Talk abstracts of The 2010 miniWorkshop on Security Frameworks "The matter between Service Users and Service Providers"

Elahe Kani-Zabihi,
Information Security Group, Royal Holloway University of London:

"Service users' requirements: towards an onlne privacy and consent dialogue"

Abstract. The user study conducted for our research is part of a project entitled Visualisation and Other Methods of Expression (VOME) whose main objective is to develop methods of expressing privacy that enable a wider range of privacy concerns to be articulated and offer a broader variety of privacy protection responses. The original premise on which the project is based is as follows: "Many users cannot and do not engage sufficiently with issues of privacy and consent in their interactions with ICT. Consequently they are not able to adequately assess the risks they run and organisations cannot develop services which adequately address users' privacy and consent needs". In order to understand users' privacy behaviour and concerns, we undertook a user-cantered study approach to learn more about the privacy practices at the point of service use and the concerns that influence those practices. Our findings show that engagement in on-line privacy dialogue is a practice that many service users would like to undertake at different times and in different contexts but are currently unable to. In my presentation I also talk about Users' requirements for privacy dialogues. I will then propose a dialogue system to help users articulate their privacy concerns and select effective privacy practices when using on-line services.

Rosario Giustolisi,
Dip. Matematica e Informatica, Università di Catania:

"Can we construct a function that preserves differential-privacy?"

Abstract. It is yet unclear whether differential privacy can be practically adopted for Internet transactions. However, we must first evaluate how feasible it is to construct a function that preserves differential privacy. More specifically, let us focus on the problem of performing statistics while preserving privacy of the individual respondents. Our aim would be to compute statistics that comply with differential privacy. This should ensure that no privacy leak may occur by joining a statistical database. If on one hand, a few recent algorithms seem to confirm that differential privacy can be achieved for this application, more recent tests, conducted on real datasets, somewhat discredit the practical usefulness of such algorithms. The talk aims at shedding some light upon this controversy.

Gabriele Lenzini,
Interdisciplinary Centre for Security, Reliability and Trust, University of Luxembourg:

"On Contextual Biometric-based Authentication"

Abstract. We introduce and comment on the concept of contextual pseudo identity. A contextual pseudo identity is a soft identity token that is built from both a user's biometric and the context. When it comes to ubiquitous authentication, a contextual pseudo identity promises better security than that offered by traditional biometrics-based identity tokens: the use of context improves the tokens' disposability and renewability, which are two essential properties in the protection of a user's real identity.

Gianpiero Costantino,
Dip. Matematica e Informatica, Università di Catania:

"Investigating the `character' of service providers"

Abstract. During my Ph.D I tackled various stringent matters of Mobile Ad hoc Networks (MANETs). Starting with trusting issues, I then moved on to collaboration and power-saving providing a combined solution in the end. That solution was implemented in the Network Simulator 2 (NS2), and a variety of simulations provide evidence that the solution is viable. Building on top of this work, I'm now approaching well-known "trust" issues with particular emphasis upon service providers. These entities can be variously collaborative, providing services of various quality, from reliable to poor, which can be assessed using established Quality of Service (QoS) techniques. I will introduce and discuss various definitions of trust that seem applicable in this context and, in particular, I will speculate that trust and security are not the same thing.