

# SpringerBriefs in Computer Science

## Series Editors

Stan Zdonik, Brown University, Providence, RI, USA

Shashi Shekhar, University of Minnesota, Minneapolis, MN, USA

Xindong Wu, University of Vermont, Burlington, VT, USA

Lakhmi C. Jain, University of South Australia, Adelaide, SA, Australia

David Padua, University of Illinois Urbana-Champaign, Urbana, IL, USA

Xuemin Sherman Shen, University of Waterloo, Waterloo, ON, Canada

Borko Furht, Florida Atlantic University, Boca Raton, FL, USA

V. S. Subrahmanian, University of Maryland, College Park, MD, USA

Martial Hebert, Carnegie Mellon University, Pittsburgh, PA, USA

Katsushi Ikeuchi, University of Tokyo, Tokyo, Japan

Bruno Siciliano, Università di Napoli Federico II, Napoli, Italy

Sushil Jajodia, George Mason University, Fairfax, VA, USA

Newton Lee, Institute for Education, Research and Scholarships, Los Angeles, CA, USA

SpringerBriefs present concise summaries of cutting-edge research and practical applications across a wide spectrum of fields. Featuring compact volumes of 50 to 125 pages, the series covers a range of content from professional to academic.

Typical topics might include:

- A timely report of state-of-the art analytical techniques
- A bridge between new research results, as published in journal articles, and a contextual literature review
- A snapshot of a hot or emerging topic
- An in-depth case study or clinical example
- A presentation of core concepts that students must understand in order to make independent contributions

Briefs allow authors to present their ideas and readers to absorb them with minimal time investment. Briefs will be published as part of Springer's eBook collection, with millions of users worldwide. In addition, Briefs will be available for individual print and electronic purchase. Briefs are characterized by fast, global electronic dissemination, standard publishing contracts, easy-to-use manuscript preparation and formatting guidelines, and expedited production schedules. We aim for publication 8–12 weeks after acceptance. Both solicited and unsolicited manuscripts are considered for publication in this series.

\*\*Indexing: This series is indexed in Scopus, Ei-Compendex, and zbMATH \*\*

Timothy Kieras • Junaid Farooq • Quanyan Zhu

# IoT Supply Chain Security Risk Analysis and Mitigation

Modeling, Computations, and Software Tools

 Springer

Timothy Kieras  
New York University  
Brooklyn, NY, USA

Junaid Farooq  
University of Michigan-Dearborn  
Dearborn, MI, USA

Quanyan Zhu  
New York University  
Brooklyn, NY, USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)  
SpringerBriefs in Computer Science  
ISBN 978-3-031-08479-9 ISBN 978-3-031-08480-5 (eBook)  
<https://doi.org/10.1007/978-3-031-08480-5>

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

*To our families whose support has been  
instrumental in the completion of this work*

# Preface

Supply chain risk is a well-studied subject in business processes and logistics management literature. However, its scope is evolving and becoming wider as the systems and processes are becoming more complex. Modern information technology (IT), operational technology (OT), and Internet of things (IoT) systems have complex global supply chains. Moreover, there is an intricate blend of software and hardware systems, which are manufactured, controlled, and operated by different entities. It is thus becoming critically important to have knowledge and understanding of what vendors are linked to the system and what risk do these vendors bring to the system operation. The cybersecurity of IoT-enabled infrastructure systems overarchingly depends on the confidentiality, integrity, and availability of the software and hardware components including their supply chain. The complex network of components involves various actors and organizations that design and integrate different sub-components of the larger system. The insecurity of one sub-component in the supply chain can have downstream effects on the security and resiliency of IoT-enabled infrastructure systems.

This book aims to provide the necessary tools for quantitative understanding and assessment of the supply chain risk threats to critical infrastructure owners and operators. In a typical IoT-enabled infrastructure system, there is a complex integration of multiple components enabling various IT and OT functions. Each component is supplied by a vendor or a network of vendors, which have different levels of trustworthiness from the perspective of the stakeholders. Certain suppliers may have a long-standing history of successful operation and comply with essential cybersecurity practices. On the other hand, there are many newer and potentially less secure vendors, which can introduce unknown vulnerabilities to the overall system security. The supply chain front adds another dimension to the system reliability on top of component reliabilities. Furthermore, a particular component in the system may itself be very reliable but may have been procured from a less trustworthy vendor. Similarly, a component may not be very reliable but may have a highly trustworthy supplier. Therefore, it is critically important to understand the delicate interplay between component reliabilities and the trustworthiness of their suppliers.

