MIT MANAGEMENT SLOAN SCHOOL

INTERDISCIPLINARY CONSORTIUM for IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (IC)³

Diversity or Concentration? Hackers' Strategy for Working Across Multiple Bug Bounty Programs

Keman Huang
Michael Siegel
Stuart Madnick
Xiaohong Li
Zhiyong Feng

Working Paper CISL# 2016-23

December 2016

Cybersecurity Interdisciplinary Systems Laboratory (CISL)
Sloan School of Management, Room E62-422
Massachusetts Institute of Technology
Cambridge, MA 02142

Diversity or Concentration?
Hackers' Strategy for Working Across Multiple Bug Bounty Programs

Keman Huang[1,2,3], Michael Siegel[3], Stuart Madnick[3,4], Xiaohong Li[1,2], Zhiyong Feng[1,2]
[1]Tianjin Key Laboratory of Cognitive Computing and Application, Tianjin 300072, China
[2]School of Computer Science and Technology, Tianjin University, Tianjin 300072, China
[3] MIT Sloan School of Management, Cambridge, MA, USA
[4]MIT School of Engineering, Cambridge, MA, USA
keman.huang@tju.edu.cn, msiegel@mit.edu, smadnick@mit.edu, xiaohongli@tju.edu.cn, zyfeng@tju.edu.cn

***Abstract*— Bug bounty programs have been proved effective in attracting external hackers to find and disclose potential flaws in a responsible way. There are many different bug bounty programs, so how do hackers balance diversity and concentration to effectively build their reputation in the vulnerability discovery ecosystem? In this paper, we present a novel methodology to understand how hackers spread their attention and earn bounties across different programs. The empirical result shows the relationship between diversity and concentration and suggests an effective strategy for hackers to work across multiple bug bounty programs.**

Keywords- Bug Bounty Program, Vulnerability Discovery Ecosystem, Diversity or Concentration Strategy

I. Introduction

Due to the "*double-edged sword*" characteristic [1], [2] vulnerability disclosure has both positive and negative effects for the community. Responsible vulnerability disclosure policy has been developed as an effective way to improve overall security [3]. Considering the effectiveness of using external experts for responsible vulnerability discovery [4], bug bounty programs have been launched by many companies including *Google, Facebook, Microsoft and Mozilla* etc. to encourage the external hackers to share their discovered vulnerabilities before publicly disclosure. Consequently, some third-party bug bounty platforms such as HackerOne, BugCrowd, Wooyun, Vulbox etc are further built to host bug bounty programs and attract hackers to locate potential vulnerabilities for different companies. Therefore, we can observe a continuously growing discovery ecosystem, providing significant contributions to companies in different sectors [5].

There are many different bug bounty programs in the ecosystem and vulnerability discovery is a non-trivial and extremely time consuming task, so *how do hackers spread their limited energy across multiple programs to build their reputations and increase their bounties*? Obviously, working in many programs can help the hackers to discover more potential vulnerabilities. However, due to the increasing complexity of the systems, it becomes more and more difficult to find more potential flaws in a given program. Additionally, only the one who first discovers the vulnerability will gain the bounty. This means that a hacker needs to *balance between diversity and concentration during the vulnerability discovery: whether to work across many different programs or just focus on few programs.*

In this paper, we develop a methodology to understand *how hackers spread their attentions across different bug bounty programs and how they gain their bounties*. Based on the data collected from HackerOne, our empirical results show the different strategies for hackers with different reputation levels in the ecosystem. This opens a gateway for us to further study the hackers' incentive and behaviors in the bug bounty programs.

II. Methodology

Generally speaking, in the vulnerability discovery ecosystem, each hacker will select a program and then devote time to work on vulnerability discovery in these programs. If a vulnerability is discovered, he/she will submit a report to program and the program will work with him/her to determine if the vulnerability is valid and first the first disclosure. Finally, the hacker can gain a bounty if the discovery meets the requirements of the program. By making more valid submissions and gaining bounties, the hackers also build their reputation in the ecosystem[1].

As the goal of this paper is to understand how hackers work across different programs. For a hacker h_i who participates in more than 1 program, we get all his/her valid submissions and then sort his/her programs based on the submission number:

$$a(h_i) =< s_{p_{i1}}, s_{p_{i2}} \dots, s_{p_{in}} > \; , \; |s_{p_{i1}}| \; \geq \; |s_{p_{i1}}| \dots \; \geq \; |s_{p_{in}}| \quad (1)$$

Here $|s_{p_{ij}}|$ refers to the number of valid reports h_i submits to the jth program.

