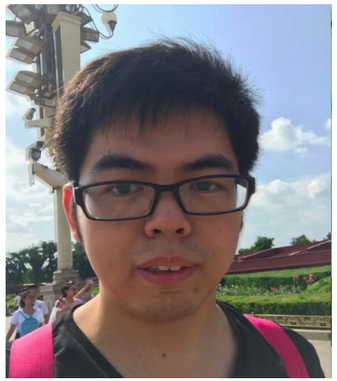

black hat
USA 2019
AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS
Biometric Authentication Under Threat:
Liveness Detection Hacking
#BHUSA @BLACK HAT EVENTS

Who Are We?

- Tencent
  - The largest social media and entertainment company in China
- Tencent Security Xuanwu Lab
  - Applied and real world security research
- About us

Yu Chen



Bin Ma (@m4bln)

HC Ma

Outline

- Preliminary and Previous Studies
- Hardware-level Video/Audio Injection
- Insecure Recognition Scene Exploiting
- Mitigation
- Conclusion

Preliminary

- What is biometric authentication?
  - Biometric Feature
    - Face, Voice, Fingerprint, Iris, Palmprint etc.
  - Areas of applications
    - Device unlock
    - Password recover
    - App login
    - Real-name authentication
  - A typical biometric authentication process

Preliminary

- What is liveness detection?
  - Definition

    Verify if the biometric being captured is an actual measurement from the authorized live person

  - Existed methodology
    - Imitative medium recognition

      texture analysis, optical flow, playback reverberation, etc.
    - Interactive action check

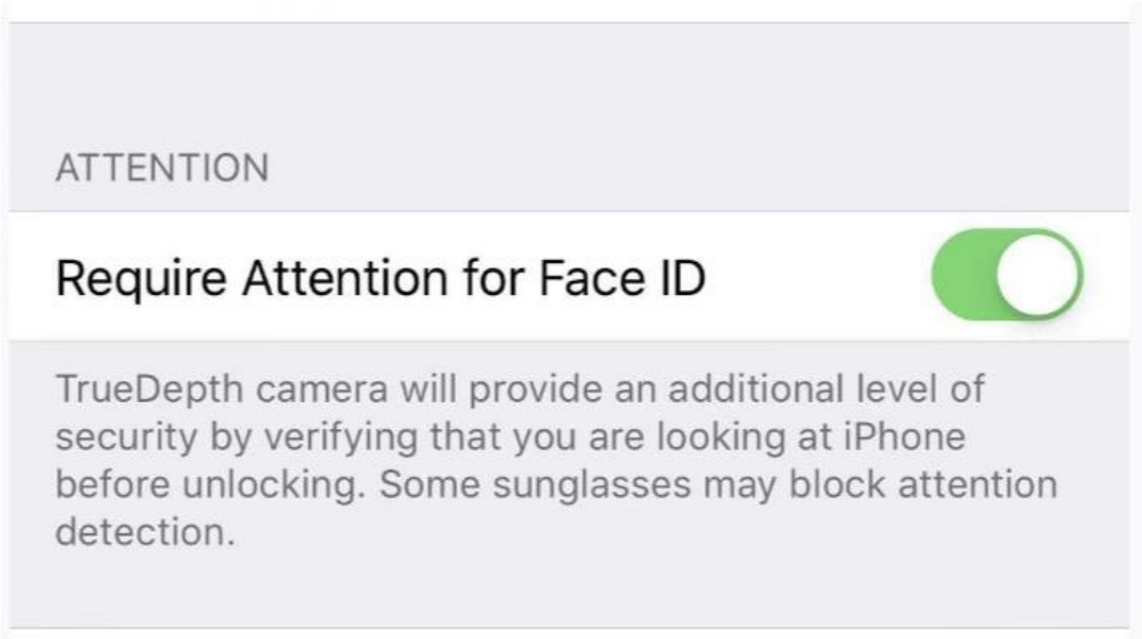
      nod / shake head, open mouth, blink, speak words, etc.
    - Specific Hardware

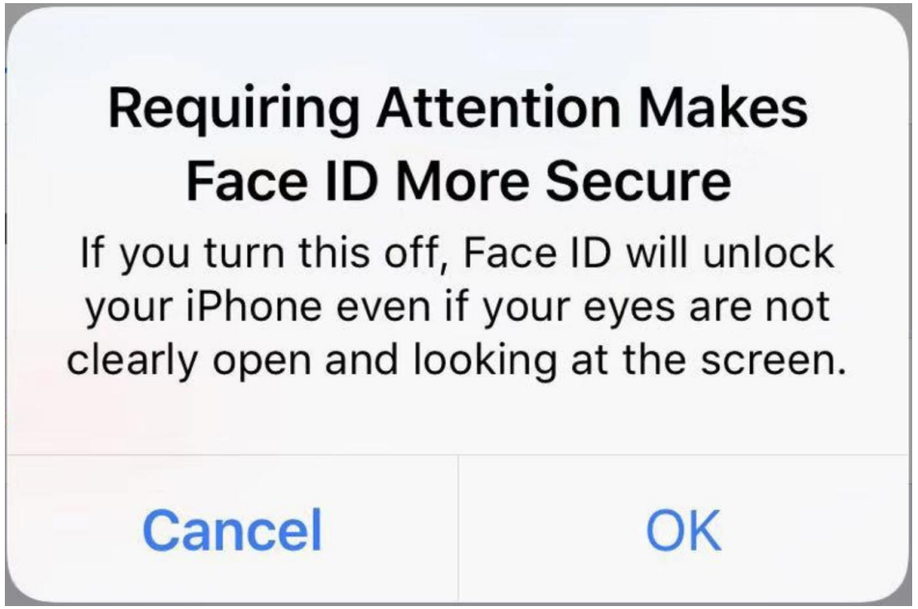
      Face ID, ToF, NIR, etc.

Preliminary

- What is Face ID attention detection ?

