# Taming insecurities with session types

(Category 1: Achievements during the project)

Ilaria Castellani, INRIA Sophia Antipolis, France

We argue that the session framework (namely, session calculi equipped with session types) facilitates the formulation and enforcement of security properties. In a handful of papers written in collaboration with BETTY colleagues from the Universities of Torino and Gröningen [1, 2, 3, 4], we investigated two classical security properties, *access control* and *secure information flow* [7], in the setting of multiparty sessions. To this end, we considered in [1, 2] a multiparty session calculus with security levels for both data and participants, and we integrated security requirements into the session type system. Thanks to the discipline imposed by session types, these security requirements need not be as strict as in the "free" $\pi$-calculus. In particular, session types help containing *termination leaks*, which are known to be an issue for concurrent programs [6, 5].

The calculus of [1] also accommodates a form of data *declassification*: this is made possible by the fact that participants have security levels and that communication is directed, a feature provided (among others) by the session framework.

The papers [1] and [2] deal respectively with static and dynamic versions of session types with security: the latter takes the form of a monitored semantics, which blocks the execution of a session in case of attempts at security breaches. In the subsequent work [4], we moved one step further by proposing two different adaptation mechanisms in case of security violations, to allow the session to proceed after a violation, in different ways depending on the gravity of the breach. In this setting, the use of session types is essential to allow the replacement of a faulty participant by a fresh one with the same communication behaviour.

Finally, in [3], we argue that the security requirements previously considered could be overly restrictive in some cases. In particular, a party is not allowed to communicate any kind of public information after receiving a secret information. To overcome this restriction, [3] proposes a new type discipline, which classifies messages according to their topics and allows unrestricted sequencing of messages on independent topics. Here again, the session framework makes it possible to identify a set of topics for the participants, since their roles are predefined.

## References


[1] S. Capecchi, I. Castellani, and M. Dezani-Ciancaglini. Typing access control and secure information flow in sessions. *Journal of Information and Computation*, 238:68 – 105, 2014. DOI = 10.1016/j.ic.2014.07.005.

[2] S. Capecchi, I. Castellani, and M. Dezani-Ciancaglini. Information Flow Safety in Multiparty Sessions. *Mathematical Structures in Computer Science*, pages 1–43, 2015. DOI = 10.1017/S0960129514000619.

[3] I. Castellani, M. Dezani-Ciancaglini, and U. De'Liguoro. Secure Multiparty Sessions with Topics. In *Proc. PLACES 2016*, volume 211 of *EPTCS*, pages 1–12. Dominic A. Orchard and Nobuko Yoshida, Eds, 2016.

[4] I. Castellani, M. Dezani-Ciancaglini, and J. A. Perez. Self-adaptation and secure information flow in multiparty communications. *Formal Aspects of Computing*, 28(4):1–28, 2016.

[5] A. Sabelfeld and A. C. Myers. Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21(1):5–19, 2003.

[6] G. Smith and D. Volpano. Secure Information Flow in a Multi-threaded Imperative Language. In *Proc. POPL'98*, pages 355–364. ACM Press, 1998.

[7] D. Volpano, G. Smith, and C. Irvine. A sound type system for secure flow analysis. *Journal of Computer Security*, 4(3):167–187, 1996.