ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Master Thesis Proposal

A universal policy miner

Supervisors: Carlos Cotrini
Professor: Prof. David Basin
Issue Date: September 9, 2019
Submission Date: TBD

1 Introduction

Organizations define access control policies that restrict who can do what in the organization. Organizations often change in many ways. New users join the organization. Other users leave. New resources may be acquired and others are removed. All these changes induce changes in the policy. When these changes accumulate through time, policies become convoluted and difficult to maintain. Moreover, policy changes are done manually. As a result, unauthorized users may obtain access to sensitive resources and potentially harm the organization.

To assist with the maintenance of access control policies, *policy miners* have been proposed [7, 3, 1, 4]. These are algorithms that use machine learning and/or combinatorial algorithms to analyze the current assignment of permissions to users and then "mine" a simple policy that is as consistent as possible with the current permission assignment.

Policy miners are, however, inflexible in that any modification to the miner's requirements necessitates its redesign and reimplementation. For example, miners that mine RBAC policies from access control matrices [4] are substantially different from those that mine RBAC policies from access logs [6]. As evidence for the difficulty of this task, despite extensive work in policy mining, no miner exists for XACML [5], which is a well-known, standardized policy language.

2 Objective

The thesis's goal is to develop a *universal policy miner* that is independent from the policy language used to specify policies. This universal miner would receive as input a policy language L and an assignment of permission to users. The miner would then output a policy that can be specified in L and that is as consistent as possible with the permission assignment. To develop this universal miner, we follow Unicorn [2], a method proposed to build policy miners that applies for a wide variety of policy languages, including RBAC, ABAC, and even XACML.

3 Tasks

1. Become familiar with Unicorn [2].
2. Propose a parser for template formulas, these are first-order formulas used to specify policy languages.
3. Propose data structures and mechanisms to store and compute expectations required by Unicorn's pseudocode.

4. Combine the mechanisms above to build a universal policy miner.

5. Conduct experiments on publicly available datasets to evaluate the universal miner's performance.

4 Deliverables

- At the end of the second week, a detailed time schedule of the project must be given and discussed with the supervisor.
- At the end of the project a presentation of 30 minutes must be given during an Infsec group seminar. It should give an overview as well as the most important details of the work.
- Software and configuration scripts must be delivered to the supervisors.
- A final report consisting of an introduction, a discussion on the related work, overview of the universal miner, and experimental results. Three copies of this report must be delivered to the supervisor.

References

[1] Suresh N Chari and Ian M Molloy. Generation of attribute based access control policy from existing authorization system, February 16 2016. US Patent 9,264,451.

[2] Carlos Cotrini, Luca Corinzia, Thilo Weghorn, and David Basin. The next 700 policy miners: A universal method for building policy miners. *arXiv preprint arXiv:1908.05994*, 2019.

[3] Carlos Cotrini, Thilo Weghorn, and David Basin. Mining ABAC rules from sparse logs. In *2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 2018.

[4] Mario Frank, Andreas P Streich, David Basin, and Joachim M Buhmann. A probabilistic approach to hybrid role mining. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 101–111. ACM, 2009.

[5] Simon Godik and Tim Moses. Oasis extensible access control markup language (XACML). *OASIS Committee Secification CS-XACML-specification-1.0*, 2002.

[6] Ian Molloy, Youngja Park, and Suresh Chari. Generative models for access control policies: applications to role mining over logs with attribution. In *Proceedings of the 17th ACM symposium on Access Control Models and Technologies*, pages 45–56. ACM, 2012.

[7] Zhongyuan Xu and Scott D Stoller. Mining attribute-based access control policies from logs. In *Data and Applications Security and Privacy XXVIII*, pages 276–291. Springer, 2014.