ARSPA'05

The Second Workshop on Automated Reasoning for Security Protocol Analysis

Pierpaolo Degano and Luca Viganò

July 16, 2005

Automated Validation of Internet Security Protocols and Applications
Shared cost RTD (FET open) project IST-2001-39252

Schedule: morning

09:00 - 09:15	**Welcome** Pierpaolo Degano and Luca Viganò
09:15 - 10:05	Invited Talk: ***Protocol Analysis: Wireless Networking and Mobility*** John C. Mitchell
10:05 - 10:45	***Cas Cremers, Sjouke Mauw, Erik de Vink*** A Syntactic Criterion for Injectivity of Authentication Protocols
10:45 - 11:15	**Coffee break**
11:15 - 11:55	***Alexey Gotsman, Fabio Massacci, Marco Pistore*** Towards an Independent Semantics and Verification Technology for the HLPSL Specification Language
11:55 - 12:35	***Kenji Imamoto and Kouichi Sakurai*** Design and Analysis of Diffie-Hellman-Based Key Exchange Using One-time ID by SVO Logic
12:45 - 14:15	**Lunch break**

Schedule: afternoon

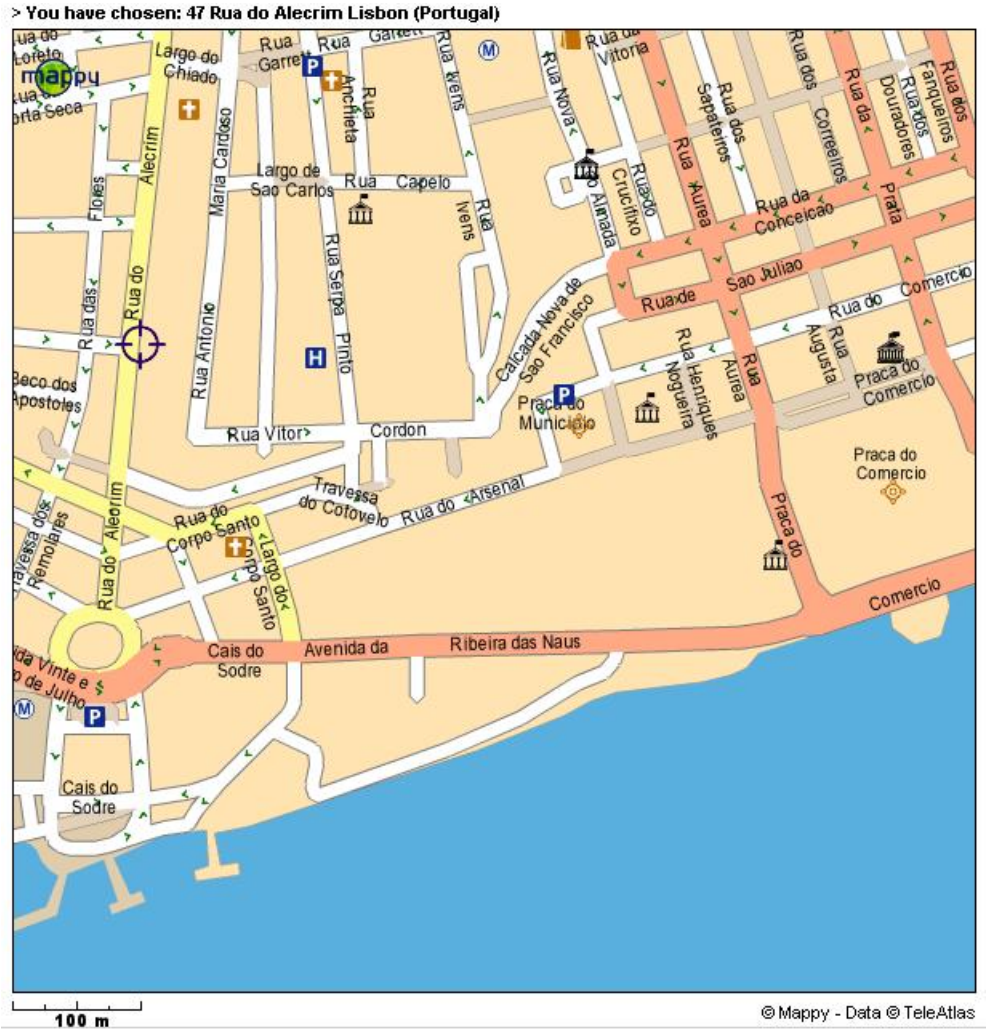
14:15 - 15:05	Invited Talk: ***Justifying Formal Methods and Cryptography under Active Attacks, and Limitations Thereof*** Michael Backes
15:05 - 15:45	***Carlos Caleiro, Luca Viganò, David Basin*** Deconstructing Alice and Bob
15:45 - 16:15	**Coffee break**
16:15 - 16:55	***C. Rosenkilde Nielsen, E. Heltoft Andersen, H. Riis Nielson*** Static Validation of a Voting Protocol
16:55 - 17:35	***Monica Nesi and Giuseppina Rucci*** Formalizing and Analyzing the Needham-Schroeder Symmetric-Key Protocol by Rewriting
17:35 - 18:15	***Deepak D'Souza, K.R. Raghavendra, Barbara Sprick*** An Automata Based Approach for Verifying Information Flow Properties
18:15 - 18:45	Final discussion
20:00 -	**Dinner**

Organization

- **Lunch**: self-service in this building.
- **Dinner**:

Restaurante Charcutaria
Rua do Alecrim 47-A

Time: 20:30



Meeting: exit of underground station in “Largo do Chiado” at 20:15.

Organization

- TCS special issue.
- ARSPA'06 (possibly with Floc in Seattle, August 2006).