2022 IEEE 35th Computer Security Foundations Symposium (CSF 2022)

Haifa, Israel
7 – 10 August 2022

IEEE Catalog Number: CFP22037-POD
ISBN: 978-1-6654-8418-3

Copyright © 2022 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:	CFP22037-POD
ISBN (Print-On-Demand):	978-1-6654-8418-3
ISBN (Online):	978-1-6654-8417-6
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

2022 IEEE 35th Computer Security Foundations Symposium (CSF)

CSF 2022

Table of Contents

Preface ix
CSF 2022 Committees x

Session 1: Security Protocols 1

Conditional Observational Equivalence and Off-Line Guessing Attacks in Multiset Rewriting 1
Petar Paradžik (Faculty of Electrical Engineering and Computing) and Ante Derek (Faculty of Electrical Engineering and Computing)

Is Eve Nearby? Analysing Protocols under the Distant-Attacker Assumption 17
Reynaldo Gil-Pons (University of Luxembourg), Ross Horne (University of Luxembourg), Sjouke Mauw (University of Luxembourg), Alwen Tiu (The Australian National University, Australia), and Rolando Trujillo-Rasua (Deakin University, Australia)

A Small Bound on the Number of Sessions for Security Protocols 33
Véronique Cortier (Université de Lorraine, CNRS, Inria, France), Antoine Dallon (DGA MI, France), and Stéphanie Delaune (Univ Rennes, CNRS, IRISA, France)

Session 2: Language-Based Security

A Formal Model of Checked C 49
Liyi Li (University of Maryland), Yiyun Liu (University of Pennsylvania), Deena Postol (University of Maryland), Leonidas Lampropoulos (University of Maryland), David Van Horn (University of Maryland), and Michael Hicks (University of Maryland)

SecurePtrs: Proving Secure Compilation with Data-Flow Back-Translation and Turn-Taking Simulation 64
Akram El-Korashy (Max Planck Institute for Software Systems (MPI-SWS)), Roberto Blanco (Max Planck Institute for Security and Privacy (MPI-SP)), Jérémy Thibault (Max Planck Institute for Security and Privacy (MPI-SP)), Adrien Durier (Max Planck Institute for Security and Privacy (MPI-SP)), Deepak Garg (Max Planck Institute for Software Systems (MPI-SWS)), and Catalin Hritcu (Max Planck Institute for Security and Privacy (MPI-SP))

Proving Full-System Security Properties under Multiple Attacker Models on Capability Machines 80
Thomas Van Strydonck (KU Leuven), Aina Linn Georges (Aarhus University), Armaël Guéneau (Aarhus University), Alix Trieu (Aarhus University), Amin Timany (Aarhus University), Frank Piessens (KU Leuven), Lars Birkedal (Aarhus University), and Dominique Devriese (KU Leuven, Vrije Universiteit Brussel)

Session 3: Privacy 1

Interpreting Epsilon of Differential Privacy in Terms of Advantage in Guessing or Approximating Sensitive Attributes 96
Alisa Pankova (Cybernetica AS, Estonia) and Peeter Laud (Cybernetica AS, Estonia)

DPL: A Language for GDPR Enforcement 112
Farzane Karami (University of Oslo, Norway), David Basin (ETH Zurich, Switzerland), and Einar Broch Johnsen (University of Oslo, Norway)

Privacy as Reachability 130
Sébastien Gondron (Danmarks Tekniske Universitet, Denmark), Sebastian Mödersheim (Danmarks Tekniske Universitet, Denmark), and Luca Viganò (King's College London, United Kingdom)

Session 4: Voting and Distributed Systems

N-Tube: Formally Verified Secure Bandwidth Reservation in Path-Aware Internet Architectures 147
Thilo Weghorn (Swisscom), Si Liu (ETH Zurich), Christoph Sprenger (ETH Zurich), Adrian Perrig (ETH Zurich), and David Basin (ETH Zurich)

Applying Consensus and Replication Securely with FLAQR 163
Priyanka Mondal (University of California, Santa Cruz), Maximilian Algehed (Chalmers University of Technology), and Owen Arden (University of California, Santa Cruz)

How Efficient are Replay Attacks against Vote Privacy? A Formal Quantitative Analysis .... N/A
David Mestel (SnT/University of Luxembourg, Luxembourg), Johannes Müller (SnT/University of Luxembourg, Luxembourg), and Pascal Reisert (University of Stuttgart, Germany)

Session 5: Cryptography 1

Contingent Payments from Two-Party Signing and Verification for Abelian Groups 195
Sergiu Bursuc (SnT, University of Luxembourg) and Sjouke Mauw (SnT and DCS, University of Luxembourg)

Collusion-Preserving Computation without a Mediator 211
Michele Ciampi (University of Edinburgh), Yun Lu (University of Edinburgh), and Vassilis Zikas (Purdue University, USA)

Bringing State-Separating Proofs to EasyCrypt - A Security Proof for Cryptobox 227
François Dupressoir (University of Bristol, UK), Konrad Kohbrok (Aalto University, Finland), and Sabine Oechsner (University of Edinburgh, UK)

