Yuqing Zhai

09/11/2024

AU10TIX, a company which provides identity verification services for companies like TikTok, Uber, Twitter, etc, has recently been found leaking sensitive user information due to exposed administrative credentials. [1] Mossab Hussein, a security researches, disclosed this situation to the journalist Joseph Cox at 404 Media. Hussein used the leaked credentials to log-in to the AU10TIX service to demonstrate the vulnerability to Cox. [1] Although Hussein's action has made 404 Media to raise concerns and put pressure on AU10TIX to fix the issue, his actions, which uses the exact same techniques hackers would use to access the data, have some ethical concerns. **This essay claims that Hussein's action is ethical using utilitarian ethics.**

AU10TIX provides identity verification services. This services requires user's identity documents, including passport and driver's license. They also have “liveness detection”, which collecting a real-time video stream from the user. [1] Using this data, they can detect the validity of user's identity and age, which are utilized by social network platform and pornography websites. [1]. **The verification process based on identity documents used by AU10TIX is intrinsically morally opaque**, that is, the ways in which the technology affects society and individuals might not be straightforward, so is the moral consequences. The identity verification could on the one side eliminate scam bots in the social network, but on the other side could be an intrusion to privacy and potential leak of sensitive information if improperly managed.

As Hussein discovered, there is massive leakage of person sensitive identity documents, given number of users of TikTok, Twitter, etc. These leaked identity documents could be used for identity theft to carry on further illegal activity. This information could be exploited by scammer and used to target vulnerable individuals. This could have serious consequence, including financial losses, legal issues, and physical harm. From the utilitarian point of view, which judges the morality of the action by the consequences it has caused, it's obvious that it's extremely immoral to accidently leak these document due to incompetent management. Conversely, it's moral for Hussein to demonstrate the vulnerability to 404 Media, to release article about the incident to raise awareness and put pressure on AU10TIX to reinforce the security system and prevent further damage.

As mentioned by 404 Media, Hussein does use leaked credentials to log in to the AU10TIX service to demonstrate the vulnerability. [1] However, since Hussein's sole purpose is to demonstrate the vulnerability, he does not cause actual losses for the users'. He only showed the leaked data to 404 Media, whose employee never used the leaked data for any purpose other than to confirm that such vulnerability is genuine. Since no actual damage and losses are caused to users, this action is not immoral.

Furthermore, referring to ACM Code of Ethics, “[a]ccess computing and communication resources only when authorized or when compelled by the public good... ” [2], **Hussein’s actions align with the ACM Code of Ethics**, as there's a compelling public good, which is to preventing further data leakage. Also, given the vulnerability discovered by Hussein, he could approach in three ways: (1) keep the vulnerability to himself (2) expose the vulnerability to public (3) only disclose vulnerability to vendor. **We see that Hussein choose to do a full disclosure**. In previous case with the company Rabbit, the company ignore the problem of hard-coded keys in Rabbit M1 disclosed from security researchers until the researchers shows the problem to 404 media. [3]. Disclosing the vulnerability publicly rather than vendor only could better force the company into fixing the problem. Some might worry that such a public disclosure could attract attention to potential hacker, therefore increase the chance that such vulnerability to be exploited. However, according to the article, the ‘infostealer’ malware, type of malware that used to steal AU10TIX’s data, has already been prevalent and AU10TIX’s credential has already been freely available on Telegram and are known to hackers. [1] The effect of the public disclosure might be negligible in increasing the attention from hackers, and the positive benefits in forcing the company to fix the problem will outweigh the potential consequence from the increasing attention from hackers. **Therefore, Hussein’s choice to fully disclose the vulnerability could produce the most beneficial results, and is thus the most morally best action.**

Therefore, from the utilitarian point of view, we see that it’s ethical for Hussein to use the leaked credentials to log-in to the AU10TIX service to demonstrate the vulnerability to 404 Media.

[4924 characters]

References:

[1]

Cox, J. (2024, June 26). ID Verification Service for TikTok, Uber, X Exposed Driver Licenses. 404 Media. https://www.404media.co/id-venfication-service-for-tiktok-uber-x-exposed-dn%25c4%25af

[2]

Association for Computing Machinery. (2024, September 11). Code of Ethics. https://www.acm.org/code-of-ethics

[3]

Koebler, J. (2024, June 26). Researchers Prove Rabbit Al Breach By Sending Email to Us as Admin. 404 Media. https://www.404media.co/researchers-prove-rabbit-ai-breach-by-sending-email-to-us-as-admin/