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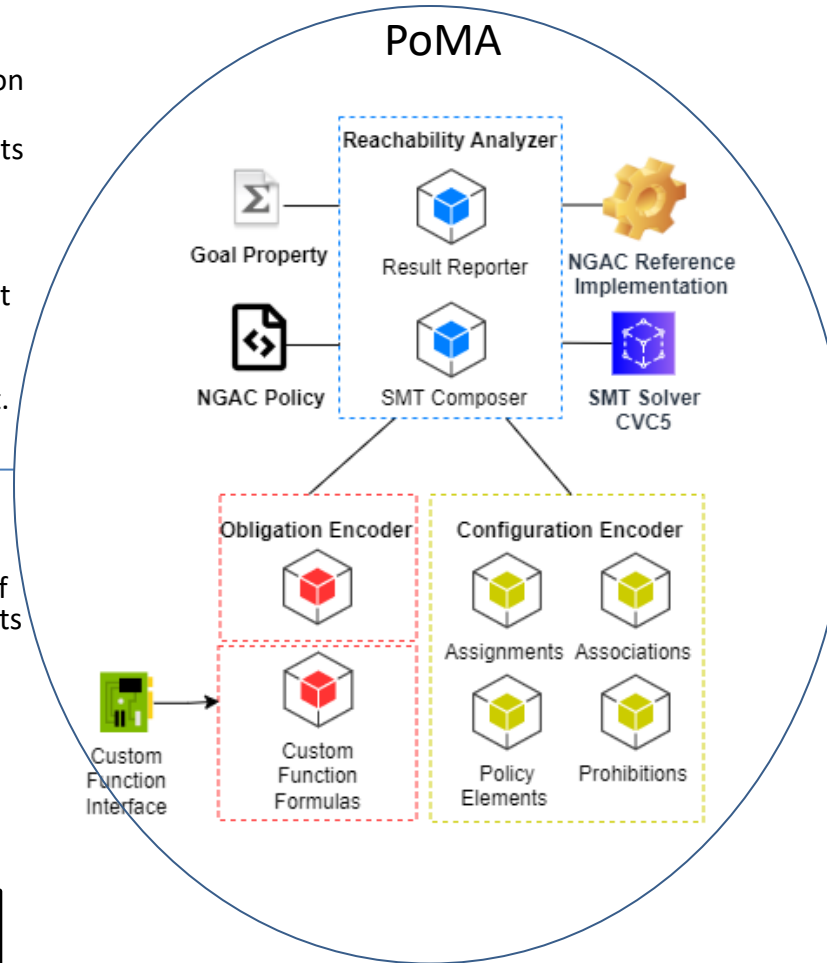
Challenge:

- Obligations in the Next Generation Access Control (NGAC) standard modify the authorization elements of the current configuration and change the access privileges at run-time.
- Ensuring the correct enforcement of dynamic access control requirements via obligation-enabled NGAC policies is difficult.

Solution:

- Exploit SMT to find a sequence of obligation-triggering access events that leads the given policy to a configuration that satisfies a desired property.
- The encoding of procedural obligations in SMT addresses the potential conflicts among the obligation actions.

Scientific Impact:

- 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
- First real-world case studies (benchmarks) of NGAC with administrative obligations

Broader Impact and Broader Participation:

- The open-source tool is hosted on github and available to the NGAC community
- Research results are integrated into instructional materials of the Software Security course
- It involves graduate and undergraduate students

NSF 2318891
University of Missouri – Kansas City
Dianxiang Xu, dxu@umkc.edu