Therefore, we can get the distribution representing how each hacker spread his/her attention to different programs:

$$pa(h_i) =< sr_{p_{i1}}, sr_{p_{i2}} \dots, sr_{p_{in}} > \quad (2)$$

$$sr_{i,k} = \frac{|s_{p_{ik}}|}{\sum_{j=1}^{n} |s_{p_{ij}}|} \quad (3)$$

Then, the average attention rate aar_j is generated to evaluate how hackers in the ecosystem spread their attentions to their j priority programs:

$$aar_j = \frac{1}{N} \sum_{i=1}^{N} sr_{i,j} \quad (4)$$

[1] In many cases, building a reputation (such as for future employment) may be as important as the amount of bounty collected.

Here N refers to the number of hackers participating into more than 1 program.

Finally, we can calculate the entropy index [6] to evaluate the concentration of each hackers' programs:

$$EI_{ar}(h_i) = -\sum_{i=1}^{n} sr_{i,j} log_{10}(sr_{i,j}) \tag{5}$$

Similarly, we can calculate the average reward rate arr_k and the entropy-based concentration rate $EI_{rr}(h_i)$ to represent how hackers gain bounties from their priority programs:

$$arr_k = \frac{1}{M}\sum_{i=1}^{M} rr_{i,k} \tag{6}$$

$$EI_{rr}(h_i) = -\sum_{i=1}^{n} rr_{i,j} log_{10}(rr_{i,j}) \tag{7}$$

$$rr_{i,k} = \frac{| r_{p_{ik}} |}{\sum_{j=1}^{n} | r_{p_{ij}} |} \tag{8}$$

Here M refers to the number of hackers who gain bounties from more than 1 program. $| r_{p_{ik}} |$ refers to the number of rewarded submissions hacker h_i gain from his/her *k*th top program.

III. Dataset and Result

A. Data Set

HackerOne is a well-known US bug bounty platform which hosts many different programs (132 public programs, as of April 1, 2016) offered by different companies including *Yahoo!*, *Twitter*, *Adobe*, *Uber*, etc. Data was collected from November 29, 2013 to October 28, 2015 on the 567 hackers who participated in more than 1 program for attention concentration analysis and the 214 hackers who gained rewards from at least 2 programs for reward concentration analysis. Detail about the dataset is in the support material.

B. Empirical Result

Due to the space limitation, the figures are presented as support material. Based on the data we collected from HackerOne, we can observe the well-known power-law distributions [7] both for the average attention rate and the average reward rate. This means that *overall, hackers in the ecosystem pay most of their attentions to the prioritized programs and gain most of their earnings from them*. Actually, it can be seen that 90.47% of submissions are from the first 3 priority programs for these hackers. The first 3 prioritized programs contribute 95.68% bounties for hackers and only 0.77% are from the programs with a priority less than 5. Additionally, the gap between the average attention rate and the average reward rate is increasing with the reduction in priority, which reveals that reports submitted to the less priority programs gain negligible reward.

Furthermore, in order to compare the different strategies for hackers with different levels, we separate the hackers into 10 groups based on their effectiveness, which we will refer to as reputation. For each group, we calculate their average entropy index for both the attention rate and the reward rate. From Figure 2, we can obverse a significant transform between the diversity and concentration for hackers: for the hackers with low reputations, they submit to different programs and get a relatively higher diversity. However, this distraction limits their ability to discover important and valuable vulnerabilities and build reputation; The ones with medium reputations, focus on their priority programs; The top hackers have a higher diversity than the overall ecosystem which means that they spread their vulnerability discovery ability to more programs. Therefore, *for the hackers, it is a reasonable strategy to focus on few programs to gain professional recognition and then diversify to different programs to build up ones reputation in the community*.

IV. Discussion and Conclusion

Bug bounty programs have been launched by many companies, attracting external hackers to discover potential vulnerabilities through responsive disclosure. It is important for hackers to balance between diversity and concentration. Our empirical study shows that most hackers concentrate on few programs, empirically less than 5, and earn most of their bounties from these programs. Additionally, the entropy-based concentration reveals the strategy between concentration and diversity: it is a good choice for hackers to initially focus on few programs and then diversify to multi-programs to build reputation in the community.

