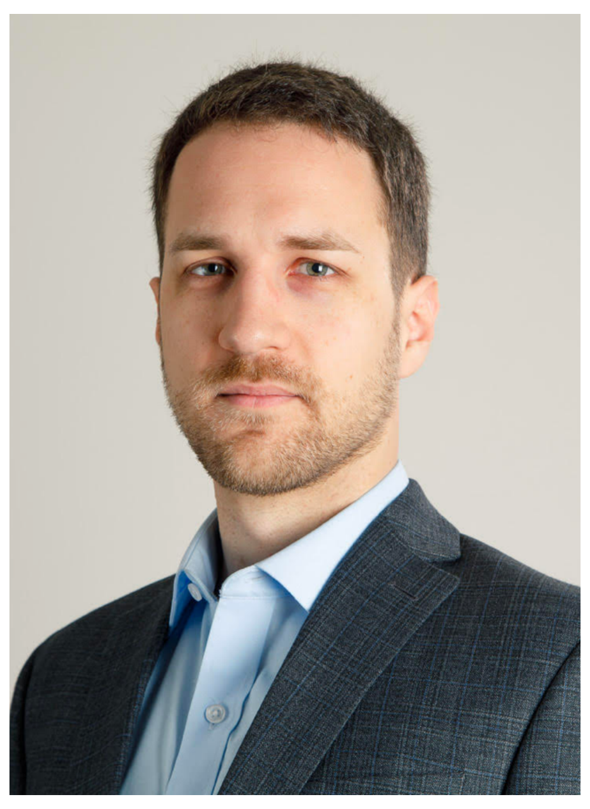
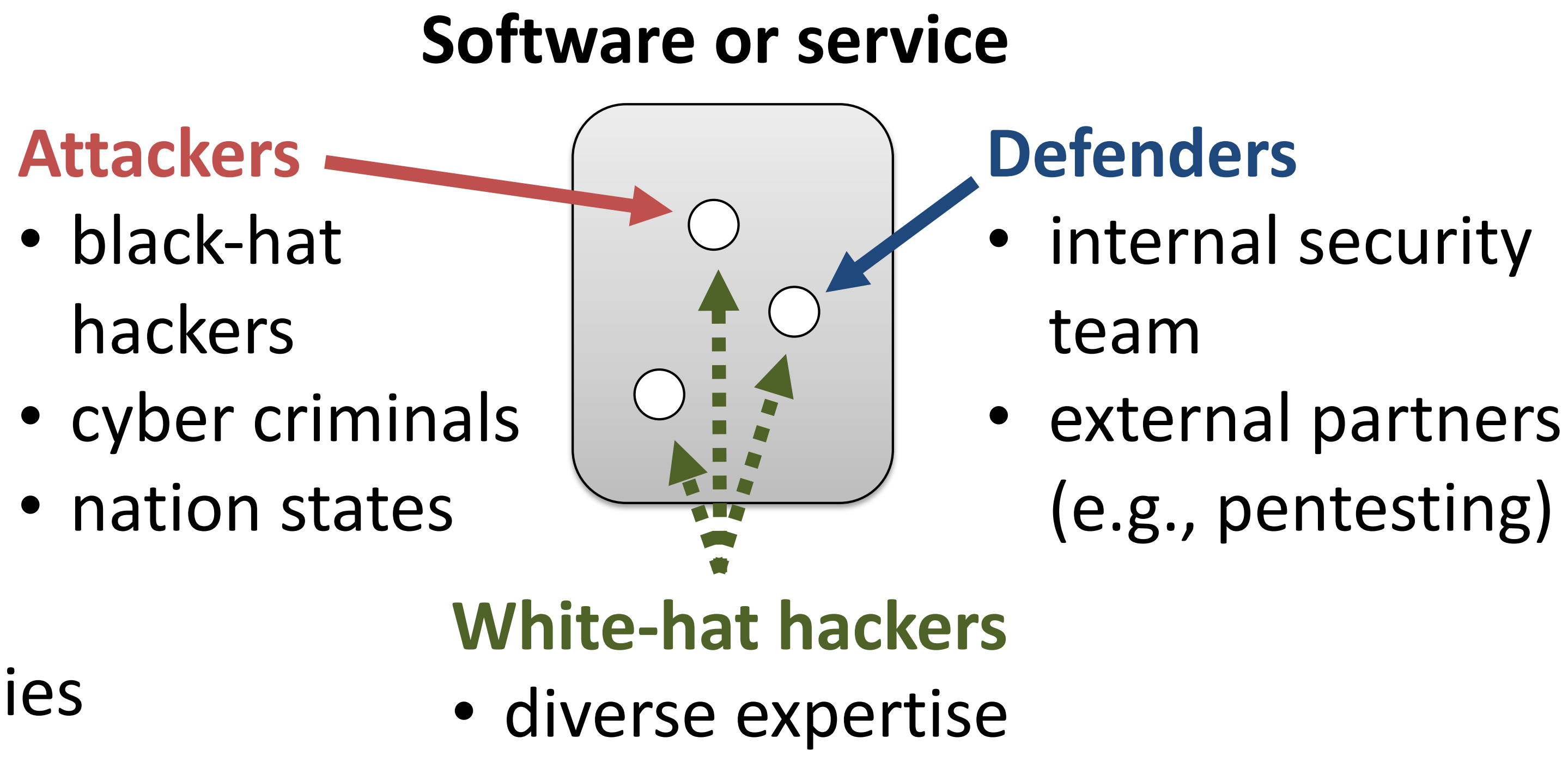
CRII: SaTC:
Towards Efficient and Scalable Crowdsourced Vulnerability-Discovery using Bug-Bounty Programs

