



Bug Bounty Marketplaces and Enabling Responsible Vulnerability Disclosure: An Empirical Analysis

Hemang Chamakuzhi Subramanian, Florida International University, Miami, USA

 <https://orcid.org/0000-0002-5095-7607>

Suresh Malladi, Cybersecurity Researcher & Consultant, Fayetteville, USA

 <https://orcid.org/0000-0003-2184-2058>

ABSTRACT

Cybercrime caused by exploited vulnerabilities bears a huge burden on societies. Most of these vulnerabilities are detectable, and the damage is preventable if software vendors and firms that deploy such software adopt right practices. Bug Bounty Programs (BBPs) by vendors and intermediaries are one of the most important creations in recent years, that helps software vendors to create marketplaces and to detect and prevent such exploits. This article develops the theory of BBPs and present a typology of BBPs using established theories of incentive compatibility and mechanism design. The authors empirically analyze the market creation function of BBPs using granular data from two different types of BBPs on a popular intermediary platform. The research findings suggest that BBPs are valuable opportunities to source vulnerabilities in software; nevertheless, the rate of disclosure and hacker participation marginally increases with vendor's rewards and other incentives. Similarly, the results show that security researchers are motivated to contribute to BBPs that offer higher remuneration and not just those programs with a higher likelihood for bug discovery. Our findings will help researchers and practitioners in information security and allied domains to develop a theoretical and empirical perspective of BBPs, and their usefulness to curb incidents of cybercrime.

KEYWORDS

Bug Bounty Programs, Equilibrium, Marketplaces, Multi-Homing, Software Vendors, Supply/Demand, Vulnerabilities, Zero Day Vulnerabilities

INTRODUCTION

Staggering annual cybercrime costs of nearly \$600 billion (Gilles, 2014), and ongoing incidents such as 2019 breach at Capital One which affected 100 million users will constantly prompt questions on how to prevent cyberattacks¹. At the heart of addressing such concerns is the ability to tackle a unique class of software security vulnerabilities categorized as Zero-day Vulnerabilities (ZDV), often traced to be root cause behind security attacks (McKinney, 2007; Miller, 2007). ZDVs refer to vulnerabilities that remain unknown to vendors and can be exploited by hackers before they are fixed (Radianti, Rich, & Gonzalez, 2009). Lucrative black markets where ZDVs are traded as information goods for downstream exploitation often necessitate that vendors should discover and fix vulnerabilities before an impending attack.

DOI: 10.4018/JDM.2020010103

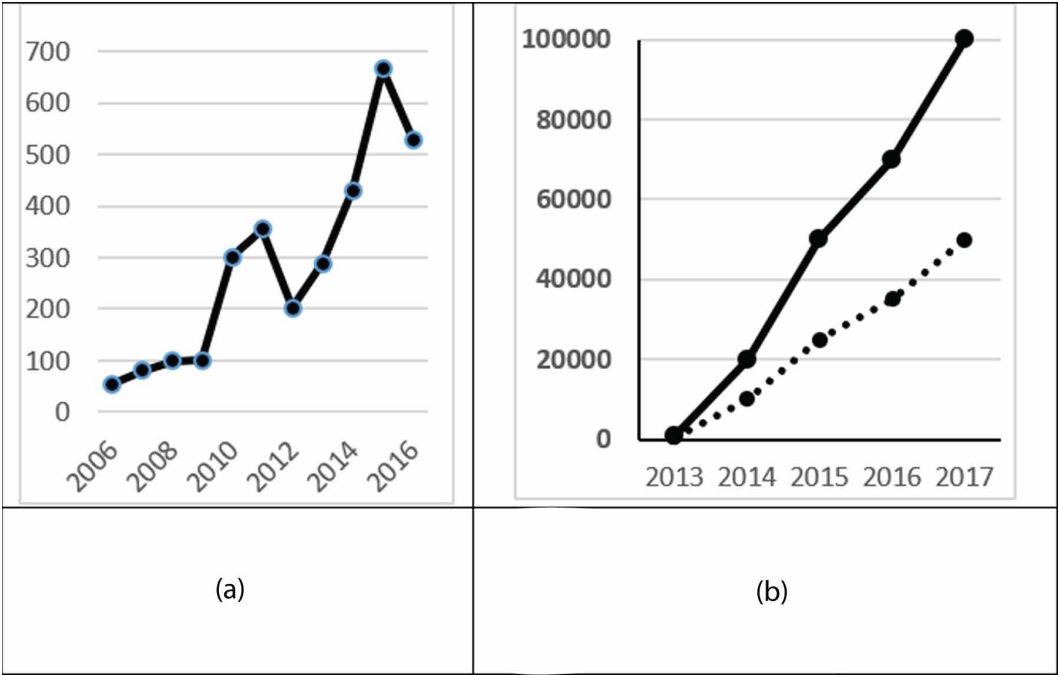
Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

