

State-of-the-Art
Survey

Joanna Kołodziej
Matteo Repetto
Armend Duzha (Eds.)

LNCS 13300

Cybersecurity of Digital Service Chains

Challenges, Methodologies, and Tools

GUARD

OPEN ACCESS



Springer

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>

Joanna Kołodziej · Matteo Repetto ·
Armend Duzha (Eds.)


Cybersecurity of Digital Service Chains


Challenges, Methodologies, and Tools

 Springer

GUARD

Editors

Joanna Kołodziej 
Naukowa i Akademicka Sieć Komputerowa -
Państwowy Instytut Badawczy (NASK-PIB)
Warsaw, Poland

Matteo Repetto 
Consiglio Nazionale delle Ricerche
(IMAT-CNR)
Genoa, Italy

Armend Duzha
Maggioli Informatica
Santarcangelo di Romagna, Italy



ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-04035-1 ISBN 978-3-031-04036-8 (eBook)
<https://doi.org/10.1007/978-3-031-04036-8>

© The Editor(s) (if applicable) and The Author(s) 2022. This book is an open access publication.

Open Access This book is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this book are included in the book's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the book's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

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

Preface

Data is the key driver for the digital economy. Besides its clear business meaning, this statement accounts for most of the innovations and new paradigms introduced by the software industry in the last decade. As a matter of fact, the most remunerative business today is not the software per se, but the possibility to create value-added services for specific domains: industry, smart city, smart grid, e-Health, multimedia, etc. The real competitive advantage in this scenario is given by the agility to implement ever new digital value chains that emerge, evolve, and dissolve much faster than ever.

New computing models and software architecture have been progressively introduced to bring more agility in the creation and management of new digital services and products. The recurring buzzword that conveniently represents this attitude is “orchestration”, meaning the capability to implement (semi-)autonomous systems that are able to evolve with self-properties (self-configuration, self-management, self-healing, self-protection, etc.). Concrete achievements in this respect consist of a number of management frameworks and interfaces for cyberphysical systems and telecommunication infrastructures, including TOSCA, ETSI NFV, and FIWARE. They actually allow us to compose digital resources from multiple domains (cloud, IoT, networks, data) into high-value services in a seamless way, without caring about technical details concerning hardware and software provisioning.

The downside of this evolution is represented by cybersecurity aspects, which have not yet been addressed in a satisfactory way. Despite the effort in making software-defined systems ever more smart and autonomous, cybersecurity processes still largely depend on human skill and expertise. Relying on individuals’ ability for hardening, verification of security properties, attack detection, and threat identification is no longer practical, and it is clearly an unacceptable practice, especially when critical infrastructures and large chains are involved.

Motivated by this substantial imbalance between software management paradigms and cybersecurity models, the GUARD project has advocated the transition towards more agile security and privacy processes, which could follow the dynamics of modern digital infrastructures and services. The scope has extended to service integrity and data sovereignty, including, therefore, attack detection and data tracking aspects. The main objective is the introduction of similar models to those already used for software management, namely ones with the ability to *orchestrate* security capabilities in order to build advanced and agile detection and analytic processes. This book provides an overall review of the main concepts, architectures, technologies, and results from the GUARD project, covering both technical and non-technical aspects, i.e., legal and ethical issues.

Contents

Structured into ten complementary chapters, this book presents the current trends in service automation, data protection, attack detection and analysis, and business chain modeling, along with practical examples of using GUARD and similar platforms. The ethical

issues related to the digital business chains are also discussed. The GUARD project partners co-authored all chapters along with GUARD collaborators from the PANELFIT H2020 project and the Cracow University of Technology, who have worked together through dedicated meetings, workshops, webinars, and conferences. The chapters are summarized below.

1. Nowadays, device-centric or infrastructural-centric conventional threat mitigation methods are primarily ineffective in coping with the multitude of digital objects and service topologies involved. In the first chapter, Carrega et al. present the GUARD architecture description and motivating reasons for its advantage to security operators. They focus on many architectural model aspects, such as containerization, elasticity, and programmability, making it a novel approach to defining a modern cyber security framework for building detection and analytics services for complex digital service chains.
2. In Chapter 2, Repetto and Carrega propose a new tool called bpfFlowMon that is useful for monitoring and analyzing network flows. The authors present the state-of-the-art network flow monitoring and motivate the selection of eBPF, which is the main focus of their tool. The tool requires minimal computational resources to enable application in virtualized environments, which is a relevant research problem. The evaluation presented in the paper compares the proposed mechanism with two standard tools for this purpose, namely Zeek and nProbe. The results show that the proposed tool yields similar performance to the baselines but significantly reduces memory and CPU consumption.
3. Kołodziej et al. provide a short state-of-the-art analysis of modern Intelligent Transportation Systems (ITSs), focusing mainly on monitoring, anomaly detection, and general security mechanisms. They also provide a simple classification of anomalies and survey promising machine learning detection methods. The practical implementation of the ITS in Wolfsburg (Germany) provided by the WOBCOM company is demonstrated at the end of the chapter.
4. In Chapter 4, Krzysztoń, Lew, and Marks develop the Net Anomaly Detector (NAD) system that uses classification machine learning techniques to detect anomalies in the network traffic. NAD was integrated with the GUARD platform as a security service component and detected attacks and anomalies in TCP/IP traffic and local (customers') networks, such as the LoRa network managed by WOBCOM company in one of the GUARD use cases.
5. Unknown cyber security attacks and anomalies in the network traffic are also discussed in Chapter 5. Skopik et al. define AMiner – an open-source tool for detecting log-based anomalies. All the machine learning algorithms implemented in AMiner are feasible for deeper analysis of the monitored system or network behavior, recognizing deviations from learned models and thus spotting a wide variety of even unknown attacks.
6. Szykiewicz describes the implementation of a system to translate packet signatures into filtering rules for the eBPF framework. In particular, the solution is built around the network telescope traffic provided by the NASK Darknet Telescope. Thanks to this traffic, it is possible to collect data and detect attacks (e.g., DDoS).

