Verification of Security Protocols

Véronique Cortier
LORIA, CNRS
Vandœuvre-lès-Nancy Cedex, France

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 and are used to efficiently detect flaws.

In this talk, we will first review results and techniques that allow automatic analysis of security protocols. In a second part, we will present recent results that demonstrate that formal abstract models used for verification are actually sound with respect to much richer models that consider issues of complexity and probability. As a consequence, it is possible to derive strong, clear security guarantees still keeping the simplicity of reasoning in symbolic models.