2020 IEEE 33rd Computer Security Foundations Symposium (CSF 2020)

Boston, Massachusetts, USA
22-25 June 2020

IEEE Catalog Number: CFP20037-POD
ISBN: 978-1-7281-6573-8

Copyright © 2020 by the Institute of Electrical and Electronics Engineers, Inc.
All Rights Reserved

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP20037-POD
ISBN (Print-On-Demand):	978-1-7281-6573-8
ISBN (Online):	978-1-7281-6572-1
ISSN:	1940-1434

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

2020 IEEE 33rd Computer Security Foundations Symposium (CSF)

CSF 2020

Table of Contents

Preface ix

Organizing Committee x

Program Committee xi

External Reviewers xii

E-Voting

Dispute Resolution in Voting 1
David Basin (ETH Zurich), Saša Radomirović (Heriot-Watt University), and Lara Schmid (ETH Zurich)

Fifty Shades of Ballot Privacy: Privacy against a Malicious Board 17
Véronique Cortier (CNRS, Loria), Joseph Lallemand (Inria, Loria & ETH Zürich), and Bogdan Warinschi (University of Bristol & Dfinity)

(Universal) Unconditional Verifiability in E-Voting without Trusted Parties 33
Vincenzo Iovino (University of Salerno, Italy), Alfredo Rial (SnT, University of Luxembourg), Peter Roenne (SnT, University of Luxembourg), and Peter Ryan (SnT, University of Luxembourg)

SoK: Techniques for Verifiable Mix Nets 49
Johannes Müller (University of Luxembourg) and Thomas Haines (Norwegian University of Science and Technology)

Information Flow (I)

Transparent IFC Enforcement: Possibility and (In) Efficiency Results 65
Maximilian Algehed (Chalmers) and Cormac Flanagan (University of California Santa Cruz)

VERONICA: Expressive and Precise Concurrent Information Flow Security 79
Daniel Schoepe (Chalmers University of Technology), Toby Murray (University of Melbourne and Data61), and Andrei Sabelfeld (Chalmers University of Technology)

Reconciling Progress-Insensitive Noninterference and Declassification 95
Johan Bay (Aarhus University) and Aslan Askarov (Aarhus University)

Language-Based Security

Language-Based Web Session Integrity 107
Stefano Calzavara (Università Ca' Foscari Venezia), Riccardo Focardi (Università Ca' Foscari Venezia), Niklas Grimm (TU Wien), Matteo Maffei (TU Wien), and Mauro Tempesta (TU Wien)

First-Order Logic for Flow-Limited Authorization 123
Andrew K. Hirsch (MPI-SWS), Pedro H. Azevedo de Amorim (Cornell University), Ethan Cecchetti (Cornell University), Ross Tate (Cornell University), and Owen Arden (University of California, Santa Cruz)

Types and Abstract Interpretation for Authorization Hook Advice 139
Christian Skalka (University of Vermont), David Darais (University of Vermont), Trent Jaeger (Penn State University), and Frank Capobianco (Penn State University)

Privacy

Optimal Obfuscation Mechanisms via Machine Learning 153
Marco Romanelli (Inria and Institute Polytechnique de Paris), Kostantinos Chatzikokolakis (University of Athens, Greece), and Catuscia Palamidessi (Inria and Institute Polytechnique de Paris)

A Method for Proving Unlinkability of Stateful Protocols 169
David Baelde (LSV, ENS Paris-Saclay & CNRS, Université Paris-Saclay, France), Stéphanie Delaune (Univ Rennes, CNRS, IRISA, France), and Solène Moreau (Univ Rennes, CNRS, IRISA, France)

Information Flow (II)

Abstracting Faceted Execution 184
Kristopher Micinski (Syracuse University), David Darais (University of Vermont), and Thomas Gilray (University of Vermont at Birmingham)

Nontransitive Security Types for Coarse-Grained Information Flow Control 199
Yi Lu (Queensland University of Technology) and Chenyi Zhang (Jinan University)

Securing Asynchronous Exceptions 214
Carlos Tomé Cortiñas (Chalmers University of Technology), Marco Vassena (CISPA Helmholz Center for Information Security), and Alejandro Russo (Chalmers University of Technology)

