3rd International Workshop in Formal Aspects in Security and Trust (FAST 2005)

www.iit.cnr.it/FAST2005

Newcastle, UK, July 18-19, 2005

Programme

Monday, July 18 2005

9.30-10.30 *Invited talk*

- **Formal Tools for Web Services Security -** Cédric Fournet

10.30-11.00 break

11.00-12.30 *Security Protocols*

- **On the Formal Analyses of the Zhou-Gollmann Non-repudiation Protocol -** Susan Pancho-Festin, Dieter Gollmann
- **Formal Reasoning about a Specification-based Intrusion Detection for Dynamic Auto-configuration Protocols in Ad hoc Networks -** Tao Song, Calvin Ko, Chinyang Tseng, Poornima Balasubramanyam, Anant Chaudhary, Karl Levitt.
- **A formal approach for reasoning about a class of Diffie-Hellman protocols -** Rob Delicata, Steve Schneider.

12.30-14.00 lunch

14.00-15.30 *Information Flow*

- **Eliminating Implicit Information Leaks by Transformational Typing and Unification -** Boris Koepf, Heiko Mantel.
- **Abstract Interpretation to Check Secure Information Flow in programs with input-output security annotations -** Nicoletta De Francesco, Luca Martini.
- **Opacity generalised to transition systems -** Jeremy Bryans, Maciej Koutny, Laurent Mazare, Peter Y A Ryan

15.30-16.00 break

16.00-18.00 *Analysis*

- **Unifying decidability results on protection systems using simulations -** Constantin Enea.
- **Proof Obligations Preserving Compilation -** Gilles Barthe, Tamara Rezk, Ando Saabas.
- **A Logic for Analyzing Subterfuge in Delegation Chains -** Hongbin Zhou, Simon Foley.
- **Probable Innocence Revisited -** Kostas Chatzikokolakis, Catuscia Palamidessi.

Tuesday, July 19 2005

9.30-10.30 *Invited talk*

- **Voting Technologies and Trust -** Brian Randell

10.30-11.00 break

11.00-12.30 *Trust management*

- **Relative trustworthiness -** Johan Kluwer, Arild Waaler.
- **Securing Untrusted Binaries --- Provably! -** Simon Winwood, Manuel Chakravarty.
- **Normative specification of software systems: a tool for trust and security -** Olga Pacheco.

12.30-14.00 lunch

14.00-15.30 *Access control and anonimity*

- **Typed Access Control vs. Untyped Attackers -** Tom Chothia and Dominic Duggan
- **A security management information model derivation framework: from goals to configurations -** Romain Laborde, François Barrere, Abdelmalek Benzekri.
- **On Anonymity with Identity Escrow -** Aybek Mukhamedov, Mark Ryan.

15.30-16.00 Break

16.00- 17.00 Short papers

- **Relational Structuring of Security Databases -** Mohamed Hamdi, Noureddine Boudriga.
- **Towards Verification of Timed Non-repudiation Protocols -** Kun Wei, James Heather.