Contents

List of Contributors xvii
Foreword xxiii
Preface xxv
Acknowledgments xxix

1 Overview of Security and Privacy in Cyber-Physical Systems 1
Glenn A. Fink, Thomas W. Edgar, Theora R. Rice, Douglas G. MacDonald and Cary E. Crawford
1.1 Introduction 1
1.2 Defining Security and Privacy 1
1.2.1 Cybersecurity and Privacy 2
1.2.2 Physical Security and Privacy 3
1.3 Defining Cyber-Physical Systems 4
1.3.1 Infrastructural CPSs 5
1.3.1.1 Example: Electric Power 5
1.3.2 Personal CPSs 5
1.3.2.1 Example: Smart Appliances 6
1.3.3 Security and Privacy in CPSs 6
1.4 Examples of Security and Privacy in Action 7
1.4.1 Security in Cyber-Physical Systems 7
1.4.1.1 Protecting Critical Infrastructure from Blended Threat 8
1.4.1.2 Cyber-Physical Terrorism 8
1.4.1.3 Smart Car Hacking 9
1.4.1.4 Port Attack 10
1.4.2 Privacy in Cyber-Physical Systems 11
1.4.2.1 Wearables 11
1.4.2.2 Appliances 12
1.4.2.3 Motivating Sharing 12
1.4.3 Blending Information and Physical Security and Privacy 12
1.5 Approaches to Secure Cyber-Physical Systems 14
1.5.1 Least Privilege 14
1.5.2 Need-to-Know 15
1.5.3 Segmentation 15
1.5.4 Defensive Dimensionality 16
Contents

1.5.4.1 Defense-in-Depth 16
1.5.4.2 Defense-in-Breadth 16
1.5.5 User-Configurable Data Collection/Logging 17
1.5.6 Pattern Obfuscation 17
1.5.7 End-to-End Security 17
1.5.8 Tamper Detection/Security 18
1.6 Ongoing Security and Privacy Challenges for CPSs 18
1.6.1 Complexity of Privacy Regulations 18
1.6.2 Managing and Incorporating Legacy Systems 19
1.6.3 Distributed Identity and Authentication Management 20
1.6.4 Modeling Distributed CPSs 20
1.7 Conclusion 21
References 21

2 Network Security and Privacy for Cyber-Physical Systems 25
Martin Henze, Jens Hiller, René Hummen, Roman Matzutt, Klaus Wehrle and Jan H. Ziegeldorf
2.1 Introduction 25
2.2 Security and Privacy Issues in CPSs 26
2.2.1 CPS Reference Model 27
2.2.1.1 Device Level 27
2.2.1.2 Control/Enterprise Level 27
2.2.1.3 Cloud Level 28
2.2.2 CPS Evolution 28
2.2.3 Security and Privacy Threats in CPSs 30
2.3 Local Network Security for CPSs 31
2.3.1 Secure Device Bootstrapping 32
2.3.1.1 Initial Key Exchange 33
2.3.1.2 Device Life Cycle 33
2.3.2 Secure Local Communication 34
2.3.2.1 Physical Layer 34
2.3.2.2 Medium Access 34
2.3.2.3 Network Layer 35
2.3.2.4 Secure Local Forwarding for Internet-Connected CPSs 35
2.4 Internet-Wide Secure Communication 36
2.4.1 Security Challenges for Internet-Connected CPS 37
2.4.2 Tailoring End-to-End Security to CPS 38
2.4.3 Handling Resource Heterogeneity 39
2.4.3.1 Reasonable Retransmission Mechanisms 39
2.4.3.2 Denial-of-Service Protection 40
2.5 Security and Privacy for Cloud-Interconnected CPSs 41
2.5.1 Securely Storing CPS Data in the Cloud 42
2.5.1.1 Protection of CPS Data 43
2.5.1.2 Access Control 43
2.5.2 Securely Processing CPS Data in the Cloud 44
2.5.3 Privacy for Cloud-Based CPSs 45
3 Tutorial on Information Theoretic Metrics Quantifying Privacy in Cyber-Physical Systems 57
Guido Dartmann, Mehmet Ö. Demir, Hendrik Laux, Volker Lücken, Naim Bajcinca, Gunes K. Kurt, Gerd Ascheid and Martina Ziefle
3.1 Social Perspective and Motivation 57
3.1.1 Motivation 59
3.1.2 Scenario 60
3.2 Information Theoretic Privacy Measures 62
3.2.1 Information Theoretic Foundations 62
3.2.2 Surprise and Specific Information 63
3.3 Privacy Models and Protection 64
3.3.1 $k$-Anonymity 65
3.4 Smart City Scenario: System Perspective 67
3.4.1 Attack without Anonymization 68
3.4.2 Attack with Anonymization of the ZIP 70
3.4.3 Attack with Anonymization of the Bluetooth ID 71
3.5 Conclusion and Outlook 71
Appendix A Derivation of the Mutual Information Based on the KLD 72
Appendix B Derivation of the Mutual Information In Terms of Entropy 73
Appendix C Derivation of the Mutual Information Conditioned on $x$ 73
Appendix D Proof of Corollary 3.1 74
References 74