Currently, there is a severe dearth of supply chain risk assessment tools that prevents system operators to analyze the risk to their infrastructure from a supply chain standpoint. Moreover, there is a lack of tools that can assist with supplier selection from alternatives and provide insights about supply chain decisions. This book is aimed at unfolding the emerging supply chain risk analysis ecosystem and providing a peek into a practical software tool to help analyze the risk. The described software tool, referred to as I-SCRAM, will enable critical infrastructure owners to make risk informed decisions relating to the supply chain while deploying their IT and OT systems. Providing such information to decision-makers will reduce the possibility of being affected by supply chain attacks from malicious IT and OT vendors. We hope that this book will provide a broad understanding of the emerging cyber supply chain security in the context of IoT systems to academics, industry professionals, and government officials.

Brooklyn, NY, USA  
Dearborn, MI, USA  
Brooklyn, NY, USA  
March 2022

Timothy Kieras  
Junaid Farooq  
Quanyan Zhu

# Acknowledgments

We would like to acknowledge the support of our respective institutions, New York University (NYU) and the University of Michigan-Dearborn, that have enabled us to pursue this work. We would appreciate all past and current members of the Laboratory for Agile and Resilient Complex Systems (LARX) at NYU who have provided us invaluable feedback and created an environment to allow intellectually engaging work. Specific thanks go to Yunfei Ge from LARX who has helped finish Chapter 4 with case studies and numerical examples. Without her assistance, this book would not be completed on time. We are also thankful to members of the Center of Cyber Security at NYU, in particular, Prof. Nasir Memon and Dr. Ed Amoroso, who have supported this work from the very beginning. This work is also a result of many unforgettable discussions with our colleagues and friends, to whom we are eternally thankful.

We also acknowledge the instrumental funding support from the Critical Infrastructure Resilience Institute (CIRI), a Department of Homeland Security Center of Excellence at the University of Illinois at Urbana-Champaign. We are thankful for research inputs from Randy Sandone and David Nicol and administrative support from Elaina Buhs and Andrea Whitesell at CIRI. Their continued support has made possible the development of I-SCRAM, a software tool for supply chain risk analysis and mitigation for IT, OT, and IoT systems. We are also grateful to constructive reviews from many anonymous reviewers of this work and insightful comments from many participants who attended our tutorials, workshops, and conference presentations.



# Contents

<b>1</b>	<b>IoT and Supply Chain Security</b> .....	1
1.1	Vendor Landscape of IoT Systems .....	1
1.2	Brief Taxonomy of Supply Chain Security .....	3
1.3	IoT Supply Chain Risk: Hard to Observe and Hard to Control .....	5
1.3.1	Dissecting Supply Chain Links in IoT .....	6
1.4	IoT Risk Implications and Consequences .....	7
1.4.1	Key Features of IoT Security .....	8
1.5	Challenges in Cyber Supply Chain Risk Analysis of IoT .....	9
1.6	Supply Chain Resilience .....	10
1.6.1	Top-Down Approach to Managing Risk .....	11
1.6.2	Bottom-Up Approach to Managing Risk .....	12
1.7	Overview of the Book .....	13
	References .....	13
<b>2</b>	<b>Risk Modeling and Analysis</b> .....	15
2.1	Risk Scoring in Component Graphs .....	15
2.1.1	Introduction .....	15
2.1.2	Related Work .....	16
2.1.3	Contributions .....	18
2.2	System Model for Risk Assessment .....	19
2.2.1	Model Definitions .....	19
2.2.2	Supplier Trust .....	23
2.2.3	Systemic Risk Graph .....	25
2.3	Risk Analysis Metrics .....	25
2.3.1	Systemic Risk Function .....	26
2.3.2	Supplier Involvement Measure .....	27
2.4	Uncertainties in Model Development .....	28
2.4.1	Parametric Uncertainties in Probability Estimates .....	28
2.4.2	Structural Modeling Uncertainties .....	28
2.5	Uncertainty Case Studies .....	29
2.5.1	Case 0: Ground Truth .....	29

