ARA SSIA FormaCrypt (2005)

Participants: LIENS B. Blanchet, D. Cadé, D. Monniaux, D. Pointcheval
LSV J. Goubault-Larrecq, M. Baudet, H. Comon-Lundh, S. Delaune, S. Kremer, L. Mazaré
LORIA V. Cortier, H. Horodegen, M. Turnani, B. Warinschi, E. Zalinescu
Scientific advisor: M. Abadi

Contact: Bruno Blanchet, blanchet@di.ens.fr
URL: http://www.di.ens.fr/~blanchet/formacrypt/

Objectives of the project

Two models for the verification of cryptographic protocols:

- formal, “Dolev-Yao” model
- computational model

Our goal: bridge the gap between these two models

A computationally sound prover

Goal: Build a specialized, computationally sound, automatic prover.

Results:
- An automatic, computationally sound prover, CryptoVerif, that
  - generates proofs by sequences of games, as in Shoup’s or Bellare and Rogaway’s method;
  - proves secrecy and correspondence assertions (authentication);
  - provides a generic treatment of cryptographic primitives, including shared- and public-key encryption, signatures, MACs, hash functions, computational Diffie-Hellman;
  - is sound in the presence of an active adversary, for a parametric number of sessions;
  - evaluates the probability of an attack (exact security).
- The user is allowed (but does not have) to interact with the prover to make it follow a specific sequence of games.
- CryptoVerif is available at http://www.cryptoverif.ens.fr/.

Examples handled:
- many protocols: correct versions of Needham-Schroeder, Denning-Sacco, Otway-Rees, Yahalom, . . . protocols;
- Full Domain Hash signature scheme;
- encryption schemes of Bellare and Rogaway, CCS’93;
- Kerberos, with and without PKINIT.

Planned extensions:
- Other primitives, such as decisional Diffie-Hellman, xor.
- Additional game transformations.

A computationally sound logic

Goal: Design a computationally sound logic for reasoning symbolically on protocols.

Results:
- Adaptation of the Protocol Composition Logic (PCL) to the computational model.
  - Soundness proof for a subset of PCL with positive tests.
- Extension to prove more complex properties, such as secrecy of keys.
  - This logic is compositional. For example, from the security of keys established using a key exchange protocol, one can prove the security of a secure channel application that uses these keys.

Case studies and comparison of the various approaches

Goal: Compare the results obtained by these approaches.

Result: Comparison between two analyses of the Wide-Mouth-Frog protocol, one by ProVerif and a computational soundness theorem, one by CryptoVerif.