Table of Contents

Message from the General Chair ix
Committees xi
Reviewers xiii

Session: Security Protocols 1

An Extensive Formal Analysis of Multi-factor Authentication Protocols 1
Charlie Jacomme (LSV & CNRS & ENS Paris-Saclay & Inria & Université Paris-Saclay) and Steve Kremer (LORIA, Inria Nancy-Grand Est & CNRS & Université de Lorraine)

Composition Theorems for CryptoVerif and Application to TLS 1.3 16
Bruno Blanchet (Inria)

A Cryptographic Look at Multi-party Channels 31
Patrick Eugster (University of Lugano), Giorgia Azzurra Marson (Nec Laboratories Europe), and Bertram Poettering (Royal Holloway, University of London)

Invited Paper: Secure Boot and Remote Attestation in the Sanctum Processor 46
Ilia Lebedev (Massachusetts Institute of Technology), Kyle Hogan (Massachusetts Institute of Technology), and Srinivas Devadas (Massachusetts Institute of Technology)

Guided Design of Attack Trees: A System-Based Approach 61
Maxime Audinot (Univ Rennes, CNRS, IRISA), Sophie Pinchinat (Univ Rennes, CNRS, IRISA), and Barbara Kordy (Univ Rennes, INSA Rennes, CNRS, IRISA)

Session: Cryptographic Primitives

Self-Guarding Cryptographic Protocols against Algorithm Substitution Attacks 76
Marc Fischlin (Technische Universität Darmstadt) and Sogol Mazaheri (Technische Universität Darmstadt)

Formal Security Proof of CMAC and Its Variants 91
Cécile Baritel-Ruet (UCA (Université Côte d’Azur), INRIA Sophia-Antipolis), François Dupressoir (University of Surrey), Pierre-Alain Fouque (Université de Rennes 1, Rennes, France), and Benjamin Gregoire (INRIA)
Backdoored Hash Functions: Immunizing HMAC and HKDF 105

Marc Fischlin (Technische Universität Darmstadt), Christian Janson (Technische Universität Darmstadt), and Sogol Mazaheri (Technische Universität Darmstadt)

Session: Secure Computation

Computer-Aided Proofs for Multiparty Computation with Active Security 119

Helene Haagh (Aarhus University), Aleksandr Karbyshev (Aarhus University), Sabine Oechsner (Aarhus University), Bas Spitters (Aarhus University), and Pierre-Yves Strub (Ecole Polytechnique)

Enforcing Ideal-World Leakage Bounds in Real-World Secret Sharing MPC Frameworks 132

José Bacelar Almeida (INESC TEC and Universidade do Minho, Portugal), Manuel Barbosa (INESC TEC and FCUP Universidade do Porto, Portugal), Gilles Barthe (IMDEA Software Institute, Spain), Hugo Pacheco (INESC TEC and Universidade do Minho, Portugal), Vitor Pereira (INESC TEC and FCUP Universidade do Porto, Portugal), and Bernardo Portela (INESC TEC and FCUP Universidade do Porto, Portugal)

Symbolic Security of Garbled Circuits 147

Baiyu Li (UC San Diego) and Daniele Micciancio (UC San Diego)

Session: Knowledge and Hyperproperties

The Complexity of Monitoring Hyperproperties 162

Borzoo Bonakdarpour (Iowa State University) and Bernd Finkbeiner (Saarland University)

Knowledge-Based Security of Dynamic Secrets for Reactive Programs 175

McKenna McCall (Carnegie Mellon University), Hengruo Zhang (Carnegie Mellon University), and Limin Jia (Carnegie Mellon University)

Assuming You Know: Epistemic Semantics of Relational Annotations for Expressive Flow Policies 189

Andrey Chudnov (D. E. Shaw & Co., L.P.) and David A. Naumann (Stevens Institute of Technology)

