Journal of Automata, Languages and Combinatorics **11** (2006) 4, 345–374

A TEAM AUTOMATON SCENARIO FOR THE ANALYSIS OF SECURITY PROPERTIES OF COMMUNICATION PROTOCOLS [1]

MAURICE H. TER BEEK
ISTI–CNR, via G. Moruzzi 1, I-56124 Pisa, Italy
e-mail: maurice.terbeek@isti.cnr.it

GABRIELE LENZINI
Telematica Instituut, P.O. Box 589, NL-7500 AN Enschede, The Netherlands
e-mail: gabriele.lenzini@telin.nl

and

MARINELLA PETROCCHI
IIT–CNR, via G. Moruzzi 1, I-56124 Pisa, Italy
e-mail: marinella.petrocchi@iit.cnr.it

ABSTRACT

Formal methods are a popular means to specify and verify security properties of a variety of communication protocols. In this article we take a step towards the use of team automata for the analysis of security aspects in such protocols. To this aim, we define an insecure communication scenario for team automata that is general enough to encompass various communication protocols. We then reformulate the Generalized Non-Deducibility on Compositions schema – originally introduced in the context of process algebrae – in terms of team automata. Based on the resulting team automata framework, we subsequently develop two analysis strategies that can be used to verify security properties of communication protocols. Indeed, the paper concludes with two case studies in which we show how our framework can be used to prove integrity and secrecy in two different settings: We show how integrity is guaranteed in a team automaton model of a particular instance of the Efficient Multi-chained Stream Signature protocol, a communication protocol for signing digital streams that provides some robustness against packet loss, and we show how secrecy is preserved when a member of a multicast group leaves the group in a particular run of the complementary variable approach to the N-Root/Leaf pairwise keys protocol.

Keywords: Team automata, security analysis, security properties, communication protocols

[1] The work presented here was partly supported by the EU project IST-3-016004-IP-09 SENSORIA (*Software Engineering for Service-Oriented Overlay Computers*).