SaTC: CORE: Small: Semantics-Oriented Binary Code Analysis Learning from Recent Advances in Deep Learning

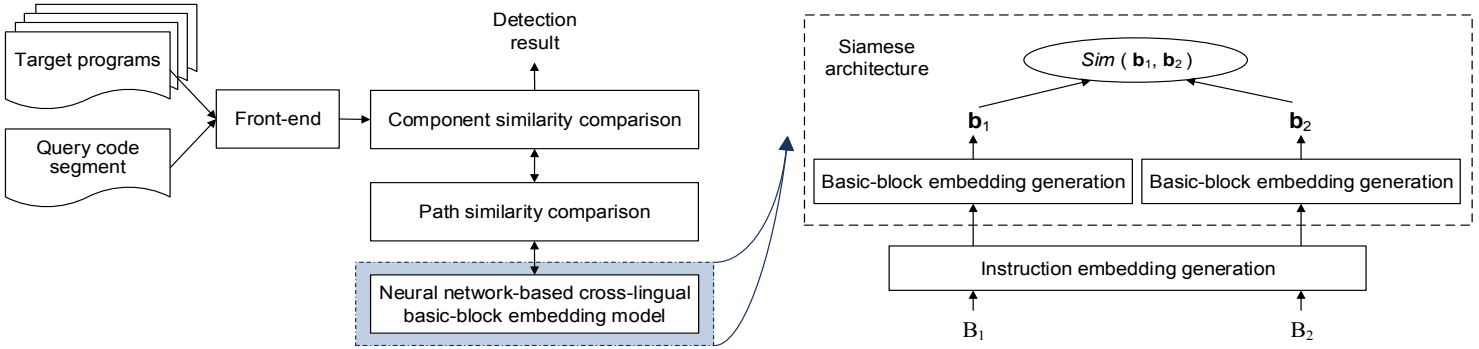
UNIVERSITY OF South Carolina

Challenge:

- Conventional binary code analysis typically suffers from being either inaccurate or unscalable.
- How to improve both the accuracy and scalability of binary code analysis is an unresolved problem.

Scientific Impact:

- This research will advance cross-architecture binary code analysis, and also propel its applications in vulnerability discovery, plagiarism, detection, and malware understanding especially in the context of heterogeneous IoT devices



Solution:

- The proposed research targets code semantics-oriented learning.
- We build deep learning based code analysis in a bottom-up approach, aiming to extract semantic information from binary code layer by layer.

Broader Impact and Broader Participation:

- Open-sourced the tools
- Funded the research of students from underrepresented groups
- Published papers in NDSS'21, MobiSys'22, etc.

CNS-1953073
University of South Carolina

PI: Lannan Luo (lluo@cse.sc.edu)