4 Cyber-Physical Systems and National Security Concerns 77
Jeff Kosseff
4.1 Introduction 77
4.2 National Security Concerns Arising from Cyber-Physical Systems 79
4.2.1 Stuxnet 80
4.2.2 German Steel Mill 81
4.2.3 Future Attacks 82
4.3 National Security Implications of Attacks on Cyber-Physical Systems 82
4.3.1 Was the Cyber-Attack a “Use of Force” That Violates International Law? 83
4.3.2 If the Attack Was a Use of Force, Was That Force Attributable to a State? 86
4.3.3 Did the Use of Force Constitute an “Armed Attack” That Entitles the Target to Self-Defense? 87
4.3.4 If the Use of Force Was an Armed Attack, What Types of Self-Defense Are Justified? 88
4.4 Conclusion 89
References 90
5  Legal Considerations of Cyber-Physical Systems and the Internet of Things  93
   Alan C. Rither and Christopher M. Hoxie
   5.1 Introduction  93
   5.2 Privacy and Technology in Recent History  94
   5.3 The Current State of Privacy Law  96
      5.3.1 Privacy  98
      5.3.2 Legal Background  98
      5.3.3 Safety  99
      5.3.4 Regulatory  100
      5.3.4.1 Executive Branch Agencies  101
      5.3.4.2 The Federal Trade Commission  101
      5.3.4.3 The Federal Communications Commission  105
      5.3.4.4 National Highway and Traffic Safety Administration  106
      5.3.4.5 Food and Drug Administration  108
      5.3.4.6 Federal Aviation Administration  109
   5.4 Meeting Future Challenges  111
   References  113

6  Key Management in CPSs  117
   Yong Wang and Jason Nikolai
   6.1 Introduction  117
   6.2 Key Management Security Goals and Threat Model  117
      6.2.1 CPS Architecture  118
      6.2.2 Threats and Attacks  119
      6.2.3 Security Goals  120
   6.3 CPS Key Management Design Principles  121
      6.3.1 Heterogeneity  122
      6.3.2 Real-Time Availability  122
      6.3.3 Resilience to Attacks  123
      6.3.4 Interoperability  123
      6.3.5 Survivability  123
   6.4 CPS Key Management  124
      6.4.1 Dynamic versus Static  124
      6.4.2 Public Key versus Symmetric Key  125
         6.4.2.1 Public Key Cryptography  125
         6.4.2.2 Symmetric Key Cryptography  127
      6.4.3 Centralized versus Distributed  128
      6.4.4 Deterministic versus Probabilistic  129
      6.4.5 Standard versus Proprietary  130
      6.4.6 Key Distribution versus Key Revocation  131
      6.4.7 Key Management for SCADA Systems  131
   6.5 CPS Key Management Challenges and Open Research Issues  132
   6.6 Summary  133
   References  133
7 Secure Registration and Remote Attestation of IoT Devices Joining the Cloud: The Stack4Things Case of Study  
Antonio Celesti, Maria Fazio, Francesco Longo, Giovanni Merlino and Antonio Puliafito

