Contents

Information Flow

Timing-Sensitive Noninterference through Composition .......................... 3
  Willard Rafnsson, Limin Jia, and Lujo Bauer

Quantifying Vulnerability of Secret Generation Using Hyper-Distributions . . 26
  Mário S. Alvim, Piotr Mardziel, and Michael Hicks

A Principled Approach to Tracking Information Flow in the Presence of Libraries ................................................................. 49
  Daniel Hedin, Alexander Sjösten, Frank Piessens, and Andrei Sabelfeld

Secure Multi-party Computation: Information Flow of Outputs and Game Theory ................................................................. 71
  Patrick Ah-Fat and Michael Huth

Security Protocols

Automated Verification of Dynamic Root of Trust Protocols ..................... 95
  Sergiu Bursuc, Christian Johansen, and Shiwei Xu

Beyond Subterm-Convergent Equational Theories in Automated Verification of Stateful Protocols ................................................. 117
  Jannik Dreier, Charles Duménil, Steve Kremer, and Ralf Sasse

On Communication Models When Verifying Equivalence Properties .......... 141
  Kushal Babel, Vincent Cheval, and Steve Kremer

A Survey of Attacks on Ethereum Smart Contracts (SoK) ....................... 164
  Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli

Security Policies

Security Analysis of Cache Replacement Policies .................................. 189
  Pablo Cañones, Boris Köpf, and Jan Reineke

Model Checking Exact Cost for Attack Scenarios .................................. 210
  Zaruhi Aslanyan and Flemming Nielson

Postulates for Revocation Schemes .................................................... 232
  Marcos Cramer and Giovanni Casini
Defense in Depth Formulation and Usage in Dynamic Access Control

Ridha Khedri, Owain Jones, and Mohammed Alabbad

253

Information Leakage

Compositional Synthesis of Leakage Resilient Programs

Arthur Blot, Masaki Yamamoto, and Tachio Terauchi

277

Combining Differential Privacy and Mutual Information for Analyzing Leakages in Workflows

Martin Pettai and Peeter Laud

298

Author Index

321
Principles of Security and Trust
Maffei, M.; Ryan, M. (Eds.)
2017, XII, 321 p. 59 illus., Softcover
ISBN: 978-3-662-54454-9