CRII: SaTC: Towards Efficient and Scalable Crowdsourced Vulnerability-Discovery using Bug-Bounty Programs

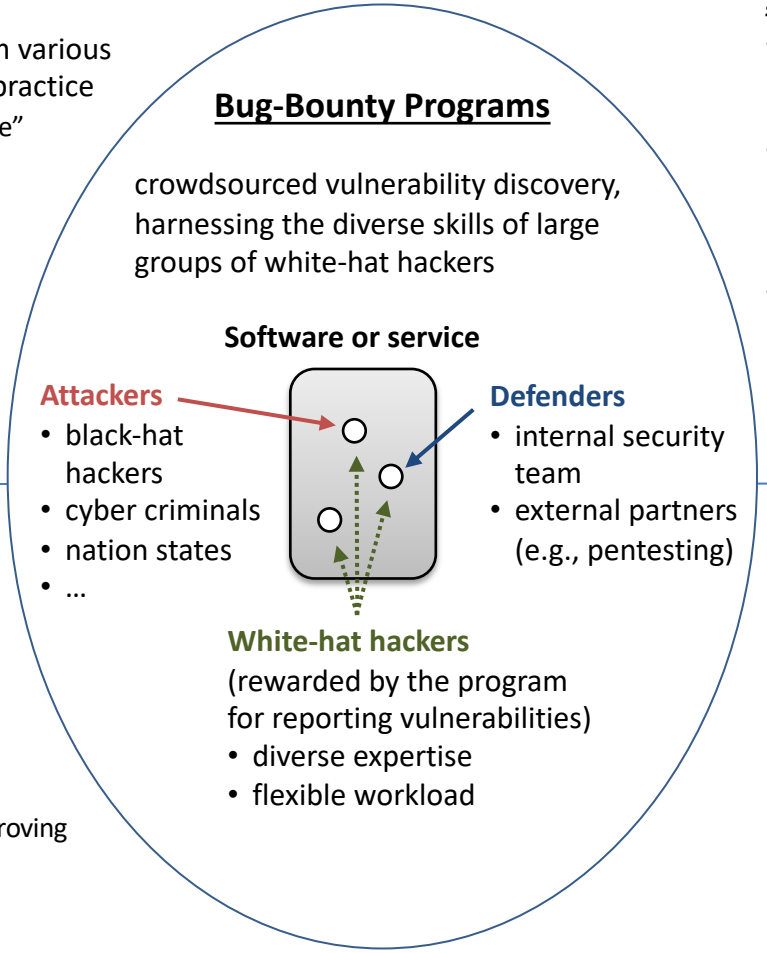
UNIVERSITY of HOUSTON

Challenge:

- Bug-bounty ecosystem suffers from various efficiency and scalability issues in practice
  - public programs receive a lot of "noise" (invalid and low-quality reports)
  - hackers often re-discover and report known vulnerabilities (duplicate reports)
  - …
- As the ecosystem grows, managing these issues becomes more challenging

Solution:

- Collect "hacktivity" data from programs and conduct interviews with white-hat hackers
- Perform qualitative and quantitative analysis of the data
- Develop a formal model of bug-bounty programs and the ecosystem
- Propose and study approaches for improving bug-bounty programs



Scientific Impact:

- Building a comprehensive bug-bounty dataset, with unified representation, formal terminology, and taxonomy
- Identifying performance factors; characterizing discovery, reporting, and triaging processes; and understanding the actors' incentives and actions
- Developing a novel interdisciplinary model that captures the entire ecosystem, including vulnerability-discovery processes, behavioral incentives, and market forces

Broader Impact:

- Organizations that run bug bounty programs will directly benefit from more efficient policies and management practices, leading to improved security
- White-hackers will benefit from increased efficiency as their skills and time will be better utilized and rewarded by programs
- Users will indirectly benefits from improved security

Award #1850510

PI: Aron Laszka (alaszka@uh.edu)
Institution: University of Houston