Selected Papers of #AoIR2024:
The 25th Annual Conference of the
Association of Internet Researchers
Sheffield, UK / 30 Oct - 2 Nov 2024

READY TO HACK: HOW BUG BOUNTY PLATFORMS CREATE THEIR WORKFORCE

Luca Perrig
University of St.Gallen

The industry

Our increasingly digitized economy has seen a recent surge in cyberattacks. Most notable a wave of ransomware attacks has targeted organizations of all sizes, and studies estimate the number of attacks is ranging in the hundreds of millions per year worldwide.[1] Governments are getting increasingly worried about the vulnerability of a networked industry and are actively seeking remedies to secure the economy.

At the heart of the problem is the detection of vulnerabilities. Information systems are riddled with vulnerabilities that are only waiting to be exploited (Schneier, 2018). Organizations however have few incentives to invest in information security. Several measures are thus pushed in order to promote incentives for a secure networked economy. Among them is the development of cyberinsurance and international standards in the hope of incentivizing cyber hygiene measures. Estimating cyber risks is however a difficult endeavor and such an insurance scheme still has trouble developing (Wolff, 2022).

Another novel solution comes from bug bounty programs. These are “arrangements between organizations and individual security researchers to trade vulnerabilities as products” (Zrahia, 2024). An organization willing to reinforce its security can thus publicly declare its willingness to pay for the disclosure of a vulnerability and expect hackers to spend time looking for vulnerabilities on its systems in exchange for a reward. This commodification of vulnerabilities has been growing in recent years, and it is widely acknowledged as a successful mechanism for vulnerability detection (Bozzini, 2023).

[1] See SonicWall (2024) “Cyber Threat Report”, p.6. URL: https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf (Accessed 1 March 2024).

Suggested Citation (APA): Perrig, L. (2024, October). *Ready to hack: How bug bounty platforms create their workforce*. Paper presented at AoIR2024: The 25th Annual Conference of the Association of Internet Researchers. Sheffield, UK: AoIR. Retrieved from http://spir.aoir.org.

Promoting such bug bounty programs has thus become a legitimate policy measure (Zrahia, 2024). Indeed, such programs not only contribute to securing the economy, they are also considered an efficient way to channel potential young criminals into a legitimate career as information security researcher (Follis & Fish, 2020), as well as a way to stifle the development of a black market for offensive zero-days (Perlroth, 2021). For this reason, institutionalizing ethical hacking has increasingly been listed among the national cyberstrategies of states worldwide.[2]

Platformization

The bug bounty industry is particularly prone to the development of labor platforms. They indeed have the advantage of making programs visible, of handling the transactions, as well as ensuring the compliance of hackers. In some sense, they are thus akin to traditional platforms of the gig economy (Ellis & Stevens, 2022). They also share a business model that relies on charging a fee on each transaction. They thus have an incentive in stimulating the market that they are enabling.

In contrast to usual platforms of the gig economy however, bug bounty platforms cannot tap on an already existing workforce (Goerzen & Coleman, 2022). Indeed, the hacker community can hardly be considered a workforce, in the sense that it is composed of self-taught hackers with varying skills in a wide range of different domains. Bug bounty platforms thus have to create a labor supply. Such an endeavor however does not come without hurdles, and this paper discusses the measures that platform managers must take in order to secure a loyal workforce.

The building of a workforce

The paper will discuss four ways in which bug bounty platforms seek to build a competent and sufficient workforce.

The first measure is to train young offensive security researchers. Hacking is notorious for being self-taught. While there exist higher-education training in information security, it is seldom focused on offensive security. Moreover, platforms rely on workers that are not yet committed in a career path, but rather willing to earn a little money on the side or expecting some intellectual challenge (Akgul, 2023). For this reason, platforms will develop sophisticated online training programs and hold events in order to ensure a skilled workforce. Hack-the-box exercices, CTF contests, and video tutorials are among the prominent educational tools that platforms provide.

Second, for pedagogical purposes, offensive security practices must be standardized. For this purpose, precise routines are established, that rely on specific software. Among the educational material online, the content is remarkably homogeneous across platforms. Ethical hacking is made accessible by providing a list of precise instructions for vulnerability detection. This ensures that a large crowd of hackers have entry-level capabilities in order to identify the lower-stakes bugs.