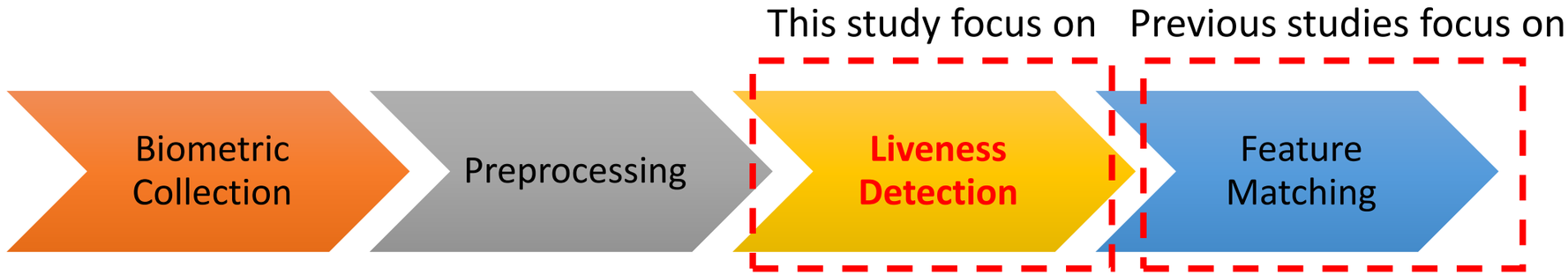
Face ID confirms attention by detecting the direction of your gaze, then uses neural networks for matching and anti-spoofing so you can unlock your phone with a glance





Previous Studies

- Previous studies mainly focused on how to generate fake video/audio, but bypassing the liveness detection algorithm is necessary in the real attack
- Bypassing Face ID by 3D mask requires victim's 3D info and is proven hard to reproduce



biometric authentication process

Outline

- Preliminary and Previous Studies
- Hardware-level Video/Audio Injection
- Insecure Recognition Scene Exploiting
- Mitigation
- Conclusion

Why do hardware-level video/audio injection?

- Avoid information loss during biometric secondary acquisition and playback
  - HSL space color loss
  - focus blur
  - playback reverberation effect
- Hide the attack medium characteristics
  - Texture
  - optical flow
  - frequency response distortion
- Be completely software-insensitive
  - Against emulators detection
  - Against anti-hook

Video/Audio Injection Requirements

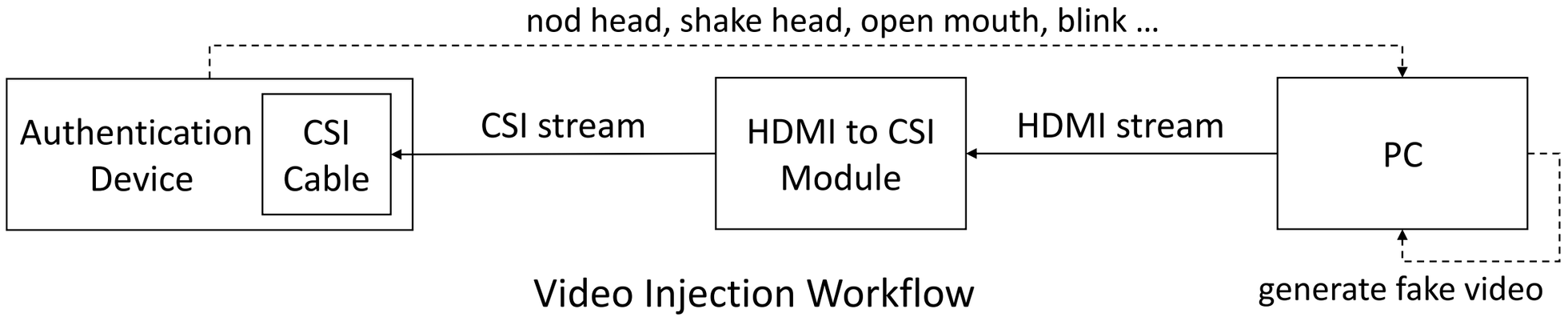
- Low Latency
  - Excessive delay will cause recognition failure
- Good Compatibility
  - Compatible with different Apps like native sensor
- Real Time Fake Data Import
  - Fake videos/audio stream can be generated and imported in real time
- Transparent
  - Can’t easily be recognized by emulators detection or anti-hook

Video Injection Example

- Using Toshiba TC358749XBG chip to make a hardware module that can converts HDMI stream to MIPI CSI stream

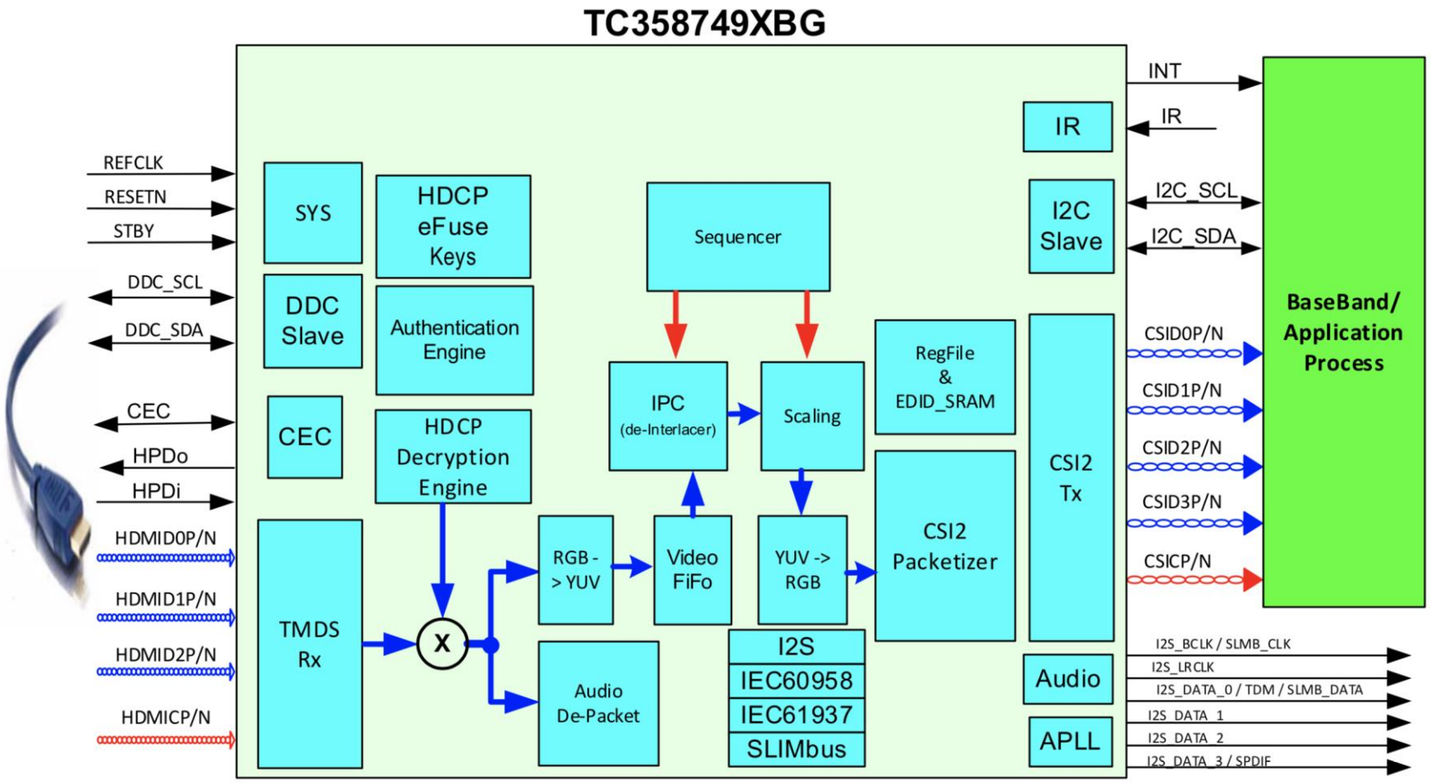
- Connecting the above module to an Android development board (RK3399) to form a complete video injection attack device