Secure Systems

PASAPTO: Policy-Aware Security and Performance Trade-Off Analysis - Computation on Encrypted Data with Restricted Leakage 230
Andreas Fischer (SAP Security Research), Jonas Janneck (SAP Security Research), Jörn Kussmaul (SAP Security Research), Nikolas Krätzschmar (SAP Security Research), Florian Kerschbaum (University of Waterloo, Canada), and Eric Bodden (Paderborn University, Heinz Nixdorf Institute & Fraunhofer IEM)

Runtime Enforcement for Control System Security 246
Ruggero Lanotte (University of Insubria, Italy), Massimo Merro (University of Verona, Italy), and Andrei Munteanu (University of Verona, Italy)

Provably Secure Isolation for Interruptible Enclaved Execution on Small Microprocessors 262
Matteo Busi (Università di Pisa, Italy), Job Noorman (imec-DistriNet, KU Leuven, Belgium), Jo Van Bulck (imec-DistriNet, KU Leuven, Belgium), Letterio Galletta (IMT School for Advanced Studies Lucca, Italy), Pierpaolo Degano (Università di Pisa, Italy), Jan Tobias Mühlberg (imec-DistriNet, KU Leuven, Belgium), and Frank Piessens (imec-DistriNet, KU Leuven, Belgium)

Applied Cryptography and Protocol Analysis

Limiting the Impact of Unreliable Randomness in Deployed Security Protocols 277
Liliya Akhmetzyanova (CryptoPro), Cas Cremers (CISPA Helmholtz Center for Information Security), Luke Garratt (Cisco Meraki), Stanislav Smyshlyaev (CryptoPro), and Nick Sullivan (Cloudflare Inc.)

Authentication in Key-Exchange: Definitions, Relations and Composition 288
Cyprien Delpech de Saint Guilhem (imec-COSIC, KU Leuven, Belgium; University of Bristol, United Kingdom), Marc Fischlin (Technische Universitat Darmstadt, Germany), and Bogdan Warinschi (University of Bristol, United Kingdom; Dfinity, Zurich, Switzerland)

Automated Analysis of PUF-Based Protocols 304
Riccardo Focardi (University Ca' Foscari, Venice) and Flaminia L. Luccio (University Ca' Foscari, Venice)

Blockchain

Anonymous Lottery in the Proof-of-Stake Setting 318
Foteini Baldimtsi (George Mason University), Varun Madathil (North Carolina State University), Alessandra Scafuro (North Carolina State University), and Linfeng Zhou (North Carolina State University)

A Composable Security Treatment of the Lightning Network 334
Aggelos Kiayias (University of Edinburgh, IOHK) and Orfeas Stefanos Thyfronitis Litos (University of Edinburgh)

Information Flow (III)

Clockwork: Tracking Remote Timing Attacks 350
Iulia Bastys (Chalmers University of Technology), Musard Balliu (KTH Royal Institute of Technology), Tamara Rezk (INRIA Sophia-Antipolis), and Andrei Sabelfeld (Chalmers University of Technology)

Controller Synthesis for Hyperproperties 366
Borzoo Bonakdarpour (Michigan State University, USA) and Bernd Finkbeiner (Saarland University)

Rely/Guarantee Reasoning for Noninterference in Non-Blocking Algorithms 380
Nicholas Coughlin (The University of Queensland) and Graeme Smith (The University of Queensland)

Attack Modeling

Exploiting Attack-Defense Trees to Find an Optimal Set of Countermeasures 395
Barbara Fila (Univ Rennes, INSA Rennes, CNRS, IRISA, Rennes, France) and Wojciech Widel (Univ Rennes, INSA Rennes, CNRS, IRISA, Rennes, France; Division of Network and Systems Engineering, KTH Royal Institute of Technology, Stockholm, Sweden)

Provably Robust Decisions Based on Potentially Malicious Sources of Information 411
Tim Muller (University of Nottingham), Dongxia Wang (Singapore Management University), and Jun Sun (Singapore Management University)

Author Index 425