SEMPO: semantic policy validation for access control

**Challenge**

Determining the effectiveness of security roles and permissions when multiple policies are being applied concurrently can be difficult. Role-based policy testing is limited and exhaustive black box testing is costly, time consuming and unachievable in a dynamic IT environment.

**Focus**

This CA Labs research project is focused on automated validation and verification techniques that systematically evaluate and detect unintended policy authorization decisions.

**Result**

Automated policy validation and verification would facilitate congruency and completeness across security policy sets and help IT security administrators to resolve conflicts, omissions and duplications more quickly, leading to higher quality access control and more efficient identity management.

The importance of ensuring security for cloud and IT-based business services has driven up the number and type of access policies. IT security organizations must manage the complexities of separate but related security policies being applied collectively as policy sets across tiers, applications and cloud services.

Testing every possible policy set combination against every IT resource is time-consuming, costly, and impossible in a dynamic environment. Current policy validation testing techniques typically validate a single policy without considering other policies in the set. IT security organizations need a way to identify the inconsistencies in permissions across policy sets. Testing and validation efforts could be focused on the inconsistencies, better assuring that separate but related security policies result in correct security enforcement when applied collectively.

The CA Labs SEMPO research project is developing validation methods and a prototype validator tool to detect inconsistencies among policies where large sets of policies are concurrently applied. The project’s goal is to create a solution that will detect possible unintended human errors made during policy creation, and enable higher quality access control and streamlined resource requirements for identity management.

The SEMPO prototype validator tool is intended to work in two distinct modes: batch mode and online mode:

- In batch mode, a policy set will be exported in the form of an XML document. The XML document would be processed by the validator tool, which will produce a report file listing inconsistencies. For each inconsistency, it would report identities, resources, calendars and attributes affected by the inconsistency, and the type of inconsistency with a list of the related policies.
- In online mode, the validator tool would evaluate policy, resource, and calendar or attribute value changes and identify behavior conflicts being introduced to the security environment.

Figure 1. SEMPO identifies conflicts, omissions and duplications across policy sets, which pinpoints trouble spots for security verification and areas for validation by IT security administrators.
SEMPO inconsistencies identified by the validator tool

It is anticipated that the SEMPO prototype validator tool will identify the following types of example inconsistencies:

- **Role Conflicts** - Resource A uses policies that have contradictory entitilements to a role:
  - Policy #1: User in Role Z can access resource
  - Policy #2: User in Role Z cannot access resource

- **Time Conflicts** - Resource A uses policies with contradictory entitlements for access times:
  - Policy #1: User cannot access resource on Tuesday
  - Policy #2: Resource is only accessible on workdays

- **Omissions** - Resource A uses policies with contradictory actions entitlements:
  - Policy #1: View and transfer actions enabled
  - Policy #2: Transfer action enabled but not view

In addition to identifying the inconsistency, the validator tool would indicate a warning that a view may be unprotected for Policy #1 users.

- **Duplication** - Resource A uses policies that define the same entitlements:
  - Policy #1: User must have Role A
  - Policy #2: User must have Role A _AND_ Role B

In addition to identifying the duplication, the validator tool would indicate a warning that Policy #1 is covered by Policy #2 and can be removed.

In another example:

- Policy #1: User must have Role A
- Policy #2: User must have Role A _OR_ Role B

In addition to identifying the duplication, the validator tool would indicate a warning that Role B is redundant.

More Information on CA Labs SEMPO research project

CA Labs is collaborating with researchers from the National Science and Engineering Research Council, Quebec, and the University of Quebec in Ottawa. The project is funded by a grant from the National Science and Engineering Research Council (NSERC) of Canada. The following are the most recent papers published about this research project:


For additional information about this or other CA Labs projects, please contact Serge Mankovskii at Serge.Mankovskii@ca.com.

About CA Labs and innovation

CA Labs is the research arm for CA Technologies and a hub for the company’s initiatives for innovation. CA Labs collaborates with the world’s foremost researchers in academia, industry and government to perform advanced research to address cloud, software-as-a-service, security, virtualization, automation, mainframe, service assurance, and service and portfolio management challenges. For more information, visit ca.com/calabs.