- 2.5.2 Case 1: Uncertainty of Single Node Logic ..... 30
- 2.5.3 Case 2: Uncertainty of Node Omission ..... 31
- 2.5.4 Case 3: Uncertainty in Edge Placement ..... 32
- 2.5.5 Case 4: Uncertainty in Probability Values ..... 34
- 2.6 Conclusion ..... 35
- References ..... 36
- 3 Risk Mitigation Decisions ..... 39**
  - 3.1 Cost Effective Vendor Selection ..... 39
    - 3.1.1 Strict Supplier Choice Problem ..... 40
  - 3.2 Supply Chain Diversification ..... 41
    - 3.2.1 Component Security Risk Minimization Problem ..... 42
    - 3.2.2 Supplier Involvement Minimization Problem ..... 44
    - 3.2.3 Relaxed Supplier Choice Problem ..... 45
  - 3.3 Case Study and Results ..... 46
    - 3.3.1 Simulation Setup ..... 47
    - 3.3.2 Example Scenarios and Results ..... 48
    - 3.3.3 Supplier Involvement Experiments ..... 54
  - 3.4 Conclusion ..... 55
  - References ..... 55
- 4 Policy Management ..... 57**
  - 4.1 Introduction ..... 57
  - 4.2 Literature Review ..... 61
  - 4.3 Accountability Models in IoT Supply Chain ..... 63
    - 4.3.1 Running Examples ..... 63
    - 4.3.2 System Modeling ..... 64
    - 4.3.3 Accountability Investigation ..... 66
    - 4.3.4 Model Extensions ..... 70
  - 4.4 Case Study 1: Autonomous Truck Platooning ..... 72
    - 4.4.1 Background ..... 73
    - 4.4.2 Vehicle Dynamics Model ..... 73
    - 4.4.3 Accountability Testing ..... 75
    - 4.4.4 Parameter Analysis ..... 77
    - 4.4.5 Investigation Performance ..... 79
  - 4.5 Case Study 2: Ransomware in IoT Supply Chain ..... 81
    - 4.5.1 Background ..... 81
    - 4.5.2 Smart Lock and Ransomware Attack ..... 81
    - 4.5.3 Accountability Investigation ..... 82
  - 4.6 Compliance and Cyber Insurance ..... 87
    - 4.6.1 Compliance Modeling ..... 87
    - 4.6.2 Contract Design ..... 88
    - 4.6.3 Cyber Insurance ..... 91
  - 4.7 Conclusion ..... 101
  - References ..... 102

- 5 Computational Tools**..... 107
  - 5.1 Introduction to I-SCRAM: A Software Tool for IoT SCRM..... 107
    - 5.1.1 Supply Chain Risk Analysis and Mitigation ..... 107
  - 5.2 Case Study 1: Autonomous Vehicle..... 110
  - 5.3 Case Study 2: Industrial Control System ..... 116
  - 5.4 Conclusions and Outlooks ..... 119
  - References ..... 125
  
- Index**..... 127

# Acronyms

ACC	Adaptive Cruise Control
APT	Advanced Persistent Threat
AROC	Accountability Receiver Operating Characteristic
AUC	Area Under the AROC
BDD	Binary Decision Diagram
BMS	Building Management Systems
CAV	Connected Autonomous Vehicle
CISA	Cybersecurity and Infrastructure Security Agency
CRAC	Computer Room Air Conditioners
CRAH	Computer Room Air Handlers
DCIM	Data Center Infrastructure Management Systems
GPU	Graphical Processing Unit
HTTP	Hypertext Transfer Protocol
HVAC	Heating Ventilation and Air Conditioning
IC	Incentive Compatibility
ICT	Information and communications technology
IoT	Internet of Things
IR	Individual Rationality
IT	Information Technology
LQR	Linear Quadratic Regulator
LRT	Likelihood Ratio Test
MAP	Maximum A posteriori
NAIC	National Association of Insurance Commissioners
NIST	National Institute of Standards and Technology
OT	Operational Technology
PDU	Power Distribution Units
ROC	Receiver Operating Curve
SCRM	Supply Chain Risk Management
SLA	Service Level Agreement

SMT	Satisfiability Modulo Theories
UPS	Uninterruptible Power Supplies
WHO	World Health Organization