

Human Factors of Security-Sensitive People

INFR11158/11230 Usable Security and Privacy

Jingjie Li

10/03/2025



THE UNIVERSITY
of EDINBURGH

Who are the “users” we are talking about?

Users are “special” because...

- They are security or safety-sensitive
 - Domain knowledge possessed
 - Unique security and safety requirements and cost-benefit tradeoffs
- When we refer to users, we also talk about their status and contexts
- Question:
 - What are their needs?
 - How to properly do research with them, and for them?

Name a type of “users” you find it unique, and discuss why?

Hackers

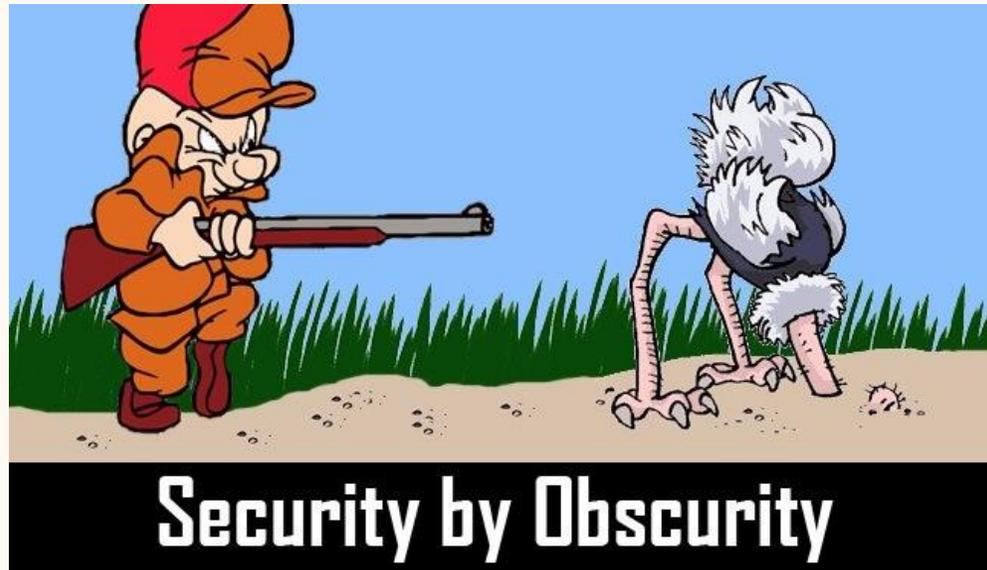
What is Hacking or Vulnerability Research?

The logo for Malwarebytes, featuring a stylized blue 'M' icon followed by the word 'malwarebytes' in a blue sans-serif font with a registered trademark symbol.A smaller version of the Malwarebytes logo, consisting of the stylized 'M' icon and the word 'malwarebytes' in a smaller font.

- <https://www.youtube.com/watch?v=pxSp6HeM4RM>
- <https://www.youtube.com/watch?v=ID34wkOcCRE>

So, you found a bug. What's next?

- Attack
- Sell it
- Disclosure



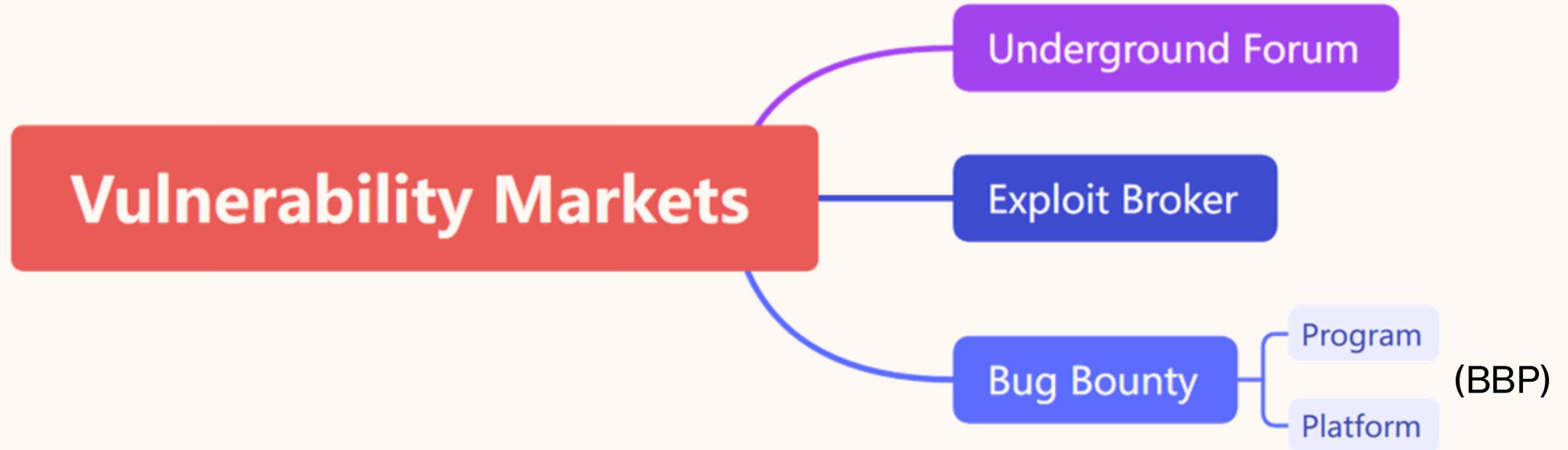
Full Disclosure

Disagree	Agree
<ul style="list-style-type: none">• Nobody except researchers need to know the details of flaws	<ul style="list-style-type: none">• FD helps the good guys more than the bad guys
<ul style="list-style-type: none">• FD results in information anarchy	<ul style="list-style-type: none">• Effective security cannot be based on obscurity
<ul style="list-style-type: none">• Good guys who publish virus code may also have malicious intention	<ul style="list-style-type: none">• Making vulnerabilities public is an important tool in forcing vendors to improve their products
<ul style="list-style-type: none">• Safer if researchers keep details about vulnerabilities and stop arming hackers with offensive tools	<ul style="list-style-type: none">• If an exploit is known and not shared, the vendor might be slower to fix the hole
<ul style="list-style-type: none">• The risk associated with the publishing information outstrip its benefit	<ul style="list-style-type: none">• Sharing information security with other professionals is an absolute necessity
<ul style="list-style-type: none">• It serves to arm hackers with tools to break systems	

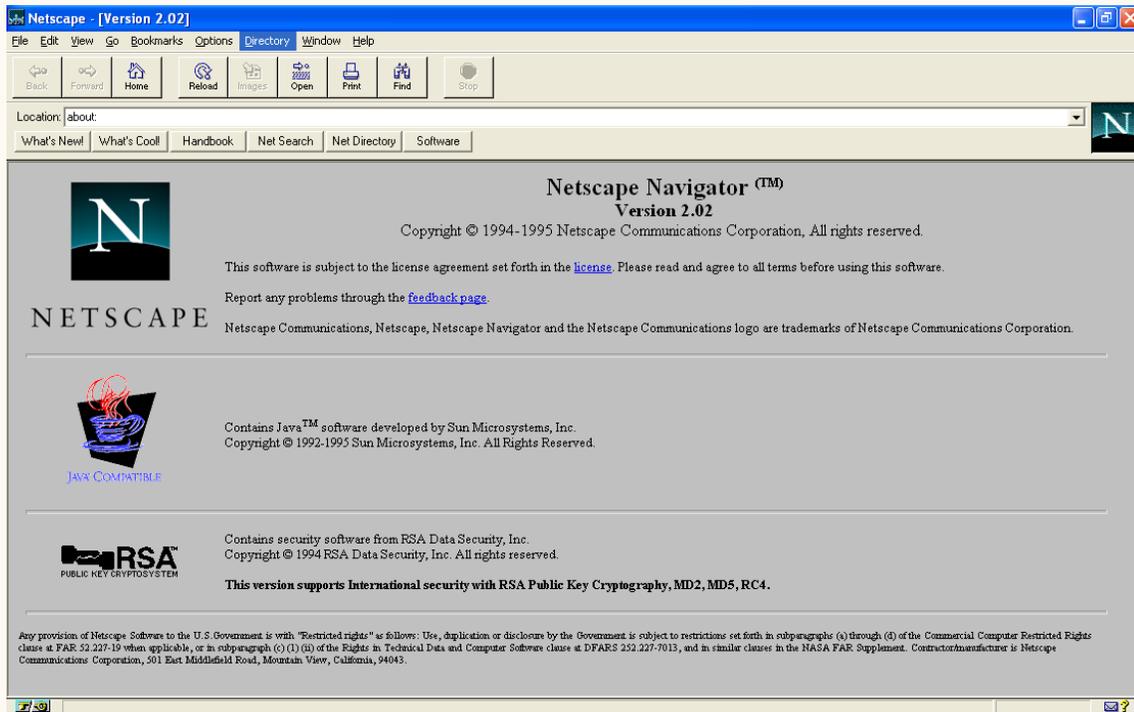
Responsible Disclosure

- Reporting directly to the affected company
- Follow the company's disclosure process
- Allow time for the company to fix the bug
- Disclosure to the public after an embargo

