial licensed evaluation facility • See CLEF
commercial off the shelf • See COTS
Common Application Environment • See CAE
Common Criteria • See CC
communication channel • 52
Communications Electronics Security Group • See CESG
Compartmented-Mode Workstation • See CMW
completeness • 51
component • 307
computable • 44
Computer and Business Equipment Manufacturers Association • See CBEMA
COMSEC • 402
Concept of Operations • See ConOps
concurrency control • 536
confidentiality • 43, 370, 406
perfect • 366
traffic flow • 402
connection-oriented abstraction • 89
connectivity • 101
ConOps • 333
consistency • 180
container • 178
content-correctness • 176
continuous protection • 143, 328
Corporation for Open Systems • See COS
correctness • 173, 176, 311
COS • 260
COTS • 298, 331
integration • 342
countermeasures • 120
cover story • 497
covered channel • 84, 117, 148, 328, 531
cryptography • 92, 350–84, 393
cryptoseal • See digital signature
CTCPEC • 244–62

D
DAC • See discretionary security policy
DAP • 302
data
exchange • 326
integrity • 42, 114, 312, 397, 435
management standards • 264
origin authentication • 406
replication • 450–52
structure • 175
terminal equipment • See DTE
Data Encryption Algorithm • See DEA
Data Encryption Standard • See DES
data-encrypting key • 381
DBMS
activity model • 588
aggregation problems • 582
data association problem • 584
inference
channels • 571
abductive • 579
deductive • 579
problems • 570–84
integrity • 617–34
multilevel relational • 460–91
object-oriented • 537, 595–617
prototypes • 542–69
relational • 462
DEA • 360
decipherment • See decryption
decomposition • 483–86
dedicated mode • 55
delete operation • 478–79
Department of Trade and Industry • See DTI
DES • 354–78, 360, 411–14
design • 337
deterministic • 178
deterrence • 109
development process • 331
device • 52, 176, 400
Diffie-Hellman • 368
digital signature • 93, 356–84, 373
disclosure • See unauthorized disclosure
discretionary security policy • 58, 63, 142–56, 179, 316
disruption • 17
distributed authority • 177
distributed DBMS • 450–52
domain • 52, 371
dominate • 60
DTE • 386–403
DTI • 304

E
ECMA • 244–60
EDI • 247–62, 424–38
EDIFACT • 430–38
electronic code book • 362
Electronic Data Interchange • See EDI. See EDI
ElGamal • 368
e-mail • 406–22
encipherment • See encryption
encryption • 351–84
block • 362
cipher block chaining • 363
cipher feedback • 365
ded-to-end • 383
initialization vector • 363
key auto-key • 365
one-time pad • 367
enforcement • 188
engineering, security • 330–49
enterprise • 99–105, 126–34
design analysis phase • See DAP
evaluation • 297–317
initial product assessment report • See IPAR
partition • 153
rating maintenance phase • See RAMP
subset • 154
target • See TOE
technical review board • See TRB
export • 90
external consistency • 180
equipment • 180–183
file encryption • 383
filter • 95
FIPS PUB 46-1 • 360
flaw • 120, 270, 287
Flaw Hypothesis Methodology • See FHM
floating label • 179
formal
description • 71
methods • 170–86, 181
model • 190–95
semantics • 182
top-level specification • See FTLS
FTLS • 77, 151, 174, 185
functionality • 306, 311
functionality class • 312

G
GCHQ • 304
Generalized Framework for Access Control • See GFAC
Generic Upper Layers Security • See GULS
GFAC • 187–89
global and persistent • 60
Government Communications Headquarters • See GCHQ
guard • 94
GULS • 252–67

H
hardware
flaw • 30
trap door • 34
hash function • 375
Hinke-Schafer • 439–44
human error • 20

