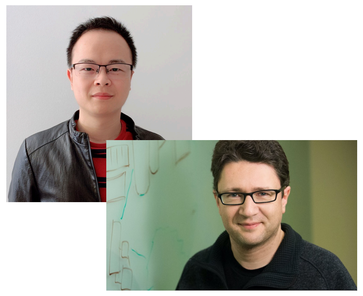
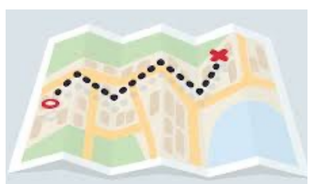
Collaborative Research: SaTC: CORE: Medium: Rethinking Fuzzing for Security

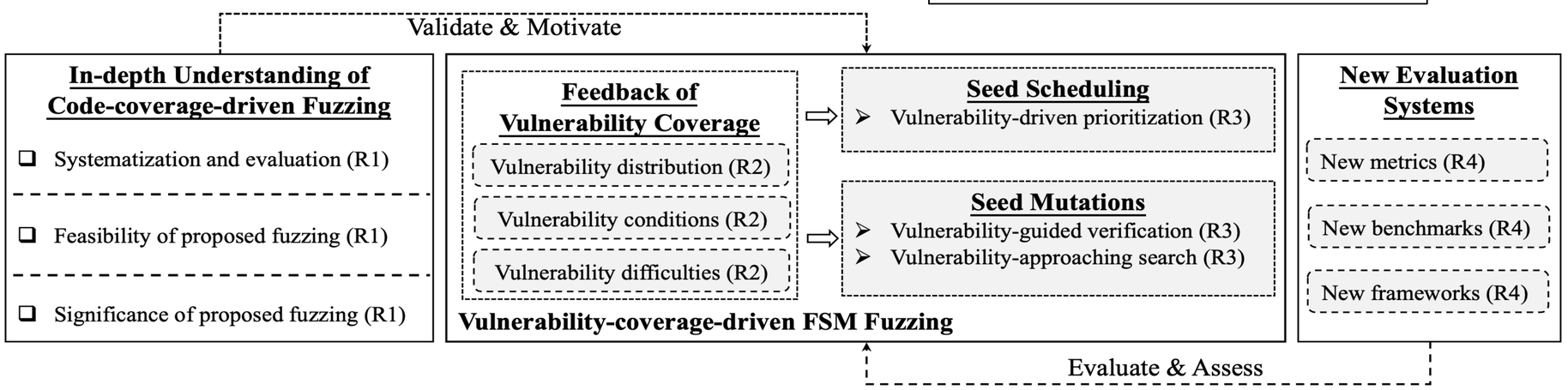
Jun Xu, The University of Utah; Engin Kirda, Northeastern University

CNS 2213727: The University of Utah
CNS 2031390: Northeastern University
Oct 2020 – September 2024





Project Roadmap



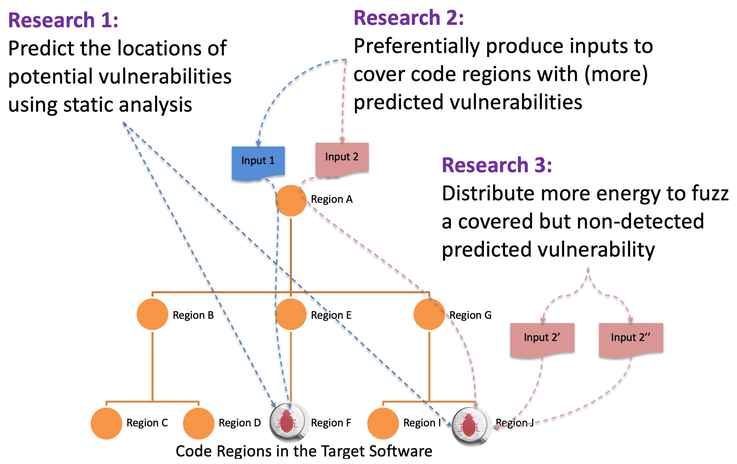
Research Problems

- Enable fuzzing to cover more vulnerabilities instead of just more code
- Design metrics and benchmarks to better evaluate fuzzing tools regarding vulnerability finding

Scientific Impact

- Develop new principles on using fuzzing for security
- Demonstrate that the new principles have the potential to revolutionize fuzzing in finding software vulnerabilities

Our Approach



Innovation and Contribution

- Idea: vulnerability-coverage driven fuzzing
- Technique: predict potential vulnerabilities using program analysis and enable fuzzing to focus on predicted vulnerabilities
- Evaluation: develop reality-approximating benchmarks and better-suited metrics to more properly understand the capability of fuzzing tools in finding vulnerabilities

Societal Impact

- Open-source tools reusable by software vendors and open-source communities: https://github.com/junxzm1990/ASAN--
- New findings and results reported through academic publications (S&P'21, SecureComm'21, NDSS'22, USENIX'22)

Education and Outreach

- Three new security courses at Stevens, NEU, and Utah (for both undergrad and grad)
- Building public cybersecurity training modules with ASU on top of https://pwn.college

Broader Impact and Broaden Participation

- 4 PhD (one female, one non-CS), 2 masters, 2 undergrad interns
- Summer camps, undergrad capstone events, K-12 science challenges, Women in Cybersecurity events