BLUES BERKELEY LABORATORY FOR USABLE AND EXPERIMENTAL SECURITY

“You’ve Got Your Nice List of Bugs, Now What?” Vulnerability Discovery and Management Processes in the Wild

Noura Alomar, Primal Wijesekera, Edward Qiu, and Serge Egelman
University of California (Berkeley) and ICSI

ICSI INTERNATIONAL COMPUTER SCIENCE INSTITUTE

CLTC Center for Long-Term Cybersecurity

King Saud University

Motivation

- Many testing strategies
  - Penetration testing
  - Blue/ red and purple teams
  - Bug bounty programs
  - Quality assurance teams

Motivation

- Many testing strategies
  - Penetration testing
  - Blue/ red and purple teams
  - Bug bounty programs
  - Quality assurance teams
- Many advanced vulnerability detection techniques
- Standards: ISO/IEC 29147 and ISO/IEC 30111

What decision makers expect from the various testing strategies?

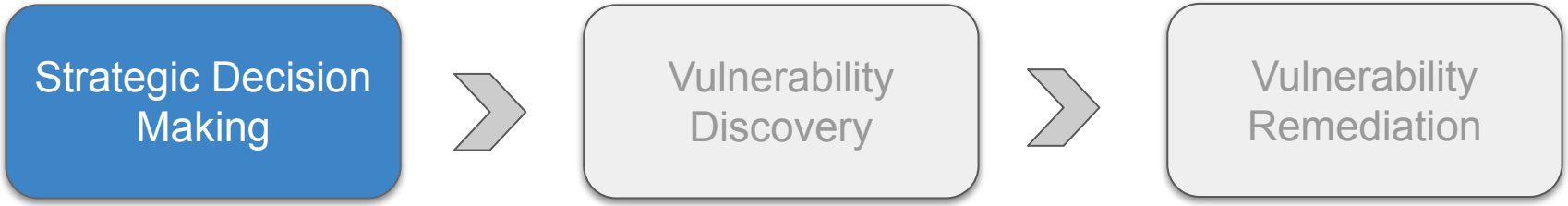
How do different teams fit in vulnerability discovery processes?

Methodology

- Interviews with 53 security practitioners
- Roles
  - CISOs, CTOs, security managers
  - Pen testers, bug bounty hunters, red/blue/purple teamers, internal security testers
- Countries
  - Bangladesh, Canada, Germany, India, Israel, Serbia, Singapore, Brazil, UK and US

Vulnerability Management Pipeline

Vulnerability Management Pipeline

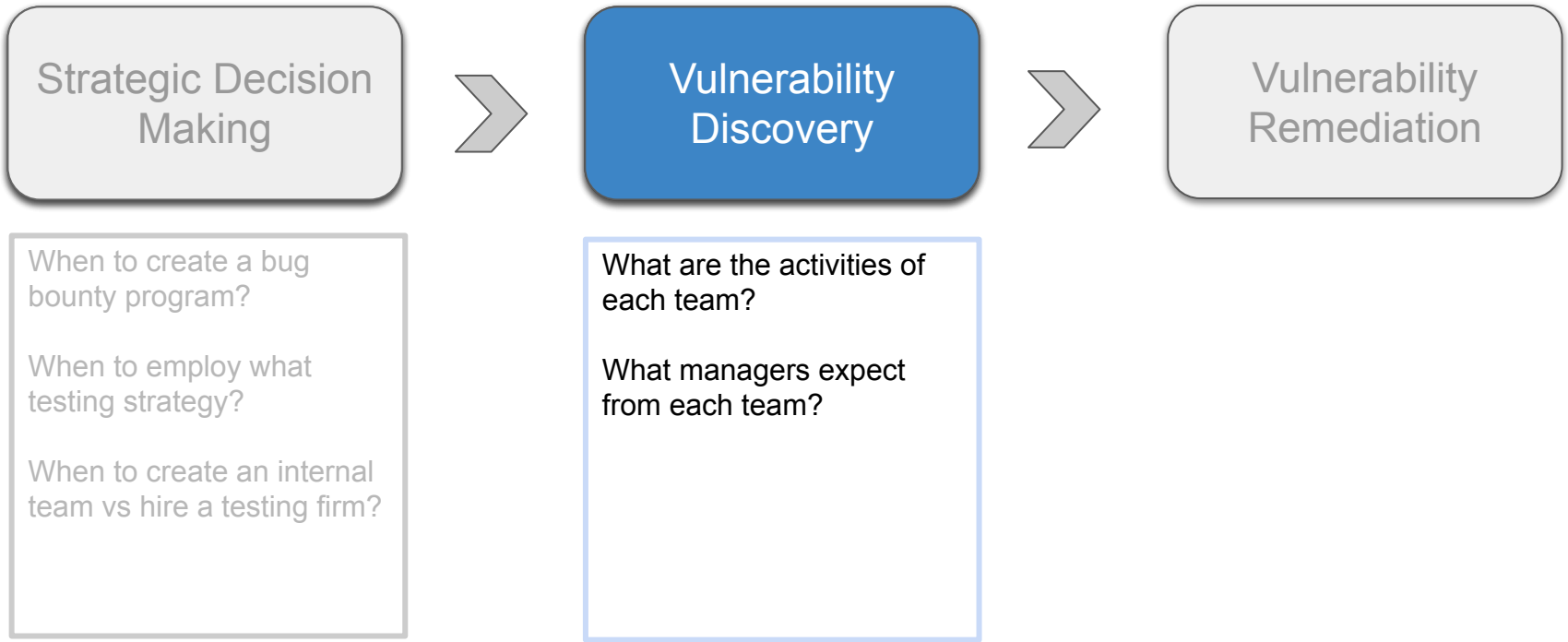


When to create a bug bounty program?

