Journal of Symbolic Computation ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Intruder deducibility constraints with negation. Decidability and application to secured service compositions ☆

Tigran Avanesov [a], Yannick Chevalier [b], Michael Rusinowitch [c], Mathieu Turuani [c]

[a] SnT, Université du Luxembourg, Luxembourg
[b] Université Paul Sabatier & IRIT, Toulouse, France
[c] INRIA Nancy–Grand Est & LORIA, 54600 Villers-lès-Nancy, France

ARTICLE INFO

Article history:
Received 23 May 2015
Accepted 19 September 2015
Available online xxxx

Keywords:
Web services
Orchestration
Security policy
Separation of duty
Deducibility constraints
Cryptographic protocols
Formal methods
Automated verification
Synthesis

ABSTRACT

We consider a problem of automated orchestration of security-aware services under additional constraints. The problem of finding a mediator to compose secured services has been reduced in previous works to the problem of solving deducibility constraints similar to those employed for cryptographic protocol analysis. We extend in this paper the mediator synthesis procedure (i.e. a solution for the orchestration problem) by allowing additional non-disclosure policies that express the fact that some data is not accessible to the mediator at a given point of its execution. We present a decision procedure that answers the question whether a mediator satisfying these policies can be effectively synthesized. The approach presented in this work extends the constraint solving procedure for cryptographic protocol analysis in a significant way as to be able to handle negation of deducibility constraints. It applies to all subterm convergent theories and therefore covers several interesting theories in formal security analysis including encryption, hashing, signature and pairing; it is also expressive enough for some RBAC policies. A variant of this procedure for

☆ This work is supported by FP7 AVANTSSAR (AVANTSSAR, 2008–2010, grant number 216471) and FP7 NESSoS (NESSoS, 2010–2014, grant number 256980) projects.

E-mail addresses: tigran.avanesov@uni.lu (T. Avanesov), ychevali@irit.fr (Y. Chevalier), rusi@loria.fr (M. Rusinowitch), mathieu.turuani@loria.fr (M. Turuani).

http://dx.doi.org/10.1016/j.jsc.2016.07.008
0747-7171/

Dolev Yao theory has been implemented in Cl-Atse, a protocol analysis tool based on constraint solving.

1. Introduction

1.1. Context

Trust and security management in distributed frameworks is known to be a non-trivial critical issue. It is particularly challenging in Service Oriented Architecture where services can be discovered and composed in a dynamic way. Implemented solutions should meet the seemingly antinomic goals of openness and flexibility on one hand and compliance with data privacy and other regulations on the other hand. We have demonstrated in previous works (Chevalier et al., 2008, 2012; Avanesov et al., 2012a) that functional agility can be achieved for services with a message-level security policy by providing an automated service synthesis algorithm. It resolves a system of deducibility constraints by synthesizing a *mediator* that may adapt, compose and analyze messages exchanged between client services and having the functionalities specified by a goal service. It is complete as long as the security policies only apply to the participants in the orchestration and not on the synthesized service nor on who is able to participate. However security policies often include such *non-deducibility* constraints on the mediator. For instance an organization may not be trusted to efficiently protect the customer's data against attackers even though it is well-meaning. In this case a client would require that the mediator synthesized to interact with this organization must not have direct access to her private data, which is an effective protection even in case of total compromise. Also it is not possible to specify that the mediator enforces *e.g.* dynamic separation of duty, *i.e.*, restrictions on the possible participants based on the messages exchanged.

Since checking whether a solution computed by our previous algorithm satisfies the non-deducibility constraints is not complete, we propose in this paper to solve during the automated synthesis of the mediator both deducibility and non-deducibility constraints. The former are employed to specify a mediator that satisfies the functional requirements and the security policy on the messages exchanged by the participants whereas the latter are employed to enforce a security policy on the mediator and the participants to the orchestration.

1.1.1. Original contribution

We have previously proposed some decision procedures (Chevalier et al., 2008, 2012; Avanesov et al., 2012a; AVANTSSAR, 2008–2010; NESSoS, 2010–2014) for generating a mediator from a high-level specification with deducibility constraints of a goal service. In this paper, we extend the formalism to include non-deducibility constraints in the specification of the mediator. Then we provide a decision procedure for the resulting class of constraint systems and therefore solve the mediator synthesis problem in this setting. This paper extends the previous publication (Avanesov et al., 2012b) in several aspects: the proofs are reorganized and improved; all omitted reasonings are included; the details on the implementation of the decision procedure for Dolev Yao theory within the Cl-Atse tool are given; and the experimental results for a Loan Origination Process case study with and without non-deducibility constraints are analyzed.

1.1.2. Related works

In order to understand and anticipate potential flaws in complex composition scenarios, several approaches have been proposed for the formal specification and analysis of secure services (Armando et al., 2012; Costa et al., 2011; Armando and Ponta, 2014; Armando et al., 2013; Viganò, 2012, 2013). Among the works dedicated to trust in multi-agent systems, the models closest to ours are Herzig et al. (2010), Lorini and Demolombe (2008) in which one can express that an agent trusts another agent in doing or forbearing of doing an action that leads to some goal. To our knowledge no work has previously considered the automatic orchestration of security services with policies altogether as ours.

Please cite this article in press as: Avanesov, T., et al. Intruder deducibility constraints with negation. Decidability and application to secured service compositions. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.07.008