

2016 IEEE 29th Computer Security Foundations Symposium (CSF 2016)

**Lisbon, Portugal
27 June – 1 July 2016**



**IEEE Catalog Number: CFP16037-POD
ISBN: 978-1-5090-2608-1**

**Copyright © 2016 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 publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP16037-POD
ISBN (Print-On-Demand):	978-1-5090-2608-1
ISBN (Online):	978-1-5090-2607-4
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

IEEE 29th Computer Security Foundations Symposium

CSF 2016

Table of Contents

Message from the General Chair.....	viii
Committees.....	x
External Reviewers	xi

Invited Talks and Invited Papers

Modular Verification for Computer Security	1
<i>Andrew W. Appel</i>	
Data-Driven Software Security: Models and Methods	9
<i>Úlfar Erlingsson</i>	
Are the Real Limits to Scale a Matter of Science, or Engineering, or of Something Else? (Abstract only)	16
<i>Ross Anderson</i>	

Software Security

On Modular and Fully-Abstract Compilation	17
<i>Marco Patrignani, Dominique Devriese, and Frank Piessens</i>	
Secure Software Licensing: Models, Constructions, and Proofs	31
<i>Sergiu Costea and Bogdan Warinschi</i>	
Beyond Good and Evil: Formalizing the Security Guarantees of Compartmentalizing Compilation	45
<i>Yannis Juglaret, Catalin Hritcu, Arthur Azevedo De Amorim, Boris Eng, and Benjamin C. Pierce</i>	

Quantitative Security

Relative Perfect Secrecy: Universally Optimal Strategies and Channel Design	61
<i>M.H.R. Khouzani and Pasquale Malacaria</i>	
Axioms for Information Leakage	77
<i>Mário S. Alvim, Konstantinos Chatzikokolakis, Annabelle McIver, Carroll Morgan, Catuscia Palamidessi, and Geoffrey Smith</i>	

Correlated Secrets in Quantitative Information Flow93
Nicolás E. Bordenabe and Geoffrey Smith

Quantitative Verification and Synthesis of Attack-Defence Scenarios105
Zaruhi Aslanyan, Flemming Nielson, and David Parker

Access Control I

In the Nick of Time: Proactive Prevention of Obligation Violations120
David Basin, Søren Debois, and Thomas T. Hildebrandt

A Calculus for Flow-Limited Authorization135
Owen Arden and Andrew C. Myers

On Access Control, Capabilities, Their Equivalence, and Confused Deputy
Attacks150
Vineet Rajani, Deepak Garg, and Tamara Rezk

Protocols and Distributed Systems I

On Post-compromise Security164
Katriel Cohn-Gordon, Cas Cremers, and Luke Garratt

Micro-policies for Web Session Security179
Stefano Calzavara, Riccardo Focardi, Niklas Grimm, and Matteo Maffei

Localizing Firewall Security Policies194
Pedro Adão, Riccardo Focardi, Joshua D. Guttman, and Flaminia L. Luccio

Information Flow I

Calculational Design of Information Flow Monitors210
Mounir Assaf and David A. Naumann

Hybrid Monitoring of Attacker Knowledge225
Frédéric Besson, Nataliia Bielova, and Thomas Jensen

Runtime Verification of k-Safety Hyperproperties in HyperLTL239
Shreya Agrawal and Borzoo Bonakdarpour

Non-interference with What-Declassification in Component-Based Systems253
Simon Greiner and Daniel Grahl

Computer-Aided Cryptography

A Certified Compiler for Verifiable Computing268
Cédric Fournet, Chantal Keller, and Vincent Laporte

Analysis of Key Wrapping APIs: Generic Policies, Computational Security281
Guillaume Scerri and Ryan Stanley-Oakes

A Verified Extensible Library of Elliptic Curves	296
<i>Jean Karim Zinzindohoué, Evmorfia-Iro Bartzia, and Karthikeyan Bhargavan</i>	

Protocols and Distributed Systems II

Automated Reasoning for Equivalences in the Applied Pi Calculus with Barriers	310
<i>Bruno Blanchet and Ben Smyth</i>	
Modeling Human Errors in Security Protocols	325
<i>David Basin, Saša Radomirovic, and Lara Schmid</i>	
sElect: A Lightweight Verifiable Remote Voting System	341
<i>Ralf Küsters, Johannes Müller, Enrico Scapin, and Tomasz Truderung</i>	

Privacy and Economics

A Methodology for Formalizing Model-Inversion Attacks	355
<i>Xi Wu, Matthew Fredrikson, Somesh Jha, and Jeffrey F. Naughton</i>	
CASH: A Cost Asymmetric Secure Hash Algorithm for Optimal Password Protection	371
<i>Jeremiah Blocki and Anupam Datta</i>	

Information Flow II

Multi-run Side-Channel Analysis Using Symbolic Execution and Max-SMT	387
<i>Corina S. Pasareanu, Quoc-Sang Phan, and Pasquale Malacaria</i>	
Fault-Resilient Non-interference	401
<i>Filippo Del Tedesco, David Sands, and Alejandro Russo</i>	
Compositional Verification and Refinement of Concurrent Value-Dependent Noninterference	417
<i>Toby Murray, Robert Sison, Edward Pierzchalski, and Christine Rizkallah</i>	

Access Control II

Resilient Delegation Revocation with Precedence for Predecessors Is NP-Complete	432
<i>Marcos Cramer, Pieter Van Hertum, Ruben Lapauw, Ingmar Dasseville, and Marc Denecker</i>	
Access Control Synthesis for Physical Spaces	443
<i>Petar Tsankov, Mohammad Torabi Dashti, and David Basin</i>	
Static Detection of Collusion Attacks in ARBAC-Based Workflow Systems	458
<i>Stefano Calzavara, Alvise Rabitti, Enrico Steffnlongo, and Michele Bugliesi</i>	

Author Index	471
---------------------------	-----