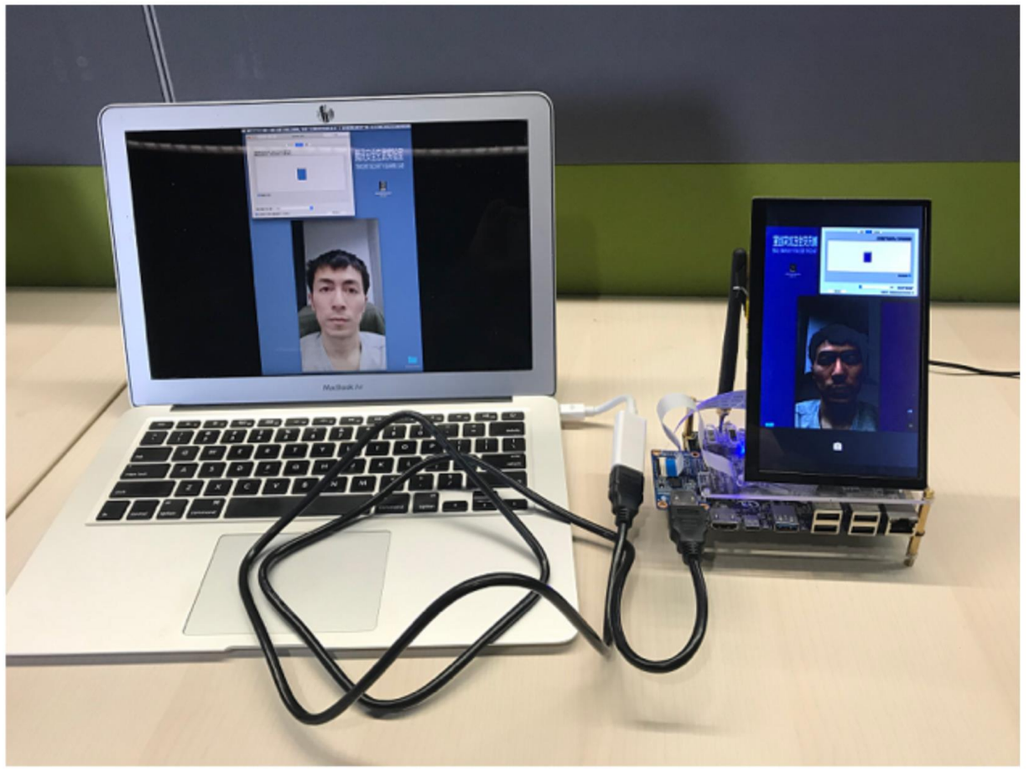
- Using the above device, we can disguise the HDMI output of a PC as a video stream captured by native camera



Video Injection Workflow

Video Injection Example

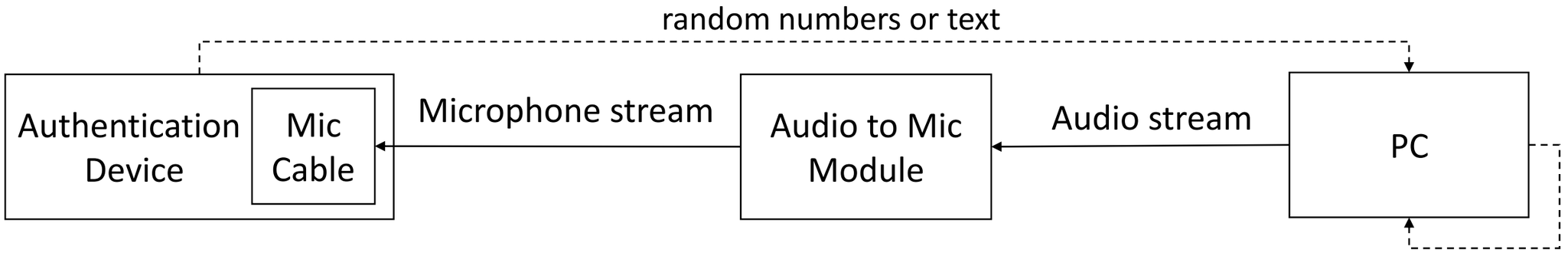




Video injection device based on TC358749XBG

Audio Injection Example

- Most voiceprint authentication systems accept authorized voice from the microphone cable
- Create a hardware module that converts the audio stream into a microphone stream
- Convert the audio stream from the sound card of PC into microphone stream and directly inject malicious voice into the authentication device