Given such a possibility of harm, vulnerabilities create a “race for access” amongst three actors i.e., buyers, black hat sellers and white hat sellers². Buyers are either legitimate entities (e.g. software vendors, etc.) or illegal actors (e.g. hackers, black-market brokers, etc.), each with different motives and incentives. Black hats either discover and exploit vulnerabilities or sell them in black markets where these vulnerabilities are used to create exploits, resold downstream or used to blackmail vendors (Denning, 2015). White hats discover and responsibly disclose vulnerabilities to vendors or legitimate intermediaries to earn compensation and to increase their reputation in the security community. Timely actions by white hats can deter misuse by black hats. However, in the absence of disclosure channels, white hats face a dilemma and cannot responsibly report discoveries to vendors. As a result, vendors must initiate mechanisms to collaborate with white hats to notice and fix vulnerabilities before exploitation.

Within this context, Bug Bounty Programs (BBP) are recognized as a legitimate channel for responsible disclosure among white hats, vendors, and intermediaries (Malladi & Subramanian, 2019). BBPs are entering the mainstream cybersecurity toolkits in organizations such as Microsoft, Google, Apple and Tesla. There are more than 300 active BBPs rewarding researchers between \$100-\$2,50,000 per vulnerability, demonstrating that BBPs are a cost- and time-effective solution to crowdsource vulnerability discovery (Ring, 2014). As seen from Figure 1(a), TippingPoint - a private intermediary received 100 disclosures in 2006 which subsequently increased to 700 disclosures in 2015³. Similarly, Figure 1(b) shows data from Bugcrowd platform that 1000 vulnerabilities that were reported in 2013 increased to 100000 disclosures in 2017. Table 1 shows the reward price ranges offered for vulnerabilities by BBP operators.

Table 2 depicts the representative categories of vulnerabilities that were compensated by four of the leading BBPs⁵. Several of these categories have resulted in massive cyberattacks (Laszka, Zhao, Malbari, & Grossklags, 2018). For example, a criminal cartel stole confidential data from nearly 420,000 websites using SQL injections amassing 1.2 billion ID credentials⁶.

Figure 1. (a) Tipping Point platform's growth in rate of disclosures; (b) Bugcrowd's growth in disclosures⁴. Dotted line depicts accepted disclosures; straight line depicts total disclosures.



24 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/bug-bounty-marketplaces-and-enabling-responsible-vulnerability-disclosure/245299

Related Content

Disclosure Control of Confidential Data by Applying Pac Learning Theory

Ling He, Haldun Aytugand Gary J. Koehler (2012). *Cross-Disciplinary Models and Applications of Database Management: Advancing Approaches* (pp. 438-450).

www.irma-international.org/chapter/disclosure-control-confidential-data-applying/63677

Temporal Object Modeling: Diagramming Conventions and Design Considerations

Richard Vidgen (1997). *Journal of Database Management* (pp. 14-24).

www.irma-international.org/article/temporal-object-modeling/51173

Object-Process Methodology Applied to Modeling Credit Card Transactions

Dov Dori (2001). *Journal of Database Management* (pp. 4-14).

www.irma-international.org/article/object-process-methodology-applied-modeling/3257

SeaDataNet: Towards a Pan-European Infrastructure for Marine and Ocean Data Management

Dick Schaap (2017). *Oceanographic and Marine Cross-Domain Data Management for Sustainable Development* (pp. 155-177).

www.irma-international.org/chapter/seadatanet/166840

FOOM - Functional and Object-Oriented Analysis and Design of Information Systems: An Integrated Methodology

Peretz Shovaland Judith Kabeli (2001). *Journal of Database Management* (pp. 15-25).

www.irma-international.org/article/foom-functional-object-oriented-analysis/3258