Ryan Son

CS338

Jeff Ondich

October 13, 2024

Ethical Analysis of a Security-Related Scenario

A. If I have the knowledge that there is a major security exploit that exists, in this case an attacker could read the contents of all private InstaToonz direct messages, do I have a moral responsibility to report it? Is it ethical to ignore reporting the security exploit if there is a very high probability that I will face legal repercussions because of it? Why do companies have the option of pursuing legal action against someone who is not taking advantage of the exploit and choosing to report it? Is it not in the company's best interest to mitigate security issues that might arise without hurting others?
B. InstaToonz is legally entitled to have their software copyrighted if it is encrypting and copy-protecting music that is shared across the platform. I as a user am allowed to use their software, but I do not have the right to modify their code because it is intellectual property. Acknowledging that their software has a bug demonstrates that I have viewed their encrypted code and tampered with it in some way allowing me to see the exploit. If the bug does not involve any encryption or copy-protection, I am less legally in trouble if I choose to report this bug. In this case, I will be examining a bug that involves encryption.

C. What was the FBI's opinion on the litigation against the bug-reporter despite not pursuing the matter further? Why does InstaToonz not want to establish a bug bounty program?

D. Possible Actions and Likely Consequences?

    a. I could report the bug. Though they had already tried to sue someone beforehand for reporting the bug, so it is highly likely that they would prosecute me, no matter the severity.

    b. I could not report the bug. I would feel bad. I would not however be prosecuted to the highest extent of the law, saving me from a major mental, physical, and financial headache.

E. ACM Code of Ethics and Professional Conduct?

    a. Some notes from the ACM Code: Consistently support the public good. All people are stakeholders in computing. Avoid harm. Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner, providing appropriate guidance and remediation.

    b. This code of ethics and professional conduct does not however outline anything about people who may face legal ramifications (like in this scenario) if they were to follow this code to a T. In a vacuum, I agree that these are very good and well thought out points, but if there's a danger to my personal well-being (financial or mental), the responsibility should not be on my individual to try to work against the current predatory legal systems that exist. If a major security exploit occurs on a company's behalf, I believe they must shoulder the ensuing consequences,

especially if they have made it so difficult for people to report bugs. I like to think of this situation of someone who would be a Good Samaritan that SHOULD have laws protecting their actions, if they aren't being financially compensated for good work, they should at least not have the fear of being prosecuted. Otherwise, if there were no Good Samaritan laws, some people would be too afraid to help anyone.

F. I believe that I have no obligation to report such an issue if I am at risk of prosecution. If that issue were to be taken advantage of and discovered, I would hope that people would pursue legal action against the company. These companies have lobbyists that have more energy, more resources, and hold more leverage over politicians where they could enact change and protections to people that report bugs, if it would limit their risk of legal trouble.