I
I.P. Sharp • 440
IBAC • 316
identification • 65, 145–52, 194, 288, 318–25, 319
identity-based access control • See IBAC
IEC • 243–68
IETF • 245
import • 90
incremental evaluation • 154
indirect access • 68
individual accountability • 64, 142, 165
inference channel • 530
information
  assets • 332
  dissemination • 166
  hiding • 78
Information Technology Security Evaluation Criteria • See ITSEC
inheritance • 539
insert operation • 470–72
integration • 299, 330–49, 331, 342
integrity • 43, 157, 164, 312
  attack • 357
  authenticated users • 627
  Biba • 74
  Clark-Wilson • 75, 180, 189–94
  continuity of operation • 627
  data • 42, 114, 435
  DBMS • 530–41, 617–34
  ease of safe use • 633
  entity • 534
  implementation-dependent • 539
  key • 532, 573
  least privilege • 627
  message integrity code • See MIC
object • 537
polyinstantiation • 469, 506
program • 42, 120
reality checks • 633
reconstruction of events • 631–32
referential • 535
separation of duties • 629–31
source • 176
system • 42
  well-formed transaction • 624–27
integrity-lock • 440–55
interface • 280
internal controls • 121
internal requirement • 172
International Electrotechnical Commission • See IEC
International Organization for Standardization • See ISO
International Telecommunications Union • See ITU-T
Internet Engineering Task Force • See IETF
Internet Protocol • See IP
interpretation • 301
invisibile polyinstantiation • 498–99
IP • 245
IPAR • 302
ISO • 243–68
isolation • 51, 102–11, 145
ITSEC • 139–56, 244–62, 293, 297–317
ITU-T • 243–68

J
Joint Technical Committee 1 • See JTC1
JTC1 • 243–68

K
kernel • 53, 77, 141, 150
kernelized DBMS • 439–44
key • 352–83
  distribution center • 380
  integrity • 532
  management • 368–82
  public • 355–79
  symmetric • 355
  translation center • 380
  key-encrypting key • 381
  keying material • 354

L
label • 59, 167
  floating • 179
LAN • 385–404
lattice • 61
least privilege • 121, 627
legal remedies • 124
link encryption • 382
LOCK • 447
Lock Data Views • See LDV
logic bomb • 28

M

MAC • See mandatory security policy, message authentication code
malicious software • 18–37, 111–24
manager • 97–110
mandatory security policy • 58, 73, 141–55, 141, 178–79, 187
MAP/TOP • 245
marking • 142, 167
masquerade • 358
master key • 380
mathematical formalism • 183
mechanical proof checker • 182
mechanism • 32, 105, 313
message authentication code • 379, 411
message digest • 375
message integrity code • See MIC
message-stream modification • 357, 390
messaging • 427
MIC • 411–22
MIME • 406
mission • 333
misuse • 15–38
model
database activity • 588
formal • 170–86, 190–95
object-oriented • 598–603
rule-set • 192
security policy • 171
state-machine • 178, 192
multilevel • 55, 330–49
relational DBMS • 460–91

N

National Computer Security Center
  • See NCSC
NCSC • 300–317
NDI • 298
need-to-know • 167
network • 86, 89, 301
network interface unit • See NIU
network TCB partition • See NTCB
NIU • 388–404
nondevelopment item • See NDI
nonrepudiation • 374, 400, 406, 433
NTCB • 86

O

object
  integrity • 537
  reuse • 325
objectives • 163, 176
object-oriented
data model • 598–600
databases • 537
security model • 600–603
ODA • 244–61
Office Document Architecture • See ODA
OIW • 261
Open Software Foundation • See OSF
open systems • 243–68, 253
Open Systems Environment Implementors Workshop • See OIW
Open Systems Interconnection • See OSI
operating systems • 301
ordering attack • 358
OSF • 244
OSI • 244, 385–97
OSI management • 265
Index

P

partially ordered set • 61
partition evaluation • 153
passive attack • 357
password • 320
PCA • 418–22
PEM • 406–22
penetration • 28, 37, 81, 138
testing • 13–29, 269–95
perimeter • 109, 147–56
plaintext • 92, 351–83. Compare
ciphertext
policy certification authority • See
PCA
policy model • 71, 72, 171
polyinstantiation • 446, 494–99, 547
entity • 494
integrity • 469, 506
invisible • 498
problem
belief approach • 514–17
derived data approach • 511
derived values approach • 510
explicit alternatives approach •
524–27
insert-low approach • 517–20
prevention • 520–27
propagation approach • 505
visible • 496
porting • 345
prevention • 16, 109, 306
privacy enhanced mail • See PEM
probing • 22–28, 22, 81
product • 297–317, 298
product cipher • 353
program integrity • 42, 120
proof • 181
protection bit mask • 63
protection rings • 57
protocol • 395
pseudorandom bit stream • 366
public key • 355–79, 408–17