7.1 Introduction 137
7.2 Background 138
7.2.1 Cloud Integration with IoT 139
7.2.2 Security and Privacy in Cloud and IoT 139
7.2.3 Technologies 140
7.2.3.1 Hardware 140
7.2.3.2 Web Connectivity 141
7.2.3.3 Cloud 141
7.3 Reference Scenario and Motivation 142
7.4 Stack4Things Architecture 143
7.4.1 Board Side 144
7.4.2 Cloud-Side – Control and Actuation 145
7.4.3 Cloud-Side – Sensing Data Collection 146
7.5 Capabilities for Making IoT Devices Secure Over the Cloud 147
7.5.1 Trusted Computing 147
7.5.2 Security Keys, Cryptographic Algorithms, and Hidden IDs 148
7.5.3 Arduino YUN Security Extensions 149
7.6 Adding Security Capabilities to Stack4Things 149
7.6.1 Board-Side Security Extension 149
7.6.2 Cloud-Side Security Extension 150
7.6.3 Security Services in Stack4Things 150
7.6.3.1 Secure Registration of IoT Devices Joining the Cloud 151
7.6.3.2 Remote Attestation of IoT Devices 152
7.7 Conclusion 152
References 153

8 Context Awareness for Adaptive Access Control Management in IoT Environments 157
Paolo Bellavista and Rebecca Montanari

8.1 Introduction 157
8.2 Security Challenges in IoT Environments 158
8.2.1 Heterogeneity and Resource Constraints 158
8.2.2 IoT Size and Dynamicity 160
8.3 Surveying Access Control Models and Solutions for IoT 160
8.3.1 Novel Access Control Requirements 160
8.3.2 Access Control Models for the IoT 162
8.3.3 State-of-the-Art Access Control Solutions 164
8.4 Access Control Adaptation: Motivations and Design Guidelines 165
8.4.1 Semantic Context-Aware Policies for Access Control Adaptation 166
8.4.2 Adaptation Enforcement Issues 167
8.5 Our Adaptive Context-Aware Access Control Solution for Smart Objects 168
8.5.1 The Proteus Model 168
8.5.2 Adapting the General Proteus Model for the IoT 170
8.5.2.1 The Proteus Architecture for the IoT 172
8.5.2.2 Implementation and Deployment Issues 173
8.6 Open Technical Challenges and Concluding Remarks 174
References 176

9 Data Privacy Issues in Distributed Security Monitoring Systems 179
Jeffery A. Mauth and David W. Archer
9.1 Information Security in Distributed Data Collection Systems 179
9.2 Technical Approaches for Assuring Information Security 181
9.2.1 Trading Security for Cost 182
9.2.2 Confidentiality: Keeping Data Private 182
9.2.3 Integrity: Preventing Data Tampering and Repudiation 186
9.2.4 Minimality: Reducing Data Attack Surfaces 188
9.2.5 Anonymity: Separating Owner from Data 188
9.2.6 Authentication: Verifying User Privileges for Access to Data 189
9.3 Approaches for Building Trust in Data Collection Systems 190
9.3.1 Transparency 190
9.3.2 Data Ownership and Usage Policies 191
9.3.3 Data Security Controls 191
9.3.4 Data Retention and Destruction Policies 192
9.3.5 Managing Data-loss Liability 192
9.3.6 Privacy Policies and Consent 192
9.4 Conclusion 193
References 193

10 Privacy Protection for Cloud-Based Robotic Networks 195
Hajoon Ko, Sye L. Keoh and Jiong Jin
10.1 Introduction 195
10.2 Cloud Robot Network: Use Case, Challenges, and Security Requirements 197
10.2.1 Use Case 197
10.2.2 Security Threats and Challenges 199
10.2.3 Security Requirements 200
10.3 Establishment of Cloud Robot Networks 200
10.3.1 Cloud Robot Network as a Community 200
10.3.2 A Policy-Based Establishment of Cloud Robot Networks 201
10.3.3 Doctrine: A Community Specification 201
10.3.3.1 Attribute Types and User-Attribute Assignment (UAA) Policies 203
10.3.3.2 Authorization and Obligation Policies 203
10.3.3.3 Constraints Specification 205
10.3.3.4 Trusted Key Specification 206
10.3.3.5 Preferences Specification 206
10.3.3.6 Authentication in Cloud Robot Community 207
10.3.3.7 Service Access Control 207
10.4 Communication Security 207
Contents

