Computational and Symbolic proofs of security
Spring school and workshop
Japan, April 2009

Supported by
Nippon Telegraph & Telephone Corp.,
Research Center for Information Security,
Centre National de la Recherche Scientifique,
Japan Science and Technology agency

November 10, 2008

1 Introduction

Security protocols take everyday a larger place in all kinds of communications: mobile telephone, internet transactions, smart cards, wireless communications, electronic voting,... A failure in the security of such protocols may have huge consequences, both socially and economically. It is therefore very important to increase our confidence in the achievement of their security goals. That is why there has been a lot of research in the area of provable security during the last decade.

Proving security requires a formal setting, in which protocols and security properties are expressed and the proofs are conducted. An issue is the choice of such a formal background. There are several candidates, in particular what we call the *computational model*, in which an attacker is modeled as any interactive probabilistic Turing machine running in worst-case polynomial time. Another candidate is the *symbolic model*, in which messages are abstracted as formal expressions and the attacker is any process, that can only use the designated primitives.

If we choose a model, which is considered as accurate, then it is extremely difficult to write down formal checkable proofs for general security properties. On the other end, if the model is rough, then security proofs are relatively easier to produce and to check, however there might still be attacks, because the model is not accurate enough.

In a pioneering work, M. Abadi and P. Rogaway have shown in 2000, how it might be possible to get strong security guarantees, while performing the proofs in a simple model. The idea is to show that a computational attacker is unlikely to succeed if a symbolic one fails, provided that the atomic security primitives satisfy some security assumptions.

M. Backes and B. Pfitzmann on the one hand and R. Canetti and R. Segala on the other hand also developped during the last 6 years frameworks aiming at the same goal: relatively simple security proofs, while getting strong security guarantees.

2 The aim of this spring school and workshop

is to survey these recent works. Here are some of the important questions that will be raised during the meeting:

- To which extent is it possible to automatize/machine check security proofs ?
- Is it possible/realistic to prove the security of real protocols in any environment ?
- How far can we go in the abstraction without loosing attacks ?
- What are the most promising techniques/approaches if we want to increase our confidence in the protocols ?

3 Format of the meeting

3.1 Scientific program

The meeting is expected to last 4 full days, during the first weeks of April, 2009. It will take place in Japan, within 2 hours from Tokyo. Every morning will be dedicated to the introduction of the different approaches, for instance:

- Provable security
- Soundness results
- Composability
- Simulatability

Invited speakers will include the best specialists of the area.

Each afternoon will be devoted to more technical presentations: we expect 4 presentations by invited senior researchers and other presentations, selected by a program committee out of submissions. We will therefore issue a call for papers.

The organizing and selection committees are chaired by:

- H. Comon-Lundh (ENS Cachan and AIST)
- M. Hagiya (Univ. of Tokyo)
- T. Okamoto (NTT research laboratories)

Evenings will be devoted to discussions.

3.2 Support

Currently, the meeting is sponsored by

- Nippon Telegraph & Telephone Corp.
- The CNRS/JST French-Japanese project on computational soundness
- The Research Center for Information Security (AIST)

The meeting is expected to gather around 40 researchers. We fix the upper limit to 50, in order to enable discussions and interactions.

Some travel grants might be available. Applications will be selected by the organizing committee.

4 Related conference/events

There is a annual workshop on formal and computational cryptography (FCC). See `http://www.di.ens.fr/~blanchet/fcc08/` for the last edition of this event. FCC is usually a satellite worshop of the IEEE symposium on Computer security foundations (CSF). There is no tutorial at this workshop.

There has been a meeting (workshop) organised at Shloß Dagstuhl `http://www.artist-embedded.org/artist/Dagstuhl-Formal-Protocol.html` in 2007, on the same topics.

The meeting presented here is the first one, which will take place in Japan on these topics. It is also the first one, which will include tutorials.