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
Contents


CSFW 2006

Preface .......................................................................................................................... viii
Workshop and Steering Committees ........................................................................... ix
Program Committee ...................................................................................................... x

Session 1:
Information Flow

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

Session 2:
Games, Plans, and Transformations

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

Session 3:
Access Control

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

v
Session 4: Security Protocol Analysis

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

Session 5: Language, Interaction, and Change

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

Session 6: Language, Obfuscation, and Robustness

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

Session 7: Authorization and Trust

Distributed Authorization Using Delegation with Acyclic Paths .................................................. 257
  Antonio Lain and Miranda Mowbray
A Framework for Establishing Decentralized Secure Coalitions .............................................. 270
  Hongbin Zhou and Simon N. Foley
Non-Interference in Constructive Authorization Logic ............................................................... 283
  Deepak Garg and Frank Pfenning
Session 8:
Protocols and Cryptographic Foundations

Refuting Security Proofs for Tripartite Key Exchange with Model Checker in Planning Problem Setting .... 297
   Kim-Kwang Raymond Choo

Simulation-Based Security with Inexhaustible Interactive Turing Machines ............................................. 309
   Ralf Küsters

Computationally Sound Compositional Logic for Key Exchange Protocols .............................................. 321
   Anupam Datta, Ante Derek, John C. Mitchell, and Bogdan Warinschi

Author Index ............................................................................................................................................. 335