Table of Contents

Preface ............................................................................................................................................................... viii
Committees ........................................................................................................................................................ ix

Language-Based Security

Language Based Secure Communication .................................................................................................................. 3
  Michele Bugliesi and Riccardo Focardi

Refinement Types for Secure Implementations ................................................................................................... 17
  Jesper Bengtson, Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon,
  and Sergio Maffeis

A Trust Management Approach for Flexible Policy Management
in Security-Typed Languages ......................................................................................................................... 33
  Sruthi Bandhakavi, William Winsborough, and Marianne Winslett

Security Models in Theory and Practice

Hyperproperties .................................................................................................................................................... 51
  Michael R. Clarkson and Fred B. Schneider

Security Decision-Making among Interdependent Organizations ......................................................................... 66
  R. Ann Miura-Ko, Benjamin Yolken, John Mitchell, and Nicholas Bambos

Declassification and Erasure

Tractable Enforcement of Declassification Policies .......................................................................................... 83
  Gilles Barthe, Salvador Cavadini, and Tamara Rezk
End-to-End Enforcement of Erasure and Declassification ................................................................. 98
Stephen Chong and Andrew C. Myers

CSF/LICS Joint Invited Talk
Cryptographically-Sound Protocol-Model Abstractions ............................................................... 115
Christoph Sprenger and David Basin

Authorization Logic I
An Authorization Logic with Explicit Time .............................................................. 133
Henry DeYoung, Deepak Garg, and Frank Pfenning

Authorization Logic II
DKAL: Distributed-Knowledge Authorization Language ...................................................... 149
Yuri Gurevich and Itay Neeman
Access-Control Policies via Belnap Logic: Effective and Efficient Composition and Analysis ............................................ 163
Glenn Bruns and Michael Huth
Evidence-Based Audit ........................................................................................................ 177
Jeffrey A. Vaughan, Limin Jia, Karl Mazurak, and Steve Zdancewic

Protocol Analysis I
Automated Verification of Remote Electronic Voting Protocols in the Applied Pi-Calculus ............................................. 195
Michael Backes, Cătălin Hrițcu, and Matteo Maffei
Specifying Secure Transport Layers ..................................................................................... 210
Christopher Dilloway and Gavin Lowe
Towards Producing Formally Checkable Security Proofs, Automatically .................................. 224
Jean Goubault-Larrecq
Composition of Password-Based Protocols ........................................................................ 239
Stéphanie Delaune, Steve Kremer, and Mark Ryan
Cryptographic Foundations

Computational Soundness of Symbolic Zero-Knowledge Proofs against Active Attackers

Michael Backes and Dominique Unruh

Joint State Theorems for Public-Key Encryption and Digital Signature Functionalities with Local Computation

Ralf Küsters and Max Tuengerthal

Information Flow and Concurrency

A Type System for Observational Determinism

Tachio Terauchi

Information Flow in Systems with Schedulers

Ron van der Meyden and Chenyi Zhang

Protocol Analysis II

A Correctness Proof of a Mesh Security Architecture

Doug Kuhlman, Ryan Moriarty, Tony Braskich, Steve Emeott, and Mahesh Tripunitara

Formal Analysis of PKCS#11

Stéphanie Delaune, Steve Kremer, and Graham Steel

Author Index