Index

A

access control 6, 7, 12, 14, 26, 27, 29, 30, 31, 32, 42, 43, 53
access control lists (ACL) 195
access control models 58, 60, 61, 62, 63, 64, 66, 73, 78, 82, 263
activity diagrams 8
ad-hoc 34
advanced encryption standard (AES) 159
agent systems 87, 98
aggregation function 93
ambient intelligence (AmI) 120, 121, 123
application audit 244
aspect-oriented security modeling 6
asymmetric binding assertion 140
asynchronous messages 154
attribute statement 197
authentication header (AH) 274, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 287, 289, 290, 292, 294
authentication statement 197
authorization statement 197
automated processing 118, 121
automated security verification 5

B

Basel II 34
BPEL 2, 16, 21, 22
business processes 1, 2, 7, 15, 16, 21, 22, 33, 34, 37, 38, 40, 41, 42, 43, 45, 46, 48
business process execution language (BPEL) 101, 112, 113, 115, 156, 157, 168
business process model 33
business workflow level 156

cardinality 70
certificate authority (CA) 88
choreography model 103, 111
class diagrams 8, 9
common object request broker architecture (CORBA) 154
countermeasure 101, 102, 103, 107, 114
control objectives for information and related technology (COBIT) 119
critical systems development using modeling languages (CSDUML) 5
cross-site scripting (XSS) 102

database management system (DBMS) 8, 263
data checking 66
data encryption 223, 243
dataflow attacks 102
data sharing 57, 58, 61, 62, 67, 69, 71, 79
data storage 243
data warehouses (DWs) 261
denial of service 138, 156
Index

deployment diagrams 8

design time policies 137
dictionary attacks 92
digital signatures 61, 96
discretionary access control (DAC) 60, 78
document type definition (DTD) 158
dual stack translation mechanism (DSTM) 274
dynamic composition 101
dynamic interaction 137
dynamic invocations 99

E
eavesdropping 102
encapsulating security payload (ESP) 274, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 294
enterprise model 37
environmentally conscious product (ECP) 5
Evaluation Processing Authority (EPA) 87, 89, 90, 91, 92, 93, 95
evaluation summary 88, 89, 90, 91, 92, 93, 95, 96
extensible access control markup language (XACML) 198, 199, 208, 209, 210, 226
external entity attacks 138

F
fair exchange 8, 9, 10
fault status 135
Federal Information Processing Standards (FIPS) 119, 121, 132, 172
Federal Information Security Management Act (FISMA) 119
federated enterprise resource planning (FERP) 85, 86, 94, 97
file transfer protocol (FTP) 274, 275, 276, 288, 289, 290, 291, 292, 293
fishing net application 103
forensic framework 99, 111, 112
forensic Web services (FWS) 99–117
functional meta-model 38, 39, 40, 41
functional system view 37

G
global functional meta-model 39
global reasoning 112
global unique identifier 111
Gramm-Leach-Bliley Act (GLBA) 119
granular policies 137
Grid systems 247, 248, 257, 259

H
Health Insurance Portability and Accountability Act (HIPAA) 119, 121
health@net 36, 39, 40, 48, 53
heterogeneity 58, 85
hierarchical composition 101
high order logic (HOL) 125
homebanking-computer-interface (HBCI) 10

I
identity-based cryptography (IBC) 197
i* framework 5
information integration 64
input validation 243
integration methods 84
integrity assertions 141
interaction diagrams 8, 31
Internet control message protocol (ICMP) 274, 275, 277, 278, 280, 281, 283, 284, 289
Internet protocol security (IPsec) 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294
Internet protocol version 4 (IPv4) 273, 274, 276, 278, 279, 280, 281, 282, 283, 284, 290, 291, 292, 293, 294
Internet protocol version 6 (IPv6) 273, 274, 276, 278, 281, 282, 283, 284, 288, 293, 294
interoperability 124, 135, 138, 145, 146, 149, 157, 163, 169, 170, 176
itinerary broker 192, 193

K
keeper of repositories 154
keeper of services 154
key differentiator 33
Index

L
leaf node 70, 71
level of abstraction 38
level of interaction 38
local reasoning 112

M
malicious data 102, 103, 104
malicious invocations 138, 144
malicious user 5
malware 250
mandatory access control (MAC) 60, 68, 73, 120
mapping function 71, 77
MASTER project 121, 132
MDA and MDS compliant approach 264
METype 105
message exchange patterns (MEP) 100
methodical approach 36
mobile computing 247, 249, 252, 255, 257, 260
mobile Grid 247, 248, 249, 250, 251, 252, 253, 255, 256, 257, 259, 260
MOBIUS project 121
model-based engineering 1
model construction 6
model driven architecture (MDA) 262
model driven security (MDS) 261, 262, 264
modularity 36, 52, 53
multidimensional (MD) model 261, 262
multidimensional modeling 262

N
National Institute of Standards and Technology (NIST) 119
natural language processing 68
networked information systems 247, 248
network nodes 83, 86
non-deterministic systems 13
non-repudiation 37, 249

O
object constraint language (OCL) 7, 12, 30, 263
object reuse 250
object security constraint language (OSCL) 263
ontologies 57, 58, 59, 62, 63, 64, 65, 66, 67, 69, 70, 77, 78, 79, 80
orchestration process model 111
Organization for the Advancement of Structured Information Standards (OASIS) 139, 142, 157, 159, 160, 164, 165, 166, 167, 168, 169, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186
oversized payloads 138

