Contents

Composition
Session chair: Simon Foley

The Composability of Non-Interference
Aris Zakinthinos and E.S. Lee

Composing and Decomposing Systems under Security Properties
A.W. Roscoe and L. Wulf

Algebraic Properties of System Composition in the LORAL, Ulysses and McLean Trace Models
A.P. Maneki

Authentication Protocols
Session chair: Michael Reiter

Optimal Authentication Protocols Resistant to Password Guessing Attacks
Li Gong

Key Distribution without Individual Trusted Authentication Servers
Liqun Chen, Dieter Gollmann, and Christopher Mitchell

Analysis of Cryptographic Protocols
Session chair: Gene Tsudik

Towards a Classification of Key Agreement Protocols
Colin Boyd

An Augmentation of BAN-Like Logics
Wenbo Mao

Panel on “What Makes a Cryptographic Protocol Dependable?”
Panel moderator: Catherine Meadows
(Panelists to be announced)

Issues in Implementations
Session chair: Jonathan Millen

The Security Checker: A Semantics-Based Tool for the Verification of Security Properties
R. Focardi, R. Gorrieri, and V. Panini

Implementation of a Discretionary Access Control Model for Script-based Systems
Trent Jaeger and Atul Prakash

Building Higher Resolution Synthetic Clocks for Signaling in Covert Timing Channels
John Janeri, Daniel Schnackenberg, and Daylan Darby

Models of Cryptographic Protocols
Session chair: Michael Merritt

Modelling and Verifying Key-Exchange Protocols Using CSP and FDR
A.W. Roscoe