Symbolic verification of workflows with security constraints

18 décembre 2013

Proposed by : Clara Bertolissi,
Laboratoire d'Informatique Fondamentale de Marseille
Parc Scientifique et Technologique de Luminy
163, avenue de Luminy
13288 Marseille
clara.bertolissi@lif.univ-mrs.fr
http ://www.lif.univ-mrs.fr/∼clara

Keywords Symbolic model checking, satisfiability modulo theories (SMT), security policies, workflow management systems.

Context Many E-services, such as business processes and commercial transactions, are modelled as workflows. A workflow specifies a collection of tasks and the causal relationships among them. Security-aware workflows are additionally required to satisfy authorization requirements such as assigning users some permissions to execute tasks (e.g. according to a pre-defined access control policy) or Separation of Duty (SoD) constraints, i.e. two tasks have to be executed by different users.

The Workflow Satisfiability Problem (WSP) consists of checking if there exists an assignment of users to tasks such that a security-aware workflow successfully terminates while satisfying all authorization constraints. Such a problem has been studied in several papers ; see, e.g., [6], [2]. The runtime version of the WSP consists of answering sequences of user requests at execution time and ensuring successful termination together with satisfaction of authorization constraints.

To address these problems, we propose a methodology based on the use of Satisfiability Modulo Theories (SMT) techniques, which have been shown quite effective when used as back-end engines in several verification tools (see, e.g., [1]). In [4] we describe a general framework of security-aware workflows and we study the verification of reachability properties of such systems. Let W be the state transition system describing the workflow together with the authorization constraints, and G be the set of states characterizing successful termination of W. Our approach consists of computing the set R(W,G) of states from which it

is possible to reach a state in G, given a finite but arbitrary number of users. Our verification technique, based on symbolic backward reachability, either detects that there is a sequence of transitions from the initial state to one in G (and it returns a concrete successfull configuration) or, on the contrary, it concludes that no such sequence of transitions exists (regardless of the number of users).

For the run-time version, the formula R(W,G) is instantiated with the set U of users that are active in a particular instance of the workflow. Then, the formula is fed to an SMT solver that can act as a monitor solving the run-time version of the WSP for the particular instance of the workflow. An example of runtime monitoring can be found in [5].

Goals : The student will start by learning the basic notions of (security-aware) workflow systems and their specification (see the *Background* section in the bibliography).

Then, taking [4] and [5] as a basis, the student will focus on a restricted (but application relevant) class of workflows in order to develop and test efficient verification procedures, both statically and at runtime.

At a later stage, it would be interesting to integrate in our approach the analysis of workflow systems dealing with data (such as user identifiers or amounts of money) or taking into consideration risk values associated to the execution of tasks.

Références

Background :

[1] L. De Moura and N. Bjrner. Satisfiability modulo theories : introduction and applications. Commun. ACM, 54 :6977, September 2011.

[2] Q. Wang and N. Li. Satisfiability and resiliency in workflow authorization systems. ACM Trans. Inf. Syst. Secur., 13 :40 :140 :35, December 2010.

[3] R. Sandhu, E. Coyne, H. Feinstein, and C. Youmann. Role-Based Access Control Models. IEEE Computer, 2(29) :3847, 1996.

[4] T. Murata. Petri nets : properties, analysis and applications. Proc. of the IEEE, 77(4) :541580, 1989.

(Security-aware) workflow verification :

[4] C. Bertolissi and S. Ranise. Verification of Composed Array-based Systems with Applications to Security-Aware Workflows. In Proc. of FROCOS13, Nancy, France, LNCS. Springer, 2013.

[5] C. Bertolissi and S. Ranise. A methodology to build run-time monitors for Security-Aware Workflows. In Proc. of ICITST13, London, UK. IEEE, 2013.

[6] J. Crampton. A reference monitor for workflow systems with constrained task execution. In 10th ACM SACMAT, pages 3847. ACM, 2005.