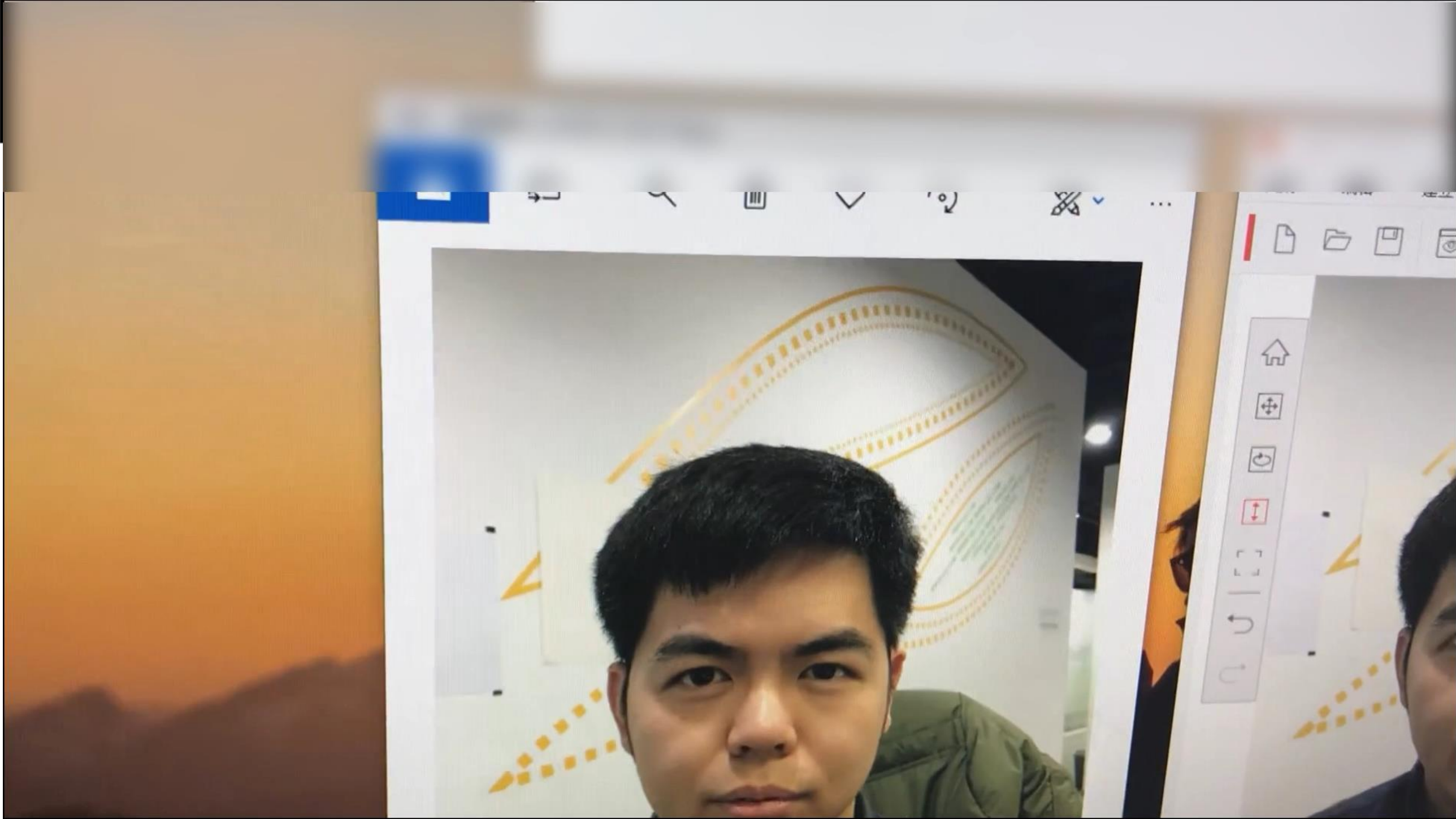
Audio Injection Workflow

Audio Injection Example

(a) For Android Devices (b) For iOS Devices

Audio injection device based on analog circuits and sound card

Demo



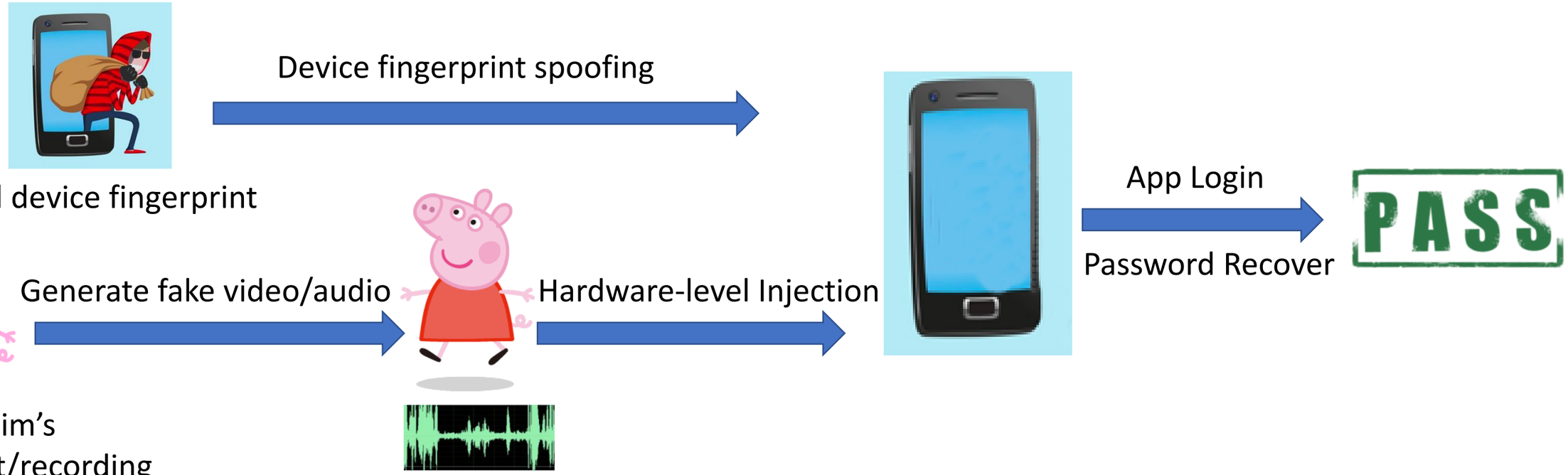
What if attacker can't physically contact the victim's equipment?

Why do device fingerprint spoofing ?

