ERCIM "Alain Bensoussan" Fellowship Scientific Report

Fellow: Stefan Dziembowski
Visited Location : Institute for Informatics and Telematics (IIT), CNR, Pisa
Duration of Visit: 9 months

I - Scientific activity

My research activities during the tenure of the ERCIM "Alain Bensoussan" Fellowship were concentrated around the problem of modelling trust in distributed environments. The starting point for our work was the paper of Steven Weeks (*Understanding trust management systems,* IEEE Symposium on Security and Privacy, 2001), where a new framework (based on lambda calculus and fix-point semantics) for reasoning about trust was proposed. Our idea was to extend this framework by considering lambda-terms with types of higher order. We have shown that this extension allows modelling trust policies that the framework of Weeks cannot capture. In particular, we are able to reason about the *recommendation depth*, which means e.g. that we are able to express the properties like: "Alice trusts that Bob can recommend someone who can recommend a good restaurant, but Alice does not trust that Bob can recommend someone who can recommend someone who can recommend a good restaurant". A real-life situation where properties of this type are needed is e.g. the public key infrastructure X.509 (where the recommendation depth is limited by restricting the length of the certification path). The paper that contains the above ideas is not yet ready and we are currently working on preparing it.

I was also continuing my previous research in cryptography. This resulted in publications [1,2] ([1] was submitted before the start of my ERCIM fellowship, but the final version was prepared during this fellowship). In [1] I proposed a new cryptographic model (that was later called the *Limited-Communication Model)*. The main idea here is to immunize cryptographic protocols against the attacks of malicious programs (like Trojan horses), by introducing an assumption that the amount of data that the adversary can transfer from the infected machine is limited. More precisely, we assume that the adversary (by installing a malicious program on the victim's machine) is able to compute any function on the secret data of the victim, but he can retrieve only an output of a limited length. (E.g. we may assume that the secret stored on the machine has 5 GB, and the adversary is allowed to retrieve only 1 GB of data.) I showed the protocols for the session-key generation and the entity-authentication [1], and the encryption scheme [2] that are secure in this model. More details can be found in [1,2]

II- Publication(s) during your fellowship

[1] S. Dziembowski. *Intrusion-resilience via the Bounded-Storage Model*. In Theory of Cryptography Conference, volume 3876 of LNCS, pages 207–224. Springer, 2006.

[2] S. Dziembowski. *On Forward-Secure Storage*. Accepted to CRYPTO 2006, volume 4117 of LNCS, pages 251–270, Springer, 2006.

III -Attended Seminars, Workshops, and Conferences

Theory of Cryptography Conference 2006, March 4-7 2006, New York City, USA. (I gave a talk)

iTrust 2005 – 4th International Conference on Trust Management, May 16-19, Pisa, Italy