10.4.1 Attribute-Based Encryption (ABE) 207
10.4.2 Preliminaries 208
10.4.3 Ciphertext-Policy Attribute-Based Encryption (CP-ABE) Scheme 208
10.4.4 Revocation Based on Shamir's Secret Sharing 209
10.4.5 Cloud Robot Community's CP-ABE Key Revocation 209
10.4.6 Integration of CP-ABE and Robot Community Architecture 210
10.5 Security Management of Cloud Robot Networks 212
10.5.1 Bootstrapping (Establishing) a Cloud Robot Community 212
10.5.2 Joining the Community 214
10.5.3 Leaving a Community 215
10.5.4 Service Access Control 216
10.6 Related Work 217
10.7 Conclusion 219

References 220

11 Toward Network Coding for Cyber-Physical Systems: Security Challenges and Applications 223

Pouya Ostovari and Jie Wu

11.1 Introduction 223
11.2 Background on Network Coding and Its Applications 225
11.2.1 Background and Preliminaries 225
11.2.2 Network Coding Applications 226
11.2.2.1 Throughput/Capacity Enhancement 226
11.2.2.2 Robustness Enhancement 227
11.2.2.3 Protocol Simplification 228
11.2.2.4 Network Tomography 228
11.2.2.5 Security 229
11.2.3 Network Coding Classification 229
11.2.3.1 Stateless Network Coding Protocols 229
11.2.3.2 State-Aware Network Coding Protocols 229
11.3 Security Challenges 230
11.3.1 Byzantine Attack 230
11.3.2 Pollution Attack 230
11.3.3 Traffic Analysis 230
11.3.4 Eavesdropping Attack 231
11.3.5 Classification of the Attacks 232
11.3.5.1 Passive versus Active 232
11.3.5.2 External versus Internal 232
11.3.5.3 Effect of Network Coding 232
11.4 Secure Network Coding 233
11.4.1 Defense against Byzantine and Pollution Attack 233
11.4.2 Defense against Traffic Analysis 234
11.5 Applications of Network Coding in Providing Security 234
11.5.1 Eavesdropping Attack 234
11.5.1.1 Secure Data Transmission 234
11.5.1.2 Secure Data Storage 236
11.5.2 Secret Key Exchange 237
Contents

11.6 Conclusion 238
Acknowledgment 239
References 239

12 Lightweight Crypto and Security 243
Lo’ai A. Tawalbeh and Hala Tawalbeh
12.1 Introduction 243
12.1.1 Cyber-Physical Systems CPSs 243
12.1.2 Security and Privacy 243
12.1.3 Lightweight Cryptography (LWC) 243
12.1.4 Chapter Organization 244
12.2 Cyber-Physical Systems 244
12.3 Security and Privacy in Cyber-Physical Systems 245
12.4 Lightweight Cryptography Implementations for Security and Privacy in CPSs 247
12.4.1 Introduction 247
12.4.2 Why Is Lightweight Cryptography Important? 249
12.4.3 Lightweight Symmetric and Asymmetric Ciphers Implementations 250
12.4.3.1 Hardware Implementations of Symmetric Ciphers 251
12.4.3.2 Software Implementations of Symmetric Ciphers 253
12.4.3.3 Hardware Implementations of Asymmetric Ciphers 254
12.4.3.4 Software Implementations of Asymmetric Ciphers 255
12.4.3.5 Secure Hash Algorithms (SHA) 256
12.5 Opportunities and Challenges 257
12.6 Conclusion 258
Acknowledgments 259
References 259

13 Cyber-Physical Vulnerabilities of Wireless Sensor Networks in Smart Cities 263
Md. Mahmud Hasan and Hussein T. Mouftah
13.1 Introduction 263
13.1.1 The Smart City Concept and Components 263
13.2 WSN Applications in Smart Cities 265
13.2.1 Smart Home 265
13.2.2 Smart Grid Applications 267
13.2.2.1 Substation Monitoring 267
13.2.3 Intelligent Transport System Applications 268
13.2.3.1 Roadside Unit 268
13.2.3.2 Vehicular Sensor Network 269
13.2.3.3 Intelligent Sensor Network 269
13.2.4 Real-Time Monitoring and Safety Alert 270
13.3 Cyber-Physical Vulnerabilities 270
13.3.1 Possible Attacks 271
13.3.2 Impacts on Smart City Lives 272
13.3.2.1 Service Interruption 272
13.3.2.2 Damage to Property 273
13.3.2.3 Damage to Life 273
13.3.2.4 Privacy Infiltration 274
13.4 Solution Approaches 274
13.4.1 Cryptography 274
13.4.2 Intrusion Detection System 276
13.4.3 Watchdog System 277
13.4.4 Game Theoretic Deployment 277
13.4.5 Managed Security 277
13.4.6 Physical Security Measures 278
13.5 Conclusion 278
Acknowledgment 278
References 279

