

**2007 IFIP WG 1.7, ACM SIGPLAN and GI
FoMSESS**

**International
Federation
for
Information
Processing**



7th International Workshop on Issues in the Theory of Security (WITS'07)

March 24 - 25, 2007, Braga, Portugal
co-located with **ETAPS 2007**



Technical Program

SATURDAY, 24 March 2007

- 9:25 - 9:30** *WELCOME*
Riccardo Focardi (University of Venice), Chair
- 9:30 - 10:30** *Invited Talk*
Session Chair: TBA

Véronique Cortier
On the use of formal models for proving cryptographic security notions [\[Abstract\]](#)
- 10:30 – 11:00** *Break*
- 11:00 – 12:30** *Computational Security*
Session Chair: TBA

Laurent Mazare
Computationally Sound Analysis of Protocols using Bilinear Pairings [\[Abstract\]](#)

Ran Canetti, Ling Cheung, Nancy Lynch and Olivier Pereira
On the Role of Scheduling in Simulation-Based Security [\[Abstract\]](#)

Arnab Roy, Anupam Datta, Ante Derek and John Mitchell
Inductive Trace Properties Imply Computational Security [\[Abstract\]](#)
- 12:30 - 14:00** *Lunch*
- 15:00 – 16:00** *Information Flow*
Session Chair: TBA

Gavin Lowe
On information flow and refinement-closure [\[Abstract\]](#)

Catalin Dima and Constantin Enea
Nondeducibility on strategies in the temporal logic of knowledge [\[Abstract\]](#)
- 16:00 – 16:30** *Break*
- 16:30 – 17:30** *Static Analysis of Authentication*
Session Chair: TBA

Han Gao, Pierpaolo Degano, Chiara Bodei and Hanne Riis Nielson
Detecting Replay Attacks by Freshness Annotations [\[Abstract\]](#)

Michael Backes, Agostino Cortesi, Riccardo Focardi and Matteo Maffei
A Calculus of Challenges and Responses [\[Abstract\]](#)

Social Dinner

SUNDAY, 25 March 2007

9:30 - 10:30 *Invited Talk*
Session Chair: TBA

Thomas Jensen
Certified access control on mobile interactive devices [\[Abstract\]](#)

10:30 - 11:00 *Break*

11:00 - 12:30 *New Models for Security Protocols*
Session Chair: TBA

Christopher Dilloway and Gavin Lowe
On the Specification of Secure Channels [\[Abstract\]](#)

Michael Backes, Agostino Cortesi and Matteo Maffei
Causality-based Abstraction of Multiplicity in Security Protocols [\[Abstract\]](#)

Joshua Guttman, Shaddin Doghmi and F. Javier Thayer
Skeletons and the Shapes of Bundles [\[Abstract\]](#)

12:30 - 14:00 *Lunch*

15:00 – 16:00 *Protocol Verification*
Session Chair: TBA

Erik Poll and Aleksy Schubert
Verifying an implementation of SSH [\[Abstract\]](#)

Wan Fokkink, Mohammad Torabi Dashti and Anton Wijs
Partial Order Reduction for Branching Security Protocols [\[Abstract\]](#)

16:00 - 16:30 *Break*

16:30 - 17:30 **IFIP WG 1.7 Business Meeting**

Back to [WITS'07 Home Page](#)