SaTC:TTP:Medium:Collaborative: Deployment-quality and Accessible Solutions for Cryptography Code Development

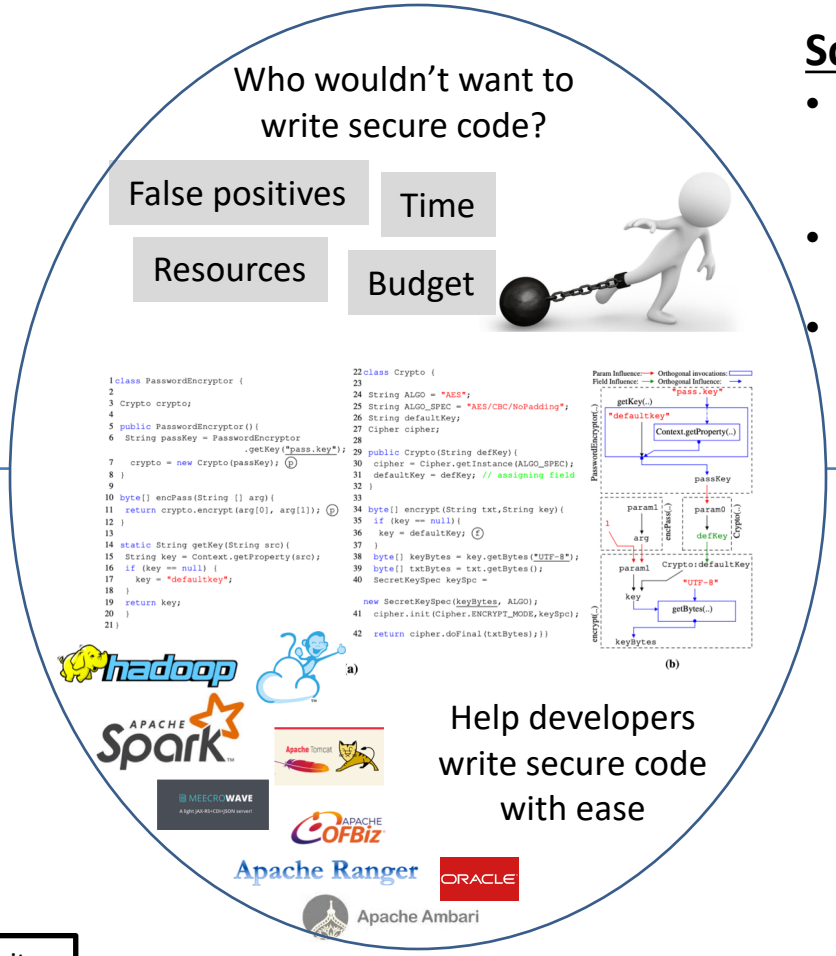
CryptoGuard

Challenge: There is a urgent demand for

- High-accuracy deployable solutions for crypto code screening
- Scientific benchmarking and measurement

Solution:

- Language-specific refinement methods for enhancing precision in static program analysis based crypto code screening
- Systematic benchmarks



Scientific Impact:

- Transition secure crypto coding research to practice
- Detect a wide range of crypto API misuses
- High-precision deployable security research is urgently needed

Broader Impact and Broader Participation:

- **We call for security researchers to understand and help developers**
- Adoption at Oracle Labs
- Integration into Oracle's internal screening framework Parfait
- Multiple 90-minute tutorials to diverse audiences

Award # 1929701. Virginia Tech and University of Wisconsin-Madison. Danfeng (Daphne) Yao (lead PI) . danfeng@vt.edu Barton Miller. bart@cs.wisc.edu Na Meng. nm8247@vt.edu