When to employ what testing strategy?

When to create an internal team vs hire a testing firm?

Vulnerability Management Pipeline



Vulnerability Management Pipeline

Main themes

1. Trust: internal vs external testers

Main themes

1. Trust: internal vs external testers
2. Communication & information sharing

Main themes

1. Trust: internal vs external testers
2. Communication & information sharing
3. Uncertainty around who is responsible for what

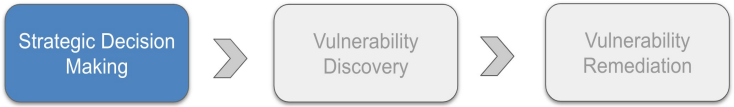
Main themes

1. Trust: internal vs external testers
2. Communication & information sharing
3. Uncertainty around who is responsible for what
4. Compliance-oriented approaches

Strategic Decision Making

- Uncertainty around what to expect from each team

“I have had clients that have suffered a breach in the past and immediately they are like, ‘Hey, we want to get a penetration test or a red team to figure out how the attacker broke in’” (P37)



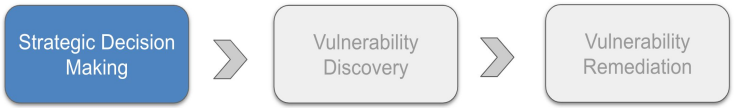
Strategic Decision Making

- Uncertainty around what to expect from each team

  “I have had clients that have suffered a breach in the past and immediately they are like, ‘Hey, we want to get a penetration test or a red team to figure out how the attacker broke in’” (P37)

- Bug bounty programs might be used as replacement to internal testing

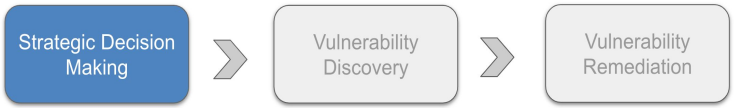
  “My CISO likes to be able to tell customers we have a bug bounty program; therefore we are very secure” (P41)



Pen testing

- Compliance requirements

“Pen tests are kind of a reproducible formula for getting the engagement done whether it is to get that compliance checkbox checked or they are just kind of going through the motions to make sure that basic security structures are in place” (P10)



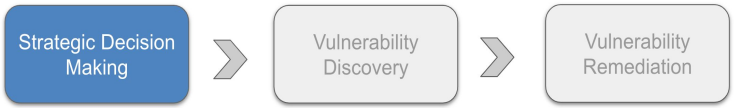
Pen testing

- Compliance requirements

  “Pen tests are kind of a reproducible formula for getting the engagement done whether it is to get that compliance checkbox checked or they are just kind of going through the motions to make sure that basic security structures are in place” (P10)

- Accountability

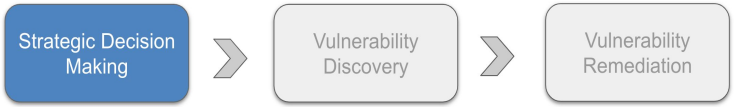
  “..the quality of that report you get from pen testing companies is much much higher. It can also hold people who did the pen test accountable” (P32)



Red teaming

- Exposure to legal liability

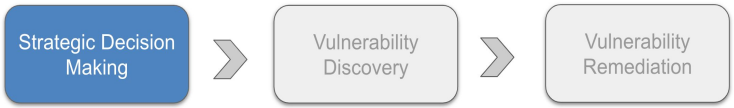
“You don’t know when someone is in the network, you don’t know what he is reading. I know that there are NDAs, but sometimes there is a code of ethic, that says if you find something illegal during a penetration test, you have to report it. And in red teaming, let’s be honest not many companies are in regulations with the law” (P24).



Bug Bounty Programs

- Sensitivity of data stored in organizations' systems

  "...trying to convince any government agency to try to offer people a reward to try to break into their financial data, I think we would have a very bad reaction to that, whereas saying, 'it's an audit' would be a much easier sell" (P44)



Trust

- Organizations → scoping decisions

  “..everybody is talking about they want a red team, they want a red team, but at the end of the day, they want to put a bunch of rules around it, just like regular penetration tests" (P38)

Trust

- Organizations → scoping decisions

  "..everybody is talking about they want a red team, they want a red team, but at the end of the day, they want to put a bunch of rules around it, just like regular penetration tests" (P38)

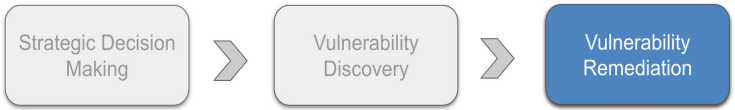
- Bug bounty hunters → legal concerns

  "I was looking around and I saw this, what looked like financial data and I started freaking out because it was a public company. But that was kind of scary that I had even looked at it and what if they saw that I looked at it" (P25)

Compliance vs. Security

- External pen testers are asked to:
  - downplay severity ratings
  - take some vulnerabilities out of reports

“We’ve been told we don’t want you to actually solve this problem, we just want you to make the check box go away” (P9)



“You’ve Got Your Nice List of Bugs, Now What?” Vulnerability Discovery and Management Processes in the Wild

Noura Alomar, Primal Wijesekera, Edward Qiu, and Serge Egelman

- ➔ Issues impacting effective vulnerability management:
  - Trust
  - Communication
  - Staffing & funding
  - Misalignment between business & security priorities
- ➔ Need to pay more attention to vulnerability remediation**!**

Thank you!

nnalomar@berkeley.edu
@Noura_7N