Model Checking Grid Policies

Presenter:

International Symposium on Grid Computing (ISGC 2010)
Open Science Grid provides an infrastructure for coordinating Virtual Organizations (VOs) and sites based on various grid policies (policies in short)

- VO have its own VO policy
- Site policy authors refer to multiple VO policies and make their own policies
Motivation

- Storage elements and computing elements in sites are shared within and across members of various VOs
  - Relatively easy to access via Internet
  - Different roles of VOs have different privileges over resources in sites
- Sensitive resource or jobs requires policy mechanisms
  - access control, job priority and scheduling, monitoring and etc
- Site policy authors write their own policies w.r.t. their interests
  - e.g., combine multiple VO policies
Motivation - cont.

How to ensure the correct behaviours of policies?
- What you specify is what you get, but not necessarily what you want

Our solution: model checking grid policies
- Property verification
- Conflict and redundancy checking
- Change impact analysis
Outline

- Approach
  - Access Control in XACML
  - Property verification
  - Conflict and redundancy checking
  - Change impact analysis
- Conclusion
Access Control in XACML

- XACML is eXtensible Access Control Markup Language standardized by OASIS
- XACML policy describes a set of rules to specify policy behaviors
- Policy Decision Point (PDP) produces a policy decision (e.g., Permit or Deny) with regards to a request from a user
Example Grid Policy

- Subjects/Roles: Admin, Tester
- Actions: execute
- Resources: DiskQuota
- Condition: DiskQuotaBytes

Rule 1: IF (Admin AND execute AND DiskQuota AND DiskQuotaBytes > 15 MB)
        Permit

Rule 2: IF (Tester AND execute AND DiskQuota AND DiskQuotaBytes > 10 MB)
        Permit

Rule 3: OTHERWISE
        Deny
Describing a policy as a state machine

- **State:** description of the decisions in the machine
- **Initial State:** Pending
- **Finite states:** Deny, Permit
- **Finite-state machine (FSM) model**

![Diagram](image)
Policy Verification

Property 1: Admin can execute a job that requires 15 MB disk quota
No violations are found

Rule 1: IF (Admin AND execute AND DiskQuota AND DiskQuotaBytes > 15 MB) Permit
Rule 2: IF (Tester ...) Deny
Rule 3: ...

Rule 1 or Rule2

Pending

Rule 1 or Rule 2

Deny

Permit
Property 2: Tester cannot execute (a job) that requires a disk quota smaller than 15 MB

Violation with a counterexample:
Tester can execute a job that requires 13 MB disk quota

Rule 1: ...
Rule 2: IF (Tester AND execute AND DiskQuota AND DiskQuotaBytes > 10 MB)
    Permit
Rule 3: ...

Diagram:
- Pending
- Permit
- Deny

Rule 1 or Rule 2

! (Rule 1 or Rule 2)
Conflict and Redundancy

- Find conflict and redundant rules
- Consider a site policy author combine multiple VO
  - Detect redundancies to remove redundant policies
  - Detect conflicts to identify which rule should be given higher priority during policy evaluation
Conflict and Redundancy

- **State**: description of the status (of redundancy or conflict) in the machine
- **Initial State**: Pending
- **Finite states**: Redundancy or Conflict
- **FSM models**: to detect redundancy and conflict
  - VO1 and VO2 denote two VO policies
Conflict and Redundancy

Property 1: Is there any ways to reach to redundancy state
This property outputs redundancies (if any)

- **Pending**
  - VO₁ = Permit and VO₂ = Permit
  - VO₁ = Deny and VO₂ = Deny

- **Redundancy**

Property 2: Is there any ways to reach to conflict state
This property outputs redundancies (if any)

- **Pending**
  - VO₁ = Permit and VO₂ = Deny
  - VO₁ = Deny and VO₂ = Permit

- **Conflict**
Policy authors change a policy A to a policy B
- Ensure correctness of a changed policy
- Output all different requests-decision pairs produced by two policies
- Outputs conflicting decisions of a policy A and policy B (conflicting decisions)
Conclusion and Future Work

- Model checking help ensure the correctness of policies
  - Property verification
  - Conflict and redundancy checking
  - Change impact analysis
Any Questions?

Thank You