

Contents

Information Flow

Timing-Sensitive Noninterference through Composition	3
<i>Willard Rafnsson, Limin Jia, and Lujo Bauer</i>	
Quantifying Vulnerability of Secret Generation Using Hyper-Distributions . . .	26
<i>Mário S. Alvim, Piotr Mardziel, and Michael Hicks</i>	
A Principled Approach to Tracking Information Flow in the Presence of Libraries	49
<i>Daniel Hedin, Alexander Sjösten, Frank Piessens, and Andrei Sabelfeld</i>	
Secure Multi-party Computation: Information Flow of Outputs and Game Theory	71
<i>Patrick Ah-Fat and Michael Huth</i>	

Security Protocols

Automated Verification of Dynamic Root of Trust Protocols	95
<i>Sergiu Bursuc, Christian Johansen, and Shiwei Xu</i>	
Beyond Subterm-Convergent Equational Theories in Automated Verification of Stateful Protocols.	117
<i>Jannik Dreier, Charles Duménil, Steve Kremer, and Ralf Sasse</i>	
On Communication Models When Verifying Equivalence Properties	141
<i>Kushal Babel, Vincent Cheval, and Steve Kremer</i>	
A Survey of Attacks on Ethereum Smart Contracts (SoK)	164
<i>Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli</i>	

Security Policies

Security Analysis of Cache Replacement Policies	189
<i>Pablo Cañones, Boris Köpf, and Jan Reineke</i>	
Model Checking Exact Cost for Attack Scenarios	210
<i>Zaruhi Aslanyan and Flemming Nielson</i>	
Postulates for Revocation Schemes	232
<i>Marcos Cramer and Giovanni Casini</i>	

Defense in Depth Formulation and Usage in Dynamic Access Control. 253
Ridha Khedri, Owain Jones, and Mohammed Alabbad

Information Leakage

Compositional Synthesis of Leakage Resilient Programs 277
Arthur Blot, Masaki Yamamoto, and Tachio Terauchi

Combining Differential Privacy and Mutual Information
for Analyzing Leakages in Workflows. 298
Martin Pettai and Peeter Laud

Author Index 321

Principles of Security and Trust

6th International Conference, POST 2017, Held as Part
of the European Joint Conferences on Theory and
Practice of Software, ETAPS 2017, Uppsala, Sweden,
April 22-29, 2017, Proceedings

Maffei, M.; Ryan, M. (Eds.)

2017, XII, 321 p. 59 illus., Softcover

ISBN: 978-3-662-54454-9