Palmy Klangsathorn
CS 338 Computer Security
October 16, 2024
Jeff Ondich

Misc/Ethics

I discovered a critical vulnerability in InstaToonz that allows attackers to access private messages, affecting millions of users. I want to report it, but InstaToonz has a history of retaliating against bug reporters, involving lawsuits and the FBI, and they lack a bug bounty program for responsible disclosure.

So, it means so far that InstaToonz doesn't want security researchers or ethical hackers to report bugs, as they believe these people might steal or sell users' information. My goal is to report the vulnerability ethically, but without a bug bounty program, I can't safely or legally report it. After reading their lawsuit, two possibilities arise:

- If the bug involves encryption or copy-protection, I might be in violation of Section 1201 of the Digital Millennium Copyright Act (DMCA), a U.S. law that protects against tampering with technological measures used to protect copyrighted materials. This could mean I'm at risk of being accused of circumventing these protections, even though my goal is to report the vulnerability for ethical reasons.
- If the bug does not involve encryption or copy-protection, I may not face the same legal risk under the DMCA, but I could still face other legal threats, given InstaToonz's aggressive stance on bug reports.

Therefore, in both cases, I should not report or take any action agains the company by myself.

Let analyze this scenario step by step:

A. Identify the main ethical question or questions faced by me in the scenario.
   - ➔ What should I do about the discovered bug in InstaToonz?
   - ➔ How can I protect the privacy and security of InstaToonz users while navigating the legal risks?
   - ➔ How can I protect myself if the company thinks that I'm an attacker who want to steal the users' information?
   - ➔ Should I consider alternative ways of disclosure to avoid negative outcomes like previous reportes?

B. Identify the stakeholder's relevant rights.
   - ➔ Right to privacy and security of their direct messages.
   - ➔ Right to protect their proprietary information and trade secrets; right to manage how security vulnerabilities are disclosed.

- ➔ Right to disclose security vulnerabilities responsibly without facing legal threats.
- ➔ Right to investigate potential breaches of law, including unauthorized access to data.

C. List any information missing from the scenario that I would like to have to help me make better choices.
   - ➔ Detailed legal implications of disclosing vulnerabilities under different circumstances (e.g., involving encryption or not).
   - ➔ InstaToonz's specific policies on vulnerability disclosure and their stance on bug bounty programs.

D. Describe my possible actions, and discuss the likely consequences of those actions.
   - ➔ Contact a third-party security organization or researcher to facilitate disclosure.
     - ◆ Likely Consequences: A third party could help report the bug without exposing me to direct retaliation from InstaToonz. This might increase the chances of the bug being fixed while protecting my identity. However, InstaToonz may still ignore the report or retaliate against the third party.
   - ➔ Contact legal experts/lawyers for advice on mitigating personal legal risks.
     - ◆ Likely Consequences: Consulting a lawyer would help I understand my legal position and reduce personal risk. While this would provide a clearer picture of potential consequences, it could also delay the disclosure, leaving the vulnerability unaddressed for longer and exposing users to continued risk.
   - ➔ Act as a victimized user and provide feedback about my leaked information/messages to InstaToonz via the App Store or other platforms.
     - ◆ Likely Consequences: This approach could bring attention to the issue without presenting myself as a security researcher. InstaToonz might take it more seriously and act on the feedback, but it might also be slower to respond if it's seen as a user complaint rather than a critical security flaw. Additionally, it may not address the issue thoroughly, leaving the vulnerability partially unresolved.
   - ➔ Write blog posts online/tiktok/tweet without mentioning the company's name, InstaToonz.
     - ◆ Likely Consequences: Writing blog posts can raise public awareness without directly targeting InstaToonz. This could pressure the company to address the issue without dragging me into legal trouble. However, if attackers discover the vulnerability from my blog before it's fixed, it could lead to greater harm. There's also a chance that InstaToonz might still identify myself and my identity, and take legal action.

E. Discuss whether the ACM Code of Ethics and Professional Conduct offers any guidance.

- ➔ Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing, I should report the vulnerability a way that ensures the protection of users, well-being, and safety of myself
- ➔ Avoid harm by disclosing the vulnerability, I should prevent potential harm to millions of users who are at risk of their private messages being exposed.
- ➔ Be honest and trustworthy, disclose potential security risks responsibly, I should act transparently but with caution to avoid the exposure of the vulnerability.
- ➔ Be fair and take action not to discriminate, I should disclose the vulnerability responsibly, even if the company does not have formal channels for doing so.
- ➔ I should not leak the bug widely during the fixing process because some attackers might learn about the vulnerabilities and exploit them before they are resolved.
- ➔ Know and respect existing rules pertaining to professional work, I need to understand the legal implications and follow best practices for vulnerability disclosure to avoid legal consequences.
- ➔ Accept and provide appropriate professional review, I should consult with third-party security organizations or legal experts/lawyers for appropriate professional oversight.

F. Describe and justify my recommended action, as well as my answers to any other questions I presented in part A.

- ➔ Hence, I will contact a third-party security organization or researcher to facilitate disclosure, because it is too risky to do it all by myself. This approach allows me to report the vulnerability without exposing my identity directly to InstaToonz, reducing the likelihood of retaliation. Third-party organizations often have established relationships with companies and can communicate findings effectively, increasing the chances that the vulnerability will be taken seriously and addressed promptly. By using a third party, I can help protect the privacy and security of InstaToonz users while minimizing my own legal risks. This method also avoids the potential negative outcomes experienced by previous reporters, who faced lawsuits and public scrutiny. In summary, my recommended action balances the ethical responsibility to report the vulnerability with the need to protect myself and others. It ensures that the issue is addressed responsibly, contributing to user safety while re personal risks I would face by approaching the company directly. I must recognize my position and the limits of my role; even though I want to report and resolve this issue immediately, the process and reality are not that straightforward.