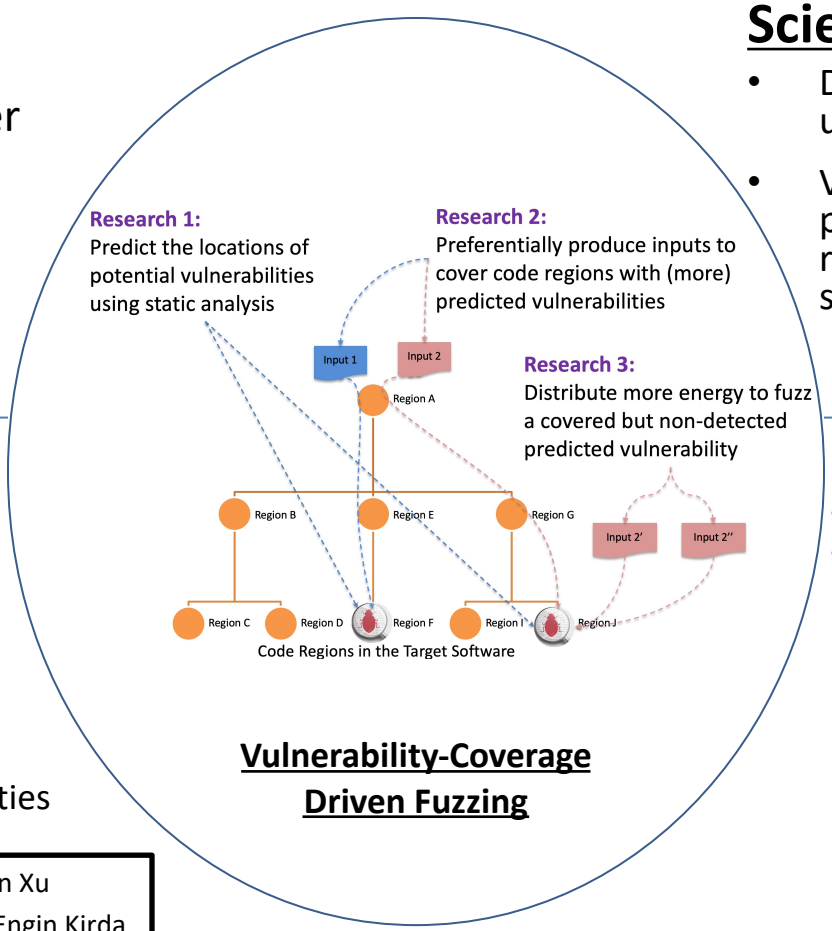
Collaborative Research: SaTC: CORE: Medium: Rethinking Fuzzing for Security

THE UNIVERSITY OF UTAH Northeastern University

Challenge:

- Enable fuzzing to cover more vulnerabilities instead of more code



Vulnerability-Coverage Driven Fuzzing

Solution:

- **Idea:** vulnerability-coverage driven fuzzing
- **Technique:** predict potential vulnerabilities using program analysis and enable fuzzing to focus on predicted vulnerabilities

CNS 2213727: The University of Utah, Jun Xu
CNS 2031390: Northeastern University, Engin Kirda
Oct 2020 – September 2024

Scientific Impact:

- Develop a new principle on using fuzzing for security
- Validate that the new principle has the potential to revolutionize fuzzing in finding software vulnerabilities

Broader Impact and Broader Participation:

- Techniques reusable by various software vendors and open-source communities
- Open source research tools and seek technology transfers
- S&P, USENIX, NDSS publications
- SecureComm Best Paper Award
- 3 new security courses at Stevens, NEU, and Utah, respectively
- 4 PhD students (one female, one non-CS)
- A group of undergraduate interns