SpringerBriefs in Computer Science

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

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 peak 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 Timothy Kieras
Dearborn, MI, USA Junaid Farooq
Brooklyn, NY, USA Quanyan Zhu
March 2022

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

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 Aposteriori
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