CryptoGuard

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

Goal: To close the huge gap between research and coding practices

Technical Challenges:

- **Many many many false positives**
- Not scalable to millions LoC
- Lack of benchmarks
- Few deployment-grade solutions
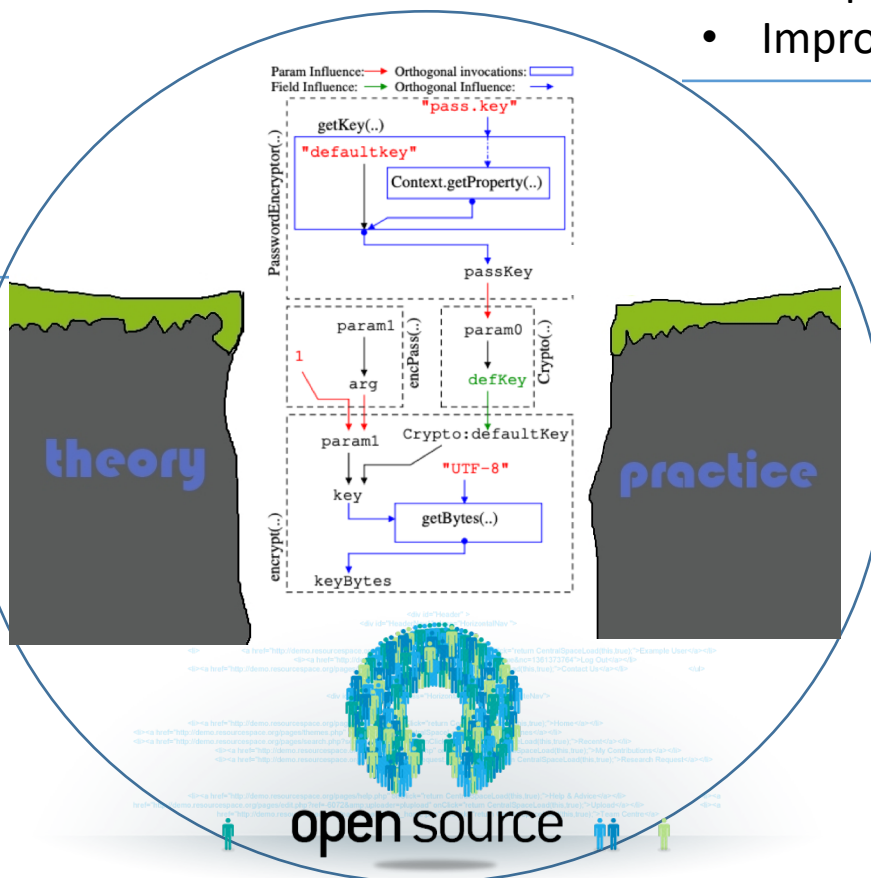- Lack of security awareness

TTP Enablers:

- **Refinement Strategies** to systematically remove false positives
- On demand flow-, context-, and field- sensitive analysis for accuracy/coverage/scalability
- **First Java crypto benchmark suite**

Scientific Impacts:

- **98.61% precision** on real-world Apache projs
- Best precision and recall on benchmarks compared w/ leading tools
- Improved **real-world Apache projects'** security

Key Ongoing Efforts:

- Transition to DHS-funded **Software Assurance Marketplace**
- Compiler for easy-to-use crypto-to-prog-analysis mapping

Broaden Participation in Computing:

- **Inclusive Excellence**: Increasing females' participation in conferences
- **Outreach**: VT's Imagination Camp for rising 7-th and 8-th graders, VT Women in Computing Day for 6-th grader girls, and computing diversity venues

Daphne Yao, Na Meng, Bart Miller

CNS-1929701 (10/01/2019 – 09/30/2023)

VT Virginia Tech | Wisconsin University of Wisconsin–Madison