

# Contents

Foreword	ix
Acknowledgments	x
<b>Introduction</b>	xi
<i>Steven King</i>	
<b>Chapter 1. Architecting Information Infrastructures for Security</b>	
<i>Cliff Wang</i>	1
<b>1.1 Architectures for Secure and Robust Distributed Infrastructures</b>	
<b>1.1.1 Overview of the ASRDI (Architectures for Secure and Robust Distributed Infrastructures) Project</b> <i>Sanjay Lall, Carolyn Beck, Stephen Boyd, John Doyle, Geir Dullerud, Chris Hadjicostis, Muriel Medard, Balaji Prabhakar, Rayadurgam Srikant, George Verghese</i>	3
<b>1.1.2 Approximate Fairness through Differential Dropping</b> <i>Rong Pan, Lee Breslau, Balaji Prabhakar, Scott Shenker</i>	35
<b>1.2 A Complex Adaptive System Approach to QoS Assurance and Stateful Resource Management for Dependable Information Infrastructure</b>	
<b>1.2.1 Quality of Service Assurance for Dependable Information Infrastructures</b> <i>Nong Ye, Ying-Cheng Lai, Toni Farley</i>	53
<b>1.2.2 Onset of Traffic Congestion in Complex Networks</b> <i>Liang Zhao, Ying-Cheng Lai, Kwangho Park, Nong Ye</i>	80
<b>1.3 Anomaly and Misuse Detection in Network Traffic Streams—Checking and Machine Learning Approaches</b>	
<b>1.3.1 Anomaly and Misuse Detection in Network Traffic Streams—Checking and Machine Learning Approaches</b> <i>Sampath Kannan, Insup Lee, Wenke Lee, Oleg Sokolsky, Diana Spears, William Spears</i>	88
<b>1.3.2 An Ensemble of Anomaly Classifiers for Identifying Cyber Attacks</b> <i>Carlos Kelly, Diana Spears, Christer Karlsson, Peter Polyakov</i>	100
<b>1.4 Distributed Systems Security via Logical Frameworks</b>	
<b>1.4.1 Distributed System Security via Logical Frameworks</b> <i>Lujo Bauer, Frank Pfenning, Michael K. Reiter</i>	108
<b>1.4.2 Device-Enabled Authorization in the Grey System</b> <i>Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, Peter Rutenbar</i>	116
<b>1.5 Distributed Immune Systems for Wireless Networks Information Assurance</b>	
<b>1.5.1 Distributed Immune Systems for Wireless Networks Information Assurance</b> <i>John S. Baras</i>	131
<b>1.5.2 A Key Management Scheme for Distributed Sensor Networks</b> <i>Laurent Eschenauer, Virgil D. Gligor</i>	159
<b>1.6 Hi-DRA High-Speed, Wide-Area Network Detection, Response, and Analysis</b>	
<b>1.6.1 Summary of the Hi-DRA Project A System for High-Speed, Wide-Area Network Detection, Response, and Analysis</b> <i>Richard A. Kemmerer, Giovanni Vigna, Antonio Carzaniga, Alexander L. Wolf</i>	168
<b>1.6.2 Stateful Intrusion Detection for High-Speed Networks</b> <i>Christopher Kruegel, Fredrik Valeur, Giovanni Vigna, Richard Kemmerer</i>	181