Vulnerability Market

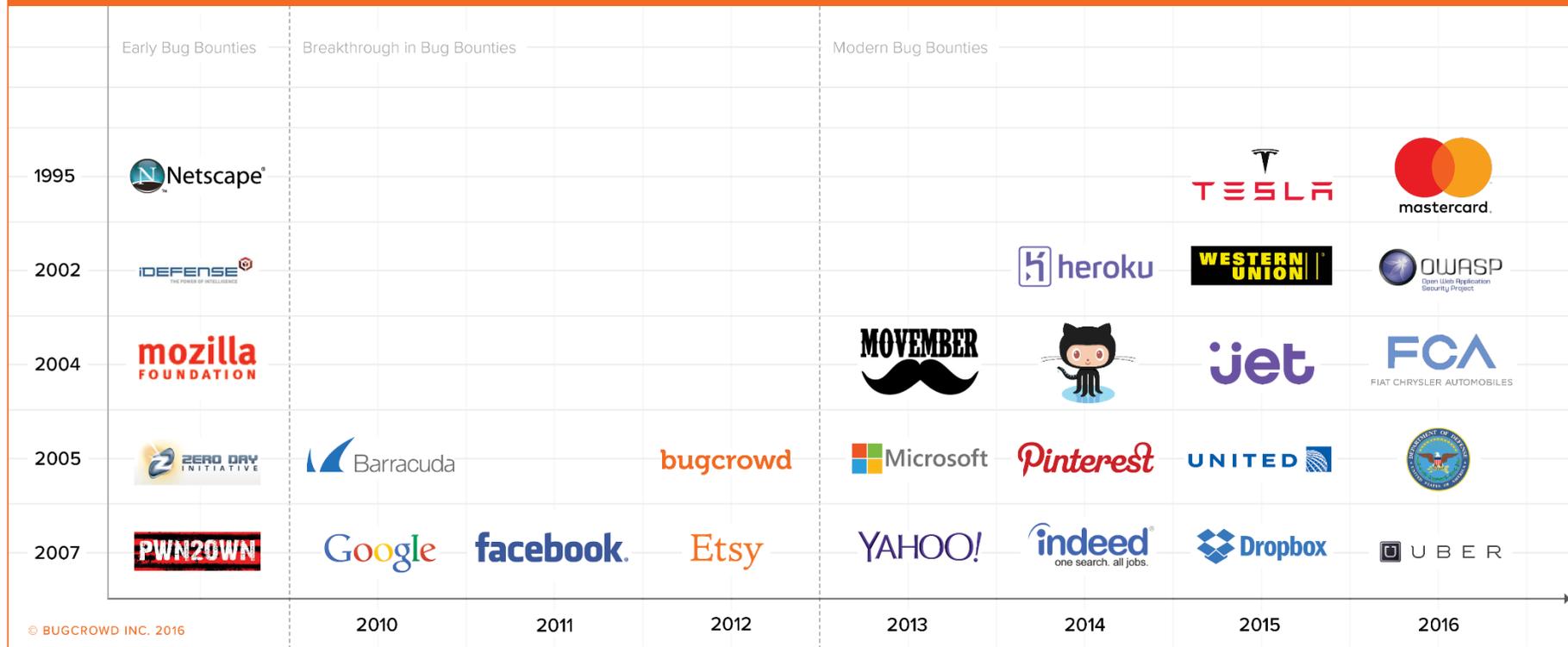


Bug Bounty



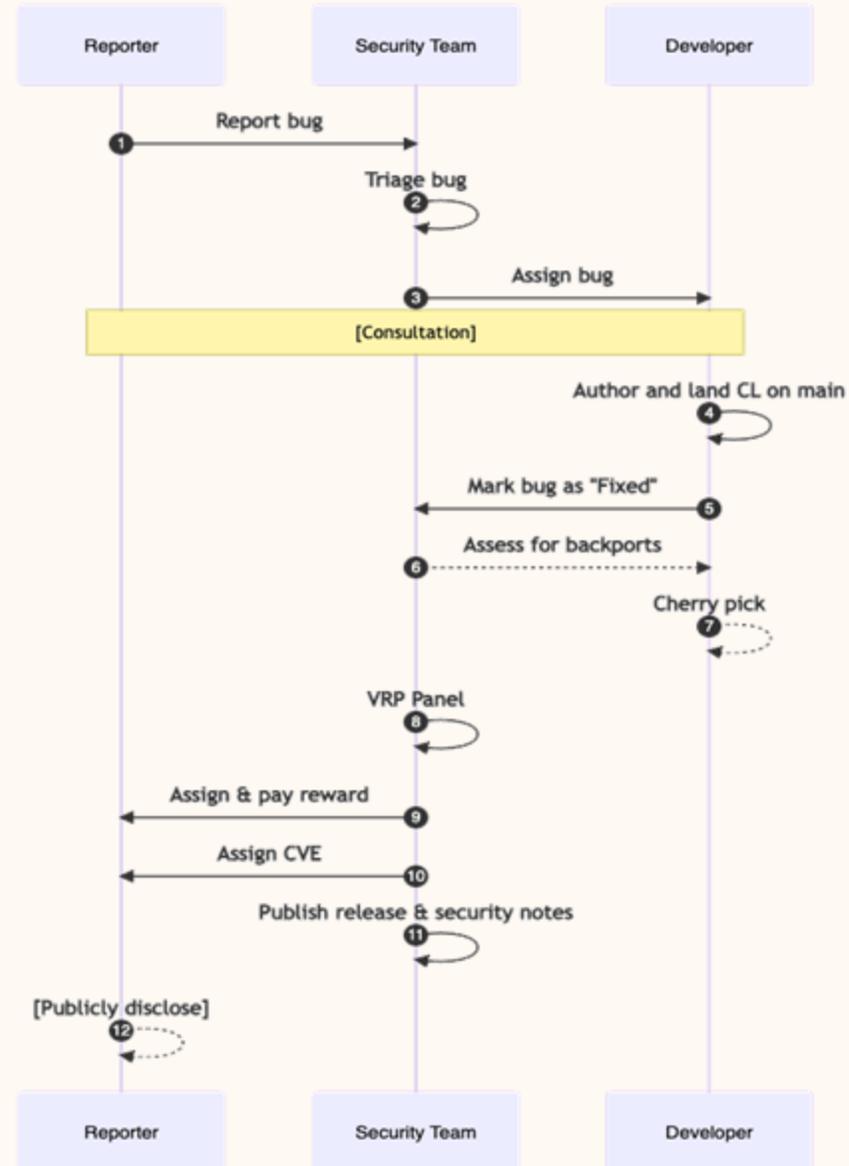
Development of Bug Bounty

The History of Bug Bounties: Abbreviated Timeline from 1995 to Present



Stakeholders

- Bug Hunter
- Platform
 - Operator
 - Triager
 - Mediator
- Vendor/Program
 - Reviewer/Security Team
 - Developer
- End User



Why companies need hackers' help?

Why Companies Need Hackers

- Given that many tech companies have their own large security departments, why do they still need hackers' help?

Google researchers uncover critical security flaw in all AMD Zen processors

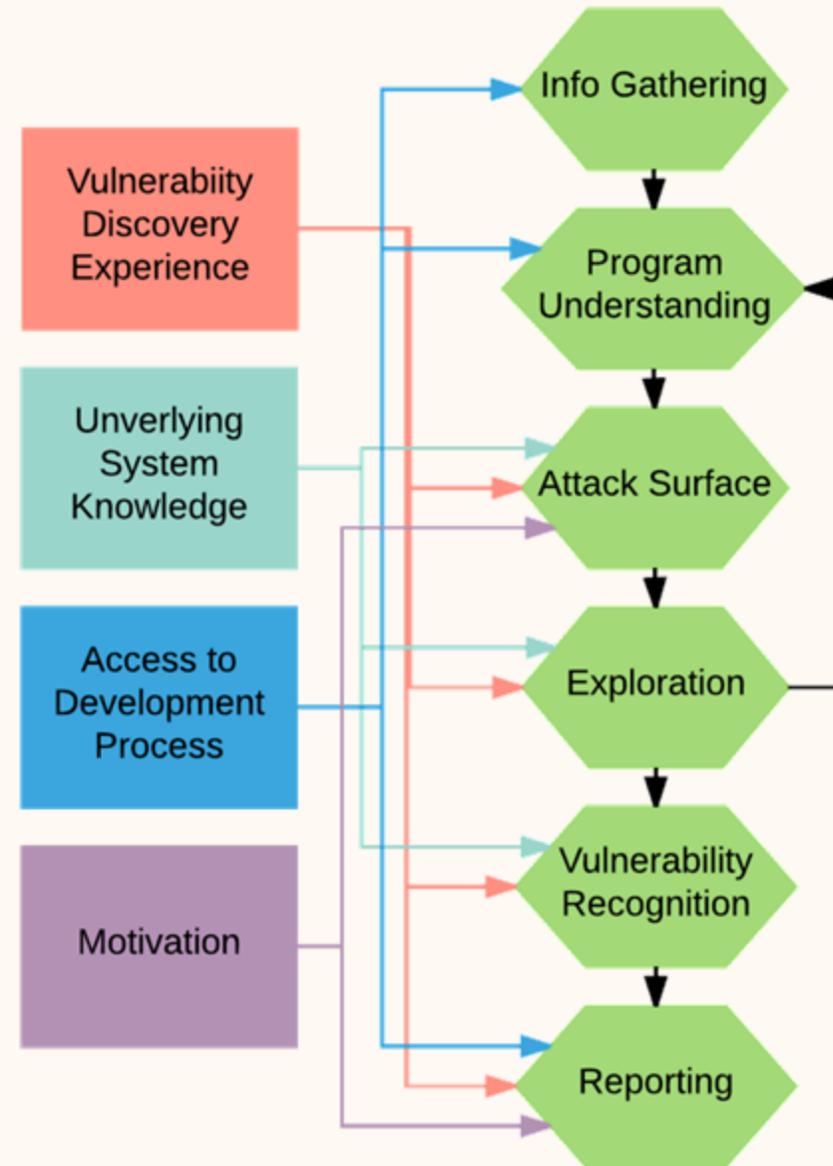
Google has released an open-source jailbreak toolkit to deploy custom microcode patches on vulnerable CPUs