R

rainbow documents • 306
RAMP • 302
reciprocity • 315
recovery • 486–91
reference monitor • 48–95, 49, 140–56
referential integrity • 535
relation
multilevel • 465
relational DBMS • 462
reliability • 326
repudiation • 164
requirements • 330–49
interface • 172
rigor • 181
risk • 20, 143, 158, 371
analysis • 111
index • 307
role • 167
RSA • 368–77
rule-set model • 192

S

scenario • 335
SeaView • 444–49, 544–53
secure distributed data views • See
SeaView
security kernel • See kernel
security-enforcing • 319
segmentation • 57
selective routing • 402
self-protection • See isolation
sensitive information • 12
sensitivity label • 167
separately accredited • 346
separation • 393
of duties • 180, 629–31
service • 243–67, 307
signaling channel • 531
signature • See digital signature
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>simple mail-transfer protocol</td>
<td>74</td>
</tr>
<tr>
<td>simple security property</td>
<td>74</td>
</tr>
<tr>
<td>single trusted system</td>
<td>346</td>
</tr>
<tr>
<td>SMTP</td>
<td>409–12</td>
</tr>
<tr>
<td>software, malicious</td>
<td>111–24</td>
</tr>
<tr>
<td>SOGITS Report</td>
<td>424</td>
</tr>
<tr>
<td>source-integrity</td>
<td>176</td>
</tr>
<tr>
<td>sponsor</td>
<td>304</td>
</tr>
<tr>
<td>standards</td>
<td>242–68</td>
</tr>
<tr>
<td>star-property</td>
<td>178, 192</td>
</tr>
<tr>
<td>state invariant</td>
<td>182</td>
</tr>
<tr>
<td>state-machine model</td>
<td>178</td>
</tr>
<tr>
<td>state-transition</td>
<td>182</td>
</tr>
<tr>
<td>storage channel</td>
<td>178</td>
</tr>
<tr>
<td>storage container</td>
<td>178</td>
</tr>
<tr>
<td>strength of mechanism</td>
<td>306</td>
</tr>
<tr>
<td>subset evaluation</td>
<td>154</td>
</tr>
<tr>
<td>substitution cipher</td>
<td>353</td>
</tr>
<tr>
<td>subversion of security mechanism</td>
<td>19–39, 141–53</td>
</tr>
<tr>
<td>supporting policy</td>
<td>64</td>
</tr>
<tr>
<td>symmetric key</td>
<td>355</td>
</tr>
<tr>
<td>system</td>
<td>297–317, 299</td>
</tr>
<tr>
<td>high</td>
<td>55</td>
</tr>
<tr>
<td>integration</td>
<td>330–49</td>
</tr>
<tr>
<td>integrity</td>
<td>42, 114–24</td>
</tr>
<tr>
<td>state invariant</td>
<td>182</td>
</tr>
<tr>
<td>storage channel</td>
<td>178</td>
</tr>
<tr>
<td>storage container</td>
<td>178</td>
</tr>
<tr>
<td>strength of mechanism</td>
<td>306</td>
</tr>
<tr>
<td>subset evaluation</td>
<td>154</td>
</tr>
<tr>
<td>substitution cipher</td>
<td>353</td>
</tr>
<tr>
<td>subversion of security mechanism</td>
<td>19–39, 141–53</td>
</tr>
<tr>
<td>supporting policy</td>
<td>64</td>
</tr>
<tr>
<td>symmetric key</td>
<td>355</td>
</tr>
<tr>
<td>system</td>
<td>297–317, 299</td>
</tr>
<tr>
<td>high</td>
<td>55</td>
</tr>
<tr>
<td>integration</td>
<td>330–49</td>
</tr>
<tr>
<td>integrity</td>
<td>42, 114–24</td>
</tr>
</tbody>
</table>