[2] For the Swiss case, see Federal Council (2023) “National Cyberstrategy”, p. 20. URL: https://www.newsd.admin.ch/newsd/message/attachments/76796.pdf (Accessed 1 March 2024).

Third, bug bounty platforms must ensure competition among hackers. Designing a scheme that favors competition is a necessary requirement in building a labor market. Implementing rankings and gamifying work are among the platforms' preferred ways to ensure workers' consent (Velthuis & van Doorn, 2020; Vasudevan & Chan, 2022). In the case of bug bounty however, ranking vulnerabilities is an additional hurdle. Indeed, in order to put a reward on a vulnerability, platforms must agree on some way to commensurate vulnerabilities. While standards exist to measure the criticality of a vulnerability, attempts at estimating the labor required to find one is still missing. The risk in mispricing vulnerabilities is that bug hunters lack incentives to find the more subtle ones and flock towards the most obvious ones.

The fourth and last observed measure is institutional backing. By securing alliances with already established organizations, bug bounty platforms can benefit from a convergence of interest from the industry, the army, or higher education institutions. Bug bounty platforms thus serve not only to secure information systems, but also as a steppingstone to a professional career, an enlistment to a cyber army unit, or a formal training. Bug bounty conferences thus benefit from the ethos of hacker conferences and attract young hackers but often serve at the same time as recruitment events for very legitimate careers (Coleman, 2010).

Bug bounty platforms thus display a prime example of the building of a labor market. The supply of workers in this case does not pre-exist the arrival of platforms. Instead, they must actively work to establish standards, routines, and measurements so that workers are equipped to answer a growing demand.

Data

The paper draws from an ongoing fieldwork in the offensive information security industry in Switzerland. It relies on interviews with all sides of the market: bug hunters, platform managers, and chief information security officers (CISOs) from partner organizations. In addition to these interviews, the fieldwork consists of a participant observation of the training of aspiring ethical hackers. It takes place online (forums and chatrooms) as well as offline (hacker events and conferences).

References

Akgul, Omer, Taha Eghtesad, Amit Elazari, Omprakash Gnawali, Jens Grossklags, Michelle L. Mazurek, Daniel Votipka, and Aron Laszka. 2023. "Bug Hunters' Perspectives on the Challenges and Benefits of the Bug Bounty Ecosystem." In *32nd USENIX Security Symposium (USENIX Security 23)*, 2275–91. Anaheim, CA: USENIX Association.

Bozzini, David. 2023. "How Vulnerabilities Became Commodities. The Political Economy of Ethical Hacking (1990-2020)." https://hal.science/hal-04068476.

Ellis, Ryan, and Yuan Stevens. 2022. *Bounty Everything: Hackers and the Making of the Global Bug Marketplace*. Data & Society.

Follis, Luca, and Adam Fish. 2020. *Hacker States*. The Information Society Series. Cambridge, MA: The MIT Press.

Goerzen, Matt, and Gabriella Coleman. 2022. *Wearing Many Hats: The Rise of the Professional Security Hacker*. Data & Society.

Schneier, Bruce. 2018. *Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World*. New York ; London: W.W. Norton & Company.

Vasudevan, Krishnan, and Ngai Keung Chan. 2022. "Gamification and Work Games: Examining Consent and Resistance among Uber Drivers." *New Media & Society* 24 (4): 866–86. https://doi.org/10.1177/14614448221079028.

Velthuis, Olav, and Niels van Doorn. 2020. "Weathering Winner-Take-All." In *The Performance Complex: Competition and Competitions in Social Life*, edited by David Stark, 167–84. Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780198861669.003.0008.

Wolff, Josephine. 2022. *Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks*. Information Policy Series. Cambridge, MA: The MIT Press.

Zrahia, Aviram. 2024. "Navigating Vulnerability Markets and Bug Bounty Programs: A Public Policy Perspective." *Internet Policy Review* 13 (1). https://doi.org/10.14763/2024.1.1740.