Access Control Policy Tool (ACPT), an assurance tool that combines symbolic model checking with combinatorial coverage

National Institute of Standards and Technology
U.S. Department of Commerce

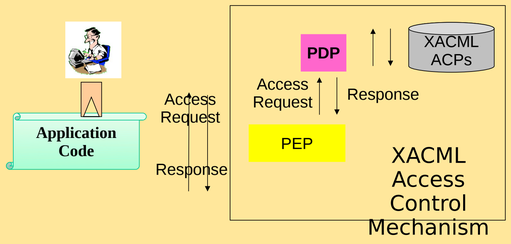
Automated Software Engineering Research Group @NCSU

Access Control

- ✓Access control is one of the most widely used privacy and security mechanisms
  - ✓protect critical IT infrastructures such as healthcare, military, intelligence systems
  - ✓prevent security vulnerabilities by controlling access to resources
- ✓Access control is often governed by security policies called Access Control Policies (ACPs)
  - ✓include rules that specify which principals such as users or processes have access to which resources

Motivation

- ✓Improper access control is a critical problem
  - ✓ranked the 5th among the most dangerous errors
  - ✓cause critical consequences (e.g., privacy issues)
- ✓Ensure correctness of ACPs
  - ✓ACP specification may not encapsulate security requirements
    - ✓manual verification of ACPs is tedious and error-prone
  - ✓ACPs are becoming more complex
    - ✓manual verification of request/response is time-consuming



Policy Generation

✓XACML is OASIS standard XML-based language to specify ACPs

```
<Rule Effect="permit"
RuleId="rule-1">
  <Target>
    <Subjects>
      <Subject>federal
employee</Subject>
    </Subjects>
    <Resources>
      <Resource>access
</Resource>
    </Resources>
    <Actions>
      <Action>confidential
document </Action>
    </Actions>
  </Target>
 </Rule>
<Rule Effect="deny"
RuleId="rule-2">
  <Target>
    <Subjects>
      <Subject>state
employee</Subject>
    </Subjects>
    <Resources>
      <Resource>access
</Resource>
    </Resources>
    <Actions>
      <Action>confidential
document </Action>
    </Actions>
  </Target>
 </Rule>
```

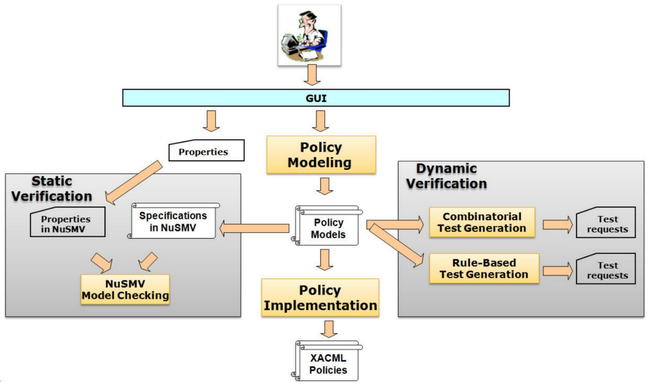
Evaluation

- ✓Coverage achieved by generated test requests
  - ✓Subject: 10 collected ACPs
    - ✓from 4 sources
  - ✓ Evaluation result:
    - ✓achieve 100% rule coverage
    - ✓achieve 100% combinatorial coverage

We demonstrated that our static verification models and verifies various policy models (e.g., RBAC, workflow, …)[4,7]

Detailed evaluation results http://research.csc.ncsu.edu/ase/projects/policy/

Our Approach



Policy Model

Support for various policy models (e.g., RBAC, workflow, …)[4,7]

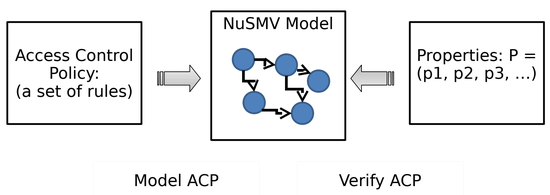
1. The federal employee is permitted to access the confidential document
2. The state employee is denied to access the confidential document

Role-based access control model

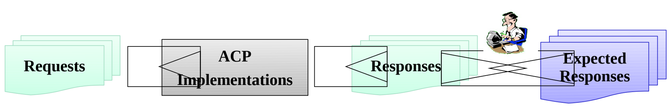
1. The federal employee ϵ Role ∧ access ϵ Action ∧ confidential document ϵ Resource → Permit
2. The state employee ϵ Role ∧ access ϵ Action ∧ confidential document ϵ Resource → Deny

Static and Dynamic Verification

- ✓Static verification verifies a formal ACP against user-specified properties
  - ✓ACPT converts a policy p in the NuSMV format (the format accepted by the NuSMV symbolic model checker)
    - ✓e.g., checking of privacy and regulation violations



- ✓Dynamic verification (i.e., test-input generation) generates and executes test requests
  - ✓based on policy structural coverage
  - ✓based on combinatorial coverage



lease and Related Work

✓ O… Policy Tool (ACPT) …nd companies …ications (e.g., [4, 5, 6, 7])

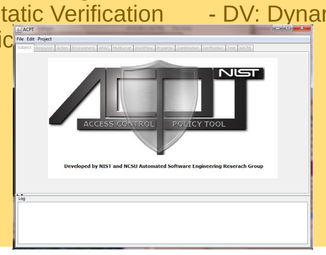
Product	GUI	SV	DV
Our approach			
Existing approaches [1,2,3]		Partial	
IBM Security Policy Manager		Partial	
Cisco Policy Manager			

inventure ENTERPRISES
SAIC
Fermilab

Comparison of ACP management tools

- ✓O… current system prototype (NIST/NCSU ACPT)
  - ✓Support for policy modeling, static and dynamic verification, and policy generation
  - ✓Beta-version on the NIST website [8]
- ✓Our future plan
  - ✓Improve our verification techniques
    - ✓Condition, e.g., time and location constraints
    - ✓Context-aware, e.g., state transition
  - ✓Extend our approach to different application domains
    - ✓Healthcare, law statutes, military, …

- GUI: Modeling via GUI
- SV: Static Verification
- DV: Dynamic Verific…



References

1. N. Zhang et al., Evaluating access control policies through model checking. In Proc. 8th ISC, 2005.
2. S. Kikuchi et al., Policy Verification and Validation Framework Based on Model Checking Approach, In Proc. ICAC, 2007.
3. A. Schaad et al., A model-checking approach to analysing organisational controls in a loan origination process, In Proc SACMAT, 2006.
4. J. Hwang, T. Xie, V. Hu, and M. Altunay. ACPT: A tool for modeling and verifying access control policies. In Proc. POLICY Demo, 2010
5. E. Martin and T. Xie. A fault model and mutation testing of access control policies. In Proc. 16th WWW, 2007.
6. E. Martin, T. Xie, and T. Yu. Defining and measuring policy coverage in testing access control policies. In Proc. 8th ICICS, 2006.
7. V. Hu, R. Kuhn, T. Xie, and J. Hwang. Model checking for verification of mandatory access control models and properties. In IJSEKE, 2010.
8. ACPT: http://csrc.nist.gov/groups/SNS/acpt/acpt-beta.html

http://csrc.nist.gov/groups/SNS/acpt/index.html