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
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
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