14 Detecting Data Integrity Attacks in Smart Grid 281
Linqiang Ge, Wei Yu, Paul Moulema, Guobin Xu, David Griffith and Nada Golmie
14.1 Introduction 281
14.2 Literature Review 283
14.3 Network and Threat Models 285
14.3.1 Network Model 285
14.3.2 Threat Model 286
14.4 Our Approach 287
14.4.1 Overview 287
14.4.2 Detection Schemes 289
14.4.2.1 Statistical Anomaly-Based Detection 289
14.4.2.2 Machine Learning-Based Detection 290
14.4.2.3 Sequential Hypothesis Testing-Based Detection 291
14.5 Performance Evaluation 292
14.5.1 Evaluation Setup 292
14.5.2 Evaluation Results 294
14.6 Extension 297
14.7 Conclusion 298
References 298

15 Data Security and Privacy in Cyber-Physical Systems for Healthcare 305
Aida Čaušević, Hossein Fotouhi and Kristina Lundqvist
15.1 Introduction 305
15.2 Medical Cyber-Physical Systems 306
15.2.1 Communication within WBANs 307
15.2.1.1 Network Topology 307
15.2.1.2 Interference in WBANs 308
15.2.1.3 Challenges with LPWNs in WBANs 308
15.2.1.4 Feedback Control in WBANs 308
15.2.1.5 Radio Technologies 309
15.2.2 Existing WBAN-Based Health Monitoring Systems 310
15.3 Data Security and Privacy Issues and Challenges in WBANs 312
15.3.1 Data Security and Privacy Threats and Attacks 314
15.4 Existing Security and Privacy Solutions in WBAN

15.4.1 Academic Contributions

15.4.1.1 Biometric Solutions

15.4.1.2 Cryptographic Solutions

15.4.1.3 Solutions on Implantable Medical Devices

15.4.2 Existing Commercial Solutions

15.5 Conclusion

References

16 Cyber Security of Smart Buildings

Steffen Wendzel, Jernej Tonejc, Jaspreet Kaur and Alexandra Kobekova

16.1 What Is a Smart Building?

16.1.1 Definition of the Term

16.1.2 The Design and the Relevant Components of a Smart Building

16.1.3 Historical Development of Building Automation Systems

16.1.4 The Role of Smart Buildings in Smart Cities

16.1.5 Known Cases of Attacks on Smart Buildings

16.2 Communication Protocols for Smart Buildings

16.2.1 KNX/EIB

16.2.2 BACnet

16.2.3 ZigBee

16.2.4 EnOcean

16.2.5 Other Protocols

16.2.6 Interoperability and Interconnectivity

16.3 Attacks

16.3.1 How Can Buildings Be Attacked?

16.3.2 Implications for the Privacy of Inhabitants and Users

16.3.3 Reasons for Insecure Buildings

16.4 Solutions to Protect Smart Buildings

16.4.1 Raising Security Awareness and Developing Security Know-How

16.4.2 Physical Access Control

16.4.3 Hardening Automation Systems

16.4.3.1 Secure Coding

16.4.3.2 Operating System Hardening

16.4.3.3 Patching

16.4.4 Network-Level Protection

16.4.4.1 Firewalls

16.4.4.2 Monitoring and Intrusion Detection Systems

16.4.4.3 Separation of Networks

16.4.5 Responsibility Matrix

16.5 Recent Trends in Smart Building Security Research

16.5.1 Visualization

16.5.2 Network Security

16.5.2.1 Traffic Normalization

16.5.2.2 Anomaly Detection

16.5.2.3 Novel Fuzzing Approaches

16.6 Conclusion and Outlook

References
The Internet of Postal Things: Making the Postal Infrastructure Smarter 353
Paola Piscioneri, Jessica Raines and Jean Philippe Ducasse