- Biometric authentication is disabled on a new device by default
  - Binding account with device fingerprint
    - IMEI, MAC address, Android ID, etc.
    - Customized ID based hardware info
- Device Fingerprint Spoofing
  - Step1: Reverse engineering on the algorithm of customized device fingerprint
  - Step2: Steal device info from victim’s device(eg. install a malicious app)
  - Step3: Cheat the server that we are using biometric authentication on an authorized device

Threat Model

- Device fingerprint spoofing to enable biometric authentication
- Hardware-level Injection to bypass liveness detection



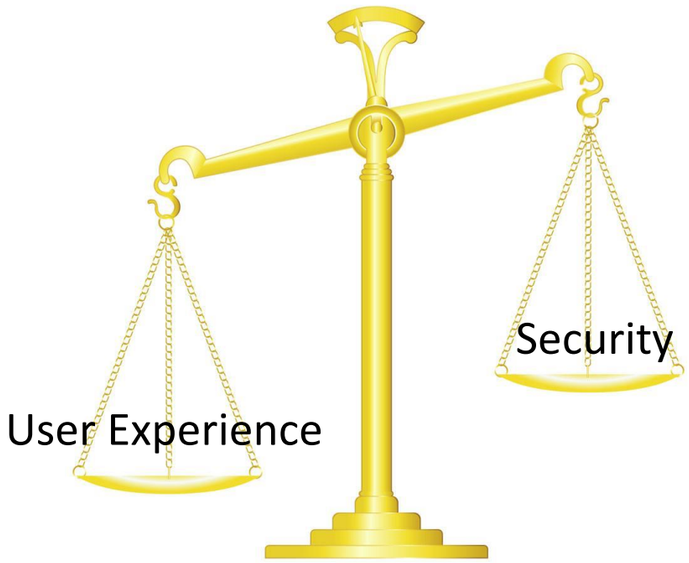
Outline

- Preliminary and Previous Studies
- Hardware-level Video/Audio Injection
- Insecure Recognition Scene Exploiting
- Mitigation
- Conclusion

Why do insecure recognition scene exploiting

Tradeoff between user experience and security under specific scenes

- Weak light environment (Facial)
- Sunshine environment (Facial)
- Glasses scene (Facial)
- Noisy environment (Voice)
- Accents and dialects scene (Voice)
- Unsharp fingerprint (Fingerprint)
- …



Attacker can induce liveness detection algorithm to walk into an insecure branch by creating above specific scene!

A case of insecure recognition scene exploiting

A funny scenario from the hit CTF-themed TV series “Go Go Squid!"

How to bypass the attention detection mechanism of Face ID ?

Challenges:

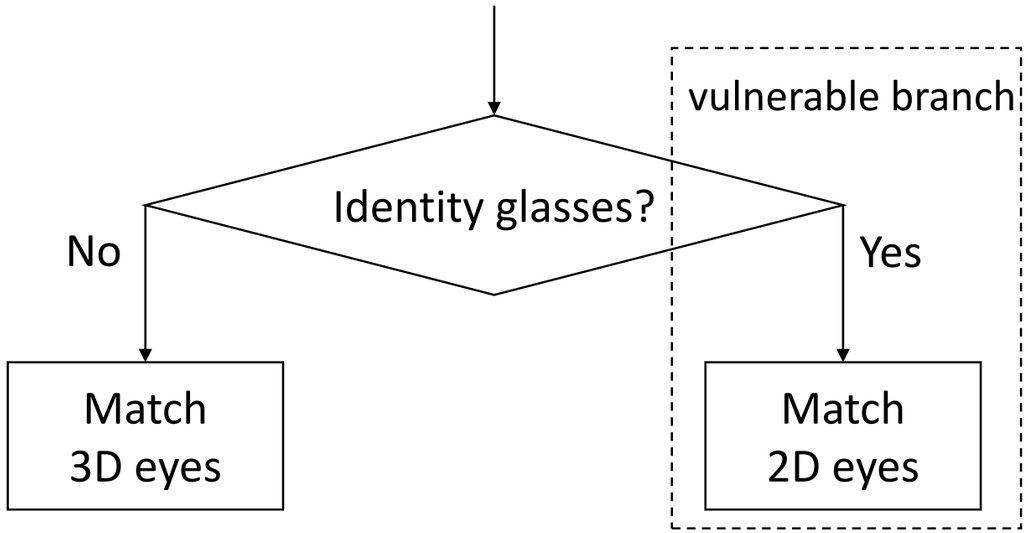
- Can't wake up the sleeping victim
- 3D eyes are difficult to forge
- Low cost & high success rate

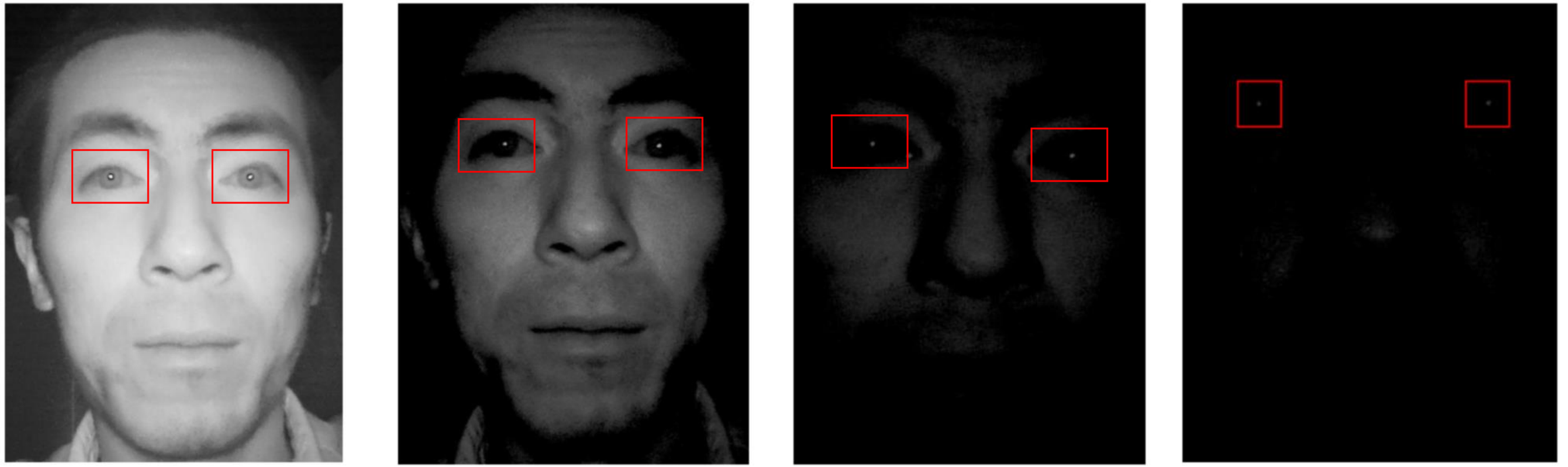
Preliminary ideas:

