Satisfiability of general intruder constraints
Application to distributed attacks

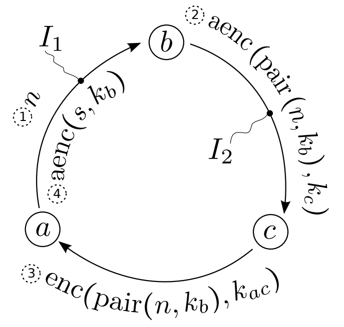
T. Avanesov, Y. Chevalier, M. Rusinowitch, and M. Turuani

Motivations. Detecting flaws in security protocol specifications under the perfect cryptography assumption in Dolev-Yao intruder model is an approach that has been extensively investigated in recent years. In particular symbolic constraint solving has proved to be a very successful approach in the area [1]. It amounts to express the possibility of mounting an attack, e.g. the derivation of a secret, as a list of steps where for each step some message 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. However all known algorithms rely on two strong assumptions about the constraints to be processed: *knowledge monotonicity* and *variable origination*. *Knowledge monotonicity* means that the left-hand side of a constraint representing the current knowledge of the intruder at some protocol step is included into the left-hand side of the constraint at the next step. *Variable origination* means that a variable appears first in the right-hand side of some constraint. Constraints satisfying these hypotheses are called *well-formed constraints* in the literature and they are not restrictive as these conditions hold when handling standard security problems with a single Dolev-Yao intruder. 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. In a distributed attack, intruders might restrict their communications for instance to avoid being detected. Recall that if intruders can communicate during protocol execution, the model becomes attack-equivalent to one with a unique Dolev-Yao intruder. As another application, we have shown in [2] how to reduce the distributed orchestration of secured services to solving general intruder constraints. A recent paper [3] proposes other applications of non well-formed constraints to routing protocols and mobile security.

Our contribution. We have shown that in this general framework of multiple intruders it is still possible to derive an NP decision procedure for detecting attacks on a bounded number of protocol sessions. Second, our result remains valid when including an associative commutative idempotent operator (ACI) that can be used for instance to model sets (like set of nodes in XML messages). The main steps to show the decidability are as follows:

(1) We present an algorithm for solving the derivability problem in Dolev-Yao model with an ACI operator;
(2) We prove that for checking intruder constraints satisfiability it is sufficient to consider normalized (modulo ACI) constraints and normalized substitutions;
(3) We show that a satisfiable normalized constraint system admits at least one conservative solution, that is a substitution σ that maps each variable of the constraint system to a set of subterms from the constraint system (instantiated with σ) and private keys;
(4) We give a bound on the size of a conservative solution, and, as a consequence, we obtain decidability.

An example with multiple intruders. Suppose three agents a, b, c execute a protocol whose normal execution is shown in Fig. 1(a), where $\mathrm{aenc}\,(x, y)$ stands for a message x asymmetrically encrypted with key y, $\mathrm{enc}\,(x, y)$ is a symmetric encryption and $\mathrm{pair}\,(x, y)$ is a concatenation of two messages. Each agent follows his sequence of actions shown in Fig. 1(b), where $!_x y$ is an action of sending to agent x message y, and $?_x y$ is a receiving from x a message matching pattern y; capital letters are placeholders (variables). The agents


I_1
b
2 $\mathrm{aenc}(\mathrm{pair}(n,k_b),k_c)$
1 n
$\mathrm{aenc}(s,k_b)$
4
I_2
a
c
3 $\mathrm{enc}(\mathrm{pair}(n,k_b),k_{ac})$

(a) Normal execution + Intruders layout

$$\begin{array}{llll}
l_a: & !_b n, & ?_c\,\mathrm{enc}\left(\mathrm{pair}\left(n,X\right),k_{ac}\right), & !_b\,\mathrm{aenc}\left(s,X\right) \\
l_b: & ?_a Y, & !_c\,\mathrm{aenc}\left(\mathrm{pair}\left(Y,k_b\right),k_c\right), & ?_a\,\mathrm{aenc}\left(s,k_b\right) \\
l_c: & & ?_b\,\mathrm{aenc}\left(Z,k_c\right), & !_a\,\mathrm{enc}\left(Z,k_{ac}\right)
\end{array}$$

