PROBLEM AND SOLUTION

PROBLEM:
- Database access control mechanism does not support Attribute-based Access Control (ABAC) by utilizing information in the database itself.

SOLUTION:
- eXtensible Access Control Markup Language (XACML) is widely accepted to describe attribute-based policies.
- Native database access control mechanism such as access control list (ACL) is efficient in enforcing Identity-based Access Control (IBAC).
- Transfer high level XACML policies into low level database ACLs to unify ABAC and IBAC.

MOTIVATION AND CHALLENGES

MOTIVATION:
- EXPRESSIVENESS AND EFFICIENCY:
  - XACML provides expressiveness while ACL provides efficiency. Utilize the advantages of both the world.

CHALLENGES:
- Maintain permission correctness when database changes.

OVERVIEW

Professors or Systems area
Assistant professors

Can select from, insert into, and delete from Graduate Admission related tables

EXTRACT USERS AND RESOURCES:
- Subject: <rank=Professor> OR <rank=Assistant Professor AND area=Systems>
- Resource: <table_comments=Graduate Admission>
- Action: <select, insert, delete>

POLICY PROCESSING

Subject: <rank=Professor> OR <rank=Assistant Professor AND area=Systems>
- Resource: <table_comments=Graduate Admission>
- Action: <select, insert, delete>

EXTRACT USERS AND RESOURCES:
- SELECT username FROM employees.info WHERE rank='Professor' OR (rank='Assistant Professor' AND area='Systems');
- SELECT table_name FROM information_schema.tables WHERE table_comment='Graduate Admission';

POPULATE ACL
- Users u0, u5, and u7 and tables t5 and t8 satisfy the policy.
- GRANT SELECT,INSERT,DELETE ON t5 TO u0, u5, u7;
- GRANT SELECT,INSERT,DELETE ON t8 TO u0, u5, u7;

CONFLICT RESOLUTION

CONFLICT (Subject S, Action A, Resource R, Policy P):
- P1 permits actions A1 to users S1 on resources R1.
- P2 denies actions A2 to users S2 on resources R2.
- S1 ∩ S2 = S (S ≠ nil), R1 ∩ R2 = R (R ≠ nil), A1 ∩ A2 = A (A ≠ nil).

COMBINING ALGORITHMS:
- Permit/Deny-overrides, First-applicable.

EXAMPLE:
- Permissions: <u0, t0, select, permit>, <u0, t0, insert, permit>, <u0, t0, select, deny>
- Combining Algorithm: Deny-overrides.
  - The 1st permission is nullified by the 3rd one.
  - The 3rd permission is revoked from the ACL if it already exists.
  - The 2nd permission is added to the ACL.

EVALUATION

- Implementation of XACML over MySQL database.
- Compilation time includes parsing, user extraction, and ACL update.
- Time is almost linear with number of rules in a policy.