**T**

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>target</td>
<td>304</td>
</tr>
<tr>
<td>target of evaluation</td>
<td>See TOE</td>
</tr>
<tr>
<td>TCB</td>
<td>71, 139–56, 172, 330–47</td>
</tr>
<tr>
<td>design</td>
<td>82</td>
</tr>
<tr>
<td>partition</td>
<td>80</td>
</tr>
<tr>
<td>subset</td>
<td>80, 154, 317</td>
</tr>
<tr>
<td>subset DBMS</td>
<td>441–57, 443</td>
</tr>
<tr>
<td>TCP</td>
<td>245</td>
</tr>
<tr>
<td>TCSEC</td>
<td>138–57, 297–317</td>
</tr>
<tr>
<td>TDI</td>
<td>154–55, 301–17, 542</td>
</tr>
<tr>
<td>technical security policy</td>
<td>56, 161</td>
</tr>
<tr>
<td>test plan</td>
<td>107, 272</td>
</tr>
<tr>
<td>theft</td>
<td>16</td>
</tr>
<tr>
<td>threat</td>
<td>20, 111–24, 270, 303, 306</td>
</tr>
<tr>
<td>Tiger team</td>
<td>See penetration testing</td>
</tr>
<tr>
<td>time bomb</td>
<td>28</td>
</tr>
<tr>
<td>timing channel</td>
<td>See covert channel</td>
</tr>
<tr>
<td>TLS</td>
<td>173</td>
</tr>
<tr>
<td>TNI</td>
<td>152–55, 301–14</td>
</tr>
<tr>
<td>TNIEG</td>
<td>306</td>
</tr>
<tr>
<td>TOE</td>
<td>297–315</td>
</tr>
<tr>
<td>top-level specification</td>
<td>See TLS, FTLS</td>
</tr>
<tr>
<td>trade-off</td>
<td>330</td>
</tr>
<tr>
<td>trading systems</td>
<td>424–38</td>
</tr>
<tr>
<td>traffic flow confidentiality</td>
<td>402</td>
</tr>
<tr>
<td>transaction atomicity</td>
<td>536</td>
</tr>
<tr>
<td>transaction processing</td>
<td>539</td>
</tr>
<tr>
<td>Transmission Control Protocol</td>
<td>See TCP</td>
</tr>
<tr>
<td>trap door</td>
<td>33, 118</td>
</tr>
<tr>
<td>TRB</td>
<td>302</td>
</tr>
<tr>
<td>triage</td>
<td>108</td>
</tr>
<tr>
<td>Trojan horse</td>
<td>25–37</td>
</tr>
<tr>
<td>trust requirements</td>
<td>332</td>
</tr>
<tr>
<td>trusted</td>
<td></td>
</tr>
<tr>
<td>computer system</td>
<td>327</td>
</tr>
<tr>
<td>computing base</td>
<td>See TCB</td>
</tr>
<tr>
<td>distribution</td>
<td>152, 328</td>
</tr>
<tr>
<td>path</td>
<td>67, 149</td>
</tr>
<tr>
<td>process</td>
<td>344</td>
</tr>
<tr>
<td>product</td>
<td>298</td>
</tr>
<tr>
<td>subject DBMS</td>
<td>441–59, 457</td>
</tr>
<tr>
<td>subjects</td>
<td>73</td>
</tr>
<tr>
<td>Trusted Computer System Evaluation Criteria</td>
<td>See TCSEC</td>
</tr>
<tr>
<td>Trusted Database Interpretation</td>
<td></td>
</tr>
<tr>
<td>See TDI</td>
<td></td>
</tr>
<tr>
<td>Trusted Network Interpretation</td>
<td></td>
</tr>
<tr>
<td>See TNI</td>
<td></td>
</tr>
<tr>
<td>type enforcement</td>
<td>57, 181, 447</td>
</tr>
</tbody>
</table>

**U**

<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>unauthorized disclosure</td>
<td>17, 114</td>
</tr>
<tr>
<td>unauthorized modification</td>
<td>18</td>
</tr>
</tbody>
</table>
unbundling • 315
unified system • 346
uniform assurance • 154
Unix • 187–91
update operations • 469–79
user abuse • 21
user agent • 407–15

V
VAP • 302
verification • 51, 82
virus • 27, 118
visible polyinstantiation • 496–97
vulnerability • 20–29, 121

W
wiretap • 390
working key • 380
worm • 28

X
X.400 • 244–61, 249, 428–38
X.435 • 430
X.500 • 249–63, 432–38
X.509 • 244–66, 416
X12 • 430–38
X9.17 • 379
X9.9 • 379