- Try to touch the victim as little as possible
- Find ways to replace 3D eyes with 2D eyes
- Try to simulate the state of eyes looking directly at phone

We found the following facts:

- Face ID allows users to unlock while **wearing glasses**
- Face ID no longer extract 3D info from the eye area when recognized glasses
- The abstraction of the eye is a black area with a white point in the center in the glasses scene

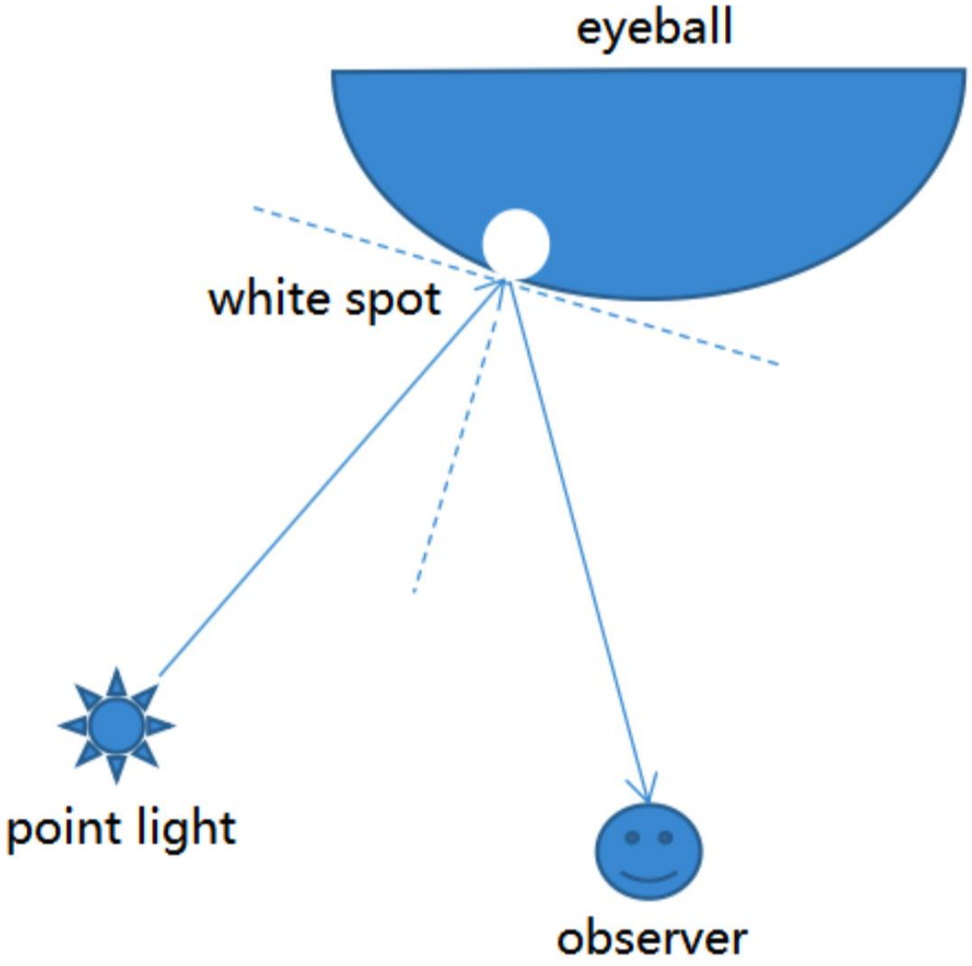


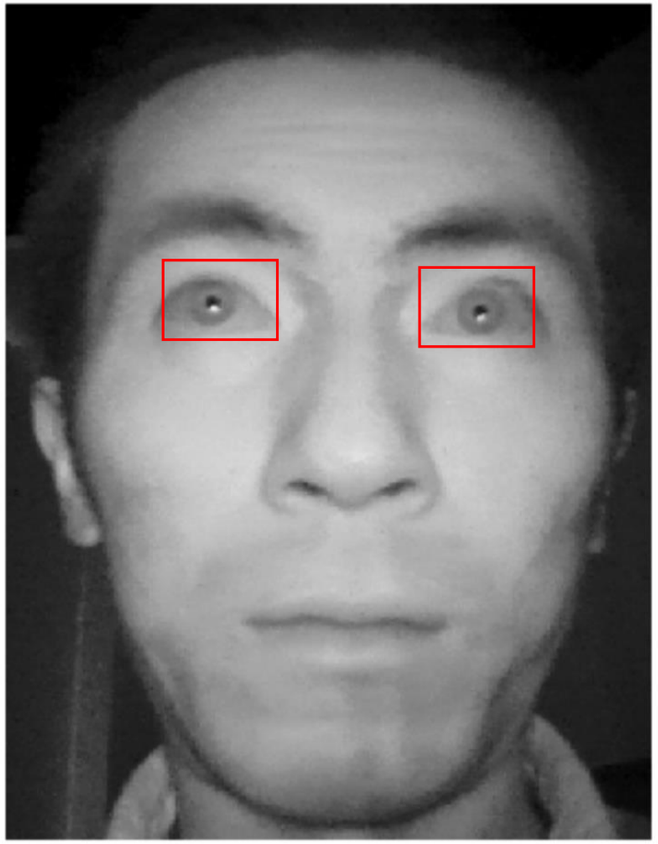


Bright light (corresponding to light sunglasses)

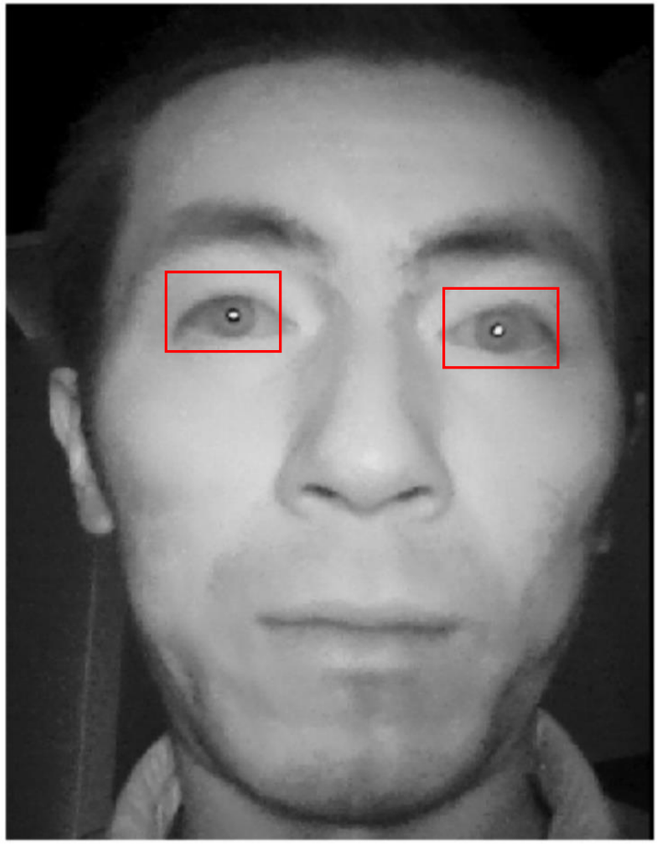
Weak light (corresponding to dark sunglasses)