Specifically, through this traffic analysis, it is possible to generate PGA signatures and automatically generate BPF code to parse likely malicious DDoS packets.

7. Wurzenberger et al. describe the approach used to implement an aggregation process to reduce the number of alerts that need to be reviewed by security analysts in the context of Intrusion Detection Systems (IDSs). In addition, all the implemented features are demonstrated by setting up an application example. The obtained results are presented using a dashboard that enables easy visualization and filtering operations management.
8. Blockchain technologies are currently viral in providing security for financial transactions and secure transmission of data and information in distributed computing environments. Blockchain was also initialized in the GUARD platform; however, more work is still required. Wilczyński and Kołodziej show in their chapter the blockchain algorithms, network, and all potential benefits from using them in several practical applications, including business chains. They have developed a new blockchain-based algorithm for scheduling tasks in distributed networks and environments, such as the GUARD platform. The blockchain mechanism in the scheduler allows improving the security aspect in data access and in scheduler itself.
9. Kozhuharova et al. provide a non-technical perspective on privacy and security aspects of modern computing paradigms. They focus on the ethical issues and define the concrete measures of protecting the privacy of data subjects that were implemented during the GUARD project lifetime with regard to the technology developed within it. What can serve as a primary recommendation, especially when creating new technologies, is to establish a list of requirements, including ethical ones, that the system must cover before any action is taken. It will ensure compliance with the ethical principles at the highest level and mitigate any adverse effect on the individuals.
10. A broader view on security and ethical aspects in general digital service chains is presented by Tronnier et al. in the last chapter of the book. The authors work on the PANELFIT H2020 project, a complementary project to GUARD. The main results from the provided analysis show that ethical challenges cannot be resolved in a general way and instead need to be discussed individually, taking into consideration the ethical principles that are violated in the specific steps of the service chains.

We hope that this book is of interest to the broad group of researchers, engineers, and professionals working in computer science and IT business units using intelligent modeling to support their interdisciplinary projects and applications in distributed cloud systems and data-intensive computing domains. We believe it contains a valuable survey of the recent modeling technologies and compelling use cases.

February 2022

Joanna Kołodziej
Matteo Repetto
Armend Duzha

Acknowledgements

We are grateful to all the contributors of this book, for their willingness to work on this interdisciplinary project. We thank the authors for their interesting proposals for the book chapters, their time and effort, and their research ideas, which makes this volume an interesting and complete state-of-the-art monograph of the latest research advances and technology development regarding next generation digital business chain support. We also would like to express our sincere thanks to the reviewers, who helped us to ensure the quality of this volume. We gratefully acknowledge their time and valuable remarks and comments.

Our special thanks go to the LNCS team of Springer Verlag for their patience, valuable editorial assistance, and excellent cooperative collaboration in this book project.

Finally, we would like to express our warmest gratitude to our friends and families for their patience, love, and support in the preparation of this volume.



Funded by the Horizon 2020 Framework Programme
of the European Union

Contents

A Reference Architecture for Management of Security Operations in Digital Service Chains	1
<i>Alessandro Carrega, Giovanni Grieco, Domenico Striccoli, Manos Papoutsakis, Tomas Lima, José Ignacio Carretero, and Matteo Repetto</i>	
Monitoring Network Flows in Containerized Environments	32
<i>Matteo Repetto and Alessandro Carrega</i>	
Intelligent Transportation Systems – Models, Challenges, Security Aspects	56
<i>Joanna Kołodziej, Cornelio Hopmann, Giovanni Coppa, Daniel Grzonka, and Adrian Widłak</i>	
NAD: Machine Learning Based Component for Unknown Attack Detection in Network Traffic	83
<i>Mateusz Krzysztoń, Marcin Lew, and Michał Marks</i>	
Detecting Unknown Cyber Security Attacks Through System Behavior Analysis	103
<i>Florian Skopik, Markus Wurzenberger, and Max Landauer</i>	
Signature-Based Detection of Botnet DDoS Attacks	120
<i>Paweł Szykiewicz</i>	
Automatic Attack Pattern Mining for Generating Actionable CTI Applying Alert Aggregation	136
<i>Markus Wurzenberger, Max Landauer, Agron Bajraktari, and Florian Skopik</i>	
Blockchain-Based Task and Information Management in Computational Cloud Systems	162
<i>Andrzej Wilczyński and Joanna Kołodziej</i>	
Ethics in Cybersecurity. What Are the Challenges We Need to Be Aware of and How to Handle Them?	202
<i>Denitsa Kozhuharova, Atanas Kirov, and Zhanin Al-Shargabi</i>	
A Discussion on Ethical Cybersecurity Issues in Digital Service Chains	222
<i>Frédéric Tronnier, Sebastian Pape, Sascha Löbner, and Kai Rannenber</i>	
Author Index	257