(b) Sequence of actions per agent

$$K^0_{I_1} \cup \{n\} \rhd Y \tag{1}$$

$$K^0_{I_2} \cup \{\mathrm{aenc}\left(\mathrm{pair}\left(Y,k_b\right),k_c\right)\} \rhd \mathrm{aenc}\left(Z,k_c\right) \tag{2}$$

$$\{\mathrm{enc}\left(\mathrm{enc}\left(Z,k_{ac}\right),k\right)\} \rhd \mathrm{enc}\left(\mathrm{enc}\left(\mathrm{pair}\left(n,X\right),k_{ac}\right),k\right) \tag{3}$$

$$K^0_{I_1} \cup \{n,\mathrm{aenc}\left(s,X\right)\} \rhd \mathrm{aenc}\left(s,k_b\right) \tag{4}$$

$$K^0_{I_1} \cup \{n,\mathrm{aenc}\left(s,X\right)\} \cup K^0_{I_2} \cup \{\mathrm{aenc}\left(\mathrm{pair}\left(Y,k_b\right),k_c\right)\} \rhd s \tag{5}$$

(c) Constraint system

Fig. 1. Multiple intruders example

are connected by three directed channels: channel $a \rightharpoonup b$ is controlled by local intruder I_1, channel $b \rightharpoonup c$ is controlled by local intruder I_2, while channel $a \rightharpoonup c$ is secure (free from intruders). We assume that the two local intruders have for initial knowledge a pair of fresh public/private keys and public keys of all participants: $K^0_{I_1} = K^0_{I_2} = \{k_i, \mathrm{priv}\left(k_i\right), k_a, k_b, k_c\}$.

The question is whether the local intruders I_1 and I_2 can cooperate in such a way that joining their final knowledge they can derive s, although they have no means (or do not want) to communicate during the protocol execution.

Following the sequence of actions shown in Fig. 1(a), we obtain the constraint system shown in Fig. 1(c), where $\rhd$ is the standard deducibility predicate.

The obtained constraint system has no solution as well as any other constraint systems generated from different interleaving of actions executed by the agents. We conclude that there is no coordinated attack under the given hypothesis. On the other hand, if I_1 and I_2 can communicate, or the same intruder controls both channels $a \rightharpoonup b$ and $b \rightharpoonup c$, a simple attack can be mounted: I_2 knows n from I_1 and forges $\mathrm{aenc}\left(\mathrm{pair}\left(n,k_i\right),k_c\right)$ that is sent to c on a second step of the normal execution; then on the fourth step a sends $\mathrm{aenc}\left(s,k_i\right)$ intercepted by I_1.

Application to distributed orchestration. In [2] we present a formal framework to model Web services, their security policies and their intercommunication. We consider a rich structure for Web services' messages including ciphered texts to ensure non-disclosure policies. This Web service composition approach relies on the notion of partner corresponding to an organization. Each partner in a composition implements its own part of the orchestration. In this setting standard orchestration is a special case in which only one partner is involved. Partners communicate to each other only data that are not protected by their respective organizations. To express these local policies well-formed constraints are not sufficient, and one has to employ general constraints that can be solved with the procedure above.

References

[1] J. Millen and V. Shmatikov. Constraint solving for bounded-process cryptographic protocol analysis. 8th ACM CCS '01, pages 166–175, 2001.

[2] T. Avanesov, Y. Chevalier, M. Rusinowitch, and M. Turuani Distributed Orchestration of Web Services under Security Constraints. DPM/SETOP, Lecture Notes in Computer Science, vol. 7122, 2012, pages 235-252.

[3] S. Mödersheim, P. Lafourcade, A. Kassem and Y. Lakhnech. Multiple independent lazy intruders. HotSpot 2013, ETAPS Workshop, Rome, March 17.