<b>Chapter 2. At the Edges of the Critical Information Infrastructure</b>	191
<i>David Hislop, Todd Combs</i>	
<b>2.1 Enabling Dynamic Security Management of Networked Systems via Device-Embedded Security</b>	
<b>2.1.1 Better Security via Smarter Devices</b>	193
<i>Gregory R. Ganger, Dawn Song, Chenxi Wang</i>	
<b>2.1.2 Storage-Based Intrusion Detection: Watching Storage Activity for Suspicious Behavior</b>	199
<i>Adam G. Pennington, John D. Strunk, John Linwood Griffin, Craig A.N. Soules, Garth R. Goodson, Gregory R. Ganger</i>	
<b>2.2 Software Model Checking for Embedded Systems</b>	
<b>2.2.1 Customizable Model Checking for Embedded Software</b>	212
<i>Xianghua Deng, John Hatcliff, Matthew Hoosier, Robby, Matthew B. Dwyer</i>	
<b>2.2.2 Exploiting Object Escape and Locking Information in Partial-Order Reductions for Concurrent Object-Oriented Programs</b>	228
<i>Matthew B. Dwyer, John Hatcliff, Robby, Venkatesh Prasad Ranganath</i>	
<b>2.3 Advanced Tool Integration for Embedded System Assurance</b>	
<b>2.3.1 Overview of the HASTEN (High Assurance Systems Tools and Environments) Project</b>	270
<i>Insup Lee, Rajeev Alur, Bob Cook, Carl Gunter, Elsa Gunter, Sampath Kannan, Kang Shin, Oleg Sokolsky</i>	
<b>2.3.2 Hierarchical Modeling and Analysis of Embedded Systems</b>	297
<i>Rajeev Alur, Thao Dang, Joel Esposito, Yerang Hur, Franjo Ivančić, Vijay Kumar, Insup Lee, Pradyumna Mishra, George J. Pappas, Oleg Sokolsky</i>	
<b>2.4 Verification Tools for Embedded Systems</b>	
<b>2.4.1 Formal Verification for High Confidence Embedded Systems</b>	315
<i>Edmund Clarke, David Garlan, Bruce H. Krogh, Reid Simmons, Jeannette Wing</i>	
<b>2.4.2 Bridging the Gap between Systems Design and Space Systems Software</b>	336
<i>David Garlan, William K. Reinholtz, Bradley Schmerl, Nicholas D. Sherman, Tony Tseng</i>	
<b>Chapter 3. Software Engineering for Assurance</b>	347
<i>Ralph Wachter, Gary Toth</i>	
<b>3.1 Static Analysis to Enhance the Power of Model Checking for Concurrent Software</b>	
<b>3.1.1 Static Analysis to Enhance the Power of Model Checking for Concurrent Software</b>	349
<i>Edmund Clarke, Daniel Kroening, Thomas Reps</i>	
<b>3.1.2 Abstraction Refinement via Inductive Learning</b>	361
<i>Alexey Loginov, Thomas Reps, Mooly Sagiv</i>	
<b>3.2 Protecting COTS from the Inside</b>	
<b>3.2.1 Analysis of COTS for Security Vulnerability Remediation</b>	375
<i>Gogul Balakrishnan, Mihai Christodorescu, Vinod Ganapathy, Jonathon T. Giffin, Shai Rubin, Hao Wang, Somesh Jha, Barton P. Miller, Thomas Reps</i>	
<b>3.2.2 Formalizing Sensitivity in Static Analysis for Intrusion Detection</b>	381
<i>Henry Hanping Feng, Jonathon T. Giffin, Yong Huang, Somesh Jha, Wenke Lee, Barton P. Miller</i>	
<b>3.3 RAPIDware: Component-Based Development of Adaptive and Dependable Middleware</b>	
<b>3.3.1 RAPIDware: Component-Based Development of Adaptive and Dependable Middleware</b>	396
<i>Philip K. McKinley, R.E. Kurt Stirewalt, Betty H.C. Cheng, Laura K. Dillon, Sandeep Kulkarni</i>	
<b>3.3.2 Composing Adaptive Software</b>	407
<i>Philip K. McKinley, Seyed Masoud Sadjadi, Eric P. Kasten, Betty H.C. Cheng</i>	
<b>3.4 Generating Efficient Trust Management Software from Policies</b>	
<b>3.4.1 Generating Efficient Security Software from Policies</b>	416
<i>Scott D. Stoller, Yanhong A. Liu</i>	
<b>3.4.2 Role-Based Access Control: A Corrected and Simplified Specification</b>	425
<i>Yanhong A. Liu, Scott D. Stoller</i>	

### 3.5 Modeling and Simulation Environment for Critical Information Protection

#### 3.5.1 Analysis, Modeling, and Simulation for Networked Systems

*Mostafa Bassiouni, Vicki M. Bier, Pascale Carayon, Jagdish Chandra, Ratan K. Guha, Sara B. Kraemer, Stephen M. Robinson, Daniel G. Schwartz, Sara Stoecklin*