17.1 Introduction 353
17.2 Scoping the Internet of Postal Things 354
17.2.1 The Rationale for an Internet of Postal Things 354
17.2.1.1 A Vast Infrastructure 354
17.2.1.2 Trust as a Critical Brand Attribute 355
17.2.1.3 Operational Experience in Data Collection and Analytics 356
17.2.1.4 Customer Demand for Information 356
17.2.2 Adjusting to a New Business Environment 356
17.2.2.1 Shifting from Unconnected to “Smart” Products and Services 357
17.2.2.2 Shifting from Competing on Price to Competing on Overall Value 357
17.2.2.3 Shifting from Industries to Ecosystems 357
17.2.2.4 Shifting from Workforce Replacement to Human-Centered Automation 357
17.3 Identifying Internet of Postal Things Applications 358
17.3.1 Transportation and Logistics 358
17.3.1.1 Predictive Maintenance 359
17.3.1.2 Fuel Management 359
17.3.1.3 Usage-Based Insurance 360
17.3.1.4 Driverless Vehicles 360
17.3.1.5 Load Optimization 360
17.3.1.6 Real-Time Dynamic Routing 360
17.3.1.7 Collaborative Last Mile Logistics 361
17.3.2 Enhanced Mail and Parcel Services: The Connected Mailbox 361
17.3.2.1 Concept and Benefits 362
17.3.2.2 The Smart Mailbox as a Potential Source of New Revenue 363
17.3.3 The Internet of Things in Postal Buildings 364
17.3.3.1 Optimizing Energy Costs 364
17.3.3.2 The Smarter Post Office 365
17.3.4 Neighborhood Services 365
17.3.4.1 Smart Cities Need Local Partners 365
17.3.4.2 Carriers as Neighborhood Logistics Managers 366
17.3.5 Summarizing the Dollar Value of IoPT Applications 367
17.4 The Future of IoPT 367
17.4.1 IoPT Development Stages 367
17.4.2 Implementation Challenges 368
17.4.3 Building a Successful Platform Strategy 371
17.5 Conclusion 371
References 372

Security and Privacy Issues in the Internet of Cows 375
Amber Adams-Progar, Glenn A. Fink, Ely Walker and Don Llewellyn

18.1 Precision Livestock Farming 375
18.1.1 Impact on Humans 376
18.1.1.1 Labor and Workforce Effects 377
18.1.1.2 Food Quality and Provenance 377
18.1.1.3 Transparency and Remote Management 378
18.1.2 Impact on Animals 379
18.1.2.1 Estrus Monitoring 379
18.1.2.2 Rumen Health 380
18.1.2.3 Other Bovine Health Conditions 381
18.1.3 Impact on the Environment 382
18.1.4 Future Directions for IoT Solutions 383
18.2 Security and Privacy of IoT in Agriculture 384
18.2.1 Cyber-Physical System Vulnerabilities 385
18.2.2 Threat Models 386
18.2.2.1 Threat: Misuse of Video Data 386
18.2.2.2 Threat: Misuse of Research Data 387
18.2.2.3 Threat: Misuse of Provenance Data 387
18.2.2.4 Threat: Data Leakage via Leased Equipment and Software 388
18.2.2.5 Threat: Political Action and Terrorism 389
18.2.3 Recommendations for IoT Security and Privacy in Agriculture 390
18.2.3.1 Data Confidentiality 391
18.2.3.2 Data Integrity 393
18.2.3.3 System Availability 393
18.2.3.4 System Safety 393
18.3 Conclusion 395
References 395

19 Admission Control-Based Load Protection in the Smart Grid 399
Paul Moulema, Sriharsha Mallapuram, Wei Yu, David Griffith, Nada Golmie and David Su
19.1 Introduction 399
19.2 Related Work 401
19.3 Our Approach 402
19.3.1 Load Admission Control 403
19.3.2 Load Shedding Techniques 404
19.3.2.1 Load-Size-Based Shedding – Smallest Load First: 405
19.3.2.2 Load-Size-Based Shedding – Largest Load First: 406
19.3.2.3 Priority-Based Load Shedding: 407
19.3.2.4 Fair Priority-Based Load Shedding: 408
19.3.3 Simulation Scenarios 410
19.4 Performance Evaluation 411
19.4.1 Scenario 1: Normal Operation 411
19.4.2 Scenario 2: Brutal Admission Control 413
19.4.3 Scenario 3: Load-Size-Based Admission Control 413
19.4.4 Scenario 4: Priority-Based Admission Control 416
19.4.5 Scenario 5: Fair Priority-Based Admission Control 417
19.5 Conclusion 419
References 419

Editor Biographies 423

Index 427