Combinatorial Testing of Access Control Policies

Bellanov Apilli
bsapilli@ncsu.edu

JeeHyun Hwang
jhwang4@ncsu.edu

Tao Xie
xie@csc.ncsu.edu

Problem
- Previous access control policy testing techniques
- Ineffective, failing to cover important rules
- Costly due to too many possible tests

Proposed Solution:
- Combinatorial Testing of Access Control Policies
- Minimizes the number of required tests considering t-way interactions of given attribute values
- Generates single-valued and multi-valued combinatorial test requests and evaluates them against policies to expose faults.

XACML Policy Evaluation

XACML [1] is a specification language used to define access control policies.
- The PEP forms an XACML request and sends it to the PDP.
- The PDP checks the request against a policy, returning a response.
- The PEP either permits or denies the request.

Single and Multi-valued Requests

Single-valued Requests:
- Contain one value for subject, resource, and action attributes

Multi-valued Requests:
- Contain multiple values for at least one attribute
- Represent each attribute value as a Boolean value
- 1 represents that a request includes the value
- 0 represents that a request does not include the value

Combinatorial Request Generation
- Test requests are generated by t-way combinations of attribute values considering their interactions. Every combination of t attribute values is covered by at least one test. Combinations are generated using a combinatorial testing tool called FireEye [2].
- For multi-valued request generation, each parameter (P1, P2, P3) represents an attribute in a policy. A value of 1/0 indicates its presence/absence within a request.

Mutation Testing

A Mutant Policy is a faulty version of the original policy.
- A fault is introduced by the deletion of a rule one at a time.
- Requests are evaluated against both the original and mutated policies.
- If the responses differ, the mutant is killed, meaning that the test case detects the fault, which is the absence of the rule.

Evaluation: Mutant-Killing Ratios

Policy Testing

Experimental Subjects and Results

Combinatorial tests (t = 2)

Subject Resource Action
Faculty Grade Assign 0 1 1
Faculty Record view 0 1 1
Student Grade view 1 0 1
Student Record Assign 1 1 0

Single-valued Requests (2 subject, 2 resource, and 2 action values)
Multi-valued Requests considering three attribute values

References