Formal Security Proofs

Hubert Comon-Lundh
LSV, CNRS & ENS de Cachan, France

The goal of the lecture is to present some aspects of formal security proofs of protocols. This is a wide area, and there is another lecture (by B. Blanchet) on related topics. The idea is therefore to explain in depth one particular technique, that relies on deducibility constraints. We rely mainly on two introductory documents [1, 3].

Here is a roadmap:

Lecture 1 We introduce the problem with examples and touch a little the question of the validity of the security models.

We describe then a small process algebra, that will serve as a model for the protocols, as well as a few security properties

Lecture 2 & 3 The core of the lecture is here: we introduce the attacker model, as a deduction system, and show how to represent any execution in the hostile environment as *deducibility constraints.* In short, a deducibility constraint is a sequence of proofs, in which some parts are unknown (and formalized with variables) and possibly re-used in other constraints. An instance of such a constraints yields an attacker's strategy.

We explain how to solve such constraints in a particular setting of a few cryptographic primitives. This is more or less what is described in the first part of [2].

Lecture 4 For the last part, there are several options (we did not decide yet which will be chosen; it may also depend on B. Blanchet's lecture):

1. More on the deducibility constraints method, for instance for other security primitives.
2. Introducing static equivalence, and touching the problem of proofs of equivalence- based security properties.
3. An introduction on the validation problems and methods (the soundness problem).
4. Composition problems and techniques.

Though the lecture aims at being self-contained, it assumes some familiarity with inference rules/formal proofs (or SOS for programming languages) and terms/substitutions/unification. Similarly, a knowledge on concurrency is not required, but will make easier the understanding of the model.

There will be exercises, possibly relying on an automatic verification tool.

References

[1] B. Blanchet, H. Comon-Lundh, S. Delaune, C. Fournet, S. Kremer, D. Pointcheval. *Cryptographic Protocols: Formal and Computational Proofs of Security.* Lecture Notes of the Parisian Master of Research in Computer Science (MPRI), 2011. Available on the MPRI web pages.

[2] H. Comon-Lundh, V. Cortier, E. Zalinescu. *Deciding Security Properties of Cryptographic Protocols. Application to Key Cycles.* Transaction on Computational Logic, 11(2), 2010.

[3] V. Cortier, S. Kremer (eds). *Formal Models and Techniques for Analyzing Security.* IOS Press, 2011.