https://github.com/berkemremert/Exercise7_IC00AI83

Berk Emre Mert
bmert24@student.oulu.fi

Task 1

In organizing a deepfake attack, the intelligence acquisition process involves gathering videos, photos, and audio of target victims in order to create convincing replicas. This is more specific compared to the broad social engineering targeting general personal data.

Deepfake threats are powerful because they can mimic trusted colleagues or managers, and their legitimacy makes employees more trusting of the request. This overrules their natural skepticism and maximizes the chances of being cheated.

Staff training is a assistance, but even that cannot completely prevent deepfakes. The more realistic deepfake technology becomes, the more difficult it will be for humans to detect it, so other measures, like technology and multi-factor authentication, are necessary.

To prevent accidents, strict verification processes need to be implemented, such as cross-verifying requests via alternative channels. Real-time transaction monitoring and open incident response plans must also be adhered to. Ongoing training must be provided to employees on existing threats, and deepfake detection systems must be installed.

A few of the current solutions to detect deepfakes are applications like Deepware Scanner, Microsoft Video Authenticator, and FakeCatcher. They look for coherence in facial expression or any other sign of tampering. They are not unbreakable and can be bypassed by sophisticated deepfakes.

I tried out Deepware Scanner, which detected some of the videos with obvious defects but not all deepfakes. A potential new solution is a live video verification platform that scans for voice, face, and background inconsistencies in live video calls. This would detect even superficial deepfakes.

Bonus Task

For this task, I used FaceFusion. I found a how to use video on Youtube: https://www.youtube.com/watch?v=h-6svh0xGiU. I cloned the Github repo and used installed the necessary tools. You can find the video in my repo.

I don’t think my video can fool someone to be honest because I didn’t render the video in the full capacity. Right now, it took 14 minutes to render it so I can’t image how long would it take with a higher quality. However, it’s good to know that there is a space to develop it. I also checked and discovered several models that they created for faceswapping so it might

also affect the quality. I used inswapper_128 model and 128x128 pixel boost but it can be increased up to 1024x1024. There is also voice factor, so I should play with voice as well to fool people.

It was easy actually, especially in comparison to our other tasks. I found this one pretty fun as well so maybe that's why it came easier to me.

Task 2

Not fully asked.

Task 3

Not fully asked.