Google Paid Out \$10 Million via Bug Bounty Programs in 2023

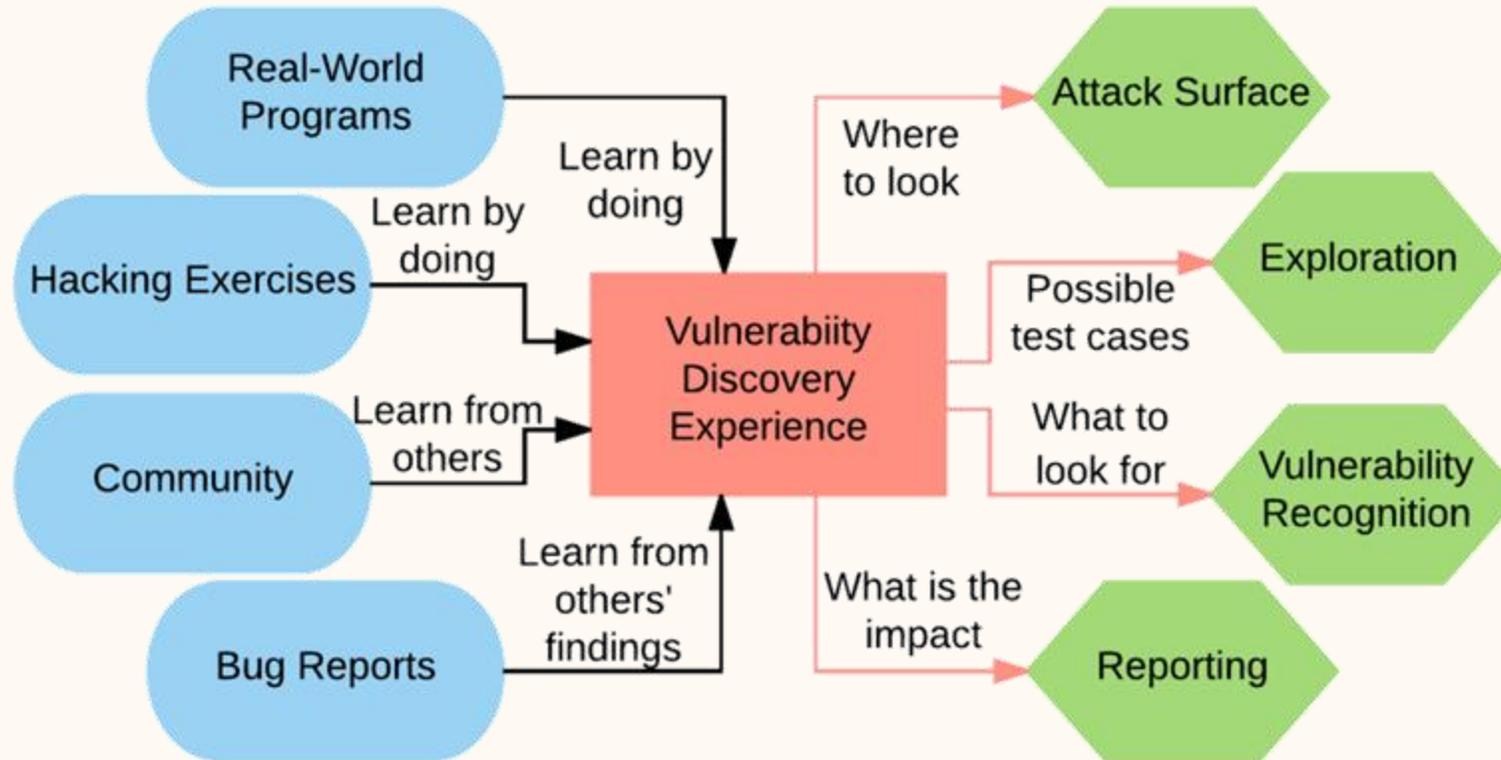
Google paid out \$10 million via its bug bounty programs in 2023, bringing the total to nearly \$60 million since 2010.

Hacker vs Tester

- What are the differences in the vulnerability discovery processes between external and internal?
- Four influencing factors

