

Index

A

access control lists (ACL) 200, 202, 204, 206
 access control models 17, 25, 26
 access control models, characterization and selection of 17
 access control systems 20
 AEGIS method 117
 affordances 260, 261, 262, 263, 269, 273, 275
 agents 262, 272, 273, 274, 275, 276
 Alloy Analyzer tool 156, 157, 158, 160, 162, 163, 165, 169, 172, 173, 183, 188
 Alloy system misuse model 160, 162
 analysis patterns 18
 analyze misuse model 162
 anonymity 215, 217, 230, 232, 233, 235, 243, 244, 245, 246, 247, 254, 257
 anonymity, receiver 217
 anonymity, sender 217
 application designers 77
 application programming interfaces (API) 286, 287, 288, 289, 290, 291, 295, 296, 297, 303
 architectural styles 33
 aspect-oriented modeling (AOM) 155, 156, 157, 163, 170, 185, 188
 aspect-oriented risk driven development (AORDD) 156, 157, 158, 159, 161, 162, 163, 164, 165, 166, 169, 170, 174, 180, 182, 183, 184, 185, 186, 187, 188
 attack trees 264
 authentication 215
 authorization 215, 243

B

Bayesian belief network (BBN) topology 156, 157, 162, 163, 164, 165, 168, 173, 180, 182, 183, 184, 185, 186, 187, 188, 190
 best-practice software development 1, 3, 8, 11, 12
 Binary Logic Diagrams 305, 306, 327
 business models 18
 business propositions 269, 270
 Byte Code Engineering Library (BCEL) 291, 303

C

capital assets 271
 card applets 286, 287, 288, 290, 292, 293, 295, 296, 302, 303
 card applets, faulty 286
 card applets, malicious 286
 card issuer 286
 Certified Information Security Specialist (CISSP) qualification 5
 Check Point 193
 Check Point GUI 193
 Cisco 193, 194, 195, 199, 201, 202, 204, 208, 209
 Cisco encryption technology (CET) 199, 200, 204, 206
 classic active server pages (CLASP) 117, 149
 commanded behaviour problem frame 34
 command line interface (CLI) 193, 194, 195, 197, 204, 205, 206, 208, 209
 commercial off the shelf (COTS) components 19, 21

Index

communicating sequential processes (CSP)
 language 33, 36, 38, 39, 55, 56, 57, 58,
 59, 60, 61, 62, 63, 70
complex trust relationships 286, 287
composite structure diagram 244
computer forensics 5
concretized security problem frames 32, 33,
 37, 38, 39, 42
consent 216, 217, 227, 232, 233, 235, 236,
 237, 238, 239, 240, 241, 243, 247, 248,
 249, 250, 254, 255, 257
constructive cost model (COCOMO) 8
control flow graphs (CFG) 289, 291, 293, 294,
 295, 296, 297, 298, 301
control systems 305, 306, 327, 328
critical systems 155, 156, 157, 186
cryptography 245, 246
CTL temporal logic 310
Cyber Security Knowledge Transfer Network
 2, 14

D

database authorization systems 20
databases 17, 19, 27
data controller 217
data encryption 246
data encryption standard (DES) 200, 202, 206
data owner 243, 244, 247, 248, 250
data processor 217
data protection 214, 215, 216, 224
data subject 216
dependencies 32, 33, 42, 46, 67
design fitness score 162
development cycle 155, 156
device configuration 192
Diffie-Hellman (DH) public key algorithm 200
digital signature standard (DSS) 200
direction-based filtering 193, 210,

E

echo request-reply (Ping) 194, 206
enhanced interior gateway routing protocol
 (EIGRP) 198, 199, 208, 209
enterprise knowledge development (EKD)
 framework 234
e-services 212, 214

extensible markup language (XML) 306

F

FindBugs open source framework 286, 287,
 289, 290, 291, 293, 294, 295, 296, 297,
 298, 300, 301, 302
firewall, application 20
firewall configuration 193
firewall, packet filter 20
firewall, proxy 20
firewalls 20, 192, 193, 202, 203, 204, 206, 207,
 210
firewalls, stateful proxy 20
firewall, stateful 20
firewalls, XML 20
formal methods 6, 8, 9
formal models 32
function block diagram (FBD) 307

G

generic security architectures 32, 33, 37, 38,
 39, 64, 65, 66, 67, 68, 70
generic security components 32, 33, 37, 39, 63,
 64, 65, 66, 68, 69, 70
graphical user interface (GUI) 192, 193, 194