This preliminary result opens a gateway for us to further dig deeper to understand the hackers' behavior and investigate the vulnerability discovery ecosystem.

Acknowledgment

This work is supported by the National Natural Science Foundation of China grant 61502333 and the MIT (IC)^3 project. Zhiyong Feng is the corresponding author.

References

[1] D. E. Denning, "Toward more secure software," Commun. ACM, vol. 58, no. 4, pp. 24–26, 2015.

[2] C. Sabottke, O. Suciu, and T. Dumitraș, "Vulnerability Disclosure in the Age of Social Media : Exploiting Twitter for Predicting Real-World Exploits," Proc. 24th USENIX Secur. Symp., 2015.

[3] H. Cavusoglu, H. Cavusoglu, and S. Raghunathan, "Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge," IEEE Trans. Softw. Eng., vol. 33, no. 3, pp. 171–185, 2007.

[4] M. Finifter, D. Akhawe, and D. Wagner, "An Empirical Study of Vulnerability Rewards Programs.," in USENIX Security, 2013, vol. 13.

[5] M. Zhao, J. Grossklags, and P. Liu, "An Empirical Study of Web Vulnerability Discovery Ecosystems," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015, pp. 1105–1117.

[6] P. J. Alexander, "Entropy and Popular Culture: Product Diversity in the Popular Music Recording Industry," Am. Sociol. Rev., vol. 61, no. 1, p. 171, 1996.

[7] K. Huang, Z. Feng, J. Li, and X. Li, "System thinking of the Software Vulnerability Market via Complex Network Theory," in IEEE Symposium on Security and Privacy 2015, 2015.

Support Material

A. *Data Set*

Table I reports the basic statistic of our dataset. "*Attention*" refers to dataset in which only hackers who submit valid reports to at least 2 programs are included. "*Reward*" refers to the dataset containing only hackers who gain bounty from at least 2 programs.

TABLE I. BASIC STATISTIC OF DATASET

	Attention	***Reward***
#Hackers	567	214
#Programs	98	48
Maximum #Programs per Hacker	44	15
#Valid Submissions	7,095	/
#Rewarded Bounty	/	$678,504.25

