University of Pittsburgh | School of Computing and Information

Proposal Defense

Doctor of Philosophy in Information Science

“**Towards Attribute-Based Access Control Policy Learning and Refinement for Dynamic Systems**” by **Leila Karimi**

Date: June 11, 2021
Time: 10:00am – 12:00pm
Place: https://pitt.co1.qualtrics.com/jfe/form/SV_3WQXvfepIAIqEiq

Committee:

- Dr. James Joshi (advisor), Professor, School of Computing and Information
- Dr. Hassan Karimi, Professor, School of Computing and Information
- Dr. Balaji Palanisamy, Associate Professor, School of Computing and Information
- Dr. Mai Abdelhakim, Assistant Professor, Department of Electrical and Computer Engineering, Swanson School of Engineering

Abstract:

With the rapid advances in computing and information technologies, traditional access control models have become inadequate in terms of capturing fine-grained, and expressive security requirements of newly emerging applications. An attribute-based access control (ABAC) model provides a more flexible approach to addressing the authorization needs of complex and dynamic systems. An ABAC model grants access to a requester based on attributes of entities in a system and an authorization policy; however, its generality and flexibility come with higher costs: the costs of policy development, enforcement, and maintenance. Hence, while organizations are interested in employing newer authorization models, migrating to such models poses as a significant challenge. Many large-scale businesses need to grant authorizations to their user populations that are potentially distributed across disparate and heterogeneous computing environments. Each of these computing environments may have its own access control (AC) model. The manual development of a single policy framework for an entire organization is tedious, costly, and error-prone. In addition, policy misconfigurations that hinder the effectiveness of AC systems expose an organization to various security threats.

In this dissertation proposal, we propose approaches and methods that facilitate ABAC policy development and management. In particular, we propose a methodology for automatically learning ABAC policy rules from access logs of a system to simplify the policy development process. The proposed approach employs a clustering-based algorithm for detecting patterns in access logs and extracting ABAC authorization rules from these patterns. In addition, we propose two policy improvement algorithms, including rule pruning and policy refinement algorithms to generate a higher quality mined policy. Further, we propose an adaptive ABAC policy learning approach to automate the authorization management task. We model ABAC policy learning as a reinforcement learning problem. In particular, we propose a contextual bandit system, in which an authorization engine adapts an ABAC model through a feedback control loop; it relies on interacting with users/administrators of the system to receive their feedback that assists the model in making authorization decisions. Finally, we propose a statistical/machine learning based approach for detecting ABAC policy misconfiguration and refining ABAC policy rules to enhance the quality of policy and prevent system exploitation.