I

identifiable person 216
identification 215
identity theft 212
IEC 61131-3 language 306
IEC 61131-3 standard 305, 306, 307, 327, 328
illicit method invocations 286, 287, 290
implementation Ladder programs 305
information display problem frame 34
information security 113, 150
informed consent 233, 247
informed consent acquisition 233, 243, 247
INSPECT language 193
internet control message protocol (ICMP) 194
Internet Service Providers (ISP) 213
ISA 5.2 Binary Logic Diagrams 305, 306, 307,
 310, 312, 316, 317, 326
iterative design-analyze cycle 162

J

Java Card framework 286, 287, 288, 289, 290, 291, 292, 293, 295, 296, 297, 298, 301, 302
 Java programming language 286, 287, 288, 289, 290, 291, 292, 293, 295, 296, 297, 298, 300, 301, 302, 303, 304
 judicial data 237

L

Ladder language 305, 306, 307, 308, 309, 310, 312, 317, 318, 323, 324, 325, 326, 327
 layered queuing network (LQN) models 156, 157, 160, 163, 174, 177, 178, 179, 188
 legacy systems 18
 loyalty applets 287, 292, 293, 294
 Lucent 193

M

misuse cases 264
 misuse patterns 17, 19, 23, 24, 25, 30
 model-driven architectures (MDA) 117, 123, 124, 133, 134, 136, 138, 142, 143, 151, 152, 153, 154
 model-driven development 155, 156
 model driven development approach 115, 122, 123, 124, 149, 154
 multi-router traffic grapher (MRTG) 194

N

non-volatile RAM (NVRAM) 200

O

object constraint language (OCL) 17, 19, 20
 object management group (OMG) 157, 175, 187, 190
 object-oriented design software methodology 18
 Open Web Application Security Project (OWASP) 5, 8, 13
 operating system access control systems 20
 operational security 7

P

pattern descriptions 20

pattern representation 76, 81, 84, 92, 93, 95, 96, 97, 100, 101, 103, 105, 108
 patterns 75, 76, 77, 78, 79, 80, 81, 83, 85, 89, 90, 91, 92, 94, 95, 96, 97, 98, 99, 100, 101, 104, 105, 107, 109, 111
 pattern systems 32, 33, 38, 39, 45, 46, 48, 49, 51, 53, 54, 72
 peer-to-peer (P2P) exchange 7
 performance by unified model analysis (PUMA) 157, 158, 160, 163, 165, 174, 177, 178, 179, 182, 183, 187, 188, 191
 personal data 214, 216, 217
 platform-specific security architecture 33, 39
 platform-specific security components 33
 privacy 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 243, 245, 246, 249, 250, 252, 257, 258
 privacy enhancing technologies (PETs) 234
 privacy policy enforcement 233
 privacy protection 212, 214
 privacy requirements in system design (PRIS) methodology 234
 problem frames 32, 33, 34, 35, 36, 37, 38, 39, 40, 42, 56, 70, 71, 72
 processing of personal data 217
 program analysis 286, 288, 289, 302
 programmable logic controllers (PLC) 306, 307, 308, 310, 311, 312, 315, 326, 327
 pseudonymity 215, 218, 233, 243

Q

quality analysis 156

R

reference monitor 20
 refinement 33, 36, 37, 38, 39, 47, 55, 58, 59, 62, 63, 68, 70, 72, 73
 relay ladder logic 307
 required behaviour problem frame 34
 requirements engineering phase 32, 70
 return on investment (ROI) 272
 role-based access control (RBAC) 19, 26, 76, 77, 79, 80, 81, 82, 83, 84, 85, 89, 90, 92, 94, 96, 98, 99, 100

round robin database tool (RRDTool) 194

S

scenarios 160, 165, 166, 175, 176, 178, 179, 180, 181

secure sockets layer (SSL) protocol 156, 170, 171, 172, 173, 174, 179, 180, 181, 182, 183, 191

secure software 1, 2, 3, 5, 6, 7, 8, 11, 12

secure software development methodology 17

secure software systems 16, 17, 29, 75, 76, 107, 114, 115, 119, 150, 264

secure software systems development 75, 107

Secure Tropos 265, 272, 283

SecureUML methodology 117, 124, 151

security 1, 2, 3, 5, 6, 7, 8, 9, 11, 12, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 147, 148, 149, 150, 151, 152, 153, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 276, 277, 279, 280, 281, 282, 283

security analysis 156, 157, 158, 159, 160, 161, 162, 163, 169, 174, 185, 186, 187

security analysis approaches 75, 79

security analysis approaches evaluation 75, 76, 77, 78, 79, 80, 83, 85, 86, 90, 97, 105, 106, 107, 108

security architectures 32, 33, 35, 39, 64, 65, 66, 67, 70

security attacks 1

security breaches 76

security engineering 32, 33, 36, 37, 38, 39, 70, 113, 114, 115, 116, 117, 119, 123, 125