PI: **Aron Laszka**, University of Houston
`http://aronlaszka.com/projects.html`



- **Bug-bounty programs** recently emerged as a key element of many organizations' security culture
- A bug-bounty program is a form of **crowdsourced vulnerability discovery**
  - gives white-hat hackers permission to test a software product or service and to **report vulnerabilities**
  - incentivizes hackers by **rewarding valid reports** with bounties
- Advantages of establishing a bug-bounty program
  - harnesses the **diverse expertise of large groups** of white-hat hackers
  - publicly signals the organization's **commitment to continuously improving security**



Software or service

Attackers
- black-hat hackers
- cyber criminals
- nation states

Defenders
- internal security team
- external partners (e.g., pentesting)

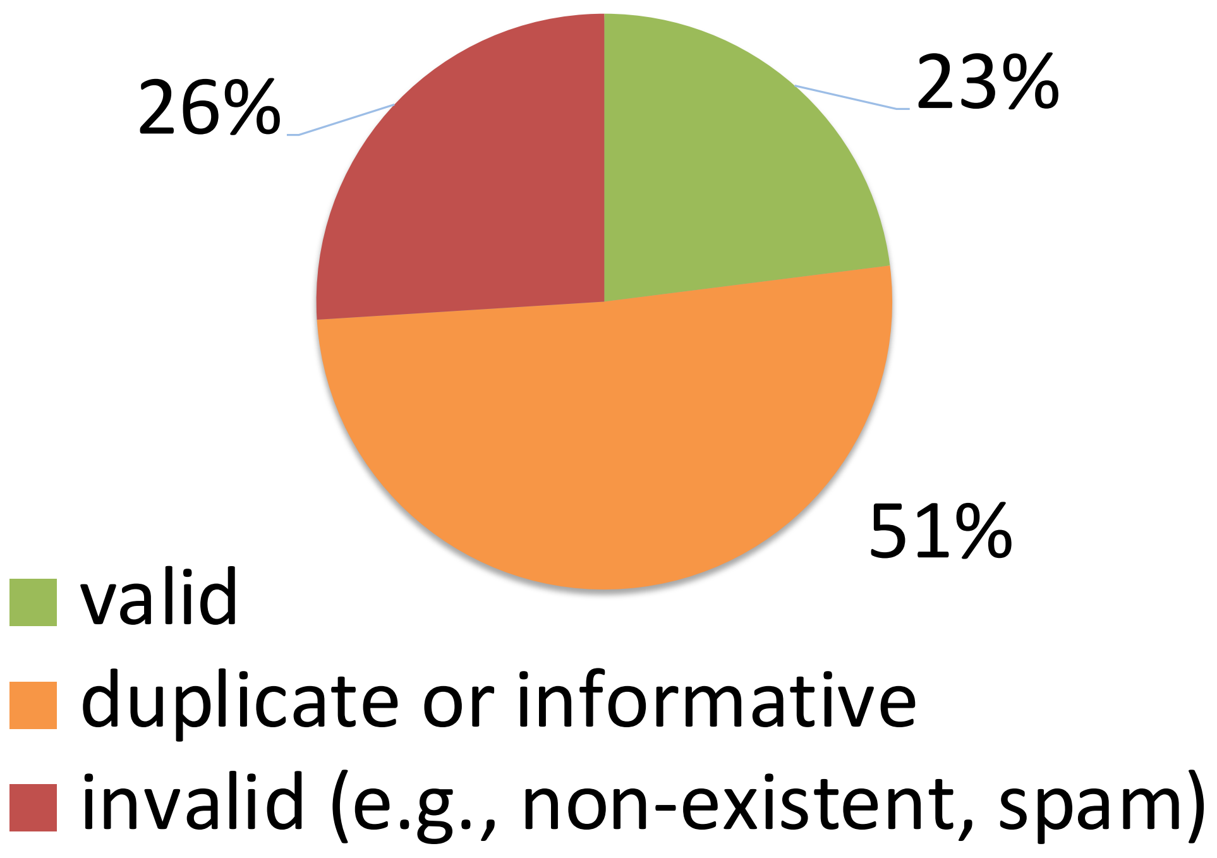
White-hat hackers
- diverse expertise

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)
- programs compete with each other to attract skilled hackers
- …

- As the ecosystem grows, these issues become more pressing

Reports received by public programs on a leading platform in 2018



Project Goals and Intellectual Merit: provide a **better understanding** and **formal model** of the **bug-bounty ecosystem** and **improve** the **efficiency** and **scalability** of bug-bounty programs

1. **Data collection**: build a comprehensive bug-bounty dataset (hackers, programs, platforms, …)
   – conduct interviews with white-hackers and key stakeholders, collect "hacktivity" data from programs
2. **Data analysis:** analyze dataset to discover overarching relations, to characterize the discovery, reporting, and triaging processes, and to understand the actors' incentives and actions
   – establish formal terminology and taxonomy of bug-bounty related terms
3. **Model:** develop a novel model that captures the entire bug-bounty ecosystem, including technological vulnerability-discovery processes, behavioral incentives, and market forces
4. **Policy, Management, Regulation:** propose, analyze, and evaluate approaches for improving the efficiency and scalability of bug-bounty programs

Broader Impact:

- **Organizations** that run bug bounty programs will **directly benefit** from **more efficient policies** and **management practices**, leading to improved security at lower cost
- **White-hat hackers** will **benefit** from improved efficiency as their skills and time will be **better utilized and rewarded**
- **Users** will **benefit** from **improved security**

Educational Impact:

- Development of **graduate course** on cybersecurity economics and management
- **Research opportunities** for students from underrepresented groups and undergraduates

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 I Alexandria, Virginia