Logical Proofs of Authentication Protocols and Type-Flaw Attacks

Pedro Adão[1] * and Gergei Bana[2]

[1] SQIG–Instituto de Telecomunicações and IST–TULisbon, Portugal
[2] LSV, ENS Cachan, France
pedro.adao@ist.utl.pt gebana@lsv.ens-cachan.fr

In this work we apply the logical system introduced by Bana *et al.* [BHO10] to the proof of authentication protocols, namely Needham-Schroeder-Lowe protocol, the amended Needham-Schroeder shared key protocol, and the Otway-Rees protocol. We have proven agreement and authentication properties of these protocols, up to their known weaknesses, for an unbounded number of sessions. The computational soundness of the logical system ensures us the soundness of the security results.

The security proof method is very intuitive and relies on the specification of a property expressing the uncorrupted nature of keys and nonces. We verify that for critical nonces and keys this property is an invariant, that is, no send action of honest agents corrupts them, and then derive the agreement and authentication properties of the protocol.

With this direct proof one does not need to show that the non existence of a symbolic adversary implies the non-existence of a computational adversary. This is implied by the fact that our logic only allows us to derive facts that are true in the computational model. Moreover, we do not need any condition on the parsing of terms.

We put particular emphasis on detection of type-flaw attacks with this proof system, and how adjustments of the axioms can reflect whether an attacker may have or cannot have the capability to computationally equate different symbolic terms. For example, there is an attack on NSL that relies on equating an arbitrary string n paired with a principal name Q chosen by the adversary, that is, $\langle n, Q\rangle$, with a fresh value N. In accordance with this, we cannot prove the NSL protocol without the axiom $\langle n, Q\rangle \neq N$. This axiom may be added as long as we are certain that $\langle n, Q\rangle$ cannot be equal to N. For example, if agents match the length of the strings that they think are nonces received from others to a pre-specified nonce-length, and the length of the pairing depends only on its inputs, then such adversarial capability is impossible.

All three protocols have weaknesses, and we show how during the course of the proof axioms that are necessary but not present in our system, as they are not necessarily sound, can be used to mount attacks against the protocol. Adding the missing axioms and the conditions in which they are sound allow us to show the security results.

We also discuss the extent to which the Otway-Rees protocol can be verified and how the known attacks to this protocol can be easily revealed in the course of the proof.

References

[BHO10] Gergei Bana, Koji Hasebe, and Mitsuhiro Okada. Secrecy-oriented first-order logical analysis of cryptographic protocols. Cryptology ePrint Archive, Report 2010/080, 2010. http://eprint.iacr.org/.

* Partially supported by FEDER/FCT project KLog PTDC/MAT/68723/2006 and FEDER/FCT project QSec PTDC/EIA/67661/2006.