P
package diagrams 8
pair-wise evidence 105, 112
parameter tampering 102, 138, 144
peer-to-peer networks 83, 87, 97
penetrate and patch 3
policy access point (PAP) 198
policy administration point 144
policy alternatives 136
policy assertions 135, 136, 139, 143, 168
policy attachments 136
policy-based access control (PBAC) 196
policy decision point (PDP) 144, 198
policy enforcement point (PEP) 144, 198
policy information point (PIP) 144, 198
policy scope 136
policy subject 136, 143
principal spoofing 156
private key 11, 24
ProSecO 33–55
protection assertions 141
protection objects 63, 64, 73, 76
protocol assertions 142
public key 11

Q
quality of service (QoS) 86, 87, 88, 97
querying engine 76
QueryString 144, 145

R
recursive payloads 138
remote procedure call (RPC) 155, 164
Index

repeated invocations 138
replay attacks 138
reputation reports 87
request-response 100, 101, 105
resource description framework (RDF) 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82
resource protection 86
rewriting attacks 66
risk assessment 6, 50, 295
risk management 6, 7, 27, 37, 52, 55
role-based access control (RBAC) 60, 78, 120, 128, 167, 177, 195, 196, 199, 207
round-trip time (RTT) 275, 283, 284
routing detours 102, 138
run time policies 137, 146

S
Sarbanes-Oxley Act 34, 119, 121, 132
schema poisoning 138
schema tree 67, 70, 71, 72, 77
secure information flow 4, 6, 8
secure socket layer (SSL) 159, 160, 172
security analysis 4, 7, 14, 17, 28, 29, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 45, 46, 51, 52, 53, 54, 55
security, and access control Models for data warehouses 263
security and dependability (S&D) 118, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 161, 162
security assets 252, 254, 255
security binding assertion 140
security engineering 1, 3, 4, 7, 8, 14, 15, 26, 28, 29, 36, 52, 55
security extensions 86
security integration, into the design process 263
security mechanisms 118, 127, 131, 137, 140, 143, 145, 161
security model 37
security patterns 5, 6, 52, 53
security requirements modelling 5
security solutions 6, 34
SELP 105, 110, 112
semantic-aware authorization framework (SAAF) 57, 58, 59, 69, 77
semantic data 70
semantic data integration 70
semantic integration 62, 64, 70
SERENITY project 5, 6, 13, 118, 120, 121, 122, 123, 124, 125, 127, 128, 131, 132, 133, 185
SERENITY run-time framework (SRF) 123, 127, 128, 130
service broker 189
service consumers 84, 85, 87, 88, 89, 90, 94, 96
service evaluation protocol (SEP) 85, 88, 94, 95
service oriented architecture (SOA) 2, 15, 16, 17, 21, 22, 23, 26, 28, 29, 33, 34, 36, 38, 52, 54, 55, 57, 58, 59, 82, 83, 84, 85, 86, 87, 93, 94, 96, 99, 100, 116, 187, 188, 189, 193, 194, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 210, 213, 223, 226, 227, 228
service-oriented computing 119, 120
service oriented systems 33, 35, 36, 51, 53
service provider 188, 189, 193, 197
service requestor 189, 201
session key 11
shared electronic health record (SEHR) 37
single sign-off 195
single sign-on 138, 169, 195
smart cards 8, 195
snooping 250
SOAP message 190, 191, 203, 215, 216, 217, 219, 220, 221, 222, 224, 227
software architecture 37
solicit-response 100
statechart diagrams 8
statelessness 34
static composition 100, 101
sub element nodes 70, 71
symmetric binding assertion 141
synchronisation bars 9
system life-cycle 3

T

tiger teams 3
tightly integrated 3
token assertions 141
traceability 36, 39, 52, 53
transactional history 99
transport binding assertion 140
trivial file transfer protocol (TFTP) 274, 276, 292, 293
trusted third party (TTP) 105, 106, 110, 112
trust extensions 86
trust relationship 83
trustworthiness 3, 7, 13, 83, 84

U

UMLsec 1, 2, 4, 5, 6, 8, 9, 10, 11, 13, 14, 21, 22, 23, 26, 28, 31, 52
uniform resource identifier (URI) 138, 145, 163
universal description discovery and integration (UDDI) 59, 60, 66, 81, 102, 128, 135, 138, 139, 158, 159, 162, 165, 179, 191, 192, 207
use case diagrams 8

V

virtual organizations (VO) 247, 249
vulnerability analysis 1, 2, 25, 31

W

Web service choreography interface (WSCI) 156, 157, 177
Web service description language (WSDL) 2, 16, 59, 80, 95, 100, 101, 102, 127, 134, 135, 138, 139, 143, 158, 161, 164, 165, 168, 169, 170, 171, 173, 178, 179, 182, 184, 185, 190, 207, 225
Web services 295
Web service secure marketing language (WSSML) 95
Web services flow language (WSFL) 156, 161
Web services inspection language (WSIL) 192, 193, 205, 207
Web services workflow 156, 157
World Wide Web Consortium (W3C) 139, 156, 157, 159, 160, 163, 164, 165, 167, 168, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186
WSDL scanning 138

X

XACML 61, 65, 82
XML data 57, 58, 59, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 77, 80
XML encryption 61
XML morphing 138
XML security 58, 61, 63, 64, 78