Self-Diagnosing Logical Access Controls

Michael D. LeMay, Omid Fatemieh, Sundeep Katasani, Nikita Borisov, Carl A. Gunter

ABAC - Background
- In attribute-based access control systems, each “subject” (usually a person) and “object” is associated with a set of attributes.
- Policies primarily deal with these attributes, at a high level of abstraction.
- Administrators modify attribute sets on a day-to-day basis, not the core policy.
- Our ABAC system is implemented in Prolog, the most popular logic language.
- Administrators restrict policies using logical constraints, to permit pre-deployment detection of undesirable policies.

Policy Correction
- System includes “wizard” for detecting policy constraint violations.
- “Intelligently” provides suggestions for resolving violations.
- Discovers all permission changes that occur with each modification, to prevent unintended consequences.

Context Sensitivity
- Arbitrary contextual information can be considered in the policies:
  - Instant messenger presence status
  - Motion detector / card swipe data
  - SCADA data points
  - Temperature, acceleration, GPS location...

Scenario #1: TA Room Assignment
- Amber is the TA of CS411.
- Curtiss is a student in CS411, and the TA of CS323.
- The assigned TA room for both CS323 and CS411 is room 4308.
- CONFLICT: Curtiss may be able to exploit Amber’s materials, since they share a room.
- Our system spots this violation and suggests a few possible resolutions:
  - Assign a new TA room to one or both of the courses.
  - Remove the TA credentials of one or both individuals, potentially granting them to someone else.

Policy Validator

Graphical Interface

Scenario #2: Experiment Integrity
- Dr. Carlson normally allows his students to access his office, to obtain books.
- He occasionally runs sensitive experiments in his office.
- Our context-sensitivity system subscribes to his instant messenger presence.
- When he sets his presence to “Do Not Disturb”, his students are barred from entering his office.

Scenario #3: SCADA Emergencies
- SCADA systems control our electrical grid.
- Our system could temporarily loosen access controls on critical resources when SCADA data indicates emergency conditions.
- Constraints ensure that these additional permissions are always acceptable to the utility and to regulatory agencies.

Future Work
- Expand suggestion framework to automatically provide a wider range of potential resolutions.
- Develop graphical tools to manage policy creation, validation, and correction.

Funded by AFOSR, MacArthur Foundation, NSF