440

#### 3.5.2 Protection of Simple Series and Parallel Systems with Components of Different Values

*Vicki M. Bier, Aniruddha Nagaraj, Vinod Abhichandani*

466

## Chapter 4. Malicious Mobile Code

*Ralph Wachter, Gary Toth*

475

### 4.1 Language-Based Security for Malicious Mobile Code

#### 4.1.1 Language-Based Security for Malicious Mobile Code

*Fred B. Schneider, Dexter Kozen, Greg Morrisett, Andrew C. Myers*

477

#### 4.1.2 Malicious Code Detection for Open Firmware

*Frank Adelstein, Matt Stillerman, Dexter Kozen*

495

### 4.2 Model-Carrying Code: A New Approach to Mobile-Code Security

#### 4.2.1 Safe Execution of Mobile and Untrusted Code: The Model-Carrying Code Project

*R. Sekar, C.R. Ramakrishnan, I.V. Ramakrishnan, Scott Smolka, Samik Basu, Sandeep Bhatkar, Abhishek Chaturvedi, Daniel DuVarney, Zhenkai Liang, Yow-Jian Lin, Dipti Saha, Weiqing Sun, Prem Uppuluri, V.N. Venkatakrishnan, Wei Xu, Mohan Channa, Yogesh Chauhan, Kumar Krishna, Shruthi Krishna, Vishwas Nagaraja, Divya Padmanabhan*

505

#### 4.2.2 Model-Carrying Code: A Practical Approach for Safe Execution of Untrusted Applications

*R. Sekar, V.N. Venkatakrishnan, Samik Basu, Sandeep Bhatkar, Daniel C. DuVarney*

519

### 4.3 Neutralizing Malicious Mobile Code

#### 4.3.1 Behavioral Detection of Malicious Code

*William Allen, Richard Ford, Jens Gregor, Gerald Marin, Mike Thomason, James Whittaker*

533

#### 4.3.2 Gatekeeper II: New Approaches to Generic Virus Prevention

*Richard Ford, Matt Wagner, Jason Michalske*

545

## Chapter 5. Dependable Critical Information Infrastructure for Command and Control

*Robert Herklotz, Chris Arney*

557

### 5.1 Trustworthy Infrastructure, Mechanisms, and Experimentation for Diffuse Computing

#### 5.1.1 Software Quality and Infrastructure Protection for Diffuse Computing

*J. Feigenbaum, J.Y. Halpern, P.D. Lincoln, J.C. Mitchell, A. Scedrov, J.M. Smith, P. Syverson*

559

#### 5.1.2 Games and the Impossibility of Realizable Ideal Functionality

*Anupam Datta, Ante Derek, John C. Mitchell, Ajith Ramanathan, Andre Scedrov*

567

### 5.2 Adaptable Situation-Aware Secure Services-Based Systems

#### 5.2.1 Adaptable Situation-Aware Secure Service-Based (AS<sup>3</sup>) Systems

*S.S. Yau, H. Davulcu, S. Mukhopadhyay, D. Huang, Y. Yao, H. Gong*

585

#### 5.2.2 Automated Agent Synthesis for Situation Awareness in Service-Based Systems

*S.S. Yau, H. Gong, D. Huang, W. Gao, L. Zhu*

597

### 5.3 Detecting Deception in the Military Infosphere: Improving and Integrating Human Detection Capabilities with Automated Tools

#### 5.3.1 Detecting Deception in the Military Infosphere: Improving and Integrating Detection Capabilities with Automated Tools

*Judee K. Burgoon, Jay F. Nunamaker Jr., Joey F. George, Mark Adkins, John Kruse, David Biro*

606

#### 5.3.2 Detecting Concealment of Intent in Transportation Screening: A Proof-of-Concept

*Judee K. Burgoon, Douglas P. Twitchell, Matthew L. Jensen, Mark Adkins, John Kruse, Amit Deokar, Shan Lu, Dimitris N. Metaxas, Jay F. Nunamaker Jr., Robert E. Younger*

628

**5.4 Vulnerability Assessment Tools for Complex Information Networks****5.4.1 Applications of Feedback Control in Information Network Security***David L. Pepyne, Weibo Gong, Yu-Chi Ho, Christos G. Cassandras, Wenke Lee, Avrom Pfeffer, Hong Liu*

645

**5.4.2 Anomaly Detection Using Call Stack Information***Henry Hanping Feng, Oleg M. Kolesnikov, Prahlad Fogla, Wenke Lee, Weibo Gong*

675