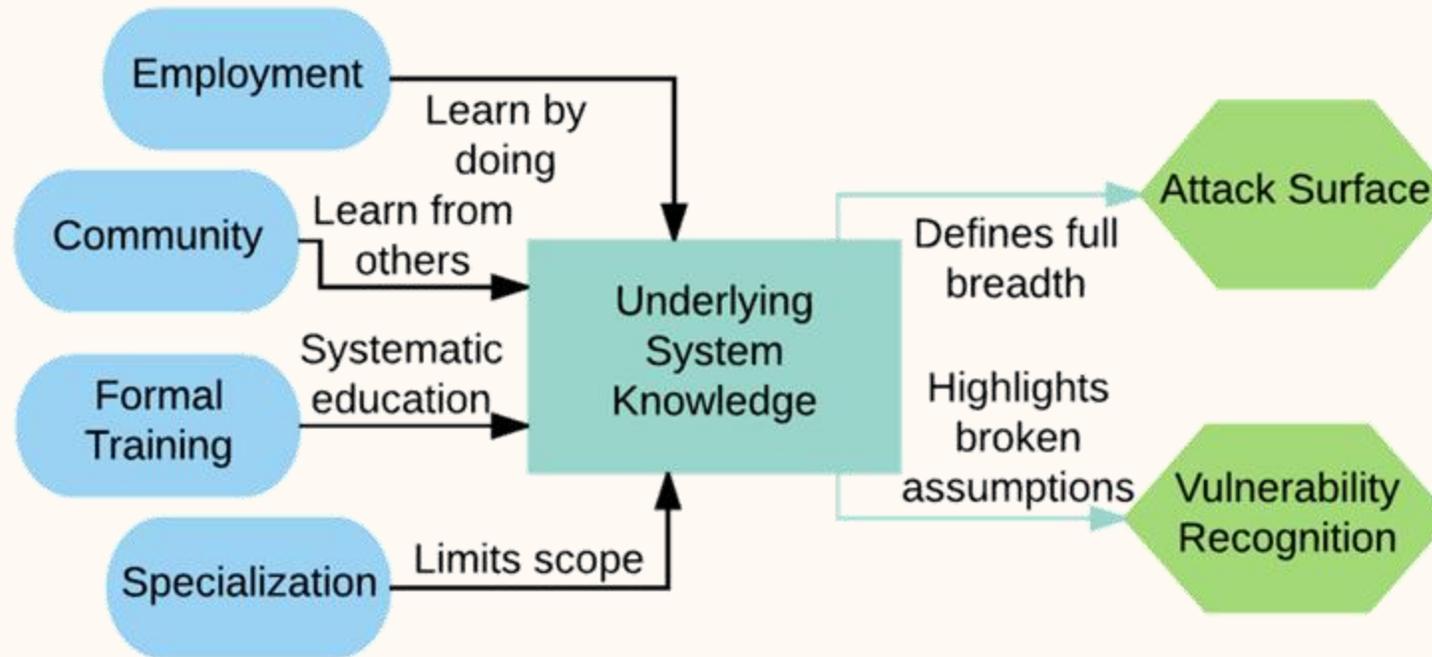


Vulnerability Discovery Experience



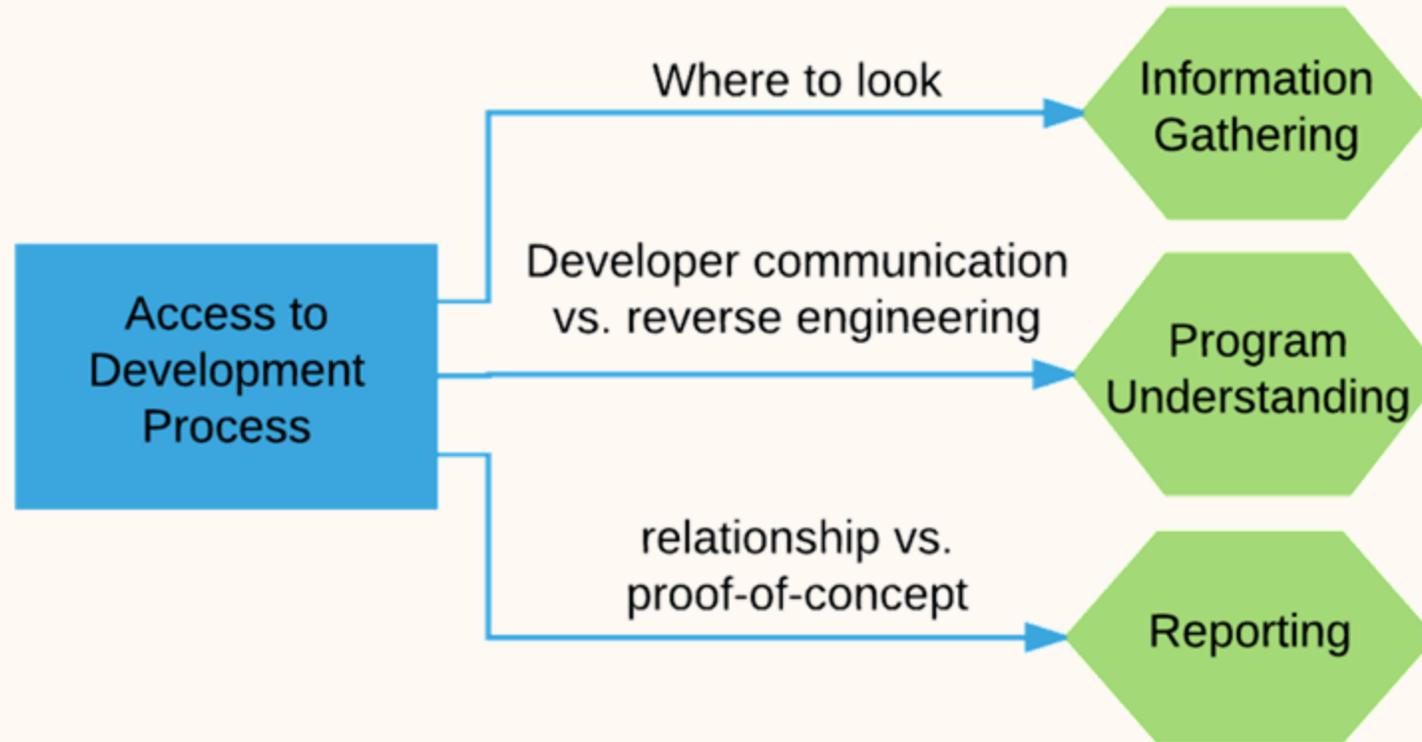
- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Underlying System Knowledge



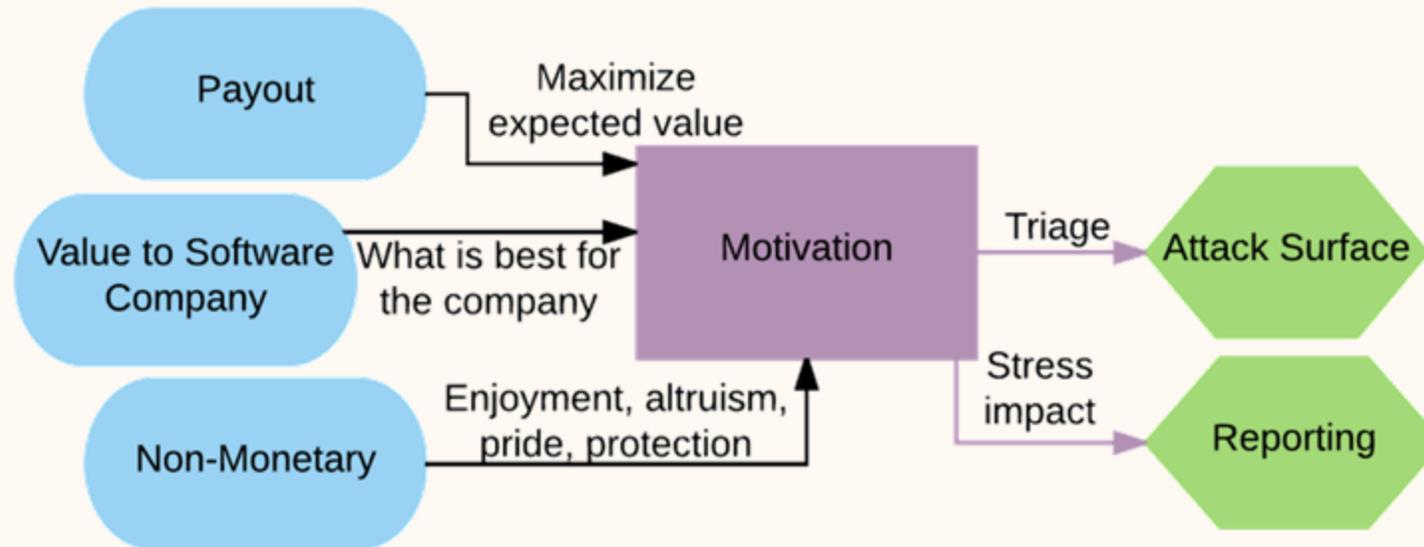
- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Access to Development Process



- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

Motivation



- Votipka, D., Stevens, R., Redmiles, E., Hu, J. and Mazurek, M. Hackers vs. testers: A comparison of software vulnerability discovery processes. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 374-391).

What benefits can companies gain? Also thinking about externalities and internalities

Benefits from Bug Bounties - Chromium

- Bugs are likely to be identified & patched during the development process
- BBP leverages the diverse expertise of external hackers
- Hackers discover bugs at a fairly constant rate

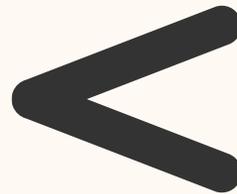
- Atefi, S., Sivagnanam, A., Ayman, A., Grossklags, J. and Laszka, . The benefits of vulnerability discovery and bug bounty programs: Case studies of Chromium and Firefox. In ACM Web Conference 2023 (pp. 2209-2219).
- Walshe, T. and Simpson, A. An empirical study of bug bounty programs. In 2020 IEEE 2nd international workshop on intelligent bug fixing (IBF) (pp. 35-44).

How about the cost?

- The average cost of operating a BBP for a year is less than the cost of hiring two additional software engineers.
- Why is that?



BBP



Software Engineers

Vendors' Perspective

- Hackers use different methods than internal testers
- Hackers can find different kind of vulnerabilities
- Hackers are more economical than employees

What are hackers' perspectives on bug bounties?

Factors that Influence Hackers' Participation

Factors

- Benefits
- Challenges
- Platform Features
- Gig-work

Factors that Influence Hackers' Participation

What are the benefits?

- Get monetary rewards
- Learning opportunities
- Legal safe harbor

Factors that Influence Hackers' Participation

What are the keys to good programs?

- Ease of payment
- Ease of reporting
- Viewing disclosed vulnerabilities

Factors that Influence Hackers' Participation

What are the challenges?

- Poor responsiveness
- Dissatisfaction with responses
- Unclear scope

Factors that Influence Hackers' Participation

What related to Gig-works?

- Flexibility
- Stress and uncertainty

Remaining Question

- Hunter main concerns:
 - Skills Development
 - Communication/Negotiating with Vendors
 - Income Uncertainty

- What is the potential solution?
(Come from the government, industry, or hunters themselves)

Hackers are motivated...Then how to bootstrap their efficiency?

Study Club, Labor Union or Start-Up? Characterizing Teams and Collaboration in the Bug Bounty Ecosystem

Yangheran Piao
University of Edinburgh
Edinburgh, UK
lawrencepiao@ed.ac.uk

Temima Hrle
University of Edinburgh
Edinburgh, UK
temima.hrle@ed.ac.uk

Daniel W. Woods
University of Edinburgh
British University in Dubai
Edinburgh, UK
daniel.woods@ed.ac.uk

Ross Anderson[†]
University of Cambridge
University of Edinburgh
Cambridge, UK

Abstract—A unique bug bounty ecosystem has evolved in China. Platforms allow groups of hackers to register together to receive team-level awards. However, little is known about the prevalence and productivity of these teams, or how team members collaborate. To address this gap, we conducted a mixed-methods study.

The first stage characterized teams from a top-down ecosystem perspective. We collected bug bounty rankings from 85 platforms, using fuzzy-matching to identify 2.1k unique teams and 5.9k hunters. We show that 46% of users are registered as part of a team, and hunters with teams are more

that BBPs are an efficient security investment [8], [32], [34], [50], [55], [60], which helps explain why Google paid out \$10 million in bug bounties in 2023 [42].

Despite the success of BBPs, communications between vendors and hunters is challenging. Vendors complain about low quality bug submissions [25], meanwhile hunters complain about slow and non-transparent decisions [1]. Another problem is the lack of established development pathways, which is especially problematic for young hackers [12] and those from diverse backgrounds [10]. Put simply, solo hunters lack market power and development opportunities.

- Piao, Y., Hrle, T., Woods, D. and Anderson, R., 2024, November. Study Club, Labor Union or Start-Up? Characterizing Teams and Collaboration in the Bug Bounty Ecosystem. In 2025 IEEE Symposium on Security and Privacy (SP).

Hacker Collaboration

- Teamwork is common in cybersecurity
- Bugcrowd allows hunters to share bounties

You

 **parker**
 India

100 %

Add collaborator

I have followed the **program brief** and agree to **Bugcrowd's terms & conditions**



**BUGCROWD RESEARCHER
COLLABORATION:
REWARD SPLITTING &
JOINT SUBMISSIONS**

Now available in Crowdcontrol!



