Operational semantics and verification of security protocols

Cremers, Cas, author

Abstrak

The authors present a methodology for formally describing security protocols and their environment. This methodology includes a model for describing protocols, their execution model, and the intruder model. The models are extended with a number of well-defined security properties, which capture the notions of correct protocols, and secrecy of data. The methodology can be used to prove that protocols satisfy these properties. Based on the model they have developed a tool set called Scyther that can automatically find attacks on security protocols or prove their correctness. In case studies they show the application of the methodology as well as the effectiveness of the analysis tool.