KEVM: A Complete Formal Semantics of the Ethereum Virtual Machine 204

Everett Hildenbrandt (University of Illinois at Urbana-Champaign), Manasvi Saxena (University of Illinois at Urbana-Champaign), Nishant Rodrigues (University of Illinois at Urbana-Champaign), Xiaoran Zhu (University of Illinois at Urbana-Champaign), Philip Daian (Runtime Verification, Inc.), Dwight Guth (Runtime Verification, Inc.), Brandon Moore (Runtime Verification, Inc.), Daejun Park (University of Illinois at Urbana-Champaign), Yi Zhang (University of Illinois at Urbana-Champaign), Andrei Stefanescu (Runtime Verification, Inc.), and Grigore Rosu (University of Illinois at Urbana-Champaign)
Session: Information Flow

A Permission-Dependent Type System for Secure Information Flow Analysis .218
Hongxu Chen (Nanyang Technological University), Alwen Tiu (Australian
National University), Zhiwu Xu (Shenzhen University), and Yang Liu
(Nanyang Technological University)

Types for Information Flow Control: Labeling Granularity and Semantic Models .233
Vineet Rajani (Max Planck Institute for Software Systems) and Deepak
Garg (Max Planck Institute for Software Systems)

Inductive Invariants for Noninterference in Multi-agent Workflows .247
Christian Müller (Technische Universität München), Helmut Seidl
(Technische Universität München), and Eugen Zlinescu (Technische
Universität München)

Invited Paper: Local Differential Privacy on Metric Spaces: Optimizing the Trade-Off with
Utility .262
Mário Alvim (UFMG, Belo Horizonte, Brazil), Konstantinos
Chatzikokolakis (CNRS, France), Catuscia Palamidessi (INRIA, France),
and Anna Pazii (INRIA and École Polytechnique, France)

Privacy Risk in Machine Learning: Analyzing the Connection to Overfitting .268
Samuel Yeom (Carnegie Mellon University), Irene Giacomelli (University
of Wisconsin--Madison), Matt Fredrikson (Carnegie Mellon University),
and Somesh Jha (University of Wisconsin--Madison)

Session: Electronic Voting

Alethea: A Provably Secure Random Sample Voting Protocol .283
David Basin (ETH Zürich), Saša Radomirović (University of Dundee,
United Kingdom), and Lara Schmid (ETH Zürich)

Machine-Checked Proofs for Electronic Voting: Privacy and Verifiability for Belenios .298
Véronique Cortier (LORIA, CNRS & Inria & Université de Lorraine),
Constantin Cîlin Drgan (University of Surrey), François Dupressoir
(University of Surrey), and Bogdan Warinschi (University of Bristol)

Session: Side Channels

Symbolic Side-Channel Analysis for Probabilistic Programs .313
Pasquale Malacaria (Queen Mary University of London, UK), MHR Khouzani
(Queen Mary University of London, UK), Corina S. Pasareanu (Carnegie
Mellon University, USA), Quoc-Sang Phan (Fujitsu Laboratories of
America, USA), and Kasper Luckow (Carnegie Mellon University, USA)

Secure Compilation of Side-Channel Countermeasures: The Case of Cryptographic
“Constant-Time” .328
Gilles Barthe (IMDEA Software Institute, Madrid, Spain), Benjamin
Grégoire (Inria, Sophia-Antipolis, France), and Vincent Laporte (IMDEA
Software Institute, Madrid, Spain)
Session: Security Protocols 2

A Little More Conversation, a Little Less Action, a Lot More Satisfaction: Global States in ProVerif 344

Vincent Cheval (Inria Nancy - Grand Est, Loria, France), Véronique Cortier (CNRS, LORIA, France), and Mathieu Turuani (Inria Nancy - Grand Est, LORIA, France)

Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR 359

Jannik Dreier (Université de Lorraine, France), Lucca Hirschi (ETH Zurich, Switzerland), Sasa Radomirovic (University of Dundee, UK), and Ralf Sasse (ETH Zurich, Switzerland)

A Typing Result for Stateful Protocols 374

Andreas Hess (Technical University of Denmark) and Sebastian Mödersheim (Technical University of Denmark)

Author Index 389