Conformance Testing of Access Control Systems that Employ Temporal RBAC Policies

Ammar Masood, Arif Ghafoor and Aditya Mathur

Long term goal

- To study the effectiveness of model based testing in the detection of security related faults in implementations of access control systems with temporal constraints.

Motivation

Access control is used widely to restrict access to information

- Temporal constraints can further limit access of valid users
- The desired access control objectives of a system can only be achieved if the corresponding policy specifications are correctly enforced by the underlying software implementation

Recent Work

- Model-based testing of access control systems that employ Role Based Access Control (RBAC) policies
- RBAC is a promising approach for addressing diverse security needs of business organizations
- Access control in organizations is based on "rules that individual users take on as part of the organization"

Model-based Testing Approach

- Construction of structural and behavioral models (Finite State Machine representation) of RBAC policy specification
- Automated generation of test suites from the structural and behavioral models for security testing of implementation

X-GTRBAC Case Study

X-GTRBAC System + Security Testing Module

Test Adequacy: Control flow & Mutation

- Code Coverage used to assess control flow test adequacy
- Evaluation against mutation revealed that the tests were able to distinguish between 88 to 94% of the generated mutants.

Current Work: Dealing with Temporal Constraints

- Extending the recently proposed model-based approach for testing of access control systems with temporal constraints
- Finite state machines (FSM) not suited for modeling temporal constraints
- Suitable modeling formalisms examined:
  - Timed Automata (TA)
  - Timed Input Output Automata (TIOA)
- Our choice
  - Timed Petri Nets (TPN)

Model-based Conformance Testing for Systems Employing Temporal RBAC

- We have considered two types of Conformance Relations (strict and weak) in regard to an implementation conformance to specifications
- Fault Model for TRBAC specification categorizes faults in two broad classes: temporal and non-temporal constraint violation faults
- TIOA based models used to capture specification requirements in terms of user-role and permission-role assignment and activation sequences permitted in the system
- Timed-WP method used to generate tests from TIOA based models
- Study of the relation between TRBAC specification fault model and the generic TIOA fault model
- Perform a case study to verify the efficacy of proposed approach