Towards the orchestration of secured services under non-disclosure policies

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

Motivations. 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. We have demonstrated in previous work [1] that functional agility can be achieved for services with a message-level security policy by providing an automated service synthesis algorithm constructing a *mediator* that may adapt, compose and analyze messages exchanged between client services and have the functionalities specified by a goal service. This method is complete, but only as long as the policies do not concern the synthesized service or the eligibility of the communication participants.However, an organisation 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. This 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 at some step. The *non-deducibility* constraints help to express such types of policies.

Our contribution. We propose here 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. Full details can be found in [2]. Related models [3] exists for trust, without the automatic orchestration of security services with policies altogether. To reach our goal, we extend the constraints in the formalism to include non-deducibility constraints in the specification of the mediator and provide a decision procedure synthesizing a mediator for the resulting constraint systems. It has been implemented as an extension of CL-AtSe [4] for the Dolev-Yao deduction system.

Example. Suppose our goal is to synthesize a mediator that selects two bank clerks satisfying a Separation of Duty property, querry them securely for expertises over a client's request for a loan, and guaranty non-leaking of client's privacy even for himself. Data are represented by first-order terms, with symmetric and assymetric encryptions, signature and pairing (pair). $\mathrm{inv}\,(k)$ is the private key associated to k, and the binary symbol rel expresses that two agents are related. A unary symbol g is employed to designate participants identity in the "relatives" database, which contains facts of the form $\mathrm{rel}(g(a), g(b))$.

The Fig. 1 and 2 shows the sequence of protected messages each service is willing to follow during the orchestration, plus their security policies. Synthetically, client C declares his intention to mediator M, who sends back the names of two clerks A and B to evaluate his request. The client then sends encrypted expertise requests (N_k is for encrypting decisions). Then the mediator furnishes the decisions of clerks, each encrypted with the proposed key N_k, plus signatures. Finally, the client uses these tokens to ask his loan. Symetrically, clerk A receives a request to participate. If he accepts, he returns his identity and public key and receives the client's request for a loan to evaluate. Then he sends back his decision. The clerk's and client's non-disclosure policy are self-explanatory. In particular, the clerk A can be used by the mediator only if the constraint $\natural g(A)$ is satisfied, showing that A is not a relative with any other actor of the protocol, as client and the other clerk (second non-disclosure constraint of Fig. 1).

Clerk's (A) communications:[1]

$$\begin{array}{rl} * \Rightarrow \mathrm{A} & : \mathrm{request.M} \\ \mathrm{A} \Rightarrow \mathrm{M} & : g(A).\,\mathrm{pk}\,(A) \\ \mathrm{M} \Rightarrow \mathrm{A} & : \{Amnt.C.K\}_{\mathrm{pk}(A)} \\ \mathrm{A} \Rightarrow \mathrm{M} & : m_1(A, Resp_A, K, C, Amnt) \end{array}$$

Non-disclosure constraints:

(1) M cannot deduce the last message before it is sent by A.
(2) M cannot deduce $g(A)$ before the second message is sent by A.

Fig. 1. Clerk's communications and non-disclosure constraints

Client's (C) communications:[1]

$$\begin{array}{rl} \mathrm{C} \Rightarrow \mathrm{M} & : \{g(C).loan.P\}^{\mathrm{sig}}_{\mathrm{inv}(pk(C))} \\ \mathrm{M} \Rightarrow \mathrm{C} & : A.B \\ \mathrm{C} \Rightarrow \mathrm{M} & : m_2(A, Amnt).m_2(B, Amnt) \\ \mathrm{M} \Rightarrow \mathrm{C} & : m_3(A, R_a).m_3(B, R_b) \\ \mathrm{C} \Rightarrow \mathrm{P} & : m_4(\mathrm{pk}\,(P)\,, A, B, R_a, R_b) \end{array}$$

Non-disclosure constraints:

(1) M cannot deduce the amount $Amnt$.
(2) M cannot deduce A's decision R_a.
(3) M cannot deduce B's decision R_b.

Fig. 2. Client's communications, and non-disclosure constraints

In contrast with other services, the goal service is only described in terms of possible operations and available initial data. *(i) Initial data:* his own private/public keys; public keys of potential partners (*e.g.* $\mathrm{pk}\,(P)$); and the relational database $\mathrm{rel}(g(a), g(c)), \mathrm{rel}(g(b), g(c)), \ldots$ to be checked against conflict of interests. *(ii) Deduction rules:* Possible operations on messages are modeled by the standard Dolev-Yao deduction system for symmetric/assymetric encryption, signature and pairing, but augmented with two rules for querying the relational database: $x, \mathrm{rel}(x, y) \to y$ and $y, \mathrm{rel}(x, y) \to x$.

To communicate with the services, a mediator must satisfy a sequence of constraints expressing that: *(i)* each message expected by a service can be deduced from all the previously sent messages plus initial knowledge; and *(ii)* each message that should not be known or disclosed (called negative constraint) is not deducible. The orchestration problem consists in finding a satisfying interleaving. If it exists, our procedure outputs a solution which can be translated automatically into a mediator. For instance, clerk's and client's constraints extracted from Fig. 1 and Fig. 2 are:

$$\left\{ \begin{array}{rl} Client(C) \triangleq & !_M\,\{g(C).loan.P\}^{\mathrm{sig}}_{\mathrm{inv}(K_C)}\ ?_M A.B\ !_M m_2(A, Amnt).m_2(B, Amnt) \\ & ?_M m_3(A, R_a).m_3(B, R_b)\ \natural_M Amnt\ \natural_M R_A\ \natural_M R_B \\ & !_P m_4(\mathrm{pk}\,(P)\,, A, B, R_a, R_b) \\ Clerk(A) \triangleq & ?request.M\ \natural_M g(A)\ !_M g(A).\,\mathrm{pk}\,(A)\ ?_M\,\{Amnt.C.K\}_{\mathrm{pk}(A)} \\ & \natural_M m_1(A, Resp_A, K, C, Amnt)\ !_M m_1(A, Resp_A, K, C, Amnt) \end{array} \right.$$

References

[1] T. Avanesov and Y. Chevalier and M.A. Mekki and M. Rusinowitch. Web Services Verification and Prudent Implementation. DPM/SETOP, LNCS 7122 pages 173-189, Springer, 2012.

[2] T. Avanesov and Y. Chevalier and M. Rusinowitch and M. Turuani Towards the Orchestration of Secured Services under Non-disclosure Policies. Proc. of MMM-ACNS, pages 130-145, 2012.

[3] A. Herzig and E. Lorini and J.F. Hübner and L. Vercouter A logic of trust and reputation. Logic Journal of IGPL vol. 18, pages 214-244, 2010.

[4] M. Turuani. The CL-Atse Protocol Analyser. Term Rewriting and Applications (RTA), LNCS 4098 pages 277-286, 2006.

[1] We have employed the following abbreviations for messages:

$$\left\{ \begin{array}{rcl} m_1(A, Resp, K, Ct, S) & = & \{h(A.S.Ct.Resp)\}^{\mathrm{sig}}_{\mathrm{inv}(pk(A))}\,.\{|Resp|\}_K \\ m_2(A, S) & = & \{S.C.N_k\}_{\mathrm{pk}(A)} \\ m_3(A, R) & = & m_1(A, R, N_k, C, Amnt) \\ m_4(K_0, A, B, R_1, R_2) & = & \{Amnt.C.A.R_1.B.R_2\}_{K_0}\,.m_3(A, R_1).m_3(B, R_2) \end{array} \right.$$