Hacker Collaboration

- A unique teaming ecosystem has evolved in China

Ranking	Team Name	Number of members	Team website	Reward Points
1	ChaMd5.Org	15	http://www.chamd5.org	6054
2	网络安全...	14	https://www.1aq.com	2960
3	URSec	8	https://www.ur-sec.com/	2811
4	TopMan-5	15		2083
5	Day1安全团...	15	http://team.day1.today/	1523
6	Ctrl+C安全...	20		1271
7	火眼人安全...	15		1103
8	渗透空间Ov...	16	https://overspace.cn	827
9	0000	21		672
10	零云安全团队	11		581

Ranking	Team Name	Captain	Number of members	Number of bugs	Points this quarter
1	Power Constr...	Brookok	1	6	3010
2	T9Sec	En0rs	12	16	3023
3	professional r...	Snow, It's me.	6	166	2409
4	reemployem...	Open Eco_n1dellw	15	113	2161
5	Day1 Safety T...	Pond Fish I	15	89	2010
6	China Water...	ylidun	10	24	1900
7	TI Safe	tl_dlx	9	15	1900
8	POI	system_gov	14	1	1000
9	WggsSec Wolf...	Lanbal	15	9	830
10	OverSpace	One_1	13	0	804



ChaMd5.Org
We crack for free

6054 **83436** **1** **9308** **70%**
Season points Total Team Points Ranking No. of bugs Report reception rate

[Official website](#) [apply for joining the league](#)

Member Name	Title	Individual Contribution Points	Time of addition
Anonymous(Captain)	crowd of onlookers	16346	2016-03-08
cairiao1232123	crowd of onlookers	6789	2021-01-13
Anonymous	crowd of onlookers	17845	2019-03-30
mingjie	crowd of onlookers	2242	2016-12-14

T9Sec Application for membership

Founder: En0rs

Team Home Page: T9Sec We Wechat Official Account

Overhead: 5%

Team Introduction: nah

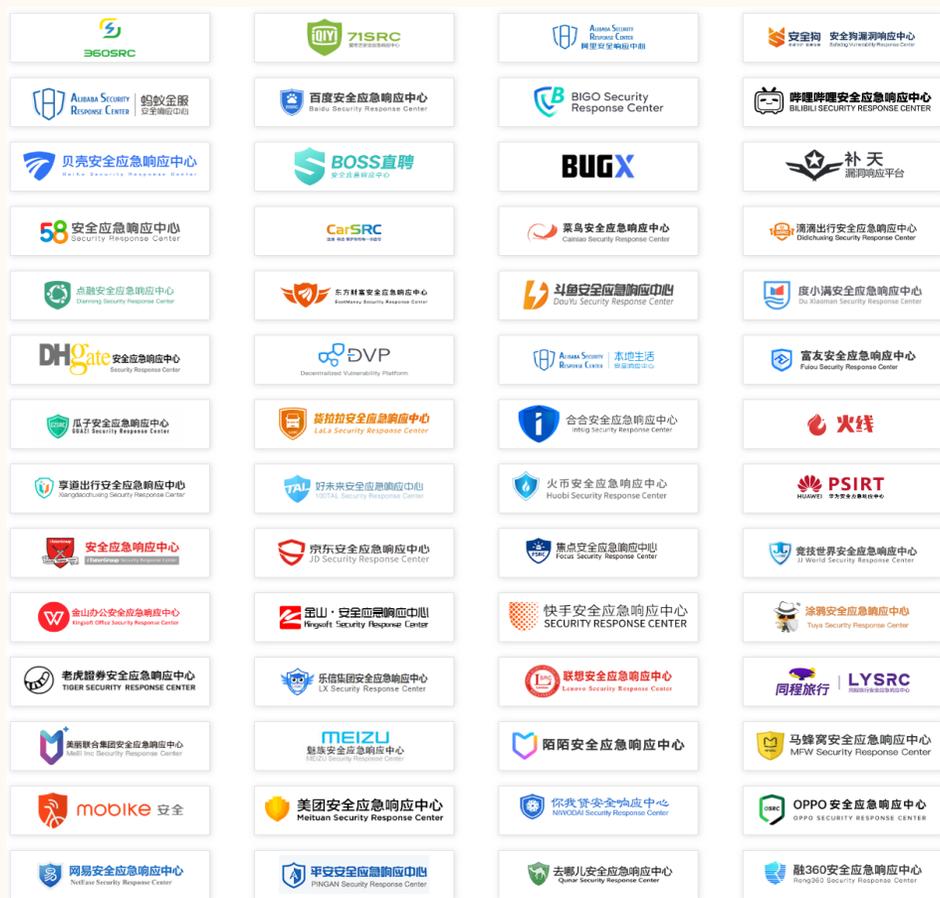
12 Seventeen. 3343
Number of me. Number of vul. Points of the s...

Member Name	Rank	Title	Ranking	Contribution points of this quarter	Time of addition
En0rs	27	Elite White Hat	35	3520	2019-04-03 12:42:08
Broken_T	27	Security Specialist	6	900	2019-07-29 21:13:58
I'm killer	27	Security Specialist	8	300	2019-08-26 19:01:03
dlx	27	Elite White Hat	38	0	2020-12-24 03:54:57
GeDKing	27	Security Specialist	10	230	2020-08-01 08:18:41
Black Wolf	27	Elite White Hat	39	0	2020-06-02 18:17:49
Hua Mulan	27	Elite White Hat	32	0	2020-10-28 10:32:20
Aura00000000	27	Elite White Hat	24	0	2020-10-25 10:44:14
casidy	27	Elite White Hat	34	0	2021-09-25 23:09:20
Atom	39	Premium White Hat	181	0	2021-12-08 17:04:04
_Jide	17	Premium White Hat	196	405	2022-02-17 19:06:44
Custom urgent	21	Premium White Hat	108	0	2022-09-18 14:28:46

Research Questions

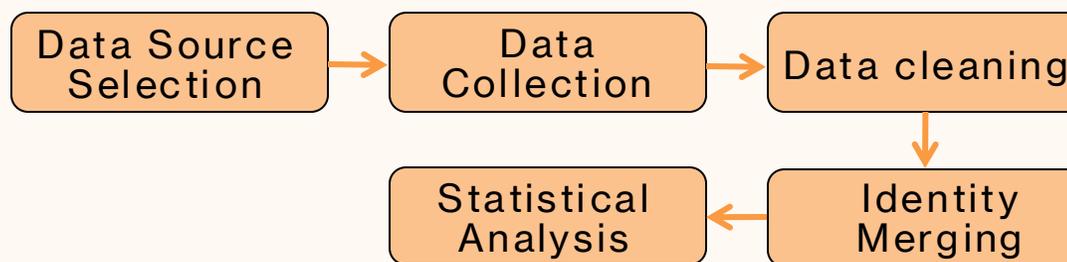
- How are teams, hunters and rewards distributed over BBPs?
- What are the functions of bug hunter teams?
- Why do bug hunters join and leave teams?

