## Table of Contents

**Preface** vii

**Committees** viii

**Reviewers** x

### Security Protocol Verification I

Guiding a General-Purpose C Verifier to Prove Cryptographic Protocols .................................................. 3  
**François Dupressoir, Andrew D. Gordon, Jan Jürjens, and David A. Naumann**

Integrated Specification and Verification of Security Protocols and Policies ........................................... 18  
**Simone Frau and Mohammad Torabi-Dashti**

StatVerif: Verification of Stateful Processes .................................................................................. 33  
**Myrto Arapinis, Eike Ritter, and Mark D. Ryan**

### Security Protocol Verification II

Automated Proofs for Diffie-Hellman-Based Key Exchanges ................................................................. 51  
**Long Ngo, Colin Boyd, and Juan González Nieto**

Formal Analysis of Protocols Based on TPM State Registers ............................................................ 66  
**Stéphanie Delaune, Steve Kremer, Mark D. Ryan, and Graham Steel**

### Authorization and Security Policies

Resource-Aware Authorization Policies for Statically Typed Cryptographic Protocols .......................... 83  
**Michele Bugliesi, Stefano Calzavara, Fabienne Eigner, and Matteo Maffei**

**David Basin, Samuel J. Burri, and Günter Karjoth**

Dynamic Enforcement of Knowledge-Based Security Policies .................................................. 114  
**Piotr Mardziel, Stephen Magill, Michael Hicks, and Mudhakar Sivatsa**
Language-Based Security
Modular Protections against Non-control Data Attacks .................................................................131
   Cole Schlesinger, Karthik Pattabiraman, Nikhil Swamy, David Walker,
   and Benjamin Zorn
Static Analysis for Efficient Hybrid Information-Flow Control ......................................................146
   Scott Moore and Stephen Chong
Local Memory via Layout Randomization ......................................................................................161
   Radha Jagadeesan, Corin Pitcher, Julian Rathke, and James Riely

Information Flow
A Statistical Test for Information Leaks Using Continuous Mutual Information .................................177
   Tom Chothia and Apratim Guha
Information-Theoretic Bounds for Differentially Private Mechanisms ..............................................191
   Gilles Barthe and Boris Köpf
The Complexity of Quantitative Information Flow Problems ..........................................................205
   Pavol Cerný, Krishnendu Chatterjee, and Thomas A. Henzinger
Assumptions and Guarantees for Compositional Noninterference ......................................................218
   Heiko Mantel, David Sands, and Henning Sudbrock

Security Notions and Specifications
Vertical Protocol Composition ..............................................................................................................235
   Thomas Groß and Sebastian Mödersheim
Termination-Insensitive Computational Indistinguishability (and Applications
to Computational Soundness) ..................................................................................................251
   Dominique Unruh
Security for Key Management Interfaces .........................................................................................266
   Steve Kremer, Graham Steel, and Bogdan Warinschi
A Formal Framework for Provenance Security ...................................................................................281
   James Cheney

Privacy and Anonymity
Attacking and Fixing Helios: An Analysis of Ballot Secrecy ...........................................................297
   Véronique Cortier and Ben Smyth
Regret Minimizing Audits: A Learning-Theoretic Basis for Privacy Protection ...............................312
   Jeremiah Blocki, Nicolas Christin, Anupam Datta, and Arunesh Sinha

Author Index .....................................................................................................................................329