


Seeing is living? Rethinking the Security of Facial Liveness Verification in the Deepfake Era

Changjiang Li[1,2], Li Wang[3], Shouling Ji[2], Xuhong Zhang[2], Zhaohan Xi[1], Shanqing Guo[3], Ting Wang[1]

[1]Pennsylvania State University, College of Information Science and Technology

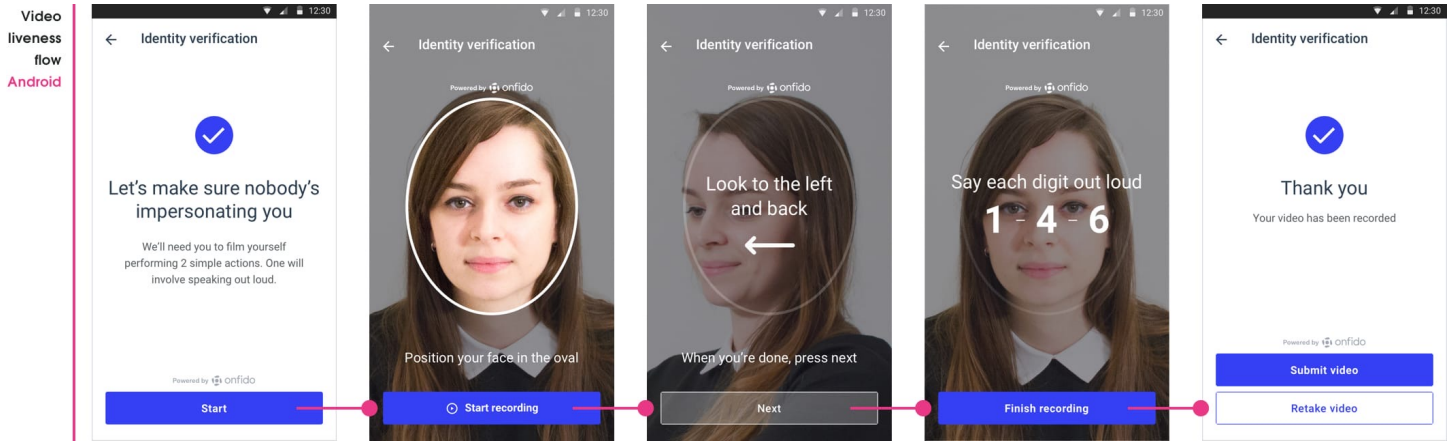
[2]Zhejiang University, College of Computer Science and Technology

[3]Shandong University, School of Cyber Science and Technology

USENIX Security 2022

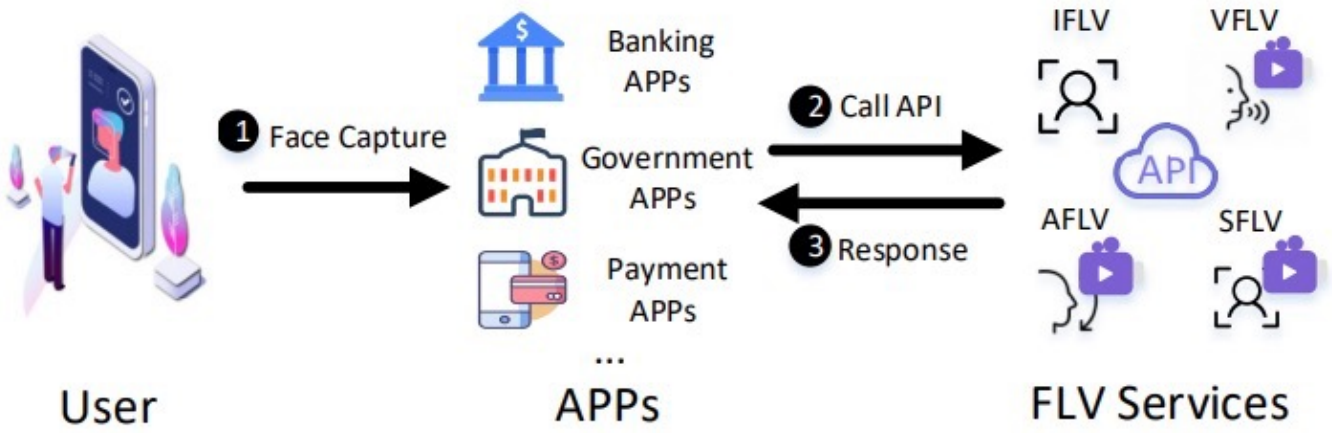
Facial Liveness Verification (FLV)

