

2013 IEEE 26th Computer Security Foundations Symposium

(CSF 2013)

New Orleans, Louisiana, USA
26 – 28 June 2013



IEEE Catalog Number: CFP13037-POD
ISBN: 978-1-4799-0488-4

2013 IEEE 26th Computer Security Foundations Symposium

CSF 2013

Table of Contents

Preface.....	vii
Committees.....	viii
Reviewers.....	x

Information Flow 1

A Theory of Information-Flow Labels	3
<i>Benoit Montagu, Benjamin C. Pierce, and Randy Pollack</i>	
Precise Enforcement of Confidentiality for Reactive Systems	18
<i>Dante Zanarini, Mauro Jaskelioff, and Alejandro Russo</i>	
Secure Multi-execution: Fine-Grained, Declassification-Aware, and Transparent	33
<i>Willard Rafnsson and Andrei Sabelfeld</i>	

Language-Based Security

Memory Trace Oblivious Program Execution	51
<i>Chang Liu, Michael Hicks, and Elaine Shi</i>	
Oblivious Program Execution and Path-Sensitive Non-interference	66
<i>Jérémie Planul and John C Mitchell</i>	
Security and Privacy by Declarative Design	81
<i>Matteo Maffei, Kim Pecina, and Manuel Reinert</i>	
Type-Based Analysis of Generic Key Management APIs	97
<i>Pedro Adão, Riccardo Focardi, and Flaminia L. Luccio</i>	

Access Control

Cryptographically Enforced RBAC	115
<i>Anna Lisa Ferrara, Georg Fuchsbauer, and Bogdan Warinschi</i>	
Quantum Information-Flow Security: Noninterference and Access Control	130
<i>Mingsheng Ying, Yuan Feng, and Nengkun Yu</i>	
Application-Sensitive Access Control Evaluation Using Parameterized Expressiveness	145
<i>Timothy L. Hinrichs, Diego Martinoia, William C. Garrison III, Adam J. Lee, Alessandro Panebianco, and Lenore Zuck</i>	

Quantitative Security

AnoA: A Framework for Analyzing Anonymous Communication Protocols	163
<i>Michael Backes, Aniket Kate, Praveen Manoharan, Sebastian Meiser, and Esfandiar Mohammadi</i>	
A Trust Framework for Evaluating GNSS Signal Integrity	179
<i>Xihui Chen, Gabriele Lenzini, Miguel Martins, Sjouke Mauw, and Jun Pang</i>	
Probabilistic Point-to-Point Information Leakage	193
<i>Tom Chothia, Yusuke Kawamoto, Chris Novakovic, and David Parker</i>	

Information Flow 2

Information Flow Analysis for a Dynamically Typed Language with Staged Metaprogramming	209
<i>Martin Lester, Luke Ong, and Max Schaefer</i>	
Gradual Security Typing with References	224
<i>Luminous Fennell and Peter Thiemann</i>	
Hybrid Information Flow Monitoring against Web Tracking	240
<i>Frederic Besson, Natalia Bielova, and Thomas Jensen</i>	

Privacy and Cryptography

Symbolic Universal Composability	257
<i>Florian Böhl and Dominique Unruh</i>	
Differential Privacy by Typing in Security Protocols	272
<i>Fabienne Eigner and Matteo Maffei</i>	
Verified Computational Differential Privacy with Applications to Smart Metering	287
<i>Gilles Barthe, George Danezis, Benjamin Grégoire, César Kunz, and Santiago Zanella-Béguelin</i>	

Author Index	303
---------------------------	------------