Lecture Notes in Computer Science 13066

More information about this subseries at http://www.springer.com/series/7410

Daniel Dougherty · José Meseguer ·
Sebastian Alexander Mödersheim ·
Paul Rowe (Eds.)

Protocols, Strands, and Logic

Essays Dedicated to Joshua Guttman on the Occasion of his 66.66th Birthday

Springer

Editors
Daniel Dougherty
Department of Computer Science
Worcester Polytechnic Institute
Worcester, MA, USA

Sebastian Alexander Mödersheim
Institute of Mathematics and Computer Science
Technical University of Denmark
Kongens Lyngby, Denmark

José Meseguer
Th.M. Siebel Center for Computer Science
University of Illinois Urbana-Champaign
Urbana, IL, USA

Paul Rowe
J83K
The MITRE Corporation
Bedford, MA, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-91630-5 ISBN 978-3-030-91631-2 (eBook)
https://doi.org/10.1007/978-3-030-91631-2

LNCS Sublibrary: SL4 – Security and Cryptology

Cover Illustration: CPSA output from Joshua Guttman's work.

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

Joshua D. Guttman

Preface

This volume contains papers written in honor of Dr. Joshua Guttman on the occasion of his 66.66th birthday, in recognition of his seminal contributions to the foundations of computer security and in celebration of the generosity of spirit that his friends and colleagues have enjoyed over many years.

Joshua, as Research Professor at Worcester Polytechnic Institute and Senior Principal Researcher at The MITRE Corporation, has been for many years a leader in the field of formal methods for security. He has generated foundational notions and results and has led the development of several tools for the analysis of systems. Through this entire time he has been a vital presence in the global community, forming collaborations, facilitating the creation and maintenance of conferences and workshops, and mentoring young researchers.

Computer security has become a rich and varied field, with an ever-expanding array of problems and techniques for their solution. Security protocols, sometimes called cryptographic protocols, are communication protocols designed to achieve goals such as authentication, confidentiality, and integrity. The problem of reasoning about security protocols has received considerable attention over the past 30 years and various algorithms and tools for checking security properties have been developed. A notable aspect of research in security is that it features the interaction between sophisticated mathematical theories and powerful software tools.

Perhaps Joshua's most influential and enduring contribution to the field has been the development of the strand space formalism for analyzing cryptographic protocols. It is one of several "symbolic approaches" to security protocol analysis in which the underlying details of cryptographic primitives are abstracted away, allowing a focus on potential flaws in the communication patterns between participants. In the strand space formalism, the history of individual protocol participants is organized into patterns of message transmissions and receptions called "strands." A network adversary's capabilities are naturally represented by strands as well. The strand space formalism lies at the foundation of at least three separate automated protocol analysis tools (CPSA, Maude-NPA, and Scyther).

The characteristic feature of Joshua's research approach is the recognition of the core principles involved in a research question and the consequent emphasis on understanding these key elements. This has resulted in research contributions to a variety of domains beyond the confines of cryptographic protocol analysis, including such topics as policy analysis for Security Enhanced Linux and Software Defined Networks, information flow, and remote attestation.

His attention to the underlying logic of strand spaces has also allowed him to merge domain-specific reasoning about protocols with general purpose, first-order logical theories. This enables analyses that explore the protocol in the base theory of strand spaces, but also reason about higher-level system processes (e.g. policies based on the protocols) in the more generic logic.

Indeed, this has led to recent work that weaves many of the threads of research described above into a single approach for analyzing Intel's SGX attestation mechanism. The power of Joshua's clarity of thought is exemplified by this combination of protocol analysis, remote attestation, and policy analysis ideas into a single approach.

The identification of clear principles in a domain paves the way to automated reasoning, and Joshua has been a leader in the development and distribution of several tools for security analysis.

Joshua is a principal architect of the Cryptographic Protocol Shapes Analyzer (CPSA). The crucial aspect of CPSA is that it provides users with the ability to play "what if?" with protocols. Users not trained in formal logic can explore the expected—and unexpected—behaviors of a protocol without necessarily having to specify formal properties they hope to be true.

In the mid 2000's Dr. Guttman, with coworkers at MITRE, designed the Cryptographic Protocol Programming Language (CPPL), a domain-specific programming language for expressing cryptographic protocols. The key innovation of CPPL is the ability to associate trust management assertions with protocol actions, so that the actions of each agent are compatible with its own trust policy.

The Security-Enhanced Linux Analysis Tool (SLAT), he developed with colleagues in the early 2000's, is a tool for verifying information-flow properties of access-control policies in the highly-influential SELinux operating system.

In the early 1990's Joshua, with colleagues William Farmer and F. Javier Thayer, developed the Interactive Mathematical Proof System (IMPS). IMPS was a novel approach to interactive theorem proving, based on higher-order classical logic, an interesting treatment of partiality, and proof tactics.

Alongside Joshua's research contributions stands the equally important impact he has had through his service and personal relationships with members of the community. Joshua was one of the founders of the Computer Security Foundations Workshop (now Symposium), and of the Principles of Security and Trust workshop. As a faculty member at Worcester Polytechnic Institute he has advised undergraduate and graduate students, at MITRE he has worked with a stream of summer interns and beginning researchers, and he routinely serves as an external committee member on international PhD committees.

We are honored to consider Joshua a colleague and friend, and it has been a pleasure to edit this volume celebrating his achievements. We thank all the authors who contributed articles and also those who helped us review them.

December 2021

Daniel Dougherty
José Meseguer
Sebastian Mödersheim
Paul Rowe

Contents