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

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Satisfiability of general intruder constraints with and without a set constructor ☆

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 31 March 2014
Accepted 15 April 2015
Available online xxxx

Keywords:
ACI
Deducibility constraints
Dolev–Yao deduction system
Multiple intruders
Security

ABSTRACT

Many decision problems on security protocols can be reduced to solving deduction constraints expressing whether an instance of a given message pattern can be constructed by the intruder. Most constraint solving procedures for protocol security rely on two properties of constraint systems called *monotonicity* and *variable-origination*. In this work we relax these restrictions by giving a decision procedure for solving general intruder constraints (that do not have these properties) that stays in NP. The result is also valid modulo an associative, commutative and idempotent theory. The procedure can be applied to verify security protocols in presence of multiple intruders.

1. Introduction

Detecting flaws in security protocol specifications under the perfect cryptography assumption in the Dolev–Yao intruder model is an approach that has been extensively investigated in recent

☆ The work presented in this paper was partially supported by the FP7-ICT-2007-1 Project no. 216471, "AVANTSSAR: Automated Validation of Trust and Security of Service-oriented Architectures" (http://www.avantssar.eu) and FP7-ICT Project no. 256980, "NESSoS: Network of Excellence on Engineering Secure Future Internet Software Services and Systems" (http://www.nessos-project.eu).

E-mail addresses: tigran.avanesov@uni.lu (T. Avanesov), yannick.chevalier@irit.fr (Y. Chevalier), michael.rusinowitch@inria.fr (M. Rusinowitch), mathieu.turuani@inria.fr (M. Turuani).

http://dx.doi.org/10.1016/j.jsc.2016.07.009
0747-7171/

years (Armando et al., 2014; Groza and Minea, 2013; Viganò, 2012; Meadows, 2011; Blanchet, 2009; Guttman, 2007; Arapinis and Duflot, 2007; Turuani, 2006). In particular, symbolic constraint solving has proved to be a very successful approach in the area. It amounts to expressing the possibility of mounting an attack, e.g. the derivation of a secret, as a list of steps where for each step an instance of the message pattern awaited according to the protocol has to be derived from the current intruder knowledge. These steps correspond in general to the progression of the protocol execution, up to the last one which is the secret derivation.

Enriching the standard Dolev–Yao intruder model with different equational theories (Comon-Lundh and Shmatikov, 2003; Comon-Lundh, 2004; Basin et al., 2005; Chevalier and Rusinowitch, 2010; Baskar et al., 2010; Escobar et al., 2011) like exclusive OR, modular exponentiation, Abelian groups, etc. (Liu and Lynch, 2011; Erbatur et al., 2011; Malladi, 2012; Chevalier et al., 2005; Küsters and Truderung, 2008) helps to find flaws that could not be detected considering free symbols only. A particularly useful theory is the theory of an *ACI* operator (that is associative, commutative and idempotent) since it allows one to express sets in cryptographic protocols.

Up to the exception of Mazaré (2005), all proposed algorithms rely on two strong assumptions about the constraints to be processed:

- knowledge monotonicity, reflecting the fact that the intruder could see everything that occurred before and forgot nothing;
- variable origination, reflecting that each variation in the protocol is introduced by the intruder.

Constraints satisfying these hypotheses are called *well-formed constraints* in the literature. Well-formed constraints are sufficient to solve security problems in the standard case where a single Dolev–Yao intruder is assumed. However, we will see that in some situations it can be quite useful to relax these hypotheses and consider *general constraints*, that is constraints without the restrictions above. General constraints naturally occur when considering security problems involving several non-communicating Dolev–Yao intruders (see § 2.1). Note that if intruders can communicate during protocol execution, the model becomes attack-equivalent to one with a unique Dolev–Yao intruder (Syverson et al., 2000). A discussion on a multiple non-collaborating attackers model as well as interesting examples can be found in Fiazza et al. (2012).

1.1. Contributions of the paper

First, we will show that as for the standard case, in this more general framework it is still possible to derive an *NP* decision procedure for detecting attacks on a bounded number of protocol sessions (Sections 5, 4). Second, our result extends previous ones by allowing non-atomic keys (which is an important feature for protocol design as it is common to build symmetric keys from shared secrets) and the usage of an associative commutative idempotent operator (Sections 3, 4) that can be used for instance to model sets of nodes in XML document (see § 2.2). This extension of well-formed constraint systems may seem trivial but a third contribution of this paper is to demonstrate this is not the case by considering subterm deduction systems which are akin to the Dolev–Yao deduction system, but in which the equational theory can be any subterm convergent one. Whereas the decidability of well-formed constraint systems for subterm deduction systems is well known, see e.g. Baudet (2005), we prove in Appendix A that the satisfiability of general constraint systems is not decidable for subterm deduction systems. Finally we will sketch several applications of our results to security analysis in Section 2.

1.2. Related work

The decision procedure for satisfiability of well-formed constraint systems can be used to decide the insecurity of cryptographic protocols with a bounded number of sessions (Rusinowitch and Turuani, 2003). In this domain, several works deviated from the perfect cryptography assumption and started to consider algebraic properties of functional symbols. For example properties of XOR operator and exponentiation were considered in Lynch and Meadows (2004), Chevalier et al. (2005, 2008),

Please cite this article in press as: Avanesov, T., et al. Satisfiability of general intruder constraints with and without a set constructor. J. Symb. Comput. (2016), http://dx.doi.org/10.1016/j.jsc.2016.07.009