

2015 IEEE 28th Computer Security Foundations Symposium (CSF 2015)

**Verona, Italy
13-17 July 2015**



**IEEE Catalog Number: CFP15037-POD
ISBN: 978-1-4673-7539-9**

2015 IEEE 28th Computer Security Foundations Symposium

CSF 2015

Table of Contents

Message from the General Chair.....	ix
About the Location.....	x
Organizing Committee.....	xi

Access Control

Analyzing First-Order Role Based Access Control	3
<i>Carlos Cotrini, Thilo Weghorn, David Basin, and Manuel Clavel</i>	
Decomposing, Comparing, and Synthesizing Access Control Expressiveness Simulations	18
<i>William C. Garrison and Adam J. Lee</i>	
Compositional Typed Analysis of ARBAC Policies	33
<i>Stefano Calzavara, Alvise Rabitti, and Michele Bugliesi</i>	
Policy Privacy in Cryptographic Access Control	46
<i>Anna Lisa Ferrara, Georg Fachsbauer, Bin Liu, and Bogdan Warinschi</i>	

Privacy

Location Privacy via Differential Private Perturbation of Cloaking Area	63
<i>Hoa Ngo and Jong Kim</i>	
Automatic Proofs of Privacy of Secure Multi-party Computation Protocols against Active Adversaries	75
<i>Martin Pettai and Peeter Laud</i>	
A Game-Theoretic Study on Non-monetary Incentives in Data Analytics Projects with Privacy Implications	90
<i>Michela Chessa, Jens Grossklags, and Patrick Loiseau</i>	

Information Flow 1

A Cut Principle for Information Flow	107
<i>Joshua D. Guttman and Paul D. Rowe</i>	
The Anatomy and Facets of Dynamic Policies	122
<i>Niklas Broberg, Bart van Delft, and David Sands</i>	
Hybrid Monitors for Concurrent Noninterference	137
<i>Aslan Askarov, Stephen Chong, and Heiko Mantel</i>	

Protocols 1

Du-Vote: Remote Electronic Voting with Untrusted Computers	155
<i>Gurchetan S. Grewal, Mark D. Ryan, Liqun Chen, and Michael R. Clarkson</i>	
Decidability of Trace Equivalence for Protocols with Nonces	170
<i>Rémy Chrétien, Véronique Cortier, and Stéphanie Delaune</i>	
Set-Pi: Set Membership π -Calculus	185
<i>Alessandro Bruni, Sebastian Mödersheim, Flemming Nielson, and Hanne Riis Nielson</i>	
A Complete Characterization of Secure Human-Server Communication	199
<i>David Basin, Saša Radomirovic, and Michael Schläepfer</i>	

Access Control and Authentication

A Definitional Framework for Functional Encryption	217
<i>Christian Matt and Ueli Maurer</i>	
Reasoning about Policy Behavior in Logic-Based Trust Management Systems: Some Complexity Results and an Operational Framework	232
<i>Edelmira Pasarella and Jorge Lobo</i>	
Picking vs. Guessing Secrets: A Game-Theoretic Analysis	243
<i>M.H.R. Khouzani, Piotr Mardziel, Carlos Cid, and Mudhakar Srivatsa</i>	

Security Models, Properties, Attacks

Program Actions as Actual Causes: A Building Block for Accountability	261
<i>Anupam Datta, Deepak Garg, Dilsun Kaynar, Divya Sharma, and Arunesh Sinha</i>	
BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations	276
<i>Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici</i>	
A Parametric Family of Attack Models for Proxy Re-encryption	290
<i>David Nuñez, Isaac Agudo, and Javier Lopez</i>	

Language-Based Security 1

A Hybrid Approach for Proving Noninterference of Java Programs	305
<i>Ralf Küsters, Tomasz Truderung, Bernhard Beckert, Daniel Bruns, Michael Kirsten, and Martin Mohr</i>	
Android Permissions Unleashed	320
<i>Alessandro Armando, Roberto Carbone, Gabriele Costa, and Alessio Merlo</i>	
Cryptographic Enforcement of Language-Based Information Erasure	334
<i>Aslan Askarov, Scott Moore, Christos Dimoulas, and Stephen Chong</i>	

Information Flow 2

Value-Sensitive Hybrid Information Flow Control for a JavaScript-Like Language	351
<i>Daniel Hedin, Luciano Bello, and Andrei Sabelfeld</i>	
Information Flow Control for Event Handling and the DOM in Web Browsers	366
<i>Vineet Rajani, Abhishek Bichhawat, Deepak Garg, and Christian Hammer</i>	
An Analysis of Universal Information Flow Based on Self-Composition	380
<i>Christian Müller, Máté Kovács, and Helmut Seidl</i>	

Protocols 2

On Power Splitting Games in Distributed Computation: The Case of Bitcoin Pooled Mining	397
<i>Loi Luu, Ratul Saha, Inian Parameshwaran, Prateek Saxena, and Aquinas Hobor</i>	
Symbolic Malleable Zero-Knowledge Proofs	412
<i>Michael Backes, Fabian Bendun, Matteo Maffei, Esfandiar Mohammadi, and Kim Pecina</i>	
A Mechanized Proof of Security for Searchable Symmetric Encryption	481
<i>Adam Petcher and Greg Morrisett</i>	

Language-Based Security 2

Probabilistic Program Modeling for High-Precision Anomaly Classification	497
<i>Kui Xu, Danfeng (Daphne) Yao, Barbara G. Ryder, and Ke Tian</i>	
A Logic of Programs with Interface-Confined Code	512
<i>Limin Jia, Shayak Sen, Deepak Garg, and Anupam Datta</i>	
Rational Protection against Timing Attacks	526
<i>Goran Doychev and Boris Köpf</i>	

Information Flow 3

Understanding and Enforcing Opacity	539
<i>Daniel Schoepe and Andrei Sabelfeld</i>	
A Methodology for Information Flow Experiments	554
<i>Michael Carl Tschantz, Amit Datta, Anupam Datta, and Jeannette M. Wing</i>	
Flow-Limited Authorization	569
<i>Owen Arden, Jed Liu, and Andrew C. Myers</i>	
Author Index	585