

2017 IEEE 30th Computer Security Foundations Symposium (CSF 2017)

**Santa Barbara, California, USA
21-25 August 2017**



**IEEE Catalog Number: CFP17037-POD
ISBN: 978-1-5386-3218-5**

**Copyright © 2017 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:	CFP17037-POD
ISBN (Print-On-Demand):	978-1-5386-3218-5
ISBN (Online):	978-1-5386-3217-8
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

2017 IEEE 30th Computer Security Foundations Symposium

CSF 2017

Table of Contents

Message from the General Chair.....	ix
Committees.....	xi
External Reviewers.....	xiii

Invited Talk I

On the Protection of Private Information in Machine Learning Systems: Two Recent Approches	1
<i>Martín Abadi, Úlfar Erlingsson, Ian Goodfellow, H. Brendan McMahan, Ilya Mironov, Nicolas Papernot, Kunal Talwar, and Li Zhang</i>	

Session 1: Security Economics

How Shall We Play a Game?: A Game-theoretical Model for Cyber-warfare Games	7
<i>Tiffany Bao, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, and David Brumley</i>	

Session 2: Information-flow Control

A Sound Flow-Sensitive Heap Abstraction for the Static Analysis of Android Applications	22
<i>Stefano Calzavara, Ilya Grishchenko, Adrien Koutsos, and Matteo Maffei</i>	
Securing Concurrent Lazy Programs Against Information Leakage	37
<i>Marco Vassena, Joachim Breitner, and Alejandro Russo</i>	
Towards a Flow- and Path-Sensitive Information Flow Analysis	53
<i>Peixuan Li and Danfeng Zhang</i>	

Session 3: Computer-Aided Cryptography

Symbolic and Computational Mechanized Verification of the ARINC823 Avionic Protocols	68
<i>Bruno Blanchet</i>	
Mechanizing the Proof of Adaptive, Information-Theoretic Security of Cryptographic Protocols in the Random Oracle Model	83
<i>Alley Stoughton and Mayank Varia</i>	
Formal Computational Unlinkability Proofs of RFID Protocols	100
<i>Hubert Comon and Adrien Koutsos</i>	

Invited Talk II

Rethinking Large-Scale Consensus	115
<i>Rafael Pass and Elaine Shi</i>	

Session 4A: Authentication and Key Management I

Formal Verification of Protocols Based on Short Authenticated Strings	130
<i>St�phanie Delaune, Steve Kremer, and Ludovic Robin</i>	
Secure Composition of PKIs with Public Key Protocols	144
<i>Vincent Cheval, V�ronique Cortier, and Bogdan Warinschi</i>	
Human Computing for Handling Strong Corruptions in Authenticated Key Exchange	159
<i>Alexandra Boldyreva, Shan Chen, Pierre-Alain Dupont, and David Pointcheval</i>	

Session 4B: Authentication and Key Management II

Run-Time Attack Detection in Cryptographic APIs	176
<i>Riccardo Focardi and Marco Squarcina</i>	
The Web SSO Standard OpenID Connect: In-depth Formal Security Analysis and Security Guidelines	189
<i>Daniel Fett, Ralf K�sters, and Guido Schmitz</i>	

Session 5: 5-minute Talks

Session 6: Security Protocols

Automatically Detecting the Misuse of Secrets: Foundations, Design Principles, and Applications	203
<i>Kevin Milner, Cas Cremers, Jiangshan Yu, and Mark Ryan</i>	
UC-Secure Non-interactive Public-Key Encryption	217
<i>Jan Camenisch, Anja Lehmann, Gregory Neven, and Kai Samelin</i>	

Symbolic Verification of Privacy-Type Properties for Security Protocols with XOR	234
<i>David Baelde, Stéphanie Delaune, Ivan Gazeau, and Steve Kremer</i>	

Session 7: Privacy

Differential Privacy in Quantum Computation	249
<i>Li Zhou and Mingsheng Ying</i>	
Rényi Differential Privacy	263
<i>Ilya Mironov</i>	
PrivatePool: Privacy-Preserving Ridesharing	276
<i>Per Hallgren, Claudio Orlandi, and Andrei Sabelfeld</i>	
Reconciling Privacy and Utility in Continuous-Time Diffusion Networks	292
<i>Michael Backes, Manuel Gomez-Rodriguez, Praveen Manoharan, and Bartłomiej Surma</i>	

Session 8: Quantitative Information-Flow Analysis

Leakage-Minimal Design: Universality, Limitations, and Applications	305
<i>Mhr Khouzani and Pasquale Malacaria</i>	
Tight Bounds on Information Leakage from Repeated Independent Runs	318
<i>David M. Smith and Geoffrey Smith</i>	
Synthesis of Adaptive Side-Channel Attacks	328
<i>Quoc-Sang Phan, Lucas Bang, Corina S. Pasareanu, Pasquale Malacaria, and Tefvik Bultan</i>	
Securing Databases from Probabilistic Inference	343
<i>Marco Guarnieri, Srdjan Marinovic, and David Basin</i>	

Session 9: Distributed Systems

A Universally Composable Treatment of Network Time	360
<i>Ran Canetti, Kyle Hogan, Aanchal Malhotra, and Mayank Varia</i>	
Types for Location and Data Security in Cloud Environments	376
<i>Ivan Gazeau, Tom Chothia, and Dominic Duggan</i>	

Session 10A: Security and Compilation

Secure Compilation and Hyperproperty Preservation	392
<i>Marco Patrignani and Deepak Garg</i>	
Verified Translation Validation of Static Analyses	407
<i>Gilles Barthe, Sandrine Blazy, Vincent Laporte, David Pichardie, and Alix Trieu</i>	

Session 10B: Embedded and Cyber-physical Security

Proving Flow Security of Sequential Logic via Automatically-Synthesized Relational Invariants	422
<i>Hyoukjun Kwon, William Harris, and Hadi Esmaeilzadeh</i>	
A Formal Approach to Cyber-Physical Attacks	438
<i>Ruggero Lanotte, Massimo Merro, Riccardo Muradore, and Luca Viganò</i>	

Session 11: Security Protocols II

Formalizing and Proving a Typing Result for Security Protocols in Isabelle/HOL	453
<i>Andreas Viktor Hess and Sebastian Mödersheim</i>	
Deciding Secrecy of Security Protocols for an Unbounded Number of Sessions: The Case of Depth-Bounded Processes	466
<i>Emanuele D'Oswaldo, Luke Ong, and Alwen Tiu</i>	
SAT-Equiv: An Efficient Tool for Equivalence Properties	483
<i>Véronique Cortier, Antoine Dallon, and Stéphanie Delaune</i>	
Author Index	497