B. *Empirical Result*

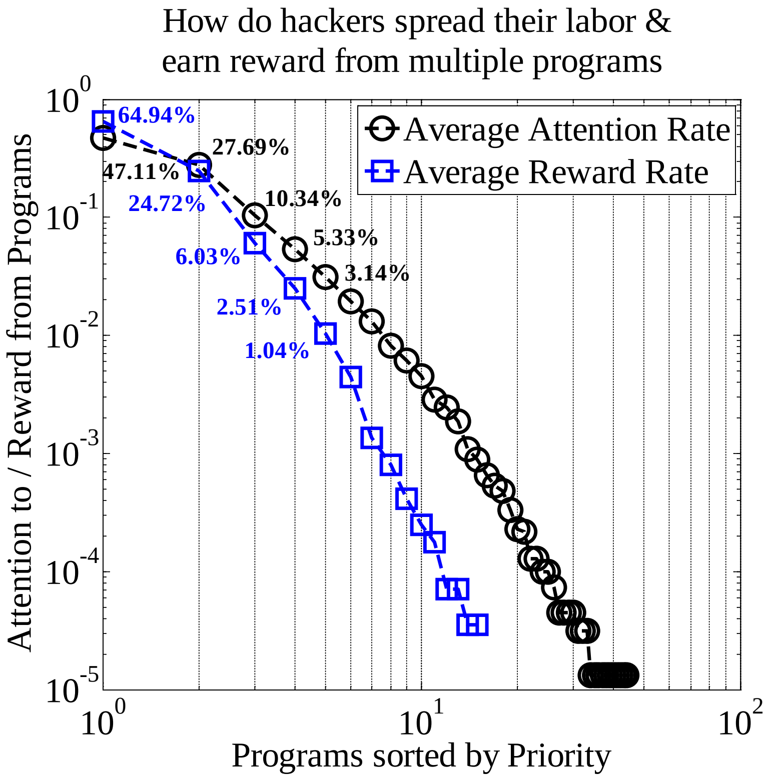
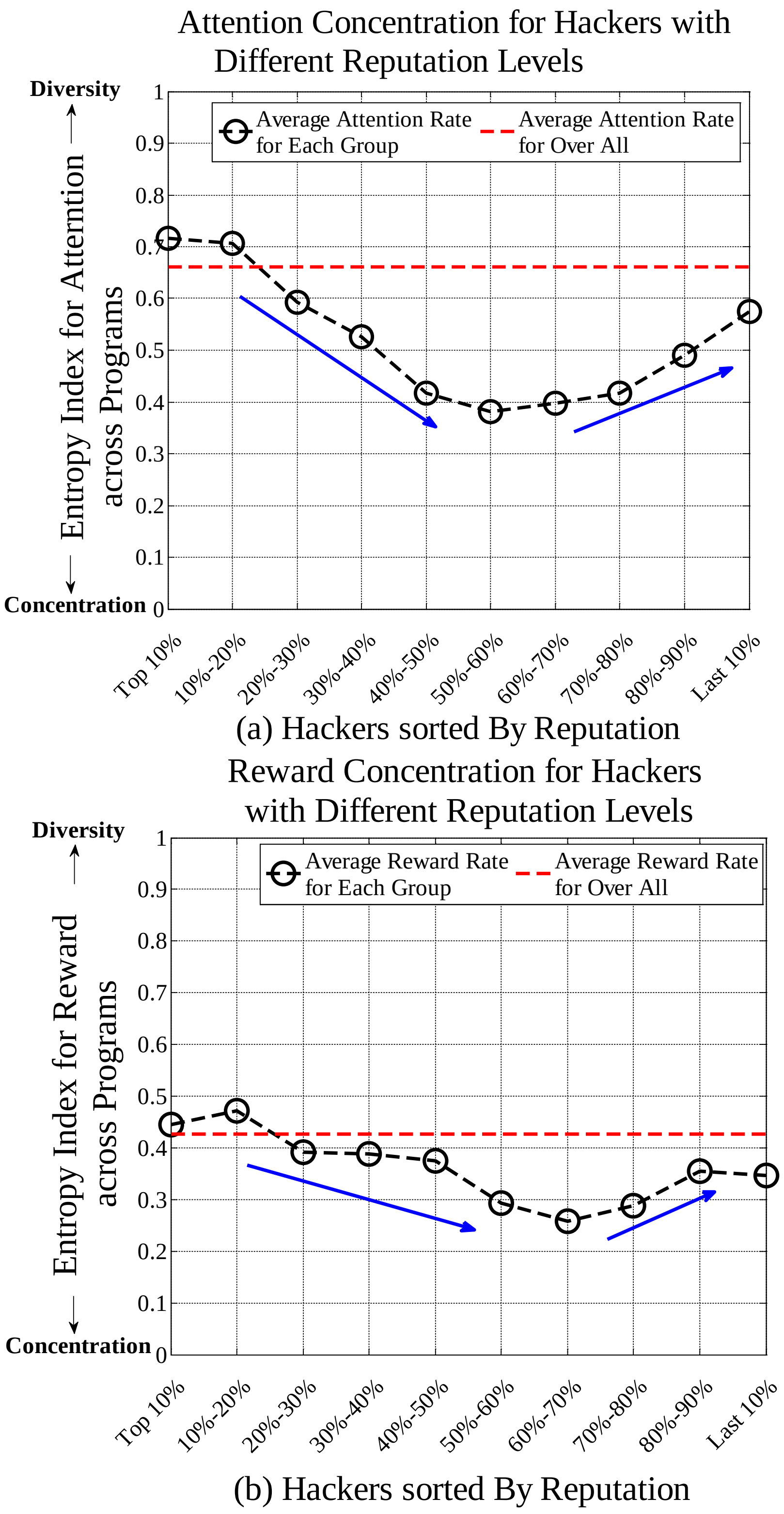


Figure 1. Average Attention Rate and Average Reward Rate for Hackers across Different Programs.



Attention Concentration for Hackers with Different Reputation Levels

(a) Hackers sorted By Reputation

Reward Concentration for Hackers with Different Reputation Levels

(b) Hackers sorted By Reputation

Figure 2. Average Attention Rate and Average Reward Rate for Hackers across Different Programs.