1. Record Nr. UNINA9910555075203321

Titolo	Modeling and design of secure Internet of things / / edited by Charles A. Kamhoua, Laurent L. Njilla, Alexander Kott, Sachin Shetty
Pubbl/distr/stampa	Hoboken, New Jersey : , : Wiley-IEEE Press, , [2020] [Piscataqay, New Jersey] : , : IEEE Xplore, , [2020]
ISBN	1-119-59339-5 1-119-59337-9 1-119-59338-7
Descrizione fisica	1 online resource (697 pages)
Collana	IEEE press
Disciplina	005.8
Soggetti	Internet of things - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	About the Editors ix -- List of Contributors xiii -- Foreword xix -- Preface xxiii -- 1 Introduction 1 /Charles A. Kamhoua, Laurent L. Njilla, Alexander Kott, and Sachin Shetty -- Part I Game Theory for Cyber Deception 27 -- 2 Game-Theoretic Analysis of Cyber Deception: Evidence-Based Strategies and Dynamic Risk Mitigation 29 /Tao Zhang, Linan Huang, Jeffrey Pawlick, and Quanyan Zhu -- 3 A Hypergame-Based Defense Strategy Toward Cyber Deception in Internet of Battlefield Things (IoBT) 59 /Bowei Xi and Charles A. Kamhoua -- 4 Cooperative Spectrum Sharing and Trust Management in IoT Networks 79 /Fatemeh Afghah, Alireza Shamsoshoara, Laurent L. Njilla, and Charles A. Kamhoua -- 5 Adaptation and Deception in Adversarial Cyber Operations 111 /George Cybenko -- 6 On Development of a Game-Theoretic Model for Deception-Based Security 123 /Satyaki Nan, Swastik Brahma, Charles A. Kamhoua, and Laurent L. Njilla -- 7 Deception for Cyber Adversaries: Status, Challenges, and Perspectives 141 /Abdullah Alshammari, Danda B. Rawat, Moses Garuba, Charles A. Kamhoua, and Laurent L. Njilla -- Part II IoT Security Modeling and Analysis 161 -- 8 Cyber-Physical Vulnerability Analysis of IoT Applications Using Multi-Modeling 163 /Ted Bapty, Abhishek Dubey, and Janos Sztipanovits -- 9 Securing Smart Cities: Implications and Challenges 185 /Ioannis Agadakos, Prashant Anantharaman, Gabriela F.

Ciocarlie, Bogdan Copos, Michael Emmi, Tancrde Lepoint, Ulf Lindqvist, Michael Locasto, and Liwei Song -- 10 Modeling and Analysis of Integrated Proactive Defense Mechanisms for Internet of Things 217 /Mengmeng Ge, Jin-Hee Cho, Bilal Ishfaq, and Dong Seong Kim -- 11 Addressing Polymorphic Advanced Threats in Internet of Things Networks by Cross-Layer Profiling 249 /Hisham Alasmary, Afsah Anwar, Laurent L. Njilla, Charles A. Kamhoua, and Aziz Mohaisen -- 12 Analysis of Stepping-Stone Attacks in Internet of Things Using Dynamic Vulnerability Graphs 273 /Marco Gamarra, Sachin Shetty, Oscar Gonzalez, David M. Nicol, Charles A. Kamhoua, and Laurent L. Njilla. 13 Anomaly Behavior Analysis of IoT Protocols 295 /Pratik Satam, Shalaka Satam, Salim Hariri, and Amany Alshawi -- 14 Dynamic Cyber Deception Using Partially Observable Monte-Carlo Planning Framework 331 /Md Ali Reza Al Amin, Sachin Shetty, Laurent L. Njilla, Deepak K. Tosh, and Charles A. Kamhoua -- 15 A Coding Theoretic View of Secure State Reconstruction 357 /Suhas Diggavi and Paulo Tabuada -- 16 Governance for the Internet of Things: Striving Toward Resilience 371 /S. E. Galaitsi, Benjamin D. Trump, and Igor Linkov -- Part III IoT Security Design 383 -- 17 Secure and Resilient Control of IoT-Based 3D Printers 385 /Zhiheng Xu and Quanyan Zhu -- 18 Proactive Defense Against Security Threats on IoT Hardware 407 /Qiaoyan Yu, Zhiming Zhang, and Jaya Dofe -- 19 IoT Device Attestation: From a Cross-Layer Perspective 435 /Orlando Arias, Fahim Rahman, Mark Tehranipoor, and Yier Jin -- 20 Software-Defined Networking for Cyber Resilience in Industrial Internet of Things (IIoT) 453 /Kamrul Hasan, Sachin Shetty, Amin Hassanzadeh, Malek Ben Salem, and Jay Chen -- 21 Leverage SDN for Cyber-Security Deception in Internet of Things 479 /Yaoqing Liu, Garegin Grigoryan, Charles A. Kamhoua, and Laurent L. Njilla -- 22 Decentralized Access Control for IoT Based on Blockchain and Smart Contract 505 /Ronghua Xu, Yu Chen, and Erik Blasch -- 23 Intent as a Secure Design Primitive 529 /Prashant Anantharaman, J. Peter Brady, Ira Ray Jenkins, Vijay H. Kothari, Michael C. Millian, Kartik Palani, Kirti V. Rathore, Jason Reeves, Rebecca Shapiro, Syed H. Tanveer, Sergey Bratus, and Sean W. Smith -- 24 A Review of Moving Target Defense Mechanisms for Internet of Things Applications 563 /Nico Saputro, Samet Tonyali, Abdullah Aydeger, Kemal Akkaya, Mohammad A. Rahman, and Selcuk Uluagac -- 25 Toward Robust Outlier Detector for Internet of Things Applications 615 /Raj Mani Shukla and Shamik Sengupta -- 26 Summary and Future Work 635 /Charles A. Kamhoua, Laurent L. Njilla, Alexander Kott, and Sachin Shetty.
Index 647.

Sommario/riassunto

"Internet of Things (IoT) devices such as sensors, wearable devices, robots, drones, and autonomous vehicles facilitate the Intelligence, Surveillance, and Reconnaissance to Command and Control and battlefield services. There are several reasons for IoT security. First, IoT devices are mass produced rapidly to be low-cost commodity items without security protection in their original design. Second, IoT devices are highly dynamic, mobile, and heterogeneous without common standards. Third, it is imperative to understand the natural world, the physical process(es) under IoT control, and how these real-world processes can be compromised before recommending any relevant security countermeasure. As a result, those systems are the frequent targets of sophisticated cyber attacks that aim to disrupt mission effectiveness."--