A Sequent Calculus for the Computationally Complete Symbolic Attacker (ongoing work) ⋆

Pedro Adão[1] and Pedro Baltazar[1]

SQIG-IT and IST-TULisbon, Portugal,
{pedro.adao,pedro.baltazar}@ist.utl.pt

Recently Bana and Comon-Lundh [2] proposed a new technique to define symbolic attackers called *computationally complete symbolic adversary*. Contrary to the "traditional" computational soundness results where the behavior of a symbolic adversary is defined and then shown that under certain hypothesis if there is no successful symbolic attack then there is no successful computational attack, they adopt a different approach where the adversary is capable of doing everything as long as it does not violate a set of axioms. These axioms are derived from the computational assumptions on the adversary (such as unable to break CCA2) and are shown to be computational sound in the presence of such assumptions. Their main result states that for a bounded number of sessions, the non-existence of symbolic attacks consistent with the axioms implies the non-existence of computational attacks against any implementation satisfying those axioms. Bana et al [1] applied this technique to show the security of the NSL protocol in the presence of a CCA2 secure encryption scheme, namely the secrecy of the exchanged names, and mutual authentication of both parties.

In this work we propose ourselves to improve on the usability of the framework introduced in [2]. First, we considered symbolic executions of protocols similar to [2] and later extend it to computational executions. Security axioms are expressed as restrictions over the allowed sequence of actions. Then we developed a proof system with two families of rules that allow us to derive both the view of the protocol by an agent and the view of the protocol by the context/environment. We then show that each execution can be associated with a proof tree and vice-versa.

The interesting aspect is that different proof trees may have the same execution in which case we call them *equivalent proof trees*. Our goal is to study authentication properties as equivalence of proof trees, that is, we want to show that given the proof tree of the view of one agent, its associated execution is also an execution of the proof tree of the view of the other agent. Another interesting property of this approach is that security axioms can also be seen as a well-formedness property of proof trees.

References

1. G. Bana, P. Adão, and H. Sakurada. Computationally complete symbolic attacker in action. In *Proceedings of FSTTCS'12*, pages 546–560, 2012. Full version available at IACR ePrint Archive, Report 2012/316.
2. G. Bana and H. Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. In *Proceedings of POST'12*, LNCS, 2012.

⋆ Partially supported by FCT projects ComFormCrypt PTDC/EIA-CCO/113033/2009 and PEst-OE/EEI/LA0008/2013.