Phase I: BBP Measurement

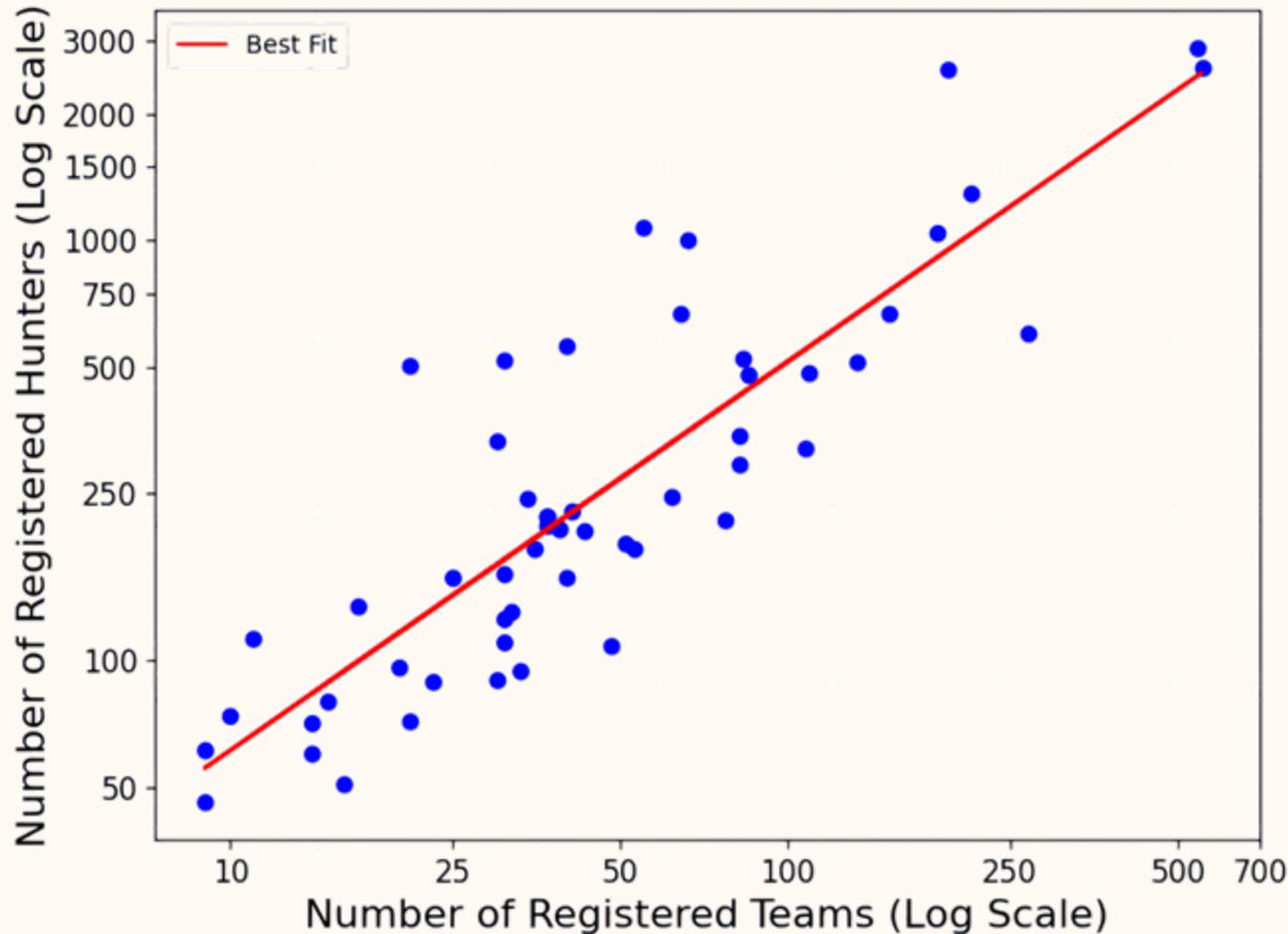


Quantitative Study

- Collect data from BBPs with teaming mechanism
- n= 85 BBPs & 5.9k hunters

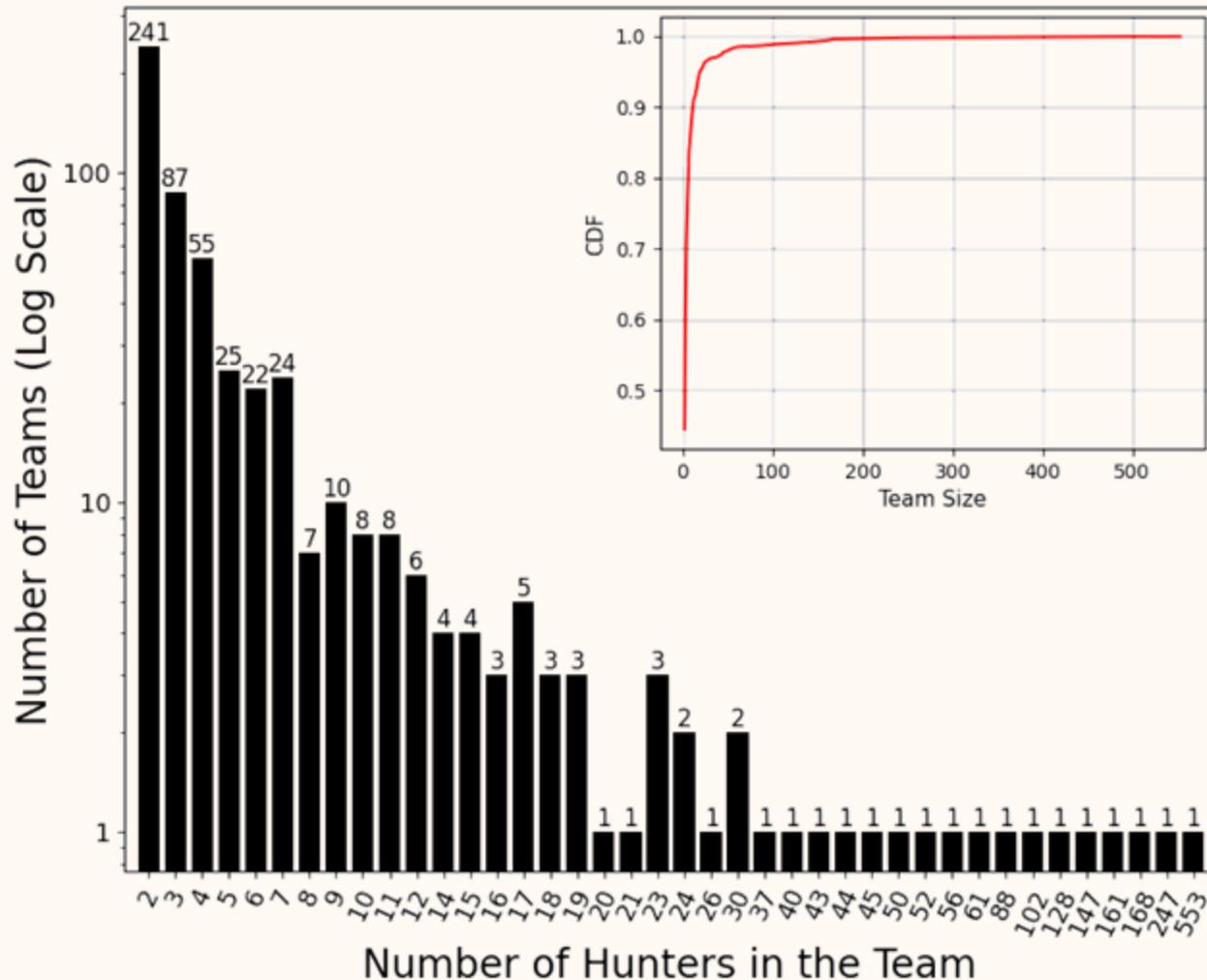


RQ1: Hunter Teaming Ecosystem

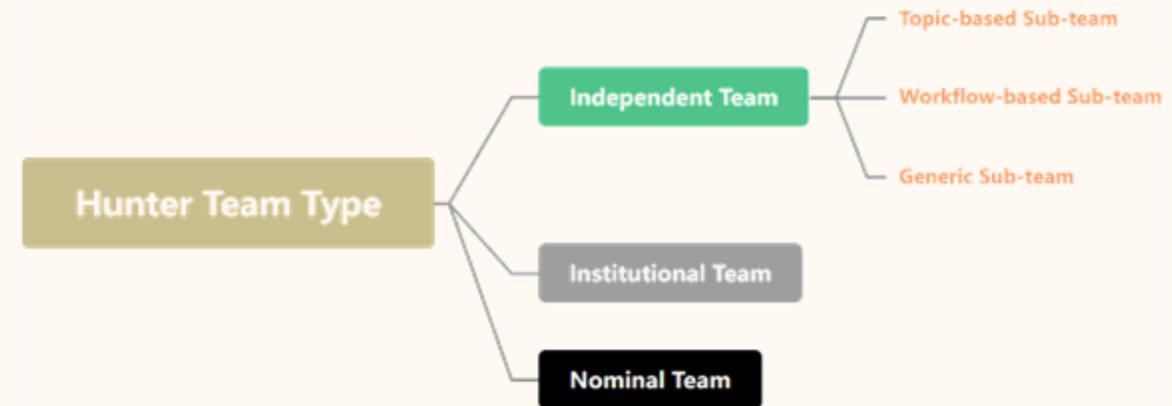


- 46% of users are part of a team
- The three largest BBPs have over 2.5k registered users

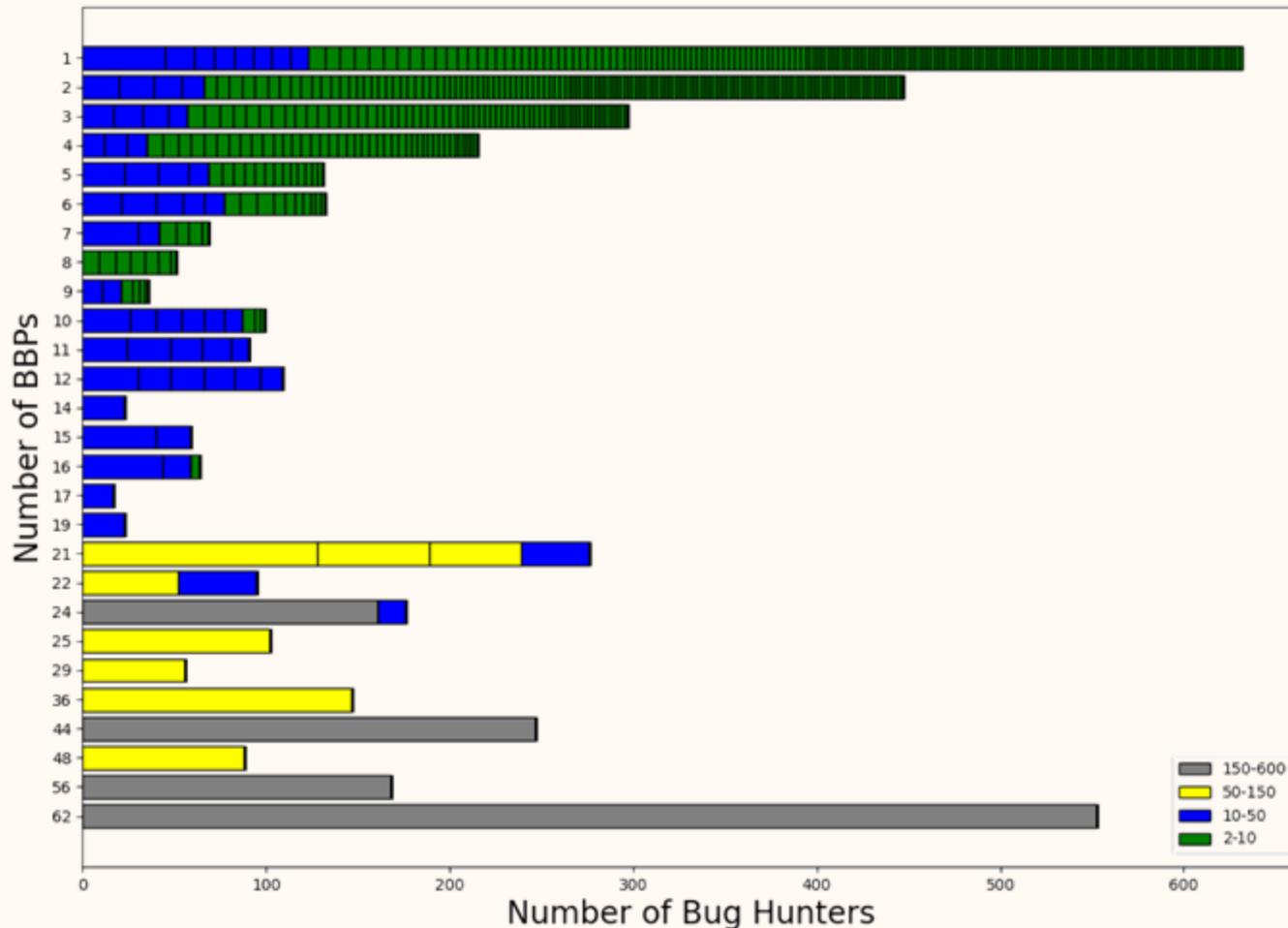
Prevalence of Users, Teams and BBPs (RQ1)