- A growing number of security-sensitive applications use FLV in their services
  - Know Your Customer (KYC) Policy (Banking, Exchanges)
  - Cloud Vendors
- Various kinds of FLV



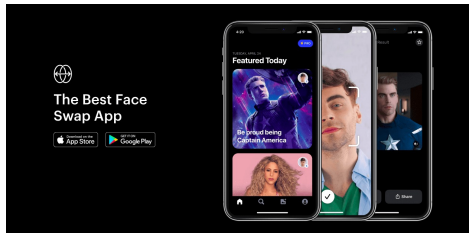
Facial Liveness Verification (FLV)

- FLV Pipeline
  - Step 1: User interacts with the application
  - Step 2: Capture the user's facial images/videos
  - Step 3: Analyzing the uploaded images/videos



DeepFake

- DeepFake has raised a great interest in recent years



- DeepFake is a growing threat to cybersecurity and society

This co-worker does not exist: FBI warns of deepfakes interviewing for tech jobs

Devin Coldewey @techcrunch / 5:26 PM EDT • June 28, 2022

Chinese government-run facial recognition system hacked by tax fraudsters: report

overnment-run identity verification system to fake tax invoices

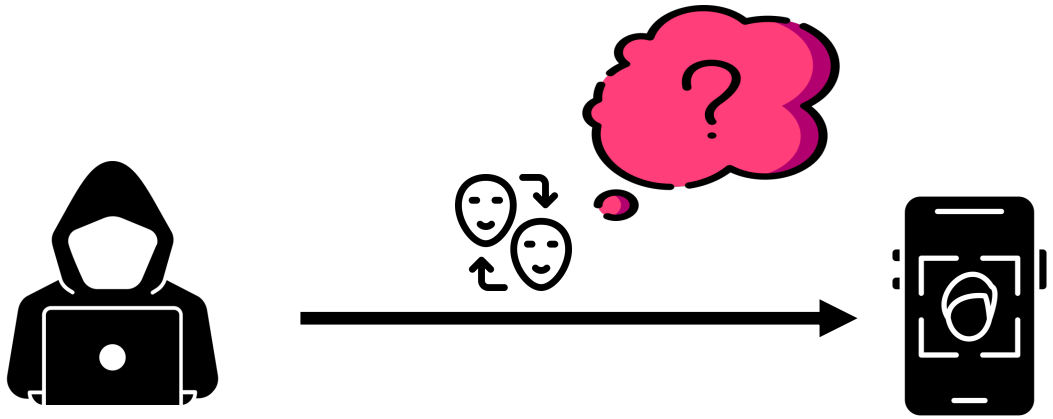
al group were valued at US$76.2 million

EVIL APPS New deep fake app scam photoshops victim's face onto PORN and sends to family if they don't pay up

Jona Jaupi, Technology and Science Reporter
13:31 ET, Jul 25 2022 | **Updated**: 13:33 ET, Jul 25 2022

