

Preliminary Program

18th IEEE Computer Security Foundations Workshop (
CSFW 18)



June 20 - 22, 2005

Aix-en-Provence, France



Sponsored by the Technical Committee on Security and
Privacy

of the IEEE Computer Society

Monday, 20 June

Session 1: Information Flow and Security Goals

9:00	Practical Information-flow Control in Web-based Information Systems
	Peng Li and Steve Zdancewic
9:30	Achieving Information Flow Security Through Precise Control of Effects
	William Lawrence Harrison and James Hook
10:00	Belief in Information Flow
	Michael R. Clarkson, Andrew C. Myers and Fred B. Schneider

Session 2: Logic and Knowledge for Protocols

11:15	An Encapsulated Authentication Logic for Reasoning About Key Distribution Protocol
	Iliano Cervesato, Catherine Meadows, and Dusko Pavlovic
11:45	Deciding knowledge in security protocols under (many more) equational theories
	Mart Abadi and V onique Cortier

Session 3: Protocol Case Studies

14:30	A Cryptographically Sound Dolev-Yao Style Security Proof of an Electronic Payment System
	Michael Backes and Markus Drmuth

15:00	Compositional Analysis of Contract Signing Protocols
	Michael Backes, Anupam Datta, Ante Derek, John C. Mitchell, and Mathieu Turuani

Session 4: Five-Minute Talks (16:15 until 17:45); Business meeting (17:45 until 18:00)

Tuesday, 21 June

Session 5: Protocol Verification Techniques

9:00	Analysis of Type-based Analyses of Authentication Protocols
	M. Bugliesi, R. Focardi, and M. Maffei
9:30	Temporal Rank Functions for Forward Secrecy
	Rob Delicata and Steve Schneider
10:00	Reconstruction of Attacks against Cryptographic Protocols
	Xavier Allamigeon and Bruno Blanchet

Session 6: Computational and Formal Models

11:15	Polynomial Runtime in Simulatability Definitions
	Dennis Hofheinz, J n Mller-Quad, and Dominique Unruh
11:45	Computational and Information-Theoretic Soundness and Completeness of Formal Encryption
	Pedro Ad , Gergei Bana, and Andre Scedrov

Session 7: Access Control and Languages

14:30	Nomad: A Security Model with Non Atomic Actions and Deadlines
	Fr ic Cuppens and Nora Cuppens-Boulahia
15:00	Type annotation for stack-based access control
	Tian Zhao
15:30	Enforcing Secure Service Composition
	Massimo Bartoletti, Pierpaolo Degano, and Gian-Luigi Ferrari

Session 8: New Foundational Problems Panel (16:45 until 18:00) or Outing

Wednesday, 22 June

Session 9: Declassification

9:00	On Declassification and the Non-Disclosure Policy
	Gerard Boudol and Ana Matos
9:30	Language-Based Information Erasure
	Stephen Chong and Andrew C. Myers
10:00	Dimensions and Principles of Declassification
	Andrei Sabelfeld and David Sands

Session 10: Availability and Denial of Service

11:15	End-to-end Availability Policies and Noninterference
	Lantian Zheng and Andrew C. Myers
11:45	Game-Based Analysis of Denial-of-Service Prevention Protocols
	Ajay Mahimkar and Vitaly Shmatikov

There are PDF and plain text versions of this programs.

For further information contact:

General Chair	Program Chair	Publications Chair
Roberto Amadio CMI, 39 rue Joliot-Curie 13453, Marseille Cedex 13 France +33 4 91 11 36 14 amadio@cmi.univ-mrs.fr	Joshua Guttman The MITRE Corporation 202 Burlington Rd Bedford, MA 01730 USA +1 781 271 2654 guttman@mitre.org	Jonathan Herzog The MITRE Corporation 202 Burlington Rd Bedford, MA 01730 USA +1 781 271 7281 jherzog@mitre.org