Journal of Automata, Languages and Combinatorics 11 (2006) 1, 7–21

RANDOM POLYNOMIAL-TIME ATTACKS AND DOLEV-YAO MODELS [1]

MATHIEU BAUDET[2]

LSV - CNRS UMR 8643 & INRIA Futurs projet SECSI & ENS Cachan
61, av. du président Wilson 94235 Cachan Cedex, France
e-mail: baudet@lsv.ens-cachan.fr

ABSTRACT

In this paper we present an extension of Dolev-Yao models for security protocols with a notion of random polynomial-time (Las Vegas) computability. First we notice that Dolev-Yao models can be seen as transition systems, possibly infinite. We then extend these transition systems with computation times and probabilities. The extended models can account for normal Dolev-Yao transitions as well as nonstandard operations such as inverting a one-way function. Our main contribution consists of showing that under reasonable assumptions the extended models are equivalent to standard Dolev-Yao models as far as (safety) security properties are concerned.

Keywords: Cryptographic protocols, random polynomial time, Dolev-Yao model, Markov decision processes

1. Introduction

Proving the security of cryptographic protocols has been a major concern ever since flaws were first discovered in some established protocols, the most well-known example being Lowe's attack on the Needham-Schroeder Protocol [23]. Rigorous approaches now exist and have allowed for the analysis of many protocols with respect to various security models. As a matter of fact, two families of models with little in common have been used for years by two different communities.

Computational (or *cryptographic*) models define security in a semantic way by requiring the probability of success of any attacker to be negligible [17, 38]. The class of attacks considered here includes virtually all logical attacks, as soon as they can be implemented by a probabilistic polynomial-time Turing machine.

Formal (or *logical*) models are used by the community of *formal methods* and typically include the Dolev-Yao model [16] and cryptographic process calculi such as the

---

[1] Full version of a submission presented at the *International Workshop on Security Analysis of Systems: Formalisms and Tools*, SASYFT 2004, (Orléans, France, June 21 – 22, 2004).

[2] Partially supported by the the RNTL projects EVA and Prouvé, the ACI Sécurité Informatique Rossignol, the ACI Cryptologie Psi-Robuste, and the ACI jeunes chercheurs "Sécurité informatique, protocoles cryptographiques et détection d'intrusions".