

Index

A

- Access and flow control 25
- Access validation error 12
- Accounting 9, 10
- Accuracy 6, 22
- Adaptability of security protection 41, 44
- Admission control 14, 29, 33, 37, 53, 57
- Anomaly detection 31, 33, 273–297, 315, 324
- Artificial Neural Network (ANN) 31, 245, 257–271, 280, 283, 284, 313, 316, 318, 323
- Assessment 32, 33, 327
- Asset 1, 3, 4, 6, 22, 37, 41, 46
- Asset attribute 4, 8–11, 37, 41, 46, 48
- Asset protection 29, 33, 37, 39
- Asset risk framework 21, 29, 41
- Asset value 4
- Atomicity error 13
- Attack 3, 16, 31, 111, 112, 119–332
 - Apache Resource Denial of Service (DoS) 111, 123
 - Address Resolution Protocol (ARP) Poison 111
 - Backdoor 16, 17
 - Bot 17
 - Botnet 17
 - Brute force 16
 - Buffer overflow 16, 44, 113, 123
 - Bypassing 16, 17
 - Code attachment 16, 18
 - Covert channel 16, 17
 - Denial of Service (DoS) 16, 18, 89, 251
 - Eavesdropping 16, 19
 - Flooding 16
 - Fork bomb 113, 123
 - Hardware keylogger 113
 - Insider threat 3, 15, 16, 21
 - Keylogger 16, 20
 - Malware 16, 18
 - Man in the middle 16, 19
 - Masquerading 16
 - Mobile code 16, 18
 - NMAP 16, 20, 114
 - Probing 16, 20
 - Remote dictionary 16, 113, 123
 - RootKit 16, 17, 19, 113
 - Scanning 16, 20
 - Security audit 114
 - Sniffing 16, 19
 - Software keylogger 114
 - Spoofing 16, 20
 - Spyware 16
 - Steganography 16, 17
 - Tampering 16, 19
 - TCP reset attack 14
 - TCP SYN flood 19
 - Traceroute 16, 20
 - Trojan program 16, 17
 - Virus 16
 - Vulnerability scan 114, 123
 - Worm 16, 17
- Attack data 105, 106, 119–325
- Attack data characteristics 119–139, 141–173, 175–195, 197–243, 257–271, 260–262, 277, 299–311
- Attack data model 31, 32, 297–325
- Attack grouping 122, 128, 130–139, 141–173, 175–195, 197–243, 257–271

