Module 11 (2) Journal Entry

Davis Plude
8/4/2025

In the article Sridhar and Ng explain bug bounty programs within the larger information security economy. Prior articles have yet to explain how cost effective these bug bounty programs can be, as well as the value of crowdsourcing vulnerability reporting. But bounty programs can also be seen to help keep malicious hackers from posting the vulnerabilities of your device. One of the greatest examples of this is Apple's one million dollar bounty for finding zero-click kernel vulnerabilities with up to a two million dollar bounty if you can find a lockdown mode vulnerability. These large rewards can keep even the most technical malicious hackers at bay as they will make more money instantly reporting the bug then trying to sell the bug and have to wait for the money to come in. With that being said the article discusses how monetary incentives are still important but only lead to a marginal increase in bug reporting. Most people reporting bugs are not malicious hackers and are just trying to hone their skills. The article also found a negative “age effect” on reports. As a program got older the bug reports would go down suggesting a more secure system as all of the easy bugs were found and fixed. That may leave some of the more important bugs still out there so expanding the attack surface can counteract this trend. There was very little impact on bug reports because of company size or brand profile. Overall I think this article expands peoples understanding of bug bounty programs greatly and understanding these programs will help the cybersecurity landscape in the long run.

References

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of bug bounties. *Journal of Cybersecurity, 7*(1), Article tyab007. https://doi.org/10.1093/cybsec/tyab007