Eli Arbogast and Jake Martens

Jeff Ondich

CS 231

14 May 2021

Ethics - Scenario 1

A.

a. What should we do?

b. What is the role of security researchers? Is it ethical to seek out flaws in the system? Could this knowledge make the system more vulnerable?

c. Do InstaToonz users deserve to know that their messages are at risk? How soon? If the bug is fixed, should they be informed that their data is/was compromised?

d. If the bug gives us access to copyrighted music, have we circumvented the barriers preventing us from accessing this encrypted/copy-protected media? Have we broken the law simply by finding a way around these barriers?

B.

a. We - We have the right to a fair trial in court should InstaToonz take action. We have the right to use InstaToonz in accordance with its own policies. Suppose we found the bug strictly while using the service and without intent to "hack" it--in this case, we should have a right to report.

b. InstaToonz - InstaToonz has the right to terminate an account if the user has violated the terms and conditions. It has the right to launch a suit or investigation to understand how the hacker discovered the bug. In the encryption scenario, InstaToonz has the right to ban all good will hacking from its service to prevent violations of section 1201.

c. Users - In the encryption scenario, the user can reasonably expect that InstaToonz's messaging service meets the requirements of section 1201 so as not to risk breaking the law. In either case, the user has the right to know that their messages are/were at risk for being leaked.

d. Record labels/artists - Strictly in the encryption/copy-protected scenario, this group has the right to protection for its music. Section 1201 makes it illegal to circumvent these measures, and this bug would put their media at risk for intellectual theft. They would also have a right to give the company notice, whereas the hacker does not necessarily.

C.

a. Is any encrypted or copy-protected media at risk from the bug?

b. Is hunting for bugs illegal? Is hunting for bugs even with a bug bounty offered illegal?

c. Do we know of anyone else who has found this bug? For example, did we read about it on a Reddit thread? In this case, we have not exactly circumvented any barriers ourselves but have simply become aware of a breach.

D.

a. We can report the bug to the company, in which case, we will be sued.

b. We can not report the bug to the company, in which case, there could be a breach of the service which we could have prevented. Otherwise, we go on with our lives.

c. We can report it to the record company in the encryption/copy-protected scenario and let them deal with protecting their own media.

d. We could steal the user data (or the encrypted files) and demand a ransom to not release it. Either law enforcement will find us and we will be in more trouble, or we get away with it and a nice pay out.

E.

a. Sections 1.1 and 3.1 call for an acknowledgment that all users hold a stake in computing and that computing should contribute to the common good. Hunting for bugs ultimately protects users and companies from threats posed by malicious actors. Additionally, section 2.5 requires the evaluation of computer systems' impacts and risks, goals which bug hunting explicitly supports.

b. In the encryption/copy-protected scenario, there is some violation of the barriers preventing access, which seems to go against the goal of respecting privacy and confidentiality as outlined in sections 1.6 and 1.7.

c. From the perspective of InstaToonz, section 2.4 suggests that the company accept appropriate professional review. That is, they should respond to bug reports in order to promote system security. A robust system of reporting supports the maintenance of the systems and responding to its risks. Finally, section 2.7 states that professionals support public awareness of computing in its consequences. We can extend this ideal to informing the public about the security risks currently present in their service.

F.

a. In the non-encrypted scenario, we should anonymously report the bug. This action protects the privacy of users and thus supports the common good. We also avoid legal action taken against us by InstaToonz, which appears unlikely to reward us with a bounty payment.
b. In the encrypted/copy-protected scenario, we should report the issue to the record labels, perhaps anonymously. Because their media is now at risk, they are likely to take action against InstaToonz because this is the service that has made their media vulnerable. It is in their interest to force InstaToonz to fix the bug.
c. Ultimately the responsibility lies with InstaToonz for developing a service that puts users and media at risk. The ACM code places the professional responsibility on the company to create a secure service and continuously review it for risks.

(We were tempted but ultimately decided against suggesting that the best route be to steal user data using the bug and hold it ransom by the company, as we are seeing more and more of these attacks occur in our day to day lives, that are often paid in full with little to no repercussions for the hackers in question. Of course this is not the ethical choice here.)