In the dark environment, the abstraction of the eye is **a black area with a white point in the center**



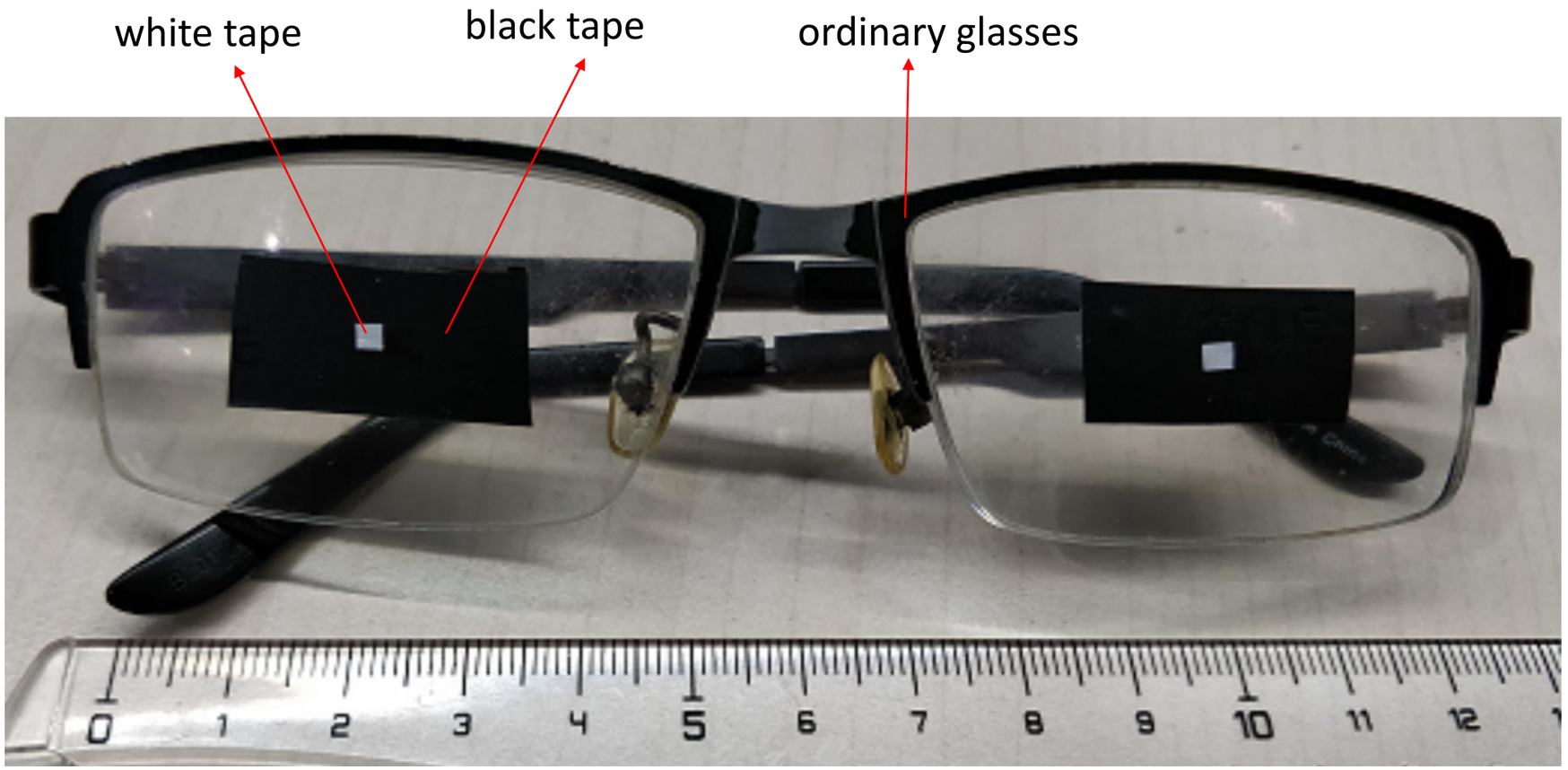


Eyes looking upwards



Eyes looking forward

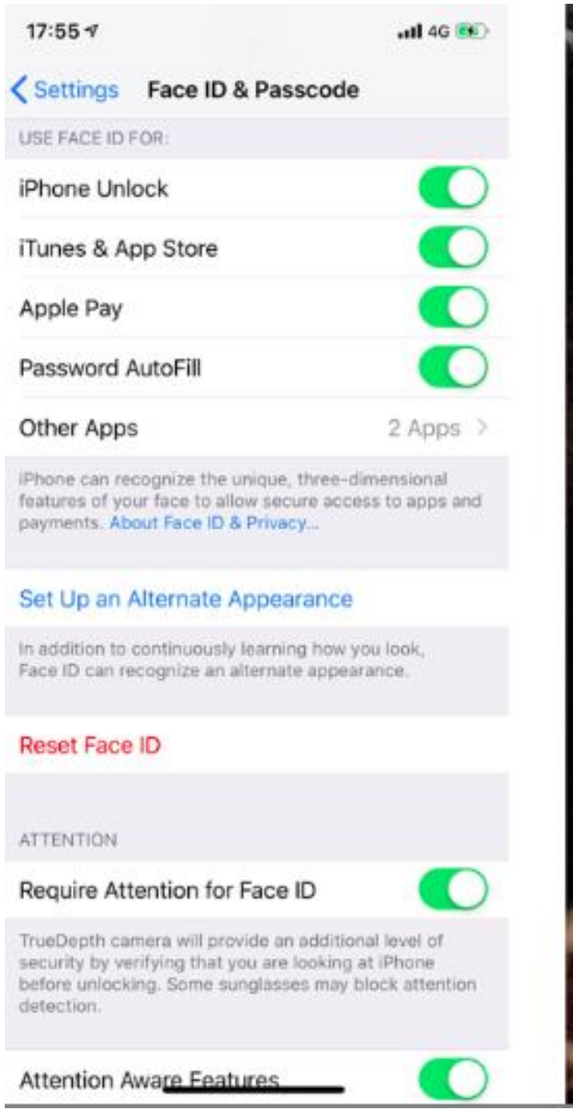
When unlocking phone, eyes must looks forward so **the white spot is in the center of the black area**



