

1. Record Nr.	UNISA996490366203316
Autore	Kieras Timothy
Titolo	IoT supply chain security risk analysis and mitigation : modeling, computations, and software tools // Timothy Kieras, Junaid Farooq and Quanyan Zhu
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-08480-2
Descrizione fisica	1 online resource (142 pages)
Collana	SpringerBriefs in computer science
Disciplina	658.7
Soggetti	Business logistics Business logistics - Security measures 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	Intro -- Preface -- Acknowledgments -- Contents -- Acronyms -- 1 IoT and Supply Chain Security -- 1.1 Vendor Landscape of IoT Systems -- 1.2 Brief Taxonomy of Supply Chain Security -- 1.3 IoT Supply Chain Risk: Hard to Observe and Hard to Control -- 1.3.1 Dissecting Supply Chain Links in IoT -- 1.4 IoT Risk Implications and Consequences -- 1.4.1 Key Features of IoT Security -- 1.5 Challenges in Cyber Supply Chain Risk Analysis of IoT -- 1.6 Supply Chain Resilience -- 1.6.1 Top-Down Approach to Managing Risk -- 1.6.2 Bottom-Up Approach to Managing Risk -- 1.7 Overview of the Book -- References -- 2 Risk Modeling and Analysis -- 2.1 Risk Scoring in Component Graphs -- 2.1.1 Introduction -- 2.1.2 Related Work -- 2.1.3 Contributions -- 2.2 System Model for Risk Assessment -- 2.2.1 Model Definitions -- 2.2.1.1 Component Security Graph -- 2.2.1.2 System Supplier Network -- 2.2.2 Supplier Trust -- 2.2.3 Systemic Risk Graph -- 2.3 Risk Analysis Metrics -- 2.3.1 Systemic Risk Function -- 2.3.2 Supplier Involvement Measure -- 2.4 Uncertainties in Model Development -- 2.4.1 Parametric Uncertainties in Probability Estimates -- 2.4.2 Structural Modeling Uncertainties -- 2.5 Uncertainty Case Studies -- 2.5.1 Case 0: Ground Truth -- 2.5.2 Case 1: Uncertainty of Single Node Logic -- 2.5.3 Case 2: Uncertainty of Node Omission --

2.5.4 Case 3: Uncertainty in Edge Placement -- 2.5.5 Case 4:  
Uncertainty in Probability Values -- 2.6 Conclusion -- References -- 3  
Risk Mitigation Decisions -- 3.1 Cost Effective Vendor Selection --  
3.1.1 Strict Supplier Choice Problem -- 3.2 Supply Chain Diversification  
-- 3.2.1 Component Security Risk Minimization Problem -- 3.2.2  
Supplier Involvement Minimization Problem -- 3.2.3 Relaxed Supplier  
Choice Problem -- 3.3 Case Study and Results -- 3.3.1 Simulation  
Setup -- 3.3.2 Example Scenarios and Results.  
3.3.3 Supplier Involvement Experiments -- 3.4 Conclusion --  
References -- 4 Policy Management -- 4.1 Introduction -- 4.2  
Literature Review -- 4.3 Accountability Models in IoT Supply Chain --  
4.3.1 Running Examples -- 4.3.2 System Modeling -- 4.3.3  
Accountability Investigation -- 4.3.4 Model Extensions -- 4.3.4.1  
Single Supplier with Multiple Types -- 4.3.4.2 Multiple Suppliers -- 4.4  
Case Study 1: Autonomous Truck Platooning -- 4.4.1 Background --  
4.4.2 Vehicle Dynamics Model -- 4.4.3 Accountability Testing -- 4.4.4  
Parameter Analysis -- 4.4.5 Investigation Performance -- 4.4.5.1  
Accountability Receiver Operating Characteristic -- 4.4.5.2 Area Under  
the AROC Curve -- 4.5 Case Study 2: Ransomware in IoT Supply Chain  
-- 4.5.1 Background -- 4.5.2 Smart Lock and Ransomware Attack --  
4.5.3 Accountability Investigation -- 4.5.3.1 Tier-1 Investigation --  
4.5.3.2 Multi-Stage Accountability Investigation -- 4.6 Compliance and  
Cyber Insurance -- 4.6.1 Compliance Modeling -- 4.6.2 Contract  
Design -- 4.6.3 Cyber Insurance -- 4.6.3.1 Background Introduction --  
4.6.3.2 Insurance Policy Design -- 4.6.3.3 Maximum Premium with Full  
Coverage -- 4.6.3.4 Coverage Level with Given Premium -- 4.6.3.5  
Trade-Off Between Accountability Investment and Cyber Insurance --  
4.7 Conclusion -- References -- 5 Computational Tools -- 5.1  
Introduction to I-SCRAM: A Software Tool for IoT SCRM -- 5.1.1 Supply  
Chain Risk Analysis and Mitigation -- 5.1.1.1 I-SCRAM Software  
Components -- 5.1.1.2 User Interface -- 5.1.1.3 Data Model -- 5.1.1.4  
Server -- 5.1.1.5 Implementation of Core Operations -- 5.2 Case Study  
1: Autonomous Vehicle -- 5.3 Case Study 2: Industrial Control System  
-- 5.4 Conclusions and Outlooks -- References -- Index.

---