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

Adwait Nadkarni (PI), Denys Poshyvanyk (Co-PI), William & Mary

https://github.com/Secure-Platforms-Lab-W-M/MASC-Artifact

Introduction

- **Correct use of cryptographic primitives is hard**.
- Security researchers make **Crypto API misuse-detectors** (*Crypto-Detectors)* to **prevent API misuse.**
- However, **we know very little regarding the actual effectiveness of crypto-detectors**.
- The **M**utation **A**nalysis for evaluating **S**tatic **C**rypto-API misuse detectors (MASC) framework can help **evaluate crypto-detectors by leveraging mutation testing**, i.e., by seeding mutants (*crypto API misuse*).

Challenges

- **Crypto-APIs are as vast as the primitives they enable**. Must express (i.e., test with) relevant misuse cases across existing crypto-APIs.
- Evaluation only using **misuse identified in the wild verbatim may not lead to robust analysis**, as it does not express the various usage patterns of such APIs.
- Efficiently creating and seeding **large numbers of compilable mutants without significant manual intervention is critical** for identifying flaws in crypto-detectors.

Scientific Impact

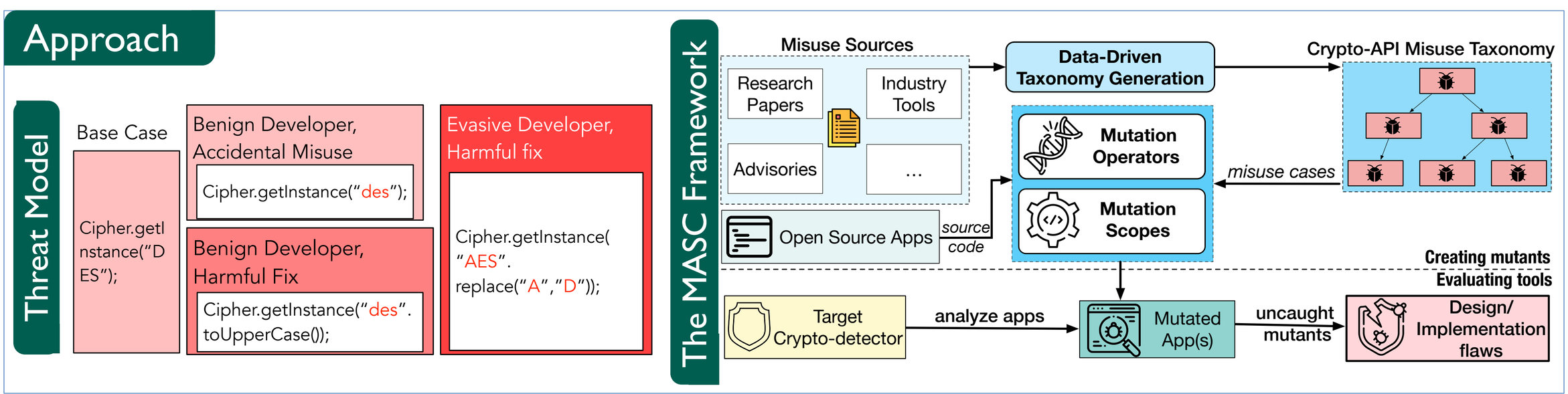
Comprehensive Crypto API Misuse Taxonomy
Contains: ***105 misuse cases*** *Covers:* **last 20 years**

Usage-based Crypto-mutation Operators allow **expressive instantiation of Crypto misuse cases**

Evaluation of 9 major crypto-detectors from industry, academia, and open-source revealed **19 previously unknown flaws**

Impact study to show that vulnerabilities relevant to **the flaws are present in real applications**

Approach



- **End-users** of apps and services will benefit from the security guarantees enabled by robust SAST tools
- **Researchers** and developers of crypto-detectors will be able to identify and mitigate flaws in their tools
- **Software developers** and practitioners (e.g., **app stores**) who use SASTs will benefit from more robust tools enabled by MASC (and mSE before it).

- Research integrated into graduate and undergraduate classes at W&M: CSCI 445: Mobile App Security, CSCI 435: Software Engineering.
- Talks: GMU, CERIAS Lab (Purdue), Chalmers University, Georgetown University, Ohio State University.
- Poster at NDSS'2022, paper talks at IEEE S&P 2022, USENIX Security 2018
- Artifact available for the community

- Mentored **6 external undergraduates** (ODU, CNU, IIT-D Bangladesh) with projects related but out of scope of this proposal.
- Advised an underrepresented undergraduate who did her honors thesis on a project emerging from mSE
- At least 5 crypto-detectors have begun addressing the flaws discovered by MASC.

Video