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

Privacy
Location Privacy via Differential Private Perturbation of Cloaking Area ............ 63
Hoa Ngo and Jong Kim
Automatic Proofs of Privacy of Secure Multi-party Computation Protocols
against Active Adversaries ............................................................................ 75
Martin Pettai and Peeter Laud
A Game-Theoretic Study on Non-monetary Incentives in Data Analytics
Projects with Privacy Implications ............................................................... 90
Michela Chessa, Jens Grossklags, and Patrick Loiseau
**Information Flow 1**

A Cut Principle for Information Flow ..........................................................107  
Joshua D. Guttman and Paul D. Rowe

The Anatomy and Facets of Dynamic Policies ............................................122  
Niklas Broberg, Bart van Delft, and David Sands

Hybrid Monitors for Concurrent Noninterference .......................................137  
Aslan Askarov, Stephen Chong, and Heiko Mantel

**Protocols 1**

Du-Vote: Remote Electronic Voting with Untrusted Computers .................155  
Gurchetan S. Grewal, Mark D. Ryan, Lijun Chen, and Michael R. Clarkson

Decidability of Trace Equivalence for Protocols with Nonces .....................170  
Remy Chrétien, Véronique Cortier, and Stéphanie Dellaune

Set-Pi: Set Membership $\pi$-Calculus ..........................................................185  
Alessandro Bruni, Sebastian Mödersheim, Flemming Nielson,  
and Hanne Riis Nielson

A Complete Characterization of Secure Human-Server Communication ..........199  
David Basin, Saša Radomirovic, and Michael Schläepfer

**Access Control and Authentication**

A Definitional Framework for Functional Encryption .................................217  
Christian Matt and Ueli Maurer

Reasoning about Policy Behavior in Logic-Based Trust Management Systems:  
Some Complexity Results and an Operational Framework ............................232  
Edelmina Pasarella and Jorge Lobo

Picking vs. Guessing Secrets: A Game-Theoretic Analysis .........................243  
M.H.R. Khouzani, Piotr Mardziel, Carlos Cid, and Mudhakar Srivatsa

**Security Models, Properties, Attacks**

Program Actions as Actual Causes: A Building Block for Accountability ..........261  
Anupam Datta, Deepak Garg, Dilsun Kaynar, Divya Sharma, and Arunesh Sinha

BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using  
Thermal Manipulations ..............................................................................276  
Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici

A Parametric Family of Attack Models for Proxy Re-encryption ....................290  
David Nuñez, Isaac Agudo, and Javier Lopez
Language-Based Security 1
A Hybrid Approach for Proving Noninterference of Java Programs ..................................................305
Ralf Küsters, Tomasz Truderung, Bernhard Beckert, Daniel Bruns,
Michael Kirsten, and Martin Mohr

Android Permissions Unleashed ...............................................................................................................320
Alessandro Armando, Roberto Carbone, Gabriele Costa, and Alessio Merlo

Cryptographic Enforcement of Language-Based Information Erasure ..................................................334
Aslan Askarov, Scott Moore, Christos Dimoulas, and Stephen Chong

Information Flow 2
Value-Sensitive Hybrid Information Flow Control for a JavaScript-Like Language ........................................351
Daniel Hedin, Luciano Bello, and Andrei Sabelfeld

Information Flow Control for Event Handling and the DOM in Web Browsers .......................................366
Vineet Rajani, Abhishek Bichhawat, Deepak Garg, and Christian Hammer

An Analysis of Universal Information Flow Based on Self-Composition ................................................380
Christian Müller, Mátě Kovács, and Helmut Seidl

Protocols 2
On Power Splitting Games in Distributed Computation: The Case of Bitcoin ...........................................397
Loi Luu, Ratul Saha, Inian Parameshwaran, Prateek Saxena, and Aquinas Hobor

Symbolic Malleable Zero-Knowledge Proofs ..............................................................................................412
Michael Backes, Fabian Bendun, Matteo Maffei, Esfandiar Mohammadi,
and Kim Pecina

A Mechanized Proof of Security for Searchable Symmetric Encryption ................................................481
Adam Petcher and Greg Morrisett

Language-Based Security 2
Probabilistic Program Modeling for High-Precision Anomaly Classification .............................................497
Kui Xu, Danfeng (Daphne) Yao, Barbara G. Ryder, and Ke Tian

A Logic of Programs with Interface-Confined Code ..................................................................................512
Limin Jia, Shayak Sen, Deepak Garg, and Anupam Datta

Rational Protection against Timing Attacks ...............................................................................................526
Goran Doychev and Boris Köpf
Information Flow 3

Understanding and Enforcing Opacity .................................................................539
  Daniel Schoepe and Andrei Sabelfeld

A Methodology for Information Flow Experiments ........................................554
  Michael Carl Tschantz, Amit Datta, Anupam Datta, and Jeannette M. Wing

Flow-Limited Authorization .................................................................................569
  Owen Arden, Jed Liu, and Andrew C. Myers

Author Index ........................................................................................................585