

Proceedings

**19th IEEE Computer Security
Foundations Workshop
(CSFW 2006)**

5–7 July 2006

Venice, Italy

Sponsored by

IEEE Computer Society Technical Committee on Security and Privacy



Los Alamitos, California

Washington • Tokyo

Copyright © 2006 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved.

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries may photocopy beyond the limits of US copyright law, for private use of patrons, those articles in this volume that carry a code at the bottom of the first page, provided that the per-copy fee indicated in the code is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

Other copying, reprint, or republication requests should be addressed to: IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, P.O. Box 133, Piscataway, NJ 08855-1331.

The papers in this book comprise the proceedings of the meeting mentioned on the cover and title page. They reflect the authors' opinions and, in the interests of timely dissemination, are published as presented and without change. Their inclusion in this publication does not necessarily constitute endorsement by the editors, the IEEE Computer Society, or the Institute of Electrical and Electronics Engineers, Inc.

IEEE Computer Society Order Number P2615

ISBN-13: 978-0-7695-2615-7

ISBN-10: 0-7695-2615-2

ISSN 1063-6900

Library of Congress Control Number

Additional copies may be ordered from:

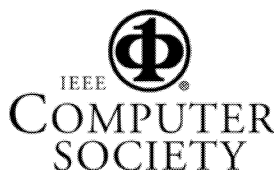
IEEE Computer Society
Customer Service Center
10662 Los Vaqueros Circle
P.O. Box 3014
Los Alamitos, CA 90720-1314
Tel: + 1 800 272 6657
Fax: + 1 714 821 4641
<http://computer.org/cspress>
csbooks@computer.org

IEEE Service Center
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
Tel: + 1 732 981 0060
Fax: + 1 732 981 9667
[http://shop.ieee.org/store/
customer-service@ieee.org](http://shop.ieee.org/store/customer-service@ieee.org)

IEEE Computer Society
Asia/Pacific Office
Watanabe Bldg., 1-4-2
Minami-Aoyama
Minato-ku, Tokyo 107-0062
JAPAN
Tel: + 81 3 3408 3118
Fax: + 81 3 3408 3553
tokyo.ofc@computer.org

Individual paper REPRINTS may be ordered at: reprints@computer.org

Editorial production by Randall S. Bilof
Cover art production by Joe Daigle/Studio Productions
Printed in the United States of America by The Printing House



IEEE Computer Society
Conference Publishing Services
<http://www.computer.org/proceedings/>

Contents

Proceedings of the 19th IEEE Computer Security Foundations Workshop

CSFW 2006

Preface	viii
Workshop and Steering Committees	ix
Program Committee	x

Session 1: Information Flow

A Temporal Logic Characterisation of Observational Determinism	3
<i>Marieke Huisman, Pratik Worah, and Kim Sunesen</i>	
Encoding Information Flow in Haskell.....	16
<i>Peng Li and Steve Zdancewic</i>	
Coercion-Resistance and Receipt-Freeness in Electronic Voting.....	28
<i>Stéphanie Delaune, Steve Kremer, and Mark Ryan</i>	

Session 2: Games, Plans, and Transformations

On the Completeness of Attack Mutation Algorithms.....	43
<i>Shai Rubin, Somesh Jha, and Barton P. Miller</i>	
Types and Effects for Secure Service Orchestration.....	57
<i>Massimo Bartoletti, Pierpaolo Degano, and Gian Luigi Ferrari</i>	
Games for Controls.....	70
<i>Krishnendu Chatterjee, Radha Jagadeesan, and Corin Pitcher</i>	

Session 3: Access Control

Privacy APIs: Access Control Techniques to Analyze and Verify Legal Privacy Policies	85
<i>Michael J. May, Carl A. Gunter, and Insup Lee</i>	
On Key Assignment for Hierarchical Access Control	98
<i>Jason Crampton, Keith Martin, and Peter Wild</i>	
Secrecy by Typing and File-Access Control.....	112
<i>Avik Chaudhuri and Martín Abadi</i>	
Policy Analysis for Administrative Role Based Access Control	124
<i>Amit Sasturkar, Ping Yang, Scott D. Stoller, and C. R. Ramakrishnan</i>	

Session 4: Security Protocol Analysis

Verified Interoperable Implementations of Security Protocols.....	139
<i>Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon, and Stephen Tse</i>	
Cryptographically Sound Theorem Proving	153
<i>Christoph Sprenger, Michael Backes, David Basin, Birgit Pfizmann, and Michael Waidner</i>	
Resolve-Impossibility for a Contract-Signing Protocol	167
<i>Aybek Mukhamedov and Mark D. Ryan</i>	

Session 5: Language, Interaction, and Change

Securing Interaction between Threads and the Scheduler	177
<i>Alejandro Russo and Andrei Sabelfeld</i>	
Information-Flow Security for Interactive Programs.....	190
<i>Kevin R. O’Neill, Michael R. Clarkson, and Stephen Chong</i>	
Managing Policy Updates in Security-Typed Languages	202
<i>Nikhil Swamy, Michael Hicks, Stephen Tse, and Steve Zdancewic</i>	

Session 6: Language, Obfuscation, and Robustness

Noninterference in the Presence of Non-Opaque Pointers.....	217
<i>Daniel Hedin and David Sands</i>	
Independence from Obfuscation: A Semantic Framework for Diversity.....	230
<i>Riccardo Pucella and Fred B. Schneider</i>	
Decentralized Robustness	242
<i>Stephen Chong and Andrew C. Myers</i>	

Session 7: Authorization and Trust

Distributed Authorization Using Delegation with Acyclic Paths	257
<i>Antonio Lain and Miranda Mowbray</i>	
A Framework for Establishing Decentralized Secure Coalitions.....	270
<i>Hongbin Zhou and Simon N. Foley</i>	
Non-Interference in Constructive Authorization Logic	283
<i>Deepak Garg and Frank Pfenning</i>	

Session 8: Protocols and Cryptographic Foundations

Refuting Security Proofs for Tripartite Key Exchange with Model Checker in Planning Problem Setting	297
<i>Kim-Kwang Raymond Choo</i>	
Simulation-Based Security with Inexhaustible Interactive Turing Machines	309
<i>Ralf Küsters</i>	
Computationally Sound Compositional Logic for Key Exchange Protocols	321
<i>Anupam Datta, Ante Derek, John C. Mitchell, and Bogdan Warinschi</i>	
Author Index	335