security engineering process 32, 33, 36, 38, 70

security human computer interface (HCI-S) 193

security integration 113, 114

security kite-marks 4

security modeling approaches 75, 76

security models, goal-oriented 76, 80, 89, 92

security models, object-oriented design 76

security models, problem-oriented 76, 80, 101, 106, 107

security-oriented requirement engineering (SRE) 234

security pattern, consequences 77, 78

security pattern, context 77, 78

security pattern designers 77

security pattern, forces 77, 78

security pattern, problem 77

security patterns 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 35, 36, 37, 38, 39, 69, 70, 71, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 94, 95, 96, 97, 98, 99, 100, 101, 105, 106, 107, 108, 111

security patterns, modeling and classification of 17

security pattern, solution 77, 78

security problem frames 32, 33, 35, 37, 38, 39, 42

security problems 75, 76, 77, 78, 79, 85, 86, 94, 105, 107, 108, 109

security problems, patterns of 76, 77, 78, 79, 80, 85, 86, 88, 89, 94, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108

security requirements 32, 33, 35, 36, 37, 38, 39, 42, 46, 47, 48, 50, 51, 52, 55, 56, 57, 58, 63, 66, 67, 68, 70, 71, 72, 74

security requirements analysis 33, 116, 119, 129, 138

security requirements engineering 113, 118, 119, 120, 126, 129, 150, 151, 152

security requirements preservation 33

security solutions, patterns of 76, 77, 78, 79, 81, 82, 83, 85, 86, 88, 89, 94, 96, 99, 100, 101, 104, 106, 107

sensitive data 233, 236, 243, 244, 245, 246, 247, 254, 255, 256

sequential function chart (SFC) 307

simple workpieces problem frame 34

single method dispatch (SMD) 195, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209

single verification technique 287, 289

smart card applications 286

smart card interfaces 286

software development process, security integration in 115, 117, 126

software engineering 75, 77, 79, 101, 109, 110,
111, 113, 114, 115, 116, 117, 119, 120,
121, 123, 146, 147, 148, 149, 150, 151,
152, 153, 154, 212, 227, 230
Special Interest Group on Secure Software
Development (SSDSIG) 2, 3, 6, 14
state model diagrams (SMD) 194, 195, 199,
207, 208, 209
state of practice 1, 3, 12
state of the art 1, 10, 12
static program analysis 286, 302
structured text (ST) 307
system requirements 113, 114, 118, 119, 120,
125, 126, 128, 129, 130, 134, 135, 138,
139, 148, 149, 150, 151, 152, 153, 154
system requirements, functional 114, 115, 116,
118, 119, 120, 130, 142
system requirements, nonfunctional 114, 115,
142
systems development 113, 114, 119, 150, 154

T

technology adoption 260, 261, 262, 263, 275,
283
trade-off analysis 156, 157, 182, 186
trade-off decisions 155, 156, 157, 158, 159,
160, 162, 163, 164, 165, 166, 167, 173,
180, 181, 182, 183, 184, 185, 186, 187,
188
transactional web e-commerce benchmark
(TPC-W) 156, 191
transformation problem frame 34, 36, 58
Tropos 260, 265, 272, 282, 283
Tropos software development methodology
116, 117, 118, 126, 147, 148, 149, 152
trust 260, 262, 263, 264, 265, 266, 267, 268,
269, 270, 271, 272, 274, 275, 276, 277,
278, 279, 280, 281, 282, 283, 284

trust complements control 271
trust (credere) 267, 268, 271, 274
trust (externality) 267, 268, 271
trust (fides) 266, 268, 271, 274
trust governance 260, 262, 264, 265, 268, 269,
270, 271, 272, 276, 280
trust, mature approach to 272
trust methodology, designing for 260, 262,
267, 268, 269, 270, 271, 272, 280, 281
timestep tracking 287, 290, 294, 295, 302

U

UML2Alloy tool 156, 160, 172, 188, 191
UML security extension (UMLSec) 19
unified process 116, 127, 129, 134, 139, 151
unifying paradigm 262, 265, 269, 272, 273
universal modeling language (UML) 17, 19,
20, 23, 24, 25, 27, 29, 75, 76, 80, 81, 82,
83, 84, 85, 86, 107, 108, 109, 110, 117,
119, 120, 124, 131, 132, 133, 134, 138,
142, 147, 149, 150, 151, 153, 154, 157,
160, 163, 165, 169, 172, 175, 176, 177,
178, 179, 185, 187, 188, 189, 190, 191,
232, 233, 234, 236, 238, 239, 248, 257,
259
unlinkability 215, 218, 230
unobservability 215, 219, 230, 233, 243
Uppaal tool 305, 306, 308, 310
Uppaal-TRON testing tool 305, 306, 324
user trust 212, 213, 214

V

verification 250, 252
verification, ex-post 250, 252
verification, run-time 250, 252
visitor design pattern 291