Computationally Sound Verification of the NSL Protocol via Computationally Complete Symbolic Attacker *

Gergei Bana[1], Pedro Adão[2], and Hideki Sakurada[3]

[1] MSR-INRIA Joint Centre, Orsay, France bana@math.upenn.edu
[2] SQIG-IT and IST-TULisbon, Portugal, pedro.adao@ist.utl.pt
[3] NTT Communication Science Laboratories, Atsugi, Kanagawa, Japan, sakurada.hideki@lab.ntt.co.jp

Contrary to many computational soundness results where 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, Bana and Comon-Lundh presented recently [2] a new technique to define symbolic attackers called *computationally complete symbolic adversary*, that is more suitable for computational soundness than the usual Dolev-Yao adversary. Instead of limiting the adversarial's moves, this 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.

In this work we apply this general framework to the verification of public-key authentication protocols, namely the NSL protocol. We define the CCA2 limitation of the symbolic adversary using one axiom for secrecy and another one for non-malleability, and then prove that there is no symbolic adversary compliant with these axioms that violates the secrecy of the exchanged names, nor the mutual authentication of both parties. These two axioms are shown to be implied by the CCA2 (computational) security property. Applying their general result one obtains that there is no possible computational attack against any implementation for which these axioms are sound—namely, implementations using CCA2 encryption, and satisfying a minimal parsing requirement for pairing [4]—except with negligible probability. This is done allowing the adversary to generate any number of bad keys, the presence of any number of other corrupted, uncorrupted, or dynamically corrupted parties besides the two honest parties, and not needing to tag pairs, encryption, nor names that are usual hypothesis in the literature.

References

1. G. Bana, P. Adão, and H. Sakurada. Computationally sound verification of the NSL protocol via computationally complete symbolic attacker, 2012. Submitted.
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/LA0008/2011.

[4] We need an this axiom expressing a certain parsing unambiguity, otherwise an attack exists.