Internship proposal

Title: Verification of security sensitive workflows with data

Location: Team Modelisation and Verification, Laboratoire d'Informatique et des Systèmes, Luminy
`http://www.lis-lab.fr`

Supervisors:
Clara Bertolissi and Pierre-Alain Reynier
Email: `{clara.bertolissi,pierre-alain.reynier}@lis-lab.fr`

Context.

This internship focuses on operational processes such as workflows, and their verification (see [dSR17]).

A workflow specifies a collection of tasks, whose execution is initiated by humans (or software agents executing on their behalf) and the constraints on the order of execution of those tasks. Workflows represent a repeatable and structured collection of tasks designed to achieve a desired goal, e.g. to provide a service or product. In addition, and of particular interest from the security point of view, security constraints may be taken into consideration. Authorization policies specify that, in an organization, a workflow task is executed by a user who have the permissions to do so; e.g., the teller of a bank may create a loan request, whereas only a manager may accept it. Additional authorization constraints are usually imposed on task execution, such as Separation or Binding of Duties (SoD or BoD), where two distinct users or the same user, respectively, must execute two tasks.

We will focus on an approach using an array-based specification to model workflows [GNRZ08]. Workflow verification is then performed by model checking via Satisfiability-Modulo-Theories (SMT) techniques. For exemple, in [BdSR15] satisfiability of workflows with security constraints (security sensitive workflows, SSW) is addressed and a methodology to build a runtime workflow monitoring is described. In [CGG$^+$19], authors address verification of safety properties over workflows including data (data-aware workflows, DAW).

Objectives.

The aim of this internship is first to become familiar with workflows and their specification as array-based systems, i.e. state transition systems implicitly specified using a declarative, logic-based formalism. Then, the objective is to study verification of data-aware security sensitive workflows (SS-DAW) by combining and extending the previous results. To support the approach, an implementation using a state-of-the-art SMT solver [GR10] may complete the internship.

References

[BdSR15] Clara Bertolissi, Daniel Ricardo dos Santos, and Silvio Ranise. Automated synthesis of run-time monitors to enforce authorization policies in business processes. In Feng Bao, Steven Miller, Jianying Zhou, and Gail-Joon Ahn, editors, *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security, ASIA CCS '15, Singapore, April 14-17, 2015*, pages 297–308. ACM, 2015.

[CGG+19] Diego Calvanese, Silvio Ghilardi, Alessandro Gianola, Marco Montali, and Andrey Rivkin. Formal modeling and smt-based parameterized verification of data-aware BPMN. In Thomas T. Hildebrandt, Boudewijn F. van Dongen, Maximilian Röglinger, and Jan Mendling, editors, *Business Process Management - 17th International Conference, BPM 2019, Vienna, Austria, September 1-6, 2019, Proceedings*, volume 11675 of *Lecture Notes in Computer Science*, pages 157–175. Springer, 2019.

[dSR17] Daniel Ricardo dos Santos and Silvio Ranise. A survey on workflow satisfiability, resiliency, and related problems. *CoRR*, abs/1706.07205, 2017.

[GNRZ08] Silvio Ghilardi, Enrica Nicolini, Silvio Ranise, and Daniele Zucchelli. Towards SMT model checking of array-based systems. In Alessandro Armando, Peter Baumgartner, and Gilles Dowek, editors, *Automated Reasoning, 4th International Joint Conference, IJCAR 2008, Sydney, Australia, August 12-15, 2008, Proceedings*, volume 5195 of *Lecture Notes in Computer Science*, pages 67–82. Springer, 2008.

[GR10] Silvio Ghilardi and Silvio Ranise. MCMT: A model checker modulo theories. In Jürgen Giesl and Reiner Hähnle, editors, *Automated Reasoning, 5th International Joint Conference, IJCAR 2010, Edinburgh, UK, July 16-19, 2010. Proceedings*, volume 6173 of *Lecture Notes in Computer Science*, pages 22–29. Springer, 2010.