Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes

Daniel Votipka, Rock Stevens, Elissa M. Redmiles, Jeremy Hu, and Michelle L. Mazurek

Research Questions
How do hackers and testers search for software vulnerabilities?

What are the differences between hackers and testers?

Populations

Testers: Bug finding generalists. Search for functionality, performance, and security bugs.

Hackers: Security specialists. Members of internal security team, contracted review, or bug bounty.

Interview Study
Participants were asked to complete a cognitive task analysis of their vulnerability discovery process.

Also asked to discuss tools used, skills needed, and communities they are members of.

15 hackers and 10 testers recruited through bug bounty platforms, related interest groups, and hacking teams.

Vulnerability Discovery Process

Vulnerability Discovery Experience

Info Gathering

Program Understanding

Underlying System Knowledge

Access to Development Process

Motivation

Attack Surface

Exploration

Vulnerability Recognition

Reporting

Key Difference

The most important difference observed between hackers and testers was the variety of experience.

Challenges:
- Timeliness
- Cognitive Diversity
- Communication

Discovery Lifecycle

Increases in these factors are expected to improve likelihood of vulnerability discovery success.

No straightforward relationship between these factors and reported vulnerability discovery success.

1. Provide a variety of training in known contexts
   - Security champions
   - Bug report-based exercises

2. Improve communication between hackers and companies
   - Establish single point of contact
   - Develop advocacy training and resources for hackers

3. Consider alternate compensation methods to match different motivations
   - Adjust payout structure as security posture matures
   - Use non-monetary motivators