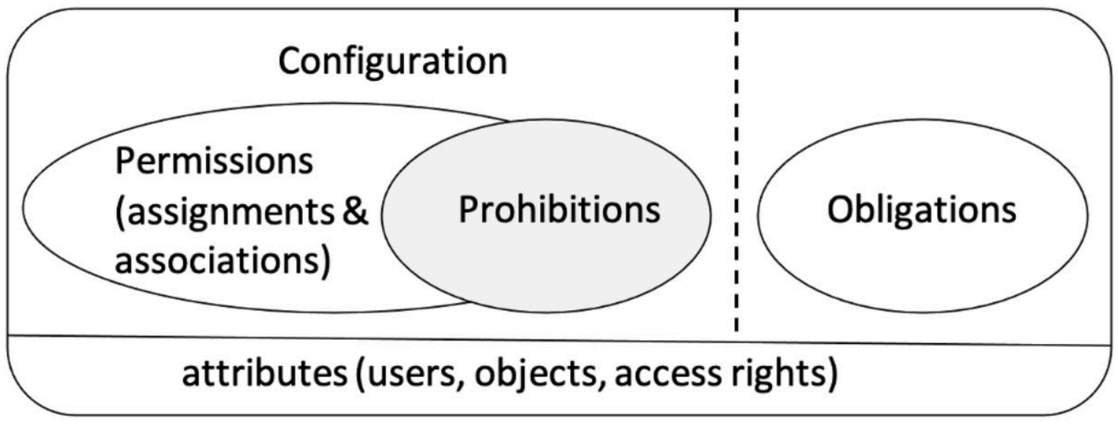
FMitF: Track II: SMT-Based Reachability Analyzer of NGAC Policies

Dianxiang Xu, University of Missouri – Kansas City

Project URL: https://github.com/dianxiangxu/PoMA-public

Background: Next Generation Access Control (NGAC)

- An attributed-based access control standard created by the American National Standard Institute
- An NGAC policy consists of an initial privilege configuration and obligations
- Obligations are triggered by access events
- Privilege configurations may be changed continuously by obligations



Problems

- The development of NGAC policies for dynamic access control is error-prone.
- Access control errors in NGAC policies may lead to fatal security failures
- Ensuring the correct enforcement of dynamic access control requirements is difficult.

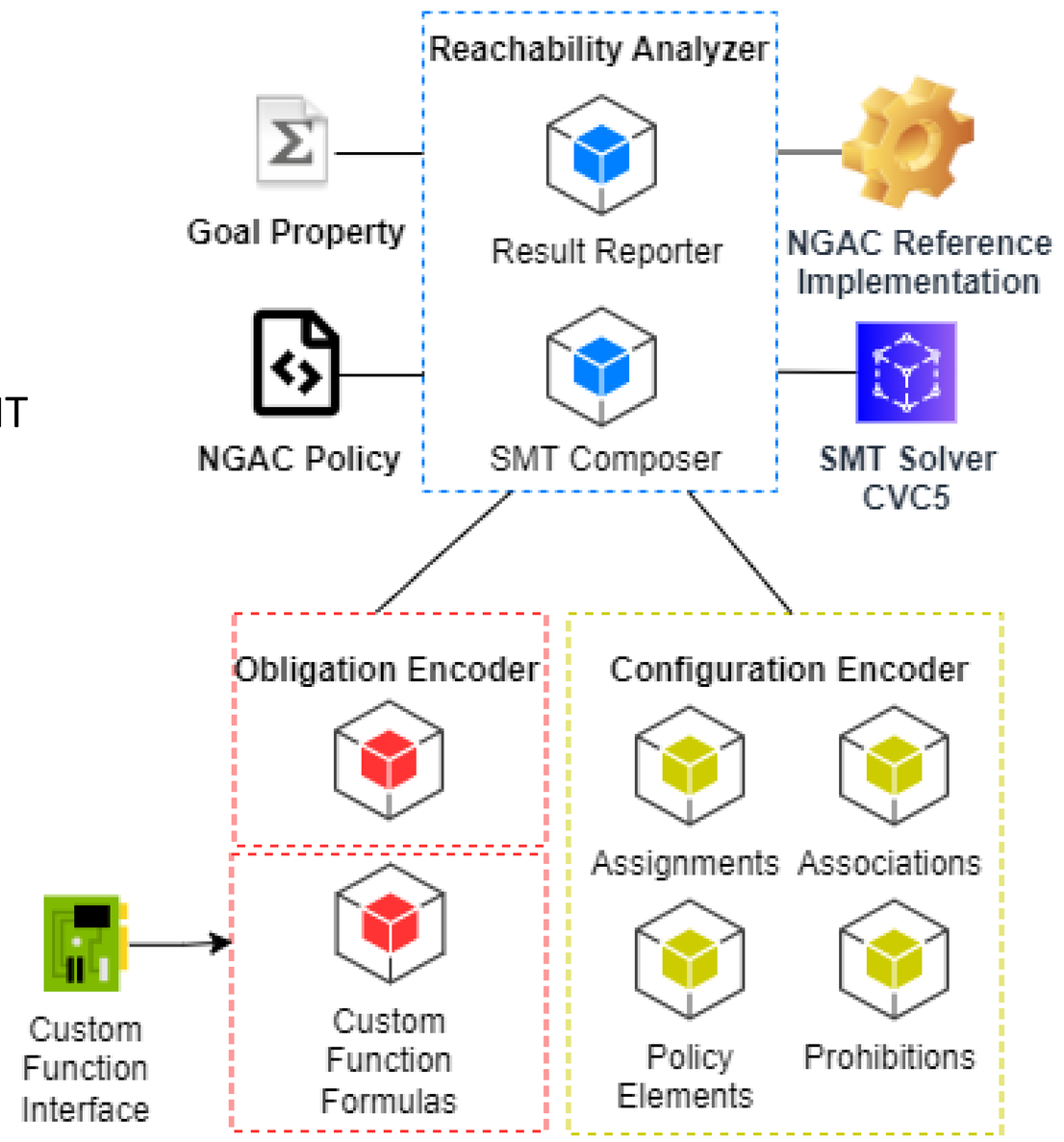
Solution

- Detect errors via reachability analysis by exploiting SMT to analyze all obligation-triggering access events and reachable configurations.
- Encode procedural obligation actions and conflicts as logical SMT formulas

Scientific Impacts

- The first formal method for verifying dynamic access control with administrative obligations
- Demonstration of a practical tool for detecting errors in real-world NGAC policies
- The first real-world case studies (benchmarks) of NGAC with administrative obligations

PoMA: Policy Machine Analyzer



Broader Impact on Society

- Advance the access control knowledge base with a new verification method and case studies
- Provide a tool for NGAC researchers and practitioners

Broader Impact on Education

- Integrate research results into curricular materials for the undergraduate and graduate Software Security course
- Provide graduate and undergraduate assistants with professional training

Broader Participation

- Introduce access control concepts in the Cybersecurity Summer Camps for high school students