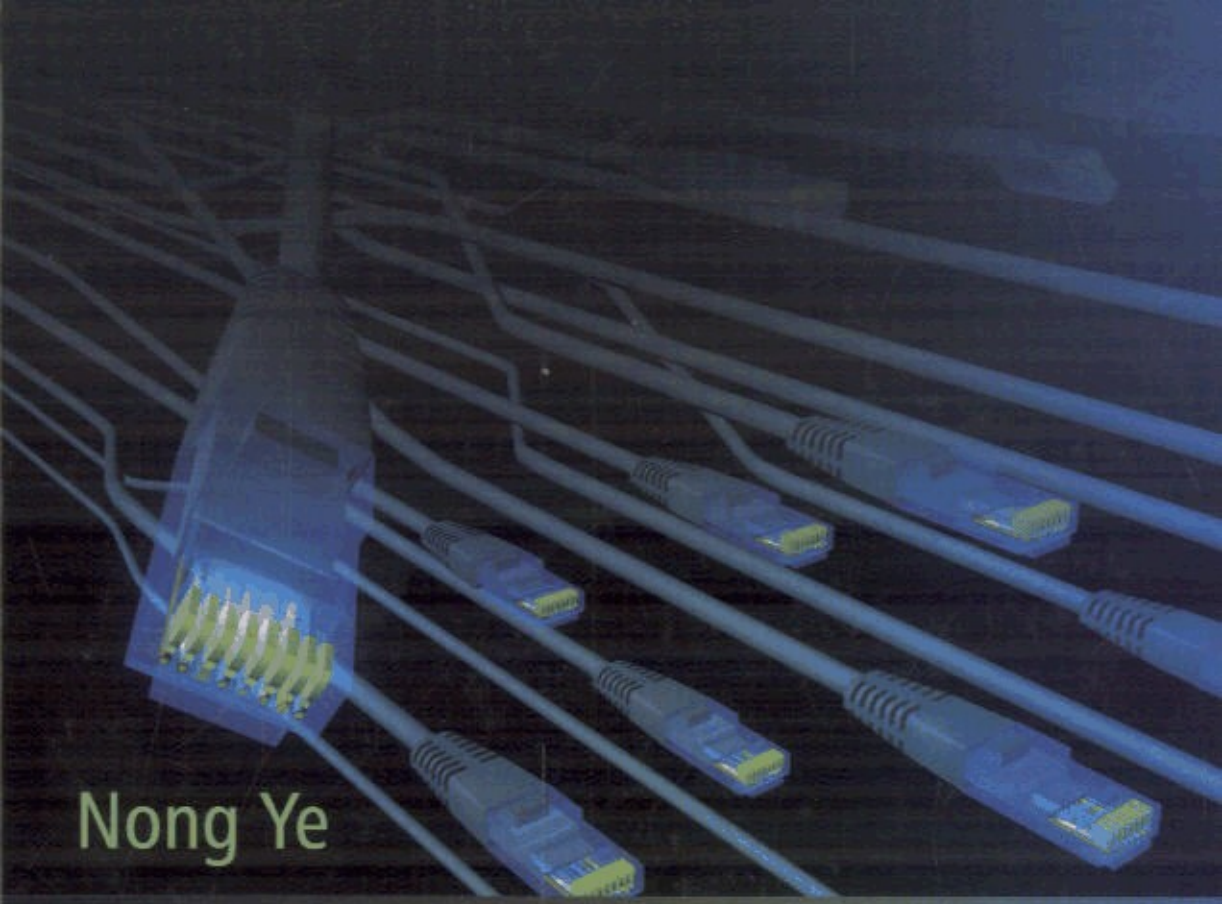

Nong Ye

Secure Computer and Network Systems

Modeling, Analysis and Design

WILEY

Contents

Preface xi

Part I An Overview of Computer and Network Security

1 Assets, vulnerabilities and threats of computer and network systems 3
1.1 Risk assessment 3
1.2 Assets and asset attributes 4
1.2.1 Resource, process and user assets and their interactions 5
1.2.2 Cause–effect chain of activity, state and performance 6
1.2.3 Asset attributes 8
1.3 Vulnerabilities 11
1.3.1 Boundary condition error 12
1.3.2 Access validation error and origin validation error 12
1.3.3 Input validation error 13
1.3.4 Failure to handle exceptional conditions 13
1.3.5 Synchronization errors 13
1.3.6 Environment error 13
1.3.7 Configuration error 14
1.3.8 Design error 14
1.3.9 Unknown error 15
1.4 Threats 15
1.4.1 Objective, origin, speed and means of threats 15
1.4.2 Attack stages 21
1.5 Asset risk framework 21
1.6 Summary 22
References 23

