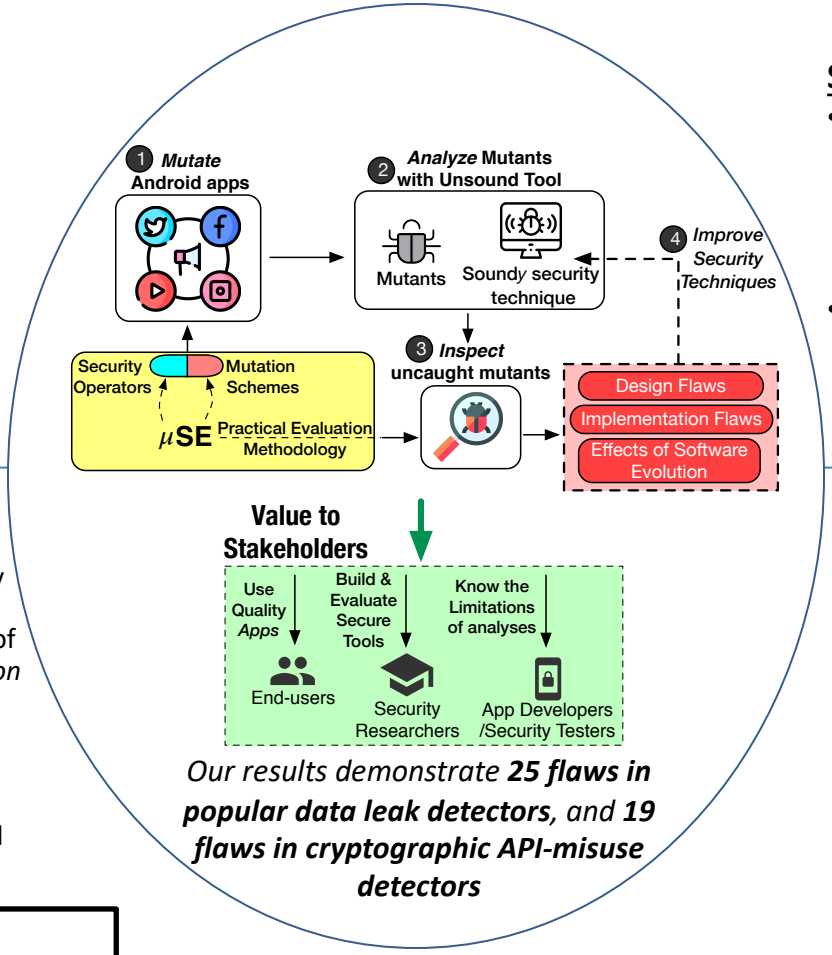
SaTC: CORE: Small: Enabling Systematic Evaluation of the Soundness of Android Security Analysis Techniques

WILLIAM & MARY
CHARTERED 1693

Challenge:

- Static security analyses for Android may contain *unknown* unsound assumptions that affect analysis accuracy, and may be hard to detect manually.



Solution:

- We contextualize mutation analysis for evaluating security techniques, by designing the *security-focused* abstractions of *security operators* and *mutation schemes*
- We have investigated the soundiness of several popular security techniques and discovered critical design-level flaws.

Scientific Impact:

- Our approach enables security researchers to systematically evaluate security techniques and discover subtle gaps in the sound core.
- We demonstrate that not only do design-level flaws exist in popular tools, but they also *propagate to emerging research*.

Broader Impact and Broader Participation:

- Consumers will be benefited through the availability of secure/safe applications
- The project enables researchers to design better techniques, and analysts to know the limitations of their analyses.
- Projects artifacts such as the framework source code and security operators/mutation schemes have been made public.
- PIs Nadkarni and Poshyvanyk have integrated this research in their “Mobile App Security” and “Software Engineering” classes, respectively.

CNS 1815336
PI: Adwait Nadkarni, Co-PI: Denys Poshyvanyk
{nadkarni,denys}@cs.wm.edu
College of William & Mary