Session 6: Information Flow

IFCIL: An Information Flow Configuration Language for SELinux 243
Lorenzo Ceragioli (University of Pisa, Italy), Letterio Galletta (IMT School for Advanced Studies Lucca, Italy; CINI Cybersecurity National Laboratory, Italy), Pierpaolo Degano (University of Pisa, Italy; IMT School for Advanced Studies Lucca, Italy), and David Basin (ETH Zurich, Switzerland)

Towards a General-Purpose Dynamic Information Flow Policy 260
Peixuan Li (Pennsylvania State University, USA) and Danfeng Zhang (Pennsylvania State University, USA)

Beware of Greeks Bearing Entanglement? Quantum Covert Channels, Information Flow and Non-Local Games 276
David Mestel (University of Luxembourg)

Session 7: Security Protocols 2

Cracking the Stateful Nut: Computational Proofs of Stateful Security Protocols using the Squirrel Proof Assistant 289
David Baelde (Univ Rennes, CNRS, IRISA, France), Stéphanie Delaune (Univ Rennes, CNRS, IRISA, France), Adrien Koutsos (Inria Paris, France), and Solène Moreau (Univ Rennes, CNRS, IRISA, France)

Exploiting Partial Order of Keys to Verify Security of a Vehicular Group Protocol 305
Felipe Boeira (Linkoping University, Sweden) and Mikael Asplund (Linköping University, Sweden)

Symbolic Protocol Verification with Dice: Process Equivalences in the Presence of Probabilities 319
Vincent Cheval (Inria Paris, France), Raphaëlle Crubillé (Aix Marseille Univ, Université de Toulon, CNRS, LIS, France), and Steve Kremer (Université de Lorraine, Inria Nancy Grand-Est & LORIA, France)

Session 8: Privacy 2

Machine-Checked Proofs of Privacy Against Malicious Boards for Selene & Co 335
Constantin Catalin Dragan (University of Surrey, United Kingdom), François Dupressoir (University of Bristol, United Kingdom), Ehsan Estaji (University of Luxembourg), Kristian Gjøsteen (NTNU, Norway), Thomas Haines (Australian National University, Australia), Peter Y. A. Ryan (University of Luxembourg), Peter B. Rønne (University of Luxembourg), and Morten Rotvold Solberg (NTNU, Norway)

Universal Optimality and Robust Utility Bounds for Metric Differential Privacy 348
Natasha Fernandes (Macquarie University, Australia; Inria and Institut Polytechnique de Paris, France; Data61, CSIRO, Australia), Annabelle McIver (Macquarie University, Australia), Catuscia Palamidessi (Inria and Institut Polytechnique de Paris, France), and Ming Ding (Data61, CSIRO, Australia)

Unlinkability of an Improved Key Agreement Protocol for EMV 2nd Gen Payments 364
Ross Horne (University of Luxembourg), Sjouke Mauw (University of Luxembourg), and Semen Yurkov (University of Luxembourg)

Session 9: Verification and Synthesis

Adversarial Robustness Verification and Attack Synthesis in Stochastic Systems 380
Lisa Oakley (Northeastern University, USA), Alina Oprea (Northeastern University, USA), and Stavros Tripakis (Northeastern University, USA)

The Complexity of Verifying Boolean Programs as Differentially Private 396
Mark Bun (Boston University, USA), Marco Gaboardi (Boston University, USA), and Ludmila Glinskih (Boston University, USA)

Adversary Safety by Construction in a Language of Cryptographic Protocols 412
Timothy Braje (MIT Lincoln Laboratory, USA), Alice Lee (Technische Universität Wien, Austria), Andrew Wagner (Northeastern University, USA), Benjamin Kaiser (Princeton University, USA), Daniel Park (Rensselaer Polytechnic Institute, USA), Martine Kalke (MIT Lincoln Laboratory, USA), Robert Cunningham (University of Pittsburg, USA), and Adam Chlipala (MIT CSAIL, USA)

Session 10: Cryptography 2

Legendre PRF (Multiple) Key Attacks and the Power of Preprocessing 428
Alexander May (Ruhr University Bochum, Germany) and Floyd Zweydinger (Ruhr University Bochum, Germany)

A Complete Characterization of Security for Linicrypt Block Cipher Modes 439
Tommy Hollenberg (Oregon State University), Mike Rosulek (Oregon State University), and Lawrence Roy (Oregon State University)

Locked Circuit Indistinguishability: A Notion of Security for Logic Locking 455
Mohamed El Massad (King Abdullah University of Science and Technology), Nahid Juma (University of Waterloo), Jonathan Shahen (University of Waterloo), Mariana Raykova (Google), Siddharth Garg (New York University), and Mahesh Tripunitara (University of Waterloo)

Session 11: Hyperproperties

Prophecy Variables for Hyperproperty Verification 471
Raven Beutner (CISPA Helmholtz Center for Information Security, Germany) and Bernd Finkbeiner (CISPA Helmholtz Center for Information Security, Germany)

Mapping Synthesis for Hyperproperties 486
Tzu-Han Hsu (Michigan State University, USA), Borzoo Bonakdarpour (Michigan State University, USA), Eunsuk Kang (Carnegie Mellon University, USA), and Stavros Tripakis (Northeastern University, USA)

Author Index **501**