

*Proceedings*

---

**20<sup>th</sup> IEEE Computer Security  
Foundations Symposium  
(CSFS20)**

**July 6-8 2007  
Venice, Italy**

**Sponsored by the  
Technical Committee on Security and Privacy  
of the IEEE Computer Society**



Los Alamitos, California  
Washington • Tokyo



# Table of Contents

## 20<sup>th</sup> IEEE Computer Security Foundations Symposium (CSF 2007)

<b>Preface</b> .....	<b>ix</b>
<b>Committees</b> .....	<b>x</b>

### Authorization

Design and Semantics of a Decentralized Authorization Language .....	3
<i>Moritz Becker, Cédric Fournet, and Andrew Gordon</i>	
Do As I SaY! Programmatic Access Control with Explicit Identities .....	16
<i>Andrew Cirillo, Radha Jagadeesan, Corin Pitcher, and James Riely</i>	
A Type Discipline for Authorization in Distributed Systems .....	31
<i>Cédric Fournet, Andrew Gordon, and Sergio Maffei</i>	

### Multi-Layer Protocols and Key Conjuring

Security Analysis of Voice-over-IP Protocols .....	49
<i>Prateek Gupta and Vitaly Shmatikov</i>	
Reasoning about Concurrency for Security Tunnels .....	64
<i>Alwyn Goodloe and Carl Gunter</i>	
A Formal Theory of Key Conjuring .....	79
<i>Véronique Cortier, Stéphanie Delaune, and Graham Steel</i>	

### Protocols and Cryptographic Foundations

Computationally Sound Mechanized Proofs of Correspondence Assertions .....	97
<i>Bruno Blanchet</i>	
Key-dependent Message Security under Active Attacks— BRSIM/UC-Soundness of Symbolic Encryption with Key Cycles .....	112
<i>Michael Backes, Birgit Pfizmann, and Andre Scedrov</i>	
Compositional Security for Task-PIOAs .....	125
<i>Ran Canetti, Ling Cheung, Dilsun Kaynar, Nancy Lynch, and Olivier Pereira</i>	
Approximated Computationally Bounded Simulation Relations for Probabilistic Automata .....	140
<i>Roberto Segala and Andrea Turrini</i>	

## Secure Implementation

Implementing STV Securely in Prêt à Voter .....	157
<i>James Heather</i>	
Secure Implementations for Typed Session Abstractions.....	170
<i>Ricardo Corin, Pierre-Malo Deniélou, Cédric Fournet, Karthikeyan Bhargavan, and James Leifer</i>	
A Library for Secure Multi-threaded Information Flow in Haskell.....	187
<i>Ta-chung Tsai, Alejandro Russo, and John Hughes</i>	

## Information Flow

Dynamic Dependency Monitoring to Secure Information Flow.....	203
<i>Paritosh Shroff, Scott Smith, and Mark Thober</i>	
Automaton-Based Confidentiality Monitoring of Concurrent Programs.....	218
<i>Gurvan Le Guernic</i>	
Secure Information Flow and Program Logics.....	233
<i>Lennart Beringer and Martin Hofmann</i>	

## Privacy

A Flow-Sensitive Analysis of Privacy Properties.....	249
<i>Hanne Riis Nielson and Fleming Nielson</i>	
Collaborative Planning with Privacy .....	265
<i>Max Kanovich, Paul Rowe, and Andre Scedrov</i>	
Privacy and Utility in Business Processes .....	279
<i>Adam Barth, John Mitchell, Anupam Datta, and Sharada Sundaram</i>	

## 20<sup>th</sup> Anniversary Invited Paper

Electing the Doge of Venice: Analysis of a 13 <sup>th</sup> Century Protocol.....	295
<i>Miranda Mowbray and Dieter Gollmann</i>	

## Vulnerability Analysis and Information-Theoretic Security

Creating Vulnerability Signatures Using Weakest Preconditions .....	311
<i>David Brumley, Hao Wang, Somesh Jha, and Dawn Song</i>	
Comparing Countermeasures against Interrupt-Related Covert Channels in an Information-Theoretic Framework .....	326
<i>Heiko Mantel and Henning Sudbrock</i>	
Probability of Error in Information-Hiding Protocols .....	341
<i>Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Prakash Panangaden</i>	

## **Security Protocol Analysis**

Causality-Based Abstraction of Multiplicity in Security Protocols .....	355
<i>Michael Backes, Agostino Cortesi, and Matteo Maffei</i>	
The Insecurity Problem: Tackling Unbounded Data .....	370
<i>Sibylle Fröschle</i>	
LTL Model Checking for Security Protocols .....	385
<i>Alessandro Armando, Roberto Carbone, and Luca Compagna</i>	
<b>Author Index</b> .....	<b>397</b>