2019 IEEE 32nd Computer Security Foundations Symposium (CSF 2019)

Hoboken, New Jersey, USA
25 – 28 June 2019

IEEE

IEEE Catalog Number:	CFP19037-POD
ISBN:	978-1-7281-1408-8

Copyright © 2019 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:	CFP19037-POD
ISBN (Print-On-Demand):	978-1-7281-1408-8
ISBN (Online):	978-1-7281-1407-1
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

2019 IEEE 32nd Computer Security Foundations Symposium (CSF)

CSF 2019

Table of Contents

Preface .ix..

Committees .xi...

Reviewers .xiii...

Session 1: Information Flow

Optimising Faceted Secure Multi-Execution .1..

Maximilian Algehed (Chalmers University of Technology), Alejandro Russo (Chalmers University of Technology), and Cormac Flanagan (University of California, Santa Cruz)

Canonical Representations of k-Safety Hyperproperties .17...

Bernd Finkbeiner (Saarland University), Lennart Haas (Saarland University), and Hazem Torfah (Saarland University)

Timing Leaks and Coarse-Grained Clocks .32..

Panagiotis Vasilikos (Technical University of Denmark, Lyngby), Hanne Riis Nielson (Technical University of Denmark, Lyngby), Flemming Nielson (Technical University of Denmark, Lyngby), and Boris Köpf (Microsoft Research, Cambridge)

Session 2: Security Protocols I

Decidability of a Sound Set of Inference Rules for Computational Indistinguishability .48.............................

Adrien Koutsos (LSV, CNRS, ENS Paris-Saclay, Université Paris-Saclay)

How to Wrap it up - A Formally Verified Proposal for the use of Authenticated Wrapping in PKCS#11 .62.......

Alexander Dax (CISPA Helmholtz Center for Information Security), Robert Künnemann (CISPA Helmholtz Center for Information Security), Sven Tangermann (CISPA Helmholtz Center for Information Security), and Michael Backes (CISPA Helmholtz Center for Information Security)

Prime, Order Please! Revisiting Small Subgroup and Invalid Curve Attacks on Protocols using Diffie-Hellman .78..

Cas Cremers (CISPA Helmholtz Center for Information Security) and Dennis Jackson (University of Oxford)

Session 3: Blockchain

Re-Thinking Untraceability in the CryptoNote-Style Blockchain .94
Jiangshan Yu (Monash University), Man Ho Allen Au (Hong Kong Polytechnic University), and Paulo Esteves-Verissimo (University of Luxembourg)

Time-Dependent Decision-Making and Decentralization in Proof-of-Work Cryptocurrencies .108
Yevhen Zolotavkin (Monash University), Julian Garcia (Monash University), and Joseph Liu (Monash University)

Analysis of Deterministic Longest-Chain Protocols .122
Elaine Shi (Cornell)

Session 4: Computer-Aided Crypto

Symbolic Methods in Computational Cryptography Proofs .136
Gilles Barthe (MPI for Security and Privacy & IMDEA Software Institute), Benjamin Grégoire (Inria Sophia-Antipolis), Charlie Jacomme (LSV, CNRS & ENS Paris-Saclay & Inria & Université Paris-Saclay), Steve Kremer (Inria Nancy), and Pierre-Yves Strub (École Polytechnique)

Formalizing Constructive Cryptography using CryptHOL .152
Andreas Lochbihler (Digital Asset (Switzerland) GmbH), S. Reza Sefidgar (ETH Zürich), David Basin (ETH Zürich), and Ueli Maurer (ETH Zürich)

EasyUC: Using EasyCrypt to Mechanize Proofs of Universally Composable Security .167
Ran Canetti (Boston University and Tel Aviv University), Alley Stoughton (Boston University), and Mayank Varia (Boston University)

Session 5: Formal Methods and Verification — Attacker Model

On the Meaning and Purpose of Attack Trees .184
Heiko Mantel (TU Darmstadt) and Christian W. Probst (Unitec Institute of Technology)

Efficient Attack-Defense Tree Analysis using Pareto Attribute Domains .200
Barbara Fila (Univ Rennes, INSA Rennes, CNRS, IRISA) and Wojciech Wideł (Univ Rennes, INSA Rennes, CNRS, IRISA)