334 Index

- Attack identification 315
 Attack norm separation 32, 33, 284, 297, 313–325
 Attack profiling 32, 33, 327, 329–332
 Attack stage 21
 Authentication 27
 Authorization 27
 Autocorrelation function 175, 302, 303
 Autoregressive and moving average (ARMA) model 301–304
 Availability 6, 22
- B**
- Back-propagation learning algorithm 257–260
 Bandwidth 7
 Bandwidth reservation 55
 Batch Scheduled Admission Control (BSAC) 37, 53, 55–63, 86
 Batch size 57, 90
 Best effort service model 14, 53, 65, 68, 81, 89, 91
 Biometric key 28
 Boundary validation error 12
- C**
- Cause-effect chain of activity, state and performance 3, 5, 6, 22
 Cause-effect chain of a security incident 22, 31, 32, 37, 42, 45, 327, 331
 Chi-Square Distance Monitoring (CSDM) 275, 284–288
 Clustering
 Hierarchical 130, 161, 187, 224
 Supervised 31, 245, 247–256
 Clustering and Classification Algorithm – Supervised (CCAS) 247–255
 Completion time mean 60, 91
 Completion time variance 60, 91
 Confidentiality 6, 22
 Configuration 9, 10
 Configuration error 14
 Consistency of security protection 41
 Course Of Action (COA) 43, 45, 49
 Cuscore detection models 32, 263, 269, 280, 283, 284, 313–325
- D**
- Data 30, 41, 49, 105
 Activity data 30, 105
 Asset and asset attribute data 43, 325
 Auditing data 30
 Basic Security Module (BSM) audit data 251, 286, 293
 Host computer data 30
 Mixed attack and norm data 32, 245, 273, 284, 293, 295, 297, 313–325
 Network data 30
 Performance data 30, 105
 State data 30, 105
 System log data 30
 Data acquisition 48
 Data characteristic 31, 105, 119–262, 297, 299, 317, 318, 327, 329–331
 Autocorrelation change, 175–195, 260–262, 297, 299, 301
 Mean shift 119–139, 260–262, 297, 299, 300
 Probability distribution change, 148–173, 260–262, 297, 299, 300
 Wavelet change 197–243, 260–262, 297, 299, 304–309
 Data correlation 32, 42, 327, 329, 331
 Data feature 31, 105, 106
 Autocorrelation 31, 106, 175–195, 243, 297, 299, 301
 Mean 31, 106, 119–139, 297, 299, 300
 Probability distribution 31, 106, 141–173, 243, 297, 299, 300
 Bimodal distribution 142, 148
 Left skewed distribution 142, 148
 Multimodal distribution 142, 147
 Normal distribution 142, 148
 Right skewed distribution 142, 148
 Uniform distribution 142, 148
 Wavelet signal strength 31, 106, 197–273, 297, 299, 304–309
 Data mining 245, 247
 Data optimization 32, 327, 329, 330
 Data pattern 141
 Random fluctuation 141, 142
 Sine-cosine wave with noise 142
 Spike 141, 142
 Steady change 142
 Step change 142
 Data rate 7
 Daubechies wavelet 106, 197–243, 304–309
 Delay 7, 54, 91
 Denial of Service (DoS) attack 14
 Derivative of Gaussian (DoG) wavelet 106, 197–243, 304–309
 Design error 14
 Detection 1, 25, 29, 42, 45, 49, 245–325, 327
 Detection accuracy 252, 273, 288, 315, 324
 Detection earliness 263, 315, 324
 Detection efficiency 40

- Detrending 301
Differencing 301
Differentiated Service (DiffServ) 53, 65, 66, 68
Digital signature 25
DIP test 146, 147, 148
Distributed Denial of Service (DDoS) attack 3, 14, 112
Drop rate 68
- E**
End-to-end delay guarantee 29, 38, 56, 81, 82, 102
Error rate 7
Encryption 28
Environment error 13
Event 30, 31, 41, 43, 49, 105, 327
 Mismatch event of asset attribute 41, 43, 46, 48
Event transition 191–196
Exponentially Weighted Moving Average (EWMA) 252
Exponentially Weighted Moving Average (EWMA) control charts 263, 269, 275–284, 291, 313, 317, 318, 323
External threat 3, 15
- F**
False alarm 253, 263, 273, 276, 278–283, 287, 288, 293–295, 318–320, 323, 324
Feedback control 54
Firewall 26
First hit 263, 280–283, 318, 321–324
Frequency distribution of events 251, 284–288, 291
- G**
Gateway 27
Generality of security protection 41, 44
- H**
Haar wavelet 106, 197–243, 304–309
Hit rate 253, 287, 293–295
Hotelling's T^2 control chart 284–286
- I**
Incident 22, 30, 31, 32, 33, 42, 43, 49, 327
Indicator of vulnerability 41
Input validation error 13
Integer programming 329, 330
- Instantaneous job 56
Instantaneous Resource Reservation Protocol (I-RSVP) 37, 81, 82, 89, 91
Integrated Service (InteServ) 37, 53, 55, 81, 82
Integrity 6, 22
Internet Protocol (IP) 26
Intrusion Detection System (IDS) 31, 245, 315
- J**
Jitter 7
- L**
Lateness 68, 93
Loss rate 68
- M**
Mann-Whitney test 119–121
Markov chain model 31, 106, 273, 288, 291–296
MATLAB 201, 300
Metadata 9–11
Mismatches of asset attributes 41
Mode 141, 146
Mode test 146, 147, 148
Monitoring 29, 40, 42, 45, 49
Morlet wavelet 106, 197–243, 304–309
- N**
Network topology 91
Normal use data 105, 106, 119–325
Normal use data model 31, 32, 273–325
- O**
OPNET Modeler 66, 67, 71
Origin validation error 12
- P**
Paul wavelet 106, 197–243, 304–309
Performance measure 7
Performance requirement 7
 Audio broadcasting 7, 8
 Web browsing 7, 8
Physical threats 15
Precision 6, 22
Prevention 1, 25
Private key 28
Process performance 5, 22
Processing time 56
Protection 1, 25
Public key 28
Public key cryptographic algorithm 28

