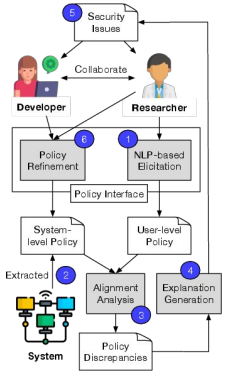
CloudSec: Collaborative Policy Alignment for Secure Scientific Computing Infrastructures

PI: Joe Stubbs (UT Austin) Co-PIs: Eunsuk Kang (CMU), Smruti Padhy (UT Austin)

Overview



- Collaborative security policy analysis for research cyberinfrastructure
- Understand abstraction gap between high-level user policies (natural language) and low-level system policies (formal language)
- Analyze gap using a combination of AI and formal methods.
- Identify vulnerabilities due to policy misconfiguration

Challenges Addressed

- Researchers and project PIs have a high-level vision of the security requirements for their projects, but technical developers must implement security policies using low-level formal semantics.
- Collaboration between researcher and developer on security policies requires bridging the abstraction gap between high-level and low-level policy descriptions.

Contributions

- Development of a new “cross-layer” policy analysis with applications to many research infrastructures
- A novel interface for eliciting policy requirements and explanations from project stakeholders
- A workflow that facilitates collaborative policy development and refinement between researchers and technical developers.

Year 1 Progress

Thurst 1: Interface for Collaborative Policy Alignment
* Designed and implemented Web REST API to manage and analyze security policies
* Conducted initial evaluation/prototype for NL -> Formal Policy translation based on LLMs
* Initial planning for the User Interface, to be implemented this summer on top of API

Thrust 2: Cross-layer Policy Alignment Analysis
* Developed a model and formal specification using Alloy for RBAC for security analysis
* Analyzed and validated various policy specifications using Alloy
* Integration of analysis as apps and launch analysis as a Tapis job in TACC resources.

Thrust 3: Tapis Deployment and Evaluation
* Defined security policies for multiple existing Tapis projects
* Aggregated all effective permission for specific users across all data sources
* Synthesized concrete Alloy tuples from unified security policies

Broader Impacts: Two UT Austin grad students (Shan Jiang and Chunyang Zhang) trained and made significant contribution to the project

Next Steps

* (Summer 2026) User Interface design and Usability Testing
* (Summer 2026 - Fall 2026) Exploring Policy synthesis and repair using LLMs
* (Fall 2026 - Spring 2027) Use SMT solvers for analysis
* (Sprint 2027) Integration of Cloudsec with Tapis

Acknowledgement. The Cloudsec project is supported by the National Science Foundation Division CiCI UCSS under Grant No. 2530889