Games for Security Under Adaptive Adversaries .216
Timos Antonopoulos (Yale University) and Tachio Terauchi (Waseda University)

Session 6: Formal Methods and Verification — Secure Compilation

Information-Flow Preservation in Compiler Optimisations .230
Frédéric Besson (Inria), Alexandre Dang (Inria), and Thomas Jensen (Inria)

Temporal Safety for Stack Allocated Memory on Capability Machines 243
Stelios Tsampas (KU Leuven), Dominique Devriese (Vrije Universiteit Brussel), and Frank Piessens (KU Leuven)

Journey Beyond Full Abstraction: Exploring Robust Property Preservation for Secure Compilation 256
Carmine Abate (Inria Paris), Roberto Blanco (Inria Paris), Deepak Garg (MPI-SWS), Catalin Hritcu (Inria Paris), Marco Patrignani (Stanford University and CISPA Helmholz Center for Information Security), and Jérémy Thibault (Inria Paris)

Session 7: Hardware-Based Security

Using Information Flow to Design an ISA that Controls Timing Channels 272
Drew Zagieboylo (Cornell University), G. Edward Suh (Cornell University), and Andrew C. Myers (Cornell University)

A Formal Approach to Secure Speculation 288
Kevin Cheang (University of California, Berkeley), Cameron Rasmussen (University of California, Berkeley), Sanjit Seshia (University of California, Berkeley), and Pramod Subramanyan (Indian Institute of Technology, Kanpur)

Information Flow Control for Distributed Trusted Execution Environments 304
Anitha Gollamudi (Harvard University), Stephen Chong (Harvard University), and Owen Arden (University of California, Santa Cruz)

Session 8: Language-Based Security

Securing Cross-App Interactions in IoT Platforms 319
Musard Balliu (KTH Royal Institute of Technology), Massimo Merro (University of Verona), and Michele Pasqua (University of Verona)

Static Enforcement of Security in Runtime Systems 335
Mathias Vorreiter Pedersen (Aarhus University) and Aslan Askarov (Aarhus University)

Beyond Labels: Permissiveness for Dynamic Information Flow Enforcement 351
Elisavet Kozyri (Cornell University), Fred B. Schneider (Cornell University), Andrew Bedford (Laval University), Josée Desharnais (Laval University), and Nadia Tawbi (Laval University)

Session 9: Security Protocols II

BeleniosVS: Secrecy and Verifiability Against a Corrupted Voting Device 367
Véronique Cortier (CNRS, Loria), Alicia Filipiak (Orange Labs), and Joseph Lallemand (Inria, Loria)

Resource-Bounded Intruders in Denial of Service Attacks 382
Abraão Aires Urquiza (UFPB), Musab A. AlTurki (KFUPM, Dhahran, Saudi, Runtime Verification Inc., USA), Max Kanovich (University College London, UK, National Research University Higher School of Economics, Moscow, Russia), Tajana Ban Kirigin (University of Rijeka), Vivek Nigam (fortiss GmbH & UFPB), Andre Scedrov (University of Pennsylvania, USA, National Research University Higher School of Economics, Moscow, Russia), and Carolyn Talcott (SRI International, USA)

Automated Verification of Accountability in Security Protocols 397
Robert Künnemann (CISPA Helmholtz Center for Information Security), Ilkan Esiyok (CISPA Helmholtz Center for Information Security), and Michael Backes (CISPA Helmholtz Center for Information Security)

Session 10: Quantitative Information Flow

Quantifying Information Flow in Interactive Systems 414
David Mestel (University of Luxembourg)

Deterministic Channel Design for Minimum Leakage 428
Arthur Américo (Queen Mary University of London), MHR. Khouzani (Queen Mary University of London), and Pasquale Malacaria (Queen Mary University of London)

Comparing Systems: Max-Case Refinement Orders and Application to Differential Privacy 442
Konstantinos Chatzikokolakis (University of Athens), Natasha Fernandes (INRIA and Ecole Polytechnique), and Catuscia Palamidessi (INRIA and Ecole Polytechnique)

Author Index 459