Access Control Policy Mining and Management

Scott D. Stoller, Stony Brook University
www.cs.stonybrook.edu/~stoller/policy-mining

ABAC & ReBAC

- Attribute-Based Access Control (ABAC) is becoming more common and more important, due to its flexibility and ease of administration, especially for complex, dynamic policies.
- ABAC policies contain rules granting permissions based on attributes of users and resources.
- Relationship-Based Access Control (ReBAC) extends ABAC with relationships between entities (subjects, resources, …) which can be chained together in path expressions.
  - Example rule (informal): A technician can view tasks associated with active contracts for customers of her department.

Project Goals

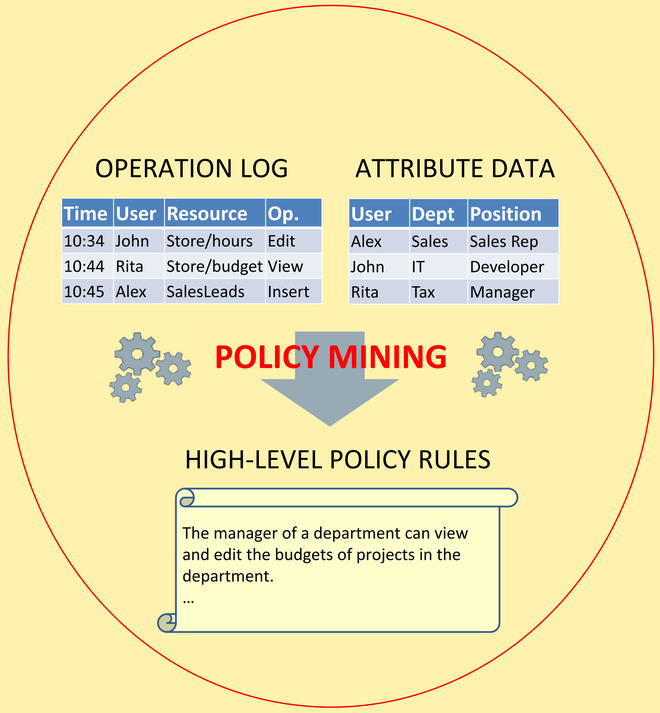
- Access control policies are increasingly large, complex, decentralized, and dynamic.
- Administrators need better tools that help them develop correct policies.
- This project is developing new techniques for policy mining and policy analysis.

Managing ABAC & ReBAC Policies

- Administrative policy controls changes to the access control policy. Essential for decentralized management of policies, e.g., in large companies.
- We express administrative policies for ABAC (and ReBAC) as rules that control addition and removal of rules and changes to attributes (and relations).
  - We define a strictness order on rules and specify in the policy the least strict rules that each subject may add or remove.
  - This helps balance flexibility and safety.
- We proposed the first general-purpose ReBAC model with a comprehensive administrative framework.

Mining ABAC & ReBAC Policies

- Policy mining algorithms can drastically reduce the cost of migrating from legacy access control to ABAC or ReBAC.
- They find the highest-quality (e.g., most concise) ABAC or ReBAC policy consistent with given ACLs (or operation logs) and attribute data.
  - They also identify and correct noise (errors).
  - When mining from logs, they "fill in" missing (unobserved) permissions.



Analyzing ABAC & ReBAC Policies

- Interleaved sequences of changes by different users may interact in subtle ways.
- Analyze policy (including administrative policy) to expose flaws and unexpected behaviors.
- Abductive analysis finds minimal conditions on initial attribute data that allow a given goal to be reached, starting from given initial policy rules.
- We developed first abductive policy analysis for an ABAC framework that allows changes to rules and attribute data. Extension to ReBAC is future work.

Algorithms and Evaluation

- We developed the first algorithms to mine ABAC and ReBAC policies from ACLs or logs and attribute data. We explored several approaches:
  - Heuristic-guided greedy algorithm
  - Evolutionary algorithm
  - Neural networks
  - Decision trees
- Successful evaluation on two large case studies based on real organizations.

Broader Impacts

- Facilitate adoption of flexible access control models that promote security and information sharing.
- Reduce cost of policy development
- Increase confidence in policy correctness.

Mining Temporal RBAC Policies

- Temporal RBAC extends role-based access control to limit the times at which roles are enabled.
- Periodic expressions denote repeating time intervals.
- We developed first temporal role mining algorithm that produces hierarchical policies and optimizes multiple metrics (policy size, interpretability, ...).
- Demonstrated its effectiveness on datasets based on real-world ACL policies.
- Best Paper Award, DBSec 2016.