# Index

## A

- abuse frames 112, 125
- Accelerated Requirements Method (ARM) 100
- Action-Effect Interface 297
- Actor-Method Utilization 79
- agile methodologies 1-3, 10, 12, 14
- agile software 1-5, 7, 13-14
- AMNESIA testbed 169, 171, 183
- asset protection model (APM) 289, 296-297, 307
- Assurance Optimization 16-17
- assurance (QA) 164

## B

- Bloom’s Taxonomy 328, 335-336
- Boehm garbage collector 197
- Broken Authentication 6
- Buffer overflow (BOF) 130, 132

## C

- Certification & Accreditation (C&A) 22
- Characterization 166, 248-252, 263, 265-267
- Chernoff Faces 277, 280
- Chief Security Officer (CSO) 329-330, 336
- Chunkinfo regions 200-201
- Collaborative Pedagogical Approach 328
- Common Weaknesses Enumeration (CWE) 27
- component architectures 111, 114
- compositional security contract (CsC) 251
- Configuration-Value Interface 297
- ConFu (CONfiguration FUzzing testing framework) 152
- continuity of operations plan (COOP) 100
- Continuous architecture evaluation 111
- Controlled Requirements Expression (CORE) 100
- Critical discourse analysis (CDA) 100
- Cross Site Scripting (XSS) 6
- Curriculum Architecture 313, 315, 319, 321-322
- cyber security 91, 104, 310-311, 313-315, 343

## D

- debugging memory allocators (Dlmalloc) 208
- degree of agility 3, 7
- DEMO Methodology 52, 57
- Designated Approval Authority (DAA) 22
- DieHard 148, 210, 212
- disallowed usage (DisU) 80
- DWARF structure 223
- Dynamic code optimizer extension 135, 137

## E

- Effect-Exposure Interface 297
- electronic services (e-services) 35
- ELF sections 221, 227
- Entailment Relation 108-109, 116, 118-119, 121, 239, 241
- European Parliamentary Technology Assessment (EPTA) 2
- Exception throwing 141
- Exposure-Action Interface 297
- extensible markup language (XML) 234

## F

- feature engineering 111, 127-128
- Feature-oriented domain analysis (FODA) 100, 106
- functional palaeontology 110
- Fuzzing Testing Framework 152

## G

- Generic System Model (GSM) 287
- Global Offset Table (GOT) 226
- Goal-Structuring Notation (GSN) 24
Index

graphical user interface (GUI) 257

H
HCI Security 269
Health Insurance Portability and Accountability Act (HIPAA) 37

I
impact of change 111
information encrypted (XOR) 209
Information Leakage 6, 44
information security 1, 15, 27-28, 30, 32, 41, 44, 102, 107, 188, 245, 267, 269-270, 279, 302, 305-306, 311, 314, 326, 328-330, 336-343
Injection Flaws 6, 169
Insecure Communications 7
Insecure Cryptographic Storage 6
Intention Grammar 171, 179-180
Intention Tree 179-181
intrusion detection systems (IDS) 5
Issue-based information systems (IBIS) 100

J
Jackson and Zave’s Entailment Relation 109, 116, 121
Java Virtual Machine (JVM) 182
Joint Application Development (JAD) 100
justifiable confidence 16, 26, 30

K
KAOS modelling 276
Katana 217, 219-227, 229-230

L
Library-based countermeasures (LibsafePlus) 211
Luxembourg Information Security Organisation (CLUSIL) 329

M
Macrobenchmarks 203-204
mandatory access control (MAC) 69-70, 73, 85
McCumber Cube 286, 290, 292
memory allocator 149, 190-193, 195, 198-199, 201, 206, 210, 212, 214, 216
Memory consumption 142-143, 147
memory managers 136, 140, 190-192, 198, 203
Method-Method Calling 79

N
National Cyber Security Division (NCSD) 313-314
National Institute of Standards and Technology (NIST) 22, 33, 90, 99
nonterminal symbol 179
Norm Analysis Method 52, 54, 57-60
Norm Analysis Method (NAM) 59
Norwegian Data Inspectorate 4

O
ontological transaction 57-59, 61, 65
Open Vulnerabilities and Assessment Language (OVAL) 28
Organizational Semiotics 52, 57, 59-60, 68

P
Pedagogical Model for Information Assurance 286-287, 298-299, 307, 310
Pedagogical Model for Information Assurance Curriculum Development (PMIACD) 298-299
personally identifiable information (PII) 37
Petri Net 57, 64-65, 67
privacy 37
privacy policy 37
process domain 66, 155
Program State Utilization 130-131, 133, 135, 137, 140, 147
Program-Type Interface 296
Protection-Configuration Interface 297

Q
Quality Function Deployment (QFD) 100

R
read security capability (RSC) 76
read security capability with a maximum value (RSC.max) 76
read security capability with a minimum value (RSC.min) 76
risk management 2, 22, 24, 34, 45, 49, 68, 105, 107, 318, 329, 340, 343
role-based access control (RBAC) 69-70, 73, 85, 112

S
Safe languages 210
Scrum approach 6
secure adaptive response potential (SARP) 292-293, 301, 304-305, 312
Secure Business Process Modeling (Secure BPM) 53-54, 65
secure code features 2
secure development lifecycle (SDLC) 11
Secure Sockets Layer (SSL) 41
secure software code development (SSCD) 299
secure software education system (SSES) 300-302, 306
Security Driven Business Process Modeling 54
Security Quality Requirements Engineering (SQUARE) 89, 91, 105, 126, 288
security-relevant objects 2
security-relevant subjects 2
SEGMEEXEC mode 143
service oriented architecture (SOA) 35, 244
Soft Systems Methodology (SSM) 100
Software assurance (SwA) 316
Software Engineering Body of Knowledge (SWE-BOK) 94, 326
Solaris 198
Specification-Program 296
SQL injection attacks (SQLIAs) 169-170
SQUARE-Lite 89-90, 95-98, 101-102, 105
State-of-the-Art Report (SOAR) 24
static object-roles mutual exclusion constraint (ME(SOR)) 80, 83
STRIDE method 12
StringBuffer 182
StringBuilder 182
Survivability and Information Assurance (SIA) 315

T
token type conformity 170, 176-178, 181, 187
toolchain 217-219, 226-227
Transport Layer Security (TLS) 41
Trustworthy Computing 14, 298
Type-Specification Interface 296

U
UML Security 26-27, 31, 33-34, 46, 49, 70, 75, 84-85, 87, 112, 124, 283
unified modeling language (UML) 69, 71
user privacy risk 37

V
Value-Protection Interface 297
verification and validation (V&V) 32
Viki Framework 26
Vocational Training 332

W
WASP 169, 174-175
World Wide Web Consortium (W3C) 234
write security capability with a maximum value (WSC.max) 76
write security capability with a minimum value (WSC.min) 76
write security capability (WSC) 76

X
XML - See extensible markup language.
XSS - See Cross Site Scripting.