CAREER: Black-Box Learning of Web Application Authorization Policies

Challenge:

- Many web applications cannot provide accurate specification of their authorization policies due to code complexity, scale, fast-paced development, …
- Users/Developers cannot reason about data protection

Solution:

Treating an app as black-box:

- Learning representation of app data objects and their relationships using automated user traces
- Actively learning formal policy specification by efficient probing of app's authorization space
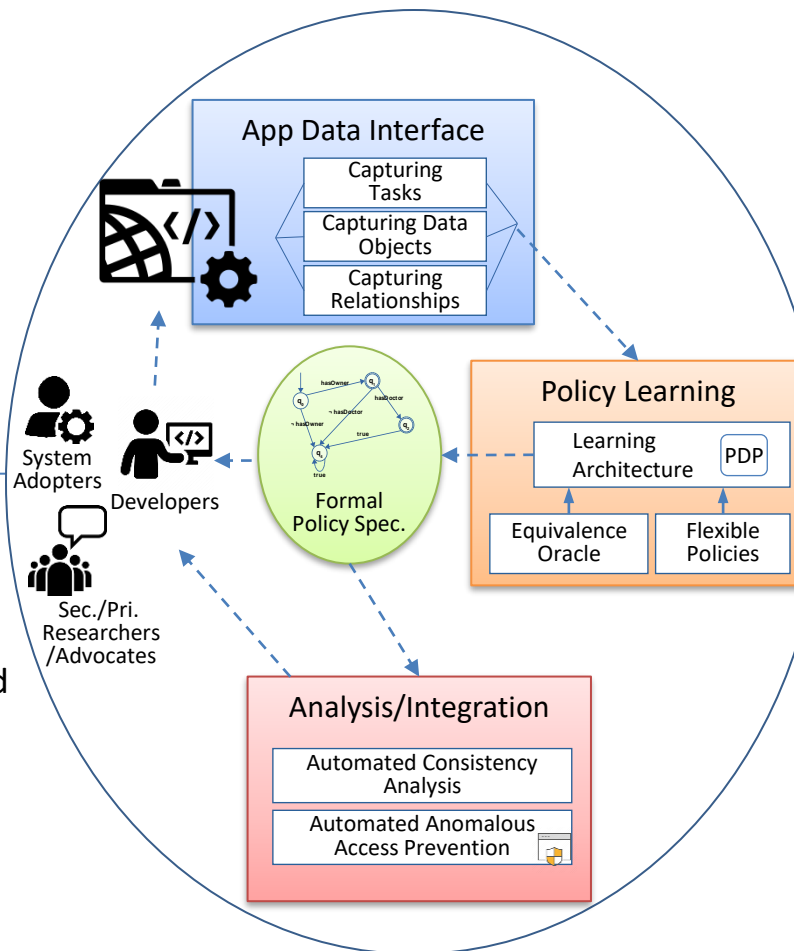
Scientific Impact:

- Novel paradigm for automated learning of enforced policies from complex web apps
- Bridge the gap between existing automated vulnerability analysis and formal & model-based analysis/testing

Broader Impact and Broader Participation:

- Provide system developers reference points/tools for analyzing enforced policies
- Allow investigating data authorization policies beyond development env. (for system adopters and researchers)
- Education plans: Curriculum development + *Albany Privacy Clinic* at UAlbany and Capital Region of New York