Lecture Notes in Computer Science 11565

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Joshua D. Guttman · Carl E. Landwehr ·
José Meseguer · Dusko Pavlovic (Eds.)

Foundations of Security, Protocols, and Equational Reasoning

Essays Dedicated to Catherine A. Meadows

Springer

Editors

Joshua D. Guttman
Worcester Polytechnic Institute
Worcester, MA, USA

Carl E. Landwehr
George Washington University
Washington, DC, USA

José Meseguer
University of Illinois
Urbana, IL, USA

Dusko Pavlovic
University of Hawai'i
Honolulu, HI, USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-19051-4 ISBN 978-3-030-19052-1 (eBook)
https://doi.org/10.1007/978-3-030-19052-1

LNCS Sublibrary: SL4 – Security and Cryptology

Cover illustration: Composite Privacy Protocol: Social Networking (SNet), p. 184

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

Catherine A. Meadows

Preface

This volume contains the papers presented at the Catherine Meadows Festschrift Symposium held during May 22–23, 2019, in Fredericksburg, Virginia.

Dr. Catherine A. Meadows, Head of the Formal Methods Group at the US Naval Research Laboratory (NRL) in Washington, D.C., has been—since the very inception of the field—a key leading researcher in formal specification and verification of cryptographic protocols. Her research ideas continue to have immense influence in shaping and advancing it.

The pervasiveness of cryptographic protocols in a massively interconnected world makes their security a direct concern, not just for governments and businesses, but also for the lives of billions of people worldwide. Formal approaches to cryptographic protocol verification are important, since even rigorous review and testing of these protocols has repeatedly failed to reveal significant vulnerabilities. The key technical point is that, even under the optimistic assumption that the cryptographic primitives used by a communication protocol cannot be broken, the protocol itself can be broken. That is, a malicious attacker can still sometimes obtain the secret information sent by an honest user without violating the protocol's specification. This subversion is typically achieved by a so-called man-in-the-middle attack. Since communication—for example, wireless or Internet communication—can often be intercepted, an attacker can listen to various communications and maliciously participate in them, impersonating various participants at various times. In this way, the attacker can obtain correctly encrypted pieces of information, combine and use them in clever ways, and reveal protected information or obtain unauthorized capabilities. Well-tested protocols have fallen victim to subtle attacks after years of practical use, dramatically demonstrating that testing by itself is not a reliable method to ensure security. Some of Dr. Meadows's most important contributions have been precisely in the development of formal specification and verification methods and tools that can uncover such subtle attacks by a systematic formal analysis that exhaustively considers all the possible malicious actions of an attacker.

This kind of formal verification is quite challenging for at least three reasons: (1) the number of actions an attacker can perform is unbounded; (2) the number of protocol sessions an attacker can participate in to obtain and combine information from various users to mount an attack is likewise unbounded; and (3) the algebraic properties of the cryptographic functions employed by the protocol can also be used by an intruder to mount even more subtle attacks. What is challenging about issues (1)–(3) is that they make it difficult to automatically verify protocols by standard model checking methods, since standard model checkers assume a finite set of reachable states, which is ruled out by both (1) and (2).

Dr. Meadows has been a pioneer in developing symbolic formal verification methods and tools that are automatic and overcome the above difficulties. Her methods can be described as a novel form of symbolic model checking of infinite-state systems that exploits the specific properties of cryptographic protocols. By using a symbolic expression to stand for a typically infinite set of concrete protocol states, both difficulties (1) and (2) can be overcome. And by reasoning symbolically about the algebraic properties of the protocol's cryptographic functions using equational unification and narrowing methods, difficulty (3) can likewise be overcome. In the 1990s, Dr. Meadows first embodied these symbolic model checking techniques in her NRL Protocol Analyzer, a tool and methodology that has been fruitfully applied to the analysis of many protocols and protocol standards and has had an enormous influence in the field. Although protocol security is an undecidable problem, by using very powerful state reduction techniques based on grammars, the NRL Protocol Analyzer was able in a good number of cases to terminate its exhaustive symbolic analysis of a given protocol security property with either an actual attack or an absence of attacks that, by the exhaustive nature of the analysis, proved the desired property.

The NRL Protocol Analyzer could reason modulo some algebraic properties of cryptographic functions, but a variety of other such properties were outside its scope. In her more recent research on the Maude-NPA tool, she and her collaborators have made key contributions to overcoming challenge (3) by endowing such a tool with powerful symbolic methods to reason modulo the algebraic properties of a wide variety of cryptographic functions. Maude-NPA has been highly innovative in enabling analysis for cryptographic protocols whose primitive operators satisfy quite a general range of algebraic properties. Actually, algebraic theories in Maude-NPA are user-definable, so new ones can be defined and combined by the user under quite general assumptions. In particular, Maude-NPA has been used to analyze a wide variety of cryptographic protocols whose algebraic properties, besides the usual theories for encryption and decryption, can include and combine complex algebraic theories such as exclusive or, Diffie–Hellman exponentiation, homomorphic encryption, and associativity of string concatenation. Furthermore, besides verifying secrecy and authentication properties, Maude-NPA has also been used to analyze protocol indistinguishability properties, and to reason not just about protocols, but also about protocol compositions and cryptographic APIs.

Dr. Meadows's research contributions go far beyond the brief outline sketched out here. She has, for example, developed a new temporal logic to specify protocol properties as well as new methods for analyzing various kinds of properties beyond secrecy, such as authentication and resilience under denial of service (DoS) attacks. Similarly, she has also developed compositional methods to specify and reason about larger protocols obtained by composing smaller ones, and has made important contributions in other areas such as wireless protocol security, intrusion detection, and the relationship between computational and symbolic approaches to cryptography. Her early cryptography work on rank schemes has also had a great impact and is very highly cited.

In advancing these and various other research directions, she has successfully enlisted the collaboration of many other colleagues in both the US and Europe. Such collaborations, many of them ongoing, have widened the depth and breadth of her contributions, multiplying the impact of her ideas. In particular, under her leadership for more than 20 years, researchers at NRL's Formal Methods Group have made pioneering research contributions to security in a wide range of topics. Given her international stature in the field, she is constantly asked to chair or serve on program committees of many international scientific conferences in her area, and also to serve in an advisory capacity in many US and international research organizations.

For us it has been a great pleasure not only to work with Dr. Meadows, but to edit this Festschrift volume and, with the collaboration of Dr. Andrew Marshall at the University of Mary Washington, to organize this symposium in Fredericksburg, Virginia, to honor Dr. Meadows. We would like to thank UMW for their excellent hospitality at the event. We deeply appreciate Andrew Marshall's work arranging the event.

We are grateful to the National Security Agency and to the National Science Foundation (SFS grant number 1662487), for providing the funding that made this event possible.

Thanks to all the researchers from Europe and North America who have contributed research papers for this volume and will present them at the symposium, as well as all other researchers participating in it; this Festschrift volume and the symposium itself will be important scientific events providing a unique opportunity for serious reflection on the long-term evolution and future prospects of research in cryptographic protocol specification and verification that Dr. Meadows has done so much to advance.

March 2019

Joshua Guttman
Carl Landwehr
José Meseguer
Dusko Pavlovic

Contents