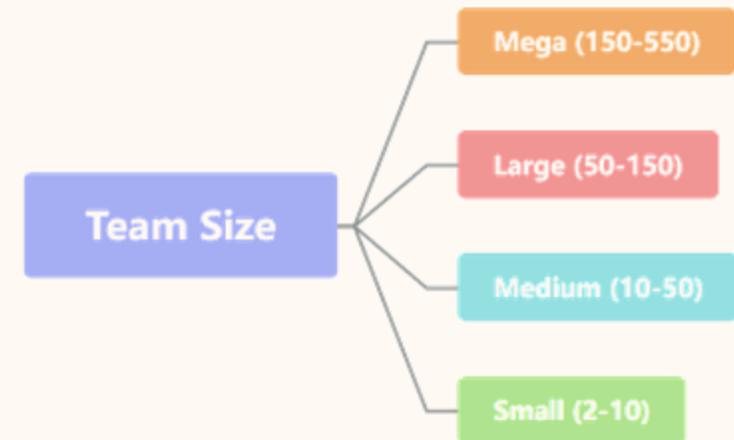
- 87% teams have less than 10 members



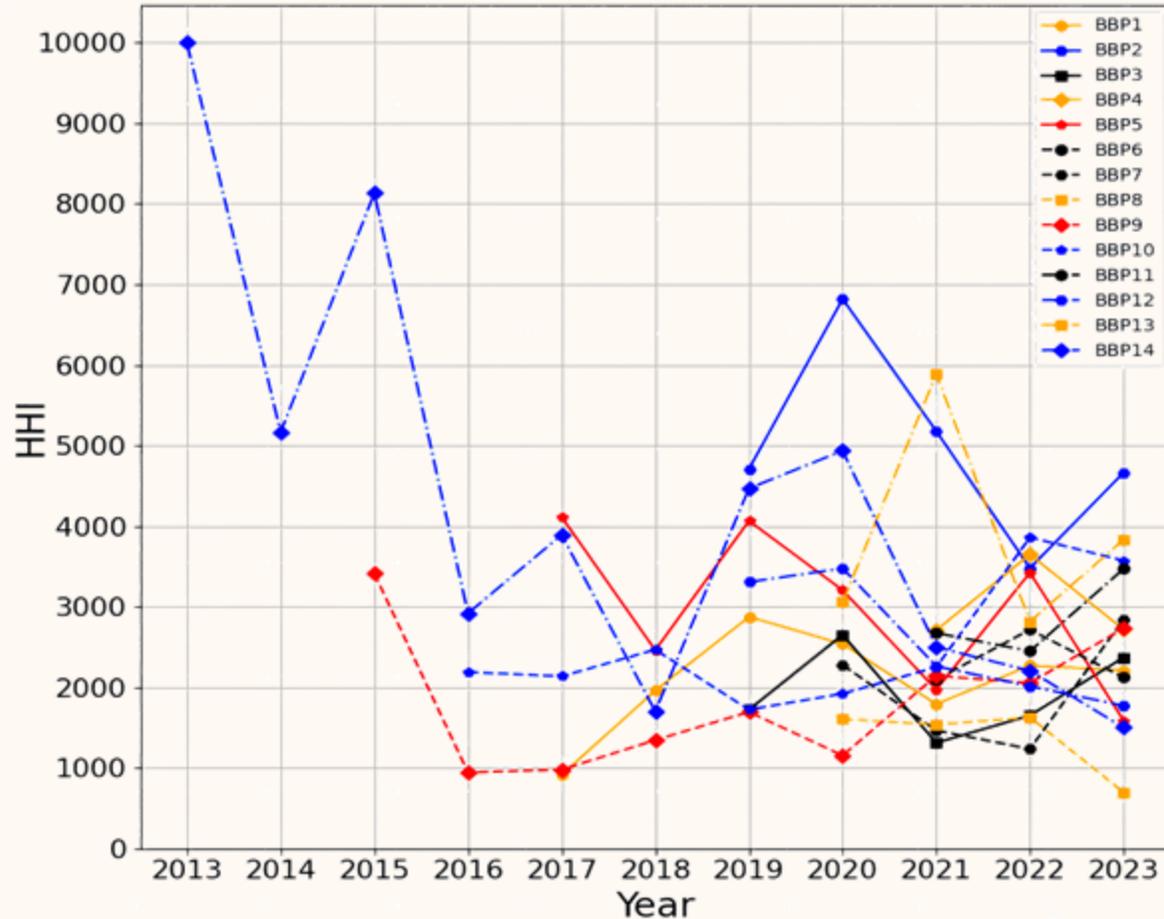
Prevalence of Users, Teams and BBPs (RQ1)



- The largest team has 553 members and on 62 BBPs
- 39% of small teams participate in just one BBP



Team Productivity (RQ1)



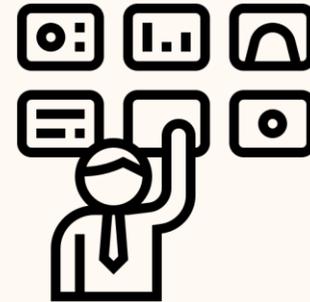
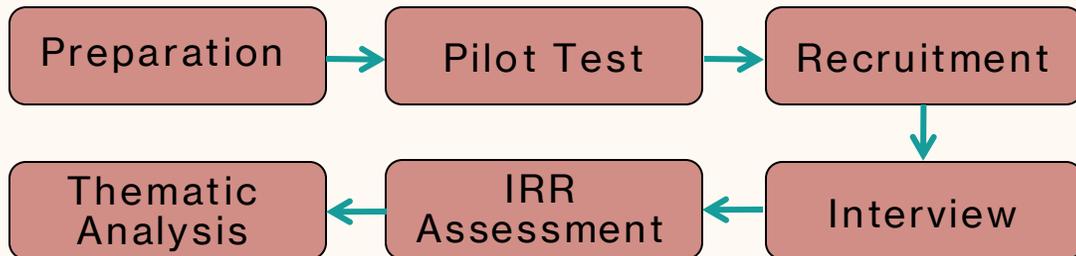
- Team members are more than twice (2.47) as productive as solo hunters
- There is a high level of market concentration

$$HHI_n = \sum_{i=1}^N x_i^2$$

Phase II: Interview

Qualitative Study

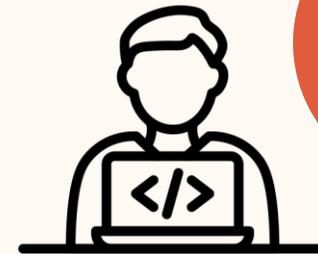
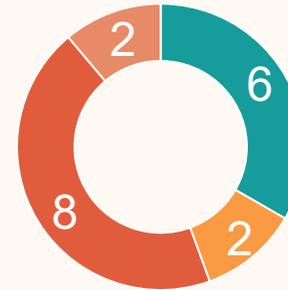
- Investigate hackers' perspectives on bug bounty teams
- n=18 hunters



