

2009 IEEE 22nd Computer Security Foundations Symposium

(CSF 2009)

**Port Jefferson, New York, USA
8 – 10 July 2009**



**IEEE Catalog Number: CFP09037-PRT
ISBN: 978-1-4244-4451-9**

2009 22nd IEEE Computer Security Foundations Symposium

CSF 2009

Table of Contents

Session on Protocol Design

More Anonymous Onion Routing Through Trust	3
<i>Aaron Johnson and Paul Syverson</i>	
Minimal Message Complexity of Asynchronous Multi-party Contract Signing	13
<i>Sjouke Mauw, Sasa Radomirovic, and Mohammad Torabi Dashti</i>	
Authentication without Elision: Partially Specified Protocols, Associated Data, and Cryptographic Models Described by Code	26
<i>Phillip Rogaway and Till Stegers</i>	

Session on Information Flow

Tight Enforcement of Information-Release Policies for Dynamic Languages	43
<i>Aslan Askarov and Andrei Sabelfeld</i>	
Updatable Security Views	60
<i>J. Nathan Foster, Benjamin C. Pierce, and Steve Zdancewic</i>	

Session on Web Security

Language-Based Isolation of Untrusted JavaScript	77
<i>Sergio Maffei and Ankur Taly</i>	
Securing Timeout Instructions in Web Applications	92
<i>Alejandro Russo and Andrei Sabelfeld</i>	

Session on Protocol Analysis

Modeling and Verifying Physical Properties of Security Protocols for Wireless Networks	109
<i>Patrick Schaller, Benedikt Schmidt, David Basin, and Srdjan Capkun</i>	
Cryptographic Protocol Synthesis and Verification for Multiparty Sessions	124
<i>Karthikeyan Bhargavan, Ricardo Corin, Pierre-Malo Deniélou, Cédric Fournet, and James J. Leifer</i>	
A Secure Cryptographic Token Interface	141
<i>Christian Cachin and Nishanth Chandran</i>	

Session on Protocols I

Using ProVerif to Analyze Protocols with Diffie-Hellman Exponentiation	157
<i>Ralf Küsters and Tomasz Truderung</i>	
ASPIER: An Automated Framework for Verifying Security Protocol Implementations	172
<i>Sagar Chaki and Anupam Datta</i>	
Inputs of Coma: Static Detection of Denial-of-Service Vulnerabilities	186
<i>Richard Chang, Guofei Jiang, Franjo Ivancic, Sriram Sankaranarayanan, and Vitaly Shmatikov</i>	

Session on Authorization

Specification and Analysis of Dynamic Authorisation Policies	203
<i>Moritz Y. Becker</i>	
Policy Compliance in Collaborative Systems	218
<i>Max Kanovich, Paul Rowe, and Andre Scedrov</i>	
Advice from Belnap Policies	234
<i>Chris Hankin, Flemming Nielson, and Hanne Riis Nielson</i>	

Session on Verification Methods

Expressive Power of Definite Clauses for Verifying Authenticity	251
<i>Gilberto Filè and Roberto Vigo</i>	
A Method for Proving Observational Equivalence	266
<i>Véronique Cortier and Stéphanie Delaune</i>	
Decidable Analysis for a Class of Cryptographic Group Protocols with Unbounded Lists	277
<i>Najah Chridi, Mathieu Turuani, and Michael Rusinowitch</i>	

Session on Protocols II

Universally Composable Symmetric Encryption	293
<i>Ralf Küsters and Max Tuengerthal</i>	
Achieving Security Despite Compromise Using Zero-knowledge	308
<i>Michael Backes, Martin P. Grochulla, Catalin Hritcu, and Matteo Maffei</i>	
A Provably Secure and Efficient Countermeasure against Timing Attacks	324
<i>Boris Köpf and Markus Dürmuth</i>	

Author Index