336 Index**Q**

Quality of Service (QoS) 37
 Quality of Service (QoS) Model 37, 53

R

Race condition error 13
 Receiver Operating Characteristic (ROC)
 252–256, 287, 293–295
 Repudiation 6, 22
 Reservation 29, 33, 55, 56, 81, 82
 Resource-process-user interaction 5, 22
 Resource Reservation Protocol (RSVP) 37, 55,
 81, 82
 Resource state 5, 22, 86
 Response 1, 32, 42
 Response time 7
 Risk Assessment 3, 22
 Risk value 4
 Rivest-Shamir-Adelman (RSA) algorithm 28
 Robustness of security protection 41, 44
 Router 26, 53, 56, 71, 72, 81, 83, 86

S

Scalability 55, 285
 Scale-free network 91
 Scheduling 14, 29, 33, 37, 65–80, 88
 Balanced Spiral (BS) 37, 70, 73
 Dynamic Balanced Spiral (DBS) 37, 78
 Dynamic Verified Spiral (DVS) 37, 78
 Earliest due date 65, 66
 First-In-First-Out (FIFO) 14, 37, 54, 65, 66, 68,
 71, 75, 79, 86, 89
 Longest Processing Time (LPT) 79
 Shortest Processing Time (SPT) 75, 77, 79
 Simplified Apparent Tardiness Cost (SATC)
 65, 66, 68
 Verified Spiral (VS) 37, 70, 73, 79
 Weighted Shortest Processing Time (WSPT)
 37, 65, 66, 68, 71
 Weighted Shortest Processing Time – Adjusted
 (WSPT-A) 37, 70, 71
 Secure design 29
 Security architecture 29, 33, 37, 39, 46
 Asset Protection Driven Security Architecture
 (APDSA) 46
 Threat-driven security architecture 39
 Security policy 37, 39, 43, 46, 66
 Security risk 1, 3, 37, 45

Serialization error 13
 Service differentiation 53, 65, 66
 Service priority 53, 73, 82
 Service stability 15, 29, 37, 53, 55, 65, 70,
 73, 78
 Signature recognition 30, 31, 33, 245–271, 297,
 316, 324
 Skewness 141, 146, 148
 SLAM 90, 92
 Stable Instantaneous Resource Reservation
 Protocol (SI-RSVP) 37, 81, 86, 89, 91
 Stationarity test 301
 Statistica 120, 121, 130, 176, 260
 Statistical data model 273–289
 Statistical Process Control (SPC) 275, 284
 Stochastic data model 291–296
 Synchronization error 13

T

Traffic condition 67, 69, 70, 72, 90
 Traffic control 55
 Traffic policing 55
 Traffic shaping 55
 Transmission Control Protocol (TCP) 26
 Threat 1, 3, 15, 22, 37
 Threat means 15
 Threat value 4
 Time series model 301
 Timeliness 6, 22
 Token bucket method 53, 54, 55

U

User activity 5

V

Vulnerability 1, 3, 11, 22, 37, 41
 Vulnerability value 4

W

Waiting time 56
 Waiting time mean (WTM) 56, 60, 76
 Waiting time variance (WTV) 56, 60, 70, 75, 76,
 79
 Waiting time variance minimization 74
 Web server model 66, 67
 Windows performance object 30, 31, 105, 106,
 108, 117, 119–139, 141–173, 175–195,
 197–243, 260, 275–284, 316, 325