Verification of Security Protocols

Véronique Cortier

LORIA, CNRS, Nancy

Abstract

Security protocols are short programs aiming at securing communications over a network. They are widely used in our everyday life. Their verification using symbolic models has shown its interest for detecting attacks and proving security properties. In particular, several automatic tools have been developed. However, the guarantees that the symbolic approach offers have been quite unclear compared to the computational approach that considers issues of complexity and probability. This later approach captures a strong notion of security, guaranteed against all probabilistic polynomial-time attacks.

In this tutorial, we will first overview several techniques used for symbolically verifying security protocols. In a second part of the presentation, we will present recent results that aim at obtaining the best of both worlds: fully automated proofs and strong, clear security guarantees. The approach consists in proving that symbolic models are *sound* with respect to computational ones, that is, that any potential attack is indeed captured at the symbolic level.