M2 Internship: Automatically finding attacks on security protocols

Hubert Comon-Lundh
LSV, École Normale Supérieure de Cachan
comon@lsv.ens-cachan.fr

October 24, 2013

Abastract

The research can go in two complementary directions (see the detailed version for the a more precise description):

1. Search for strategies of consistency proofs in a specific context (ground formulas and a fixed set of axioms); a consistency proof amounts here to finding an attack on a security protocol.
2. Axiomatize new cryptographic primitives and prove the computational soundness of these axioms.

1 Framework

The general framework is the security of cryptographic protocols. Such protocols are small distributed programs relying on cryptographic primitives such as encryption, digital signatures, one-way functions... They are used in numerous applications: internet transactions, mobile phones, smart cards, RFID cards,...

State of the art Formal methods have been used in the past decades for the verification of security protocols. Such formal mehods necessarily rely on formal models of the protocols, typically process algebras.

In such formal models, the security primitives are idealized: the messages are represented by terms in a formal algebra and the possible operations on these messages are specified using equations. For instance, we could specify the decryption as $\mathsf{dec}(k, \mathsf{enc}(x, k)) = x$.

Unfortunately, these models (so-called "Dolev Yao") are not necessarily fully abstract: it happened (and will happen) that a protocol is formally proved in such a model and later an attack is found (in a more accurate model). It is embarrassing. We therefore need to prove that our formal model is adequate (or fully abstract) w.r.t a concrete model. This is what is called *computational soundness*.

Since the landmark work of M. Abadi and Ph. Rogaway [1], several computational soundness proofs have been proposed. However, they alwas assume hypotheses that are often considered as unrealistic. Moreover, these results only apply to a fixed set of cryptographic primitives. Finally, the soundness proofs are usually very long and complex.

In a recent paper [2], we propose a completely different point of view, that avoids most of the computational proofs and does not assume the hypotheses that were required so far. The basic idea is to consider a stronger model of attacker (greatest fixed point instead of smallest fixed point) in which, everything that is not explicitly forbidden is allowed. In this way, we cannot miss an attack, but may get false attacks when the forbidden part is undespecified.

In such a setting, the existence of an attack amounts to the consistency of the attacker's actions, together with the negation of the security property and the axioms specifying what is forbidden.

The context of LSV. The LSV and its research themes are described on `http://www.lsv.ens-cachan.fr/`.

In the lab, Guillaume Scerri is currently completing a PhD thesis along the ideas that are presented in the previous section. In this area, his current main contribution is to design a polynomial time decision procedure for a fragment of first-order logic that would be relevant to the consistency proofs of the previous section [3]. He is also currently implementing the algorithm for further experiments on real protocols.

However, this is the last PhD year for G. Scerri and it is clear now that there are still many questions that will not be investigated during his thesis.

2 Goals of the internship

The work of G. Scerri is focused on the encryption primitive only, relying on the axiomatisation proposed in [2]. Moreover, his goal was to find polynomial time proof strategies only.

There are (at least) three research directions that are complementary (and also complementary to the work of G. Scerri) and that can be followed during an M2 research internship:

1. Looking for better strategies
2. Looking for a better axiomatization of integretity
3. Axiomatize new primitives

Better strategies The first step is experimental: using G. Scerri's prototype, to understand the situations that yield a combinatorial explosion. This should allow to design new strategies and prove their completeness (and possibly investigate their complexity).

New axioms In theory, without the integrity axiom, the consistency, in our framework, is in PTIME. However, with the integrity axiom, it is expected to be out of PTIME. It is therefore important to look for other axiomatisations, that would yield efficient decision procedures or to show that there is no hope.

New primitives The goal here is to propose first-order axiomatisations of security properties of other primitives. For instance "unforgeability" of signatures. This requires to complete a computational proof of the axiom.

3 Requirements

A basic knowledge in logic (for computer science) is mandatory. It is also better to have some knowledge in concurrency theory.

For some research directions (axiomatizations and computational soundness), computability/provable cryptography is useful.

Having followed the lecture 2.30 on the verification of cryptographic protocols is useful, but not mandatory.

References

[1] Martín Abadi and Phillip Rogaway. Reconciling two views of cryptography (the computational soundness of formal encryption). *J. Cryptology*, 15(2):103–127, 2002.

[2] Gergei Bana and Hubert Comon-Lundh. Towards unconditional soundness: Computationally complete symbolic attacker. In Pierpaolo Degano and Joshua D. Guttman, editors, *Proceedings of the 1st International Conference on Principles of Security and Trust (POST'12)*, volume 7215 of *Lecture Notes in Computer Science*, pages 189–208. Springer, March 2012.

[3] Hubert Comon-Lundh, Véronique Cortier, and Guillaume Scerri. Tractable inference systems: an extension with a deducibility predicate. In *Proceedings of the 24th International Conference on Automated Deduction (CADE'13)*, volume 7898 of *Lecture Notes in Artificial Intelligence*, Lake Placid, New York, USA, 2013. Springer.