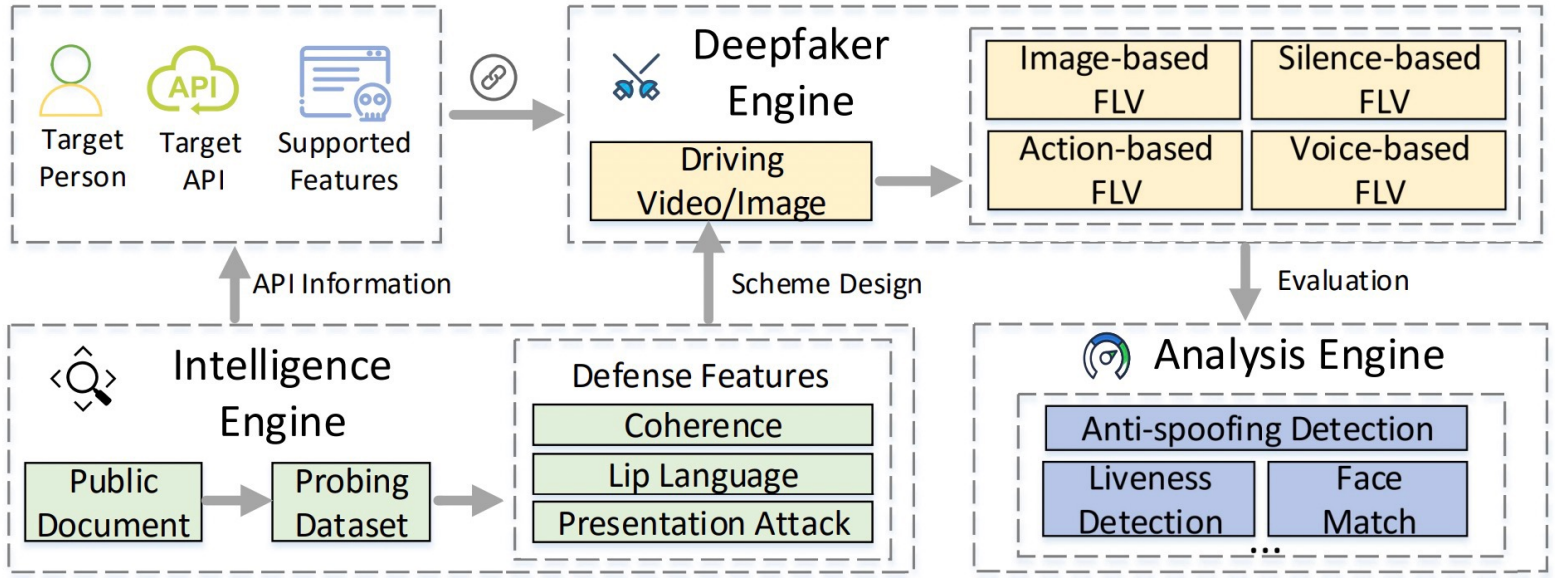
Security Question

- How is FLV vulnerable to DeepFake-powered attacks?