Non-Security Industry



Students

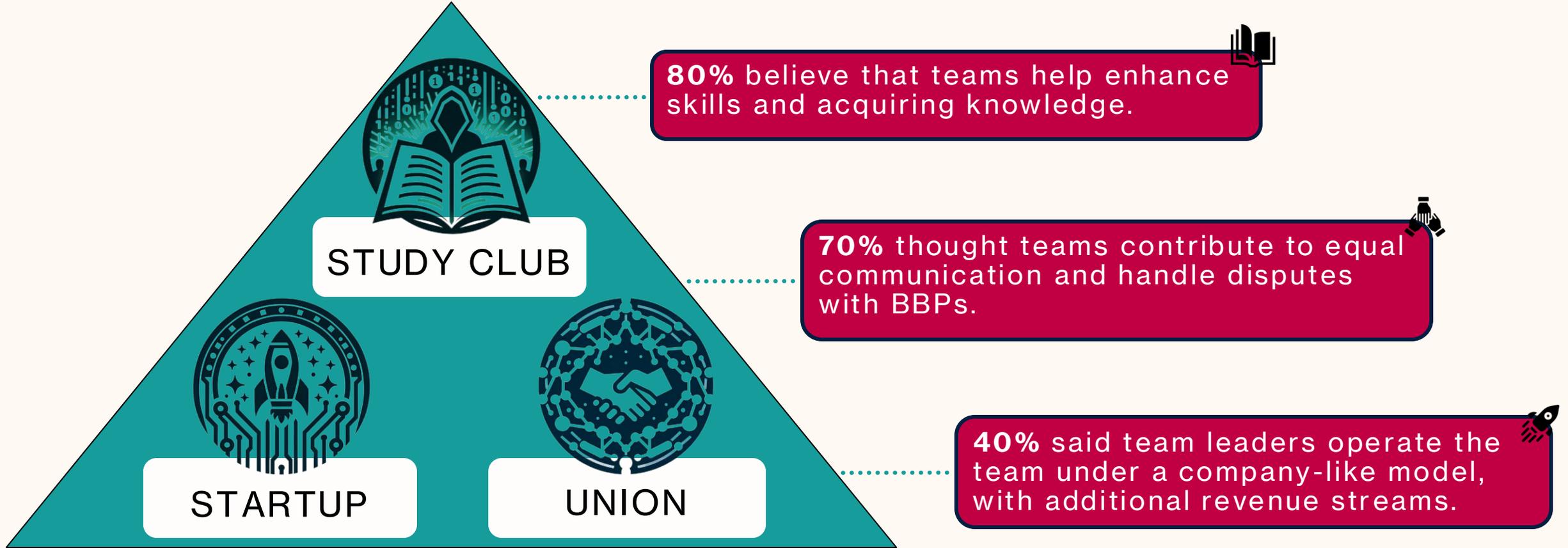


Security Industry



Full-time Bug Hunters

RQ2: Multifaceted Functions of Team



RQ3: Reasons for Joining & Leaving

• Motivations

- Learning and Growth
- Revenue Sharing
- Team Prestige



• Issues and Challenges

- Lack of activity
- Interpersonal conflicts
- Lack of time



Key Insights

- **Teams are central to the Chinese bug bounty ecosystem**
 - Almost half of hunters are team members
 - Team members have over twice the productivity of solo ones
 - The largest team participates in 73% of BBPs

Key Insights

- **Functions of hunter teams could solve concerns**

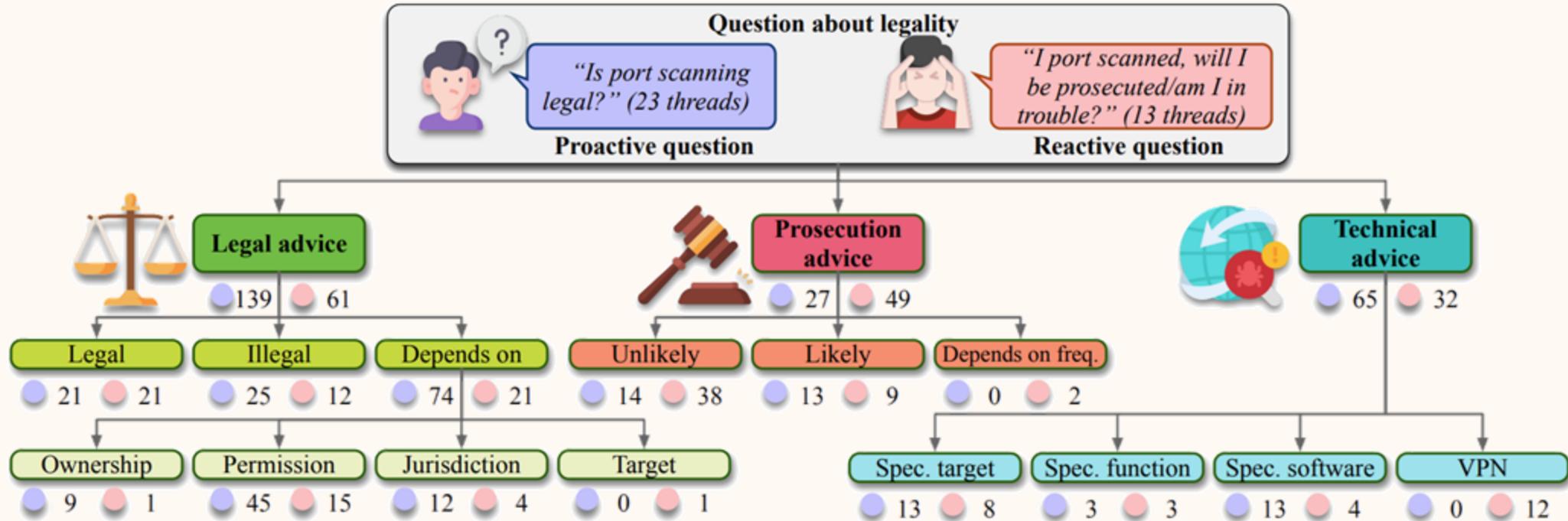
 Maintaining educational resources (*Skills development*)

 Earning more revenue like additional bounties (*Income Uncertainty*)

 Establish equal communication channels with BBPs (*Negotiation*)

Negative impacts and legal implications on security-sensitive users

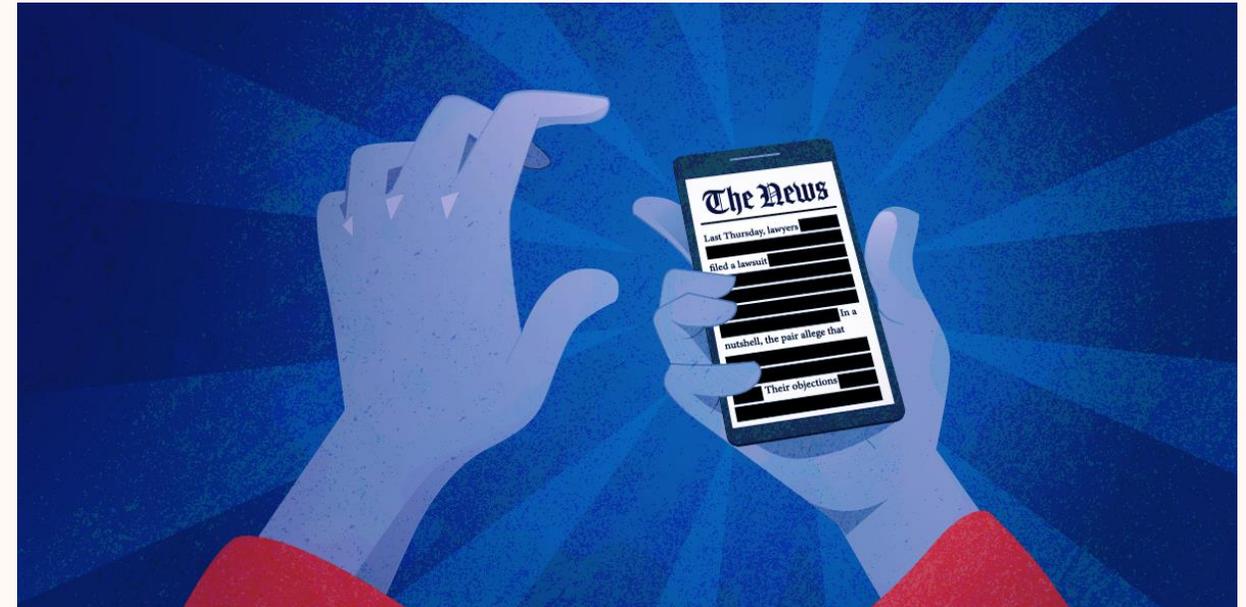
Legal Concerns on Port Scanning



- Hrle, T., Milad, M., Li, J., & Woods, D. "Just a tool, until you stab someone with it": Exploring Reddit Users' Questions and Advice on the Legality of Port Scans. In 2024 European Symposium on Usable Security (EuroUSEC 24) (pp. 322-336).

Journalist

- High domain requirements for privacy and safety but lack of technical expertise
 - Focusing on source rather than sensitivity of information
 - Relying on third-party techniques
- Facing threats against highly capable adversaries



How do we do research with these security-sensitive users?

Take-home

- Akgul, O., Eghtesad, T., Elazari, A, et al. [Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem.](#) In *32nd USENIX Security Symposium (USENIX Security 23)* (pp. 2275-2291).
- Fulton, K.R., Katcher, S., Song, K., et al. [Vulnerability discovery for all: Experiences of marginalization in vulnerability discovery.](#) In *2023 IEEE Symposium on Security and Privacy (SP)* (pp. 1997-2014).
- The Record Media – ['UK Home Office's new vulnerability reporting mechanism leaves researchers open to prosecution'](#)