The Prototype of “X-glasses”

Features:

- Low cost
- High success rate
- Practical
- Less than two minutes
- Suitable for any victim


17:55
4G
Settings
Face ID & Passcode
USE FACE ID FOR:
iPhone Unlock
iTunes & App Store
Apple Pay
Password AutoFill
Other Apps
2 Apps
iPhone can recognize the unique, three-dimensional features of your face to allow secure access to apps and payments. About Face ID & Privacy...
Set Up an Alternate Appearance
In addition to continuously learning how you look, Face ID can recognize an alternate appearance.
Reset Face ID
ATTENTION
Require Attention for Face ID
TrueDepth camera will provide an additional level of security by verifying that you are looking at iPhone before unlocking. Some sunglasses may block attention detection.
Attention Aware Features


21:31

Demo

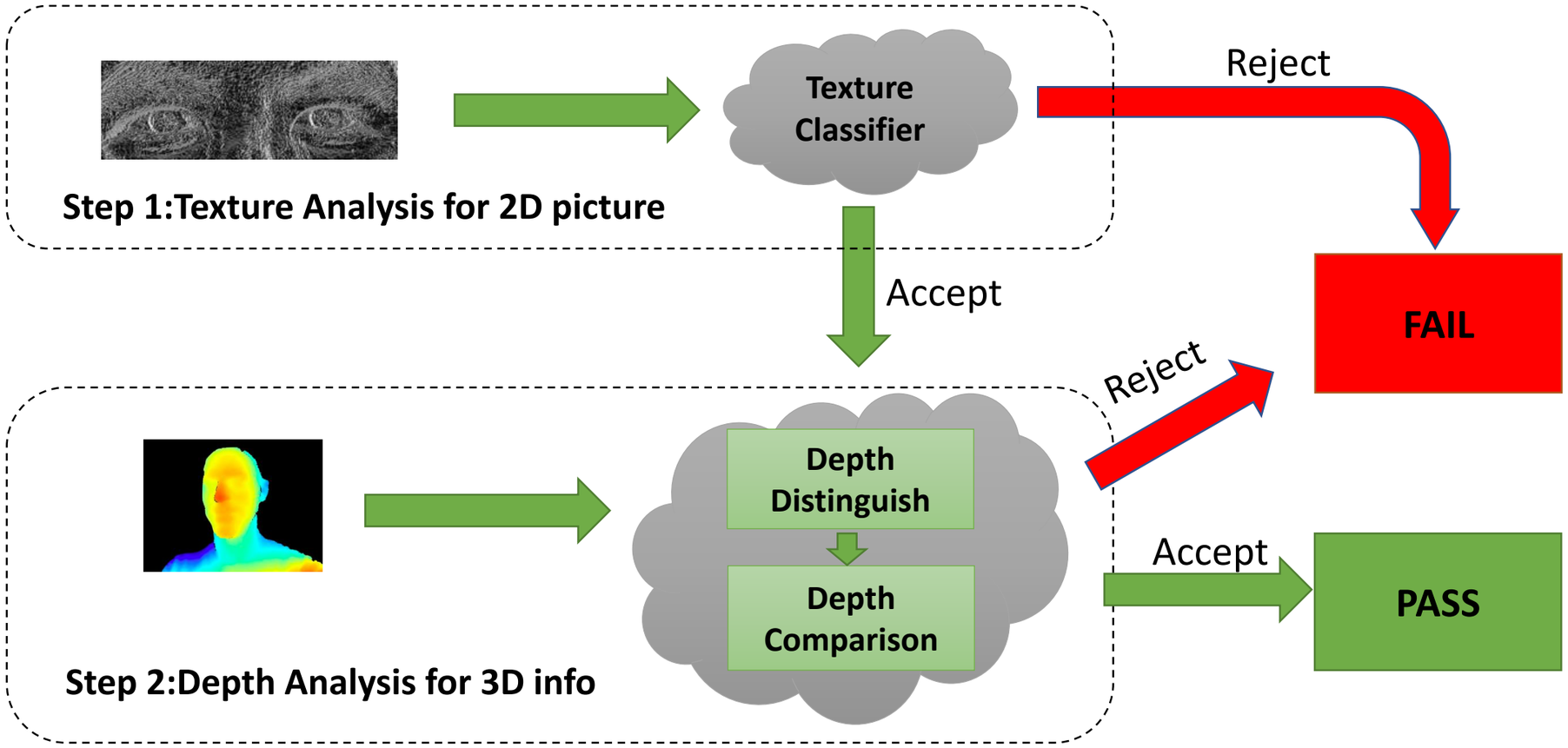
Outline

- Preliminary and Previous Studies
- Hardware-level Video/Audio Injection
- Insecure Recognition Scene Exploiting
- Mitigation
- Conclusion

Mitigation: for hardware-layer injection & device ID spoofing

- Add identity authentication for native camera
- Forbidden to accept authenticated voice from the microphone cable
- Increase the weight of video/audio synthesis detection
- Design a device binding mechanism to against device fingerprint spoofing

Mitigation: for X-glasses attack



Combine texture features with depth information to against X-glasses attack

Outline

- Preliminary and Previous Studies
- Hardware-level Video/Audio Injection
- Insecure Recognition Scene Exploiting
- Mitigation
- Conclusion

Conclusion

- We proposed a universal methodology for bypassing liveness detection
  - Injecting fake video/audio stream by evil hardware to hide attack media
  - Creating specific recognition scene to trigger the defect of liveness detection algorithm
- We found a new threat to app login or password recovery based on biometric authentication by hardware-level injection and device fingerprint spoofing
- We reversed the attention detection mechanism of Face ID and bypass it with X-glasses at ultra-low cost and high success rate

Thanks

Tencent Security Xuanwu Lab
@XuanwuLab
xlab.tencent.com

Tencent