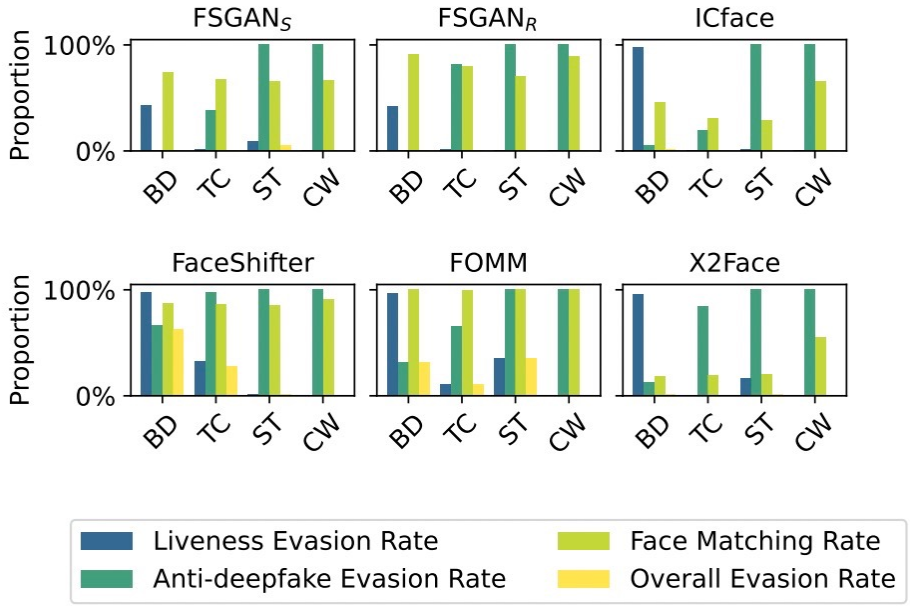
Approach Overview

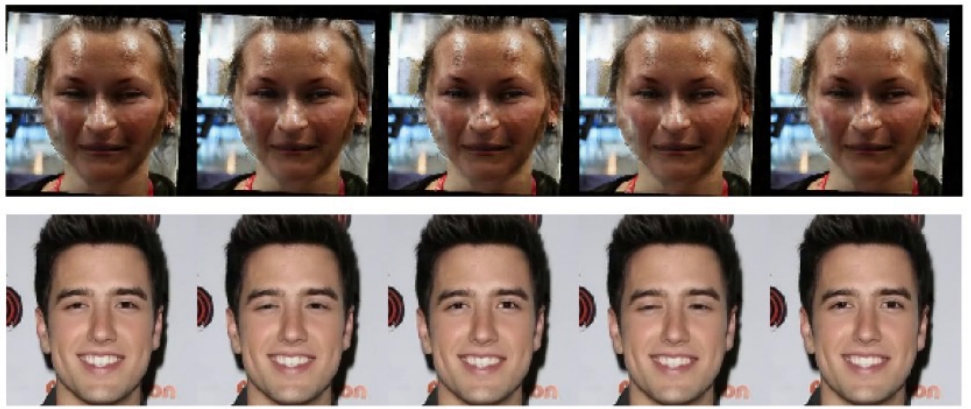
- We design and implement LiveBugger, a framework that integrates various SOTA DeepFake techniques for evaluating the security of FLV systems



Results

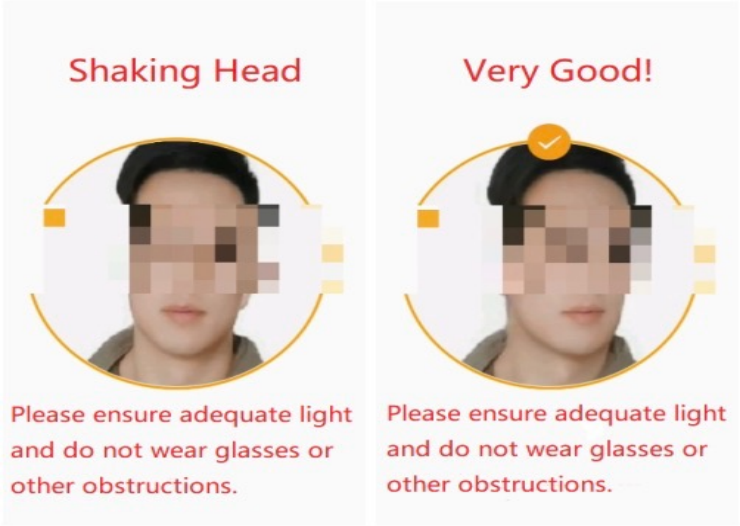
- All types of FLV are vulnerable to DeepFake-powered attacks
- Anti-DeepFake should be further improved





POC Attack

- We conduct a POC attack to demonstrate the feasibility of DeepFake-powered attack in the real world
  - Hijack video stream
  - Synthesize the fake video in a real time manner
  - Feed the fake video stream to the application



Security Insights

- Anti-DeepFake detection is necessary for FLV systems
- FLV should consider the match of lip movements with the audio signal or even voiceprint to improve the security
- Adopt actions that are hard to be synthesized by DeepFake
- Increase the diversity of actions or voice prompts

Implication

- We report our findings to the affected vendors, and receive active feedback

Dear Li Wang,

Thank you for reaching us. Deep fake use is known issue for facial recognition, our company is aware of it and we are working on nev approaches to counter the flaw.

Best regards,

Hi Li Wang,

Thanks for your email.

Yes, we are aware of deepfake attacks using hijacked video streams.

Do you have any means or recommendation to prevent this?

Jeanne

Deepfake Detection Research Funded by German Federal Ministry of Education and Research

Nuremberg, Germany – November 30th, 2021: German biometrics company BioID today announced its engagement in FAKE-ID, a project on deepfake detection funded by the German Federal Ministry of Education and Research (BMBF). This work on **deepfakes** is part of the Federal Government's framework programme Research for Civil Security and the BMBF funding call on artificial intelligence in security research.

Conclusion

- We design and implement LiveBugger, a first-of-its-kind security evaluation framework for FLV
- An extensively evaluation demonstrates that most representative FLV systems are vulnerable to DeepFake-powered attacks
- We perform POC attacks in real-world setting
- We provide a set of suggestions to improve the security of FLV

Thanks

changjiang.li@psu.edu