SpringerBriefs in Applied Sciences and Technology

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 publications can be:

- A timely report of state-of-the art methods
- An introduction to or a manual for the application of mathematical or computer techniques
- A bridge between new research results, as published in journal articles
- A snapshot of a hot or emerging topic
- An in-depth case study
- A presentation of core concepts that students must understand in order to make independent contributions

SpringerBriefs are characterized by fast, global electronic dissemination, standard publishing contracts, standardized manuscript preparation and formatting guidelines, and expedited production schedules.

On the one hand, **SpringerBriefs in Applied Sciences and Technology** are devoted to the publication of fundamentals and applications within the different classical engineering disciplines as well as in interdisciplinary fields that recently emerged between these areas. On the other hand, as the boundary separating fundamental research and applied technology is more and more dissolving, this series is particularly open to trans-disciplinary topics between fundamental science and engineering.

Indexed by EI-Compendex, SCOPUS and Springerlink.

More information about this series at https://link.springer.com/bookseries/8884

Benjamin Aziz

Formal Analysis by Abstract Interpretation

Case Studies in Modern Protocols

Springer

Benjamin Aziz
School of Computing
University of Portsmouth
Portsmouth, UK

ISSN 2191-530X ISSN 2191-5318 (electronic)
SpringerBriefs in Applied Sciences and Technology
ISBN 978-3-030-91152-2 ISBN 978-3-030-91153-9 (eBook)
https://doi.org/10.1007/978-3-030-91153-9

© 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 my loving family

Preface

The book outlines how formal static analysis techniques can be defined and applied to modern protocols related to new paradigms such as the IoT, Industry 4.0 and Smart Energy. The application of such robust techniques can lead to better understanding of modern-day protocols and systems, both within the context of classical requirements, such as functional security, and the more challenging properties related to the presence of vulnerabilities at levels of specification and design. The book challenges current mainstream thinking that large-scale systems are simply infeasible and non-suitable case studies for formal analysis techniques, and goes to demonstrate that such systems can benefit from the application of such techniques.

The book gives us a static analysis framework with a focus on capturing name substitutions occurring as a result of processes communicating with one another. First, a non-standard denotational semantics for the formal language is constructed based on domain theory. The semantics is shown to be sound with respect to transitions in the standard structural operational semantics. Finally, the non-standard semantics is abstracted to operate over finite domains so as to ensure the termination of the static analysis. The safety of the abstract semantics is proven with respect to the non-standard semantics. This framework demonstrates that the choice of the name-substitution property is a fundamental one, in that it can be used to understand a wide range of system and protocol properties ranging from security and safety-related ones to testing coverage to mutation-based properties. As such, the book lays down a simple but effective method for the static analysis of systems and protocols that go beyond simple toy examples into the realm of complex systems.

One of the main motivations in writing this book was to give the reader the benefit of understanding how a highly theoretical area in computer science can have applications in complex industrial settings, two universes that are often hard to combine. More specifically, it is envisaged that the readers will first gain knowledge and experience of the abstract interpretation method of formal analysis, and how it can be varied, to express various properties, and applied for different purposes, for example, in testing, mutation and semantic ambiguity resolution contexts. Second, they will be challenged to think of how such method can be used in analysing modern protocols, in other words, protocols of significance of complexity as opposed to the majority of

current literature that applies only to toy-style protocols. The expectation is that the book will encourage readers, in particular those working in research, to think and reflect on new directions for future research benefiting from the approach discussed throughout.

The book is composed of five chapters along with the introduction (Chap. 1) and the conclusion (Chap. 7). From these five chapters, the first two (Chaps. 2 and 3) define the formal language and its denotational semantics, both concrete and abstract, and hence are an essential reading in order to understand any of the three case studies presented in the following three chapters (Chaps. 4–6). The case studies themselves can be read individually, in any order, and according to the needs of the reader, as they are not inter-related.

The primary audience of this book is the academic community (postgraduate and researchers), particularly at the intersection of formal methods, IoT systems, networks and program analysis areas. The book is also suitable for the industrial research community, particularly those working with the IoT and communication networks research. Finally, the book is also expected to be useful to anyone interested in the standardisation of protocols, particularly, IoT and Industry 4.0 protocol standards.

Special thanks to my Ph.D. supervisor, Dr. Geoff Hamilton, whose comments and feedback over the years were inspirational in defining the static analysis framework.

Basingstoke, UK Benjamin Aziz
September 2021

Contents

Acronyms

BNF	Backus–Naur Form
CA	Certification Authority
CCS	Calculus of Communicating Systems
CFA	Control Flow Analysis
CoAP	Constrained Application Protocol
CoSeC	Compositional Security Checker
CPO	Complete Partial Order
CPS	Cyber-Physical System
CS	Charging Station
CSMS	Charging Station Management System
CSP	Communicating Sequential Processes
EV	Electric Vehicle
EVSE	Electric Vehicle Supply Equipment
FTP	File Transfer Protocol
HTML	HyperText Markup Language
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPC	Institute for Printed Circuits
IPC-CFX	Institute for Printed Circuits Connected Factory Exchange
LAN	Local Area Network
LF	(Edinburgh) Logical Framework
LMAC	Lightweight Medium Access
MiM	Man-in-the-Middle
ML	Meta-Language
MMC	Mobility Model Checker
MOM	Message Oriented Middleware
MQTT	Message Queuing Telemetry Transport
OASIS	Organization for the Advancement of Structured Information Standards
OCA	Open Charge Alliance
OCPP	Open Charge Point Protocol

OPC	Open Platform Communications
PCB	Printed Circuit Board
PKI	Public Key Infrastructure
PPMP	Production Performance Management Protocol
QoS	Quality of Service
RD	Reaching Definitions
RFID	Radio Frequency Identification
RMI	Remote Method Invocation
RPC	Remote Procedure Call
SMV	Symbolic Model Checking
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UML	Unified Modelling Language
VDL	Vienna Definition Language