

2012 IEEE 25th Computer Security Foundations Symposium

(CSF 2012)

**Cambridge, Massachusetts, USA
25 – 27 June 2012**



IEEE Catalog Number: CFP12037-PRT
ISBN: 978-1-4673-1918-8

2012 IEEE 25th Computer Security Foundations Symposium

CSF 2012

Table of Contents

Preface.....	viii
Committees.....	ix
External Reviewers.....	xi

Information-Flow Security I

Information-Flow Security for a Core of JavaScript	3
<i>Daniel Hedin and Andrei Sabelfeld</i>	
Secure Information Flow for Concurrent Programs under Total Store Order	19
<i>Jeffrey A. Vaughan and Todd Millstein</i>	
ENCoVer: Symbolic Exploration for Information Flow Security	30
<i>Musard Balliu, Mads Dam, and Gurvan Le Guernic</i>	
Information-Flow Control for Programming on Encrypted Data	45
<i>John C. Mitchell, Rahul Sharma, Deian Stefan, and Joe Zimmerman</i>	

Symbolic Protocol Verification I

Symbolic Analysis of Cryptographic Protocols Containing Bilinear Pairings	63
<i>Alisa Pankova and Peeter Laud</i>	
Automated Analysis of Diffie-Hellman Protocols and Advanced Security Properties	78
<i>Benedikt Schmidt, Simon Meier, Cas Cremers, and David Basin</i>	
Verifying Privacy-Type Properties in a Modular Way	95
<i>Myrto Arapinis, Vincent Cheval, and Stéphanie Delaune</i>	

Access Control

Security Analysis of Role-Based Access Control through Program Verification	113
<i>Anna Lisa Ferrara, P. Madhusudan, and Gennaro Parlato</i>	
Gran: Model Checking Grsecurity RBAC Policies	126
<i>Michele Bugliesi, Stefano Calzavara, Riccardo Focardi, and Marco Squarcina</i>	
Labeled Sequent Calculi for Access Control Logics: Countermodels, Saturation and Abduction	139
<i>Valerio Genovese, Deepak Garg, and Daniele Rispoli</i>	

Systems Security

Mashic Compiler: Mashup Sandboxing Based on Inter-frame Communication	157
<i>Zhengqin Luo and Tamara Rezk</i>	
Secure Compilation to Modern Processors	171
<i>Pieter Agten, Raoul Strackx, Bart Jacobs, and Frank Piessens</i>	
Cache-Leakage Resilient OS Isolation in an Idealized Model of Virtualization	186
<i>Gilles Barthe, Gustavo Betarte, Juan Diego Campo, and Carlos Luna</i>	
A Framework for the Cryptographic Verification of Java-Like Programs	198
<i>Ralf Küsters, Tomasz Truderung, and Jürgen Graf</i>	

Symbolic Protocol Verification II

Constructing Optimistic Multi-party Contract Signing Protocols	215
<i>Barbara Kordy and Saša Radomirović</i>	
Refining Key Establishment	230
<i>Christoph Sprenger and David Basin</i>	
Discovering Concrete Attacks on Website Authorization by Formal Analysis	247
<i>Chetan Bansal, Karthikeyan Bhargavan, and Sergio Maffeis</i>	

Information Theory

Measuring Information Leakage Using Generalized Gain Functions	265
<i>Mário S. Alvim, Kostas Chatzikokolakis, Catuscia Palamidessi, and Geoffrey Smith</i>	
The Thermodynamics of Confidentiality	280
<i>Pasquale Malacaria and Fabrizio Smeraldi</i>	

Information-Flow Security II

Securing Interactive Programs	293
<i>Willard Rafnsson, Daniel Hedin, and Andrei Sabelfeld</i>	

Learning is Change in Knowledge: Knowledge-Based Security for Dynamic Policies	308
<i>Aslan Askarov and Stephen Chong</i>	
Proving Cryptography	
Automatically Verified Mechanized Proof of One-Encryption Key Exchange	325
<i>Bruno Blanchet</i>	
Generic Indifferentiability Proofs of Hash Designs	340
<i>Marion Daubignard, Pierre-Alain Fouque, and Yassine Lakhnech</i>	
Verified Security of Merkle-Damgård	354
<i>Michael Backes, Gilles Barthe, Matthias Berg, Benjamin Grégoire, César Kunz, Malte Skoruppa, and Santiago Zanella Béguelin</i>	
Provably Secure and Practical Onion Routing	369
<i>Michael Backes, Ian Goldberg, Aniket Kate, and Esfandiar Mohammadi</i>	
Author Index	387