Models and Techniques for Analyzing Security Protocols

Véronique Cortier
CNRS, Loria, Nanca, France

Security protocols aims at securing communications over untrusted networks such as Internet. Their design is notoriously error-prone, with aws discovered years later. Formal methods have been successful in reasoning about the security of protocols and detect attacks. Automatic tools have been designed and applied to many protocols, from academic ones to deployed protocols such as SSL or Kerberos. In these lectures, we explain how security protocols can be modeled in symbolic models such as Horn clauses (a fragment of first-order logic) or applied-pi calculus (a process algebra). We describe and discuss decision techniques to automatically verify properties such as authentication or confidentiality. To practice the modeling and analysis of protocols, we use the automatic tool ProVerif.

These lectures will also be the opportunity to play a security game where students design security protocols of their own and find aws in other protocols using ProVerif.

Note: We strongly encourage students to install the ProVerif tool before attending the school, in case the network would not be reliable.

References

- The ProVerif tool can be downloaded and installed from the webpage of the tool `http://prosecco.gforge.inria.fr/personal/bblanche/proverif/`

  On this webpage, you will also find a useful User Manual.

- Lecture notes corresponding to this course have been published in the following reference: *Formal Models and Techniques for Analyzing Security Protocols: A Tutorial*. V. Cortier, St. Kremer. Foundations and Trends in Programming Languages, 1(3):151267, 2014.