2 Protection of computer and network systems 25
2.1 Cyber attack prevention 25
2.1.1 Access and flow control 25
2.1.2 Secure computer and network design 29
2.2 Cyber attack detection 29
2.2.1 Data, events and incidents 30
2.2.2 Detection 31
2.2.3 Assessment 32

2.3 Cyber attack response 32
2.4 Summary 33
References 33

Part II Secure System Architecture and Design

3 Asset protection-driven, policy-based security protection architecture 39
3.1 Limitations of a threat-driven security protection paradigm 39
3.2 A new, asset protection-driven paradigm of security protection 40
3.2.1 Data to monitor: assets and asset attributes 41
3.2.2 Events to detect: mismatches of asset attributes 41
3.2.3 Incidents to analyze and respond: cause–effect chains of mismatch events 42
3.2.4 Proactive asset protection against vulnerabilities 42
3.3 Digital security policies and policy-based security protection 43
3.3.1 Digital security policies 43
3.3.2 Policy-based security protection 45
3.4 Enabling architecture and methodology 46
3.4.1 An Asset Protection Driven Security Architecture (APDSA) 46
3.4.2 An Inside-Out and Outside-In (IOOI) methodology of gaining knowledge about data, events and incidents 47
3.5 Further research issues 48
3.5.1 Technologies of asset attribute data acquisition 48
3.5.2 Quantitative measures of asset attribute data and mismatch events 48
3.5.3 Technologies for automated monitoring, detection, analysis and control of data, events, incidents and COA 49
3.6 Summary 49
References 50

4 Job admission control for service stability 53
4.1 A token bucket method of admission control in DiffServ and InteServ models 53
4.2 Batch Scheduled Admission Control (BSAC) for service stability 55
4.2.1 Service stability in service reservation for instantaneous jobs 56
4.2.2 Description of BSAC 57
4.2.3 Performance advantage of the BSAC router model over a regular router model 60
4.3 Summary 64
References 64

5 Job scheduling methods for service differentiation and service stability 65
5.1 Job scheduling methods for service differentiation 65
5.1.1 Weighted Shortest Processing Time (WSPT), Earliest Due Date (EDD) and Simplified Apparent Tardiness Cost (SATC) 65
5.1.2 Comparison of WSPT, ATC and EDD with FIFO in the best effort model and in the DiffServ model in service differentiation 66
5.2 Job scheduling methods for service stability 70
5.2.1 Weighted Shortest Processing Time – Adjusted (WSPT-A) and its performance in service stability 70

5.2.2 Verified Spiral (VS) and Balanced Spiral (BS) methods for a single service resource and their performance in service stability 73
5.2.3 Dynamics Verified Spiral (DVS) and Dynamic Balanced Spiral (DBS) methods for parallel identical resources and their performance in service stability 78
5.3 Summary 79
References 79

6 Job reservation and service protocols for end-to-end delay guarantee 81
6.1 Job reservation and service in InteServ and RSVP 81
6.2 Job reservation and service in I-RSVP 82
6.3 Job reservation and service in SI-RSVP 86
6.4 Service performance of I-RSVP and SI-RSVP in comparison with the best effort model 89
6.4.1 The simulation of a small-scale computer network with I-RSVP, SI-RSVP and the best effort model 89
6.4.2 The simulation of a large-scale computer network with I-RSVP, SI-RSVP and the best effort model 91
6.4.3 Service performance of I-RSVP, SI-RSVP and the best effort model 93
6.5 Summary 102
References 103

Part III Mathematical/Statistical Features and Characteristics of Attack and Normal Use Data

7 Collection of Windows performance objects data under attack and normal use conditions 107
7.1 Windows performance objects data 107
7.2 Description of attacks and normal use activities 111
7.2.1 Apache Resource DoS 111
7.2.2 ARP Poison 111
7.2.3 Distributed DoS 112
7.2.4 Fork Bomb 113
7.2.5 FTP Buffer Overflow 113
7.2.6 Hardware Keylogger 113
7.2.7 Remote Dictionary 113
7.2.8 Rootkit 113
7.2.9 Security Audit 114
7.2.10 Software Keylogger 114
7.2.11 Vulnerability Scan 114
7.2.12 Text Editing 114
7.2.13 Web Browsing 114
7.3 Computer network setup for data collection 115
7.4 Procedure of data collection 115
7.5 Summary 118
References 118

8 Mean shift characteristics of attack and normal use data **119**
8.1 The mean feature of data and two-sample test of mean difference 119
8.2 Data pre-processing 121
8.3 Discovering mean shift data characteristics for attacks 121
8.4 Mean shift attack characteristics 122
8.4.1 Examples of mean shift attack characteristics 122
8.4.2 Mean shift attack characteristics by attacks and windows performance objects 124
8.4.3 Attack groupings based on the same and opposite attack characteristics 128
8.4.4 Unique attack characteristics 136
8.5 Summary 139
References 139

9 Probability distribution change characteristics of attack and normal use data **141**
9.1 Observation of data patterns 141
9.2 Skewness and mode tests to identify five types of probability distributions 146
9.3 Procedure for discovering probability distribution change data characteristics for attacks 148
9.4 Distribution change attack characteristics 150
9.4.1 Percentages of the probability distributions under the attack and normal use conditions 150
9.4.2 Examples of distribution change attack characteristics 151
9.4.3 Distribution change attack characteristics by attacks and Windows performance objects 151
9.4.4 Attack groupings based on the same and opposite attack characteristics 161
9.4.5 Unique attack characteristics 167
9.5 Summary 173
References 174

10 Autocorrelation change characteristics of attack and normal use data **175**
10.1 The autocorrelation feature of data 175
10.2 Discovering the autocorrelation change characteristics for attacks 176
10.3 Autocorrelation change attack characteristics 178
10.3.1 Percentages of variables with three autocorrelation levels under the attack and normal use conditions 178
10.3.2 Examples of autocorrelation change attack characteristics 179
10.3.3 Autocorrelation change attack characteristics by attacks and Windows performance objects 182
10.3.4 Attack groupings based on the same and opposite attack characteristics 182
10.3.5 Unique attack characteristics 193
10.4 Summary 193
References 196

11 Wavelet change characteristics of attack and normal use data **197**
11.1 The wavelet feature of data 197
11.2 Discovering the wavelet change characteristics for attacks 201

11.3 Wave change attack characteristics 203
11.3.1 Examples of wavelet change attack characteristics 203
11.3.2 Wavelet change attack characteristics by attacks and Windows performance objects 204
11.3.3 Attack groupings based on the same and opposite attack characteristics 222
11.3.4 Unique attack characteristics 225
11.4 Summary 243
References 243

Part IV Cyber Attack Detection: Signature Recognition

12 Clustering and classifying attack and normal use data 247
12.1 Clustering and Classification Algorithm – Supervised (CCAS) 248
12.2 Training and testing data 251
12.3 Application of CCAS to cyber attack detection 251
12.4 Detection performance of CCAS 253
12.5 Summary 256
References 256

13 Learning and recognizing attack signatures using artificial neural networks 257
13.1 The structure and back-propagation learning algorithm of feedforward ANNs 257
13.2 The ANN application to cyber attack detection 260
13.3 summary 270
References 271

Part V Cyber Attack Detection: Anomaly Detection

14 Statistical anomaly detection with univariate and multivariate data 275
14.1 EWMA control charts 275
14.2 Application of the EWMA control chart to cyber attack detection 277
14.3 Chi-Square Distance Monitoring (CSDM) method 284
14.4 Application of the CSDM method to cyber attack detection 286
14.5 Summary 288
References 288

15 Stochastic anomaly detection using the Markov chain model of event transitions 291
15.1 The Markov chain model of event transitions for cyber attack detection 291
15.2 Detection performance of the Markov chain model-based anomaly detection technique and performance degradation with the increased mixture of attack and normal use data 293
15.3 Summary 295
References 296

Part VI Cyber Attack Detection: Attack Norm Separation

16 Mathematical and statistical models of attack data and normal use data 299
16.1 The training data for data modeling 299
16.2 Statistical data models for the mean feature 300
16.3 Statistical data models for the distribution feature 300
16.4 Time-series based statistical data models for the autocorrelation feature 301
16.5 The wavelet-based mathematical model for the wavelet feature 304
16.6 Summary 309
References 312

17 Cuscore-based attack norm separation models 313
17.1 The cuscore 313
17.2 Application of the cuscore models to cyber attack detection 314
17.3 Detection performance of the cuscore detection models 316
17.4 Summary 323
References 325

Part VII Security Incident Assessment

18 Optimal selection and correlation of attack data characteristics in attack profiles 329
18.1 Integer programming to select an optimal set of attack data characteristics 329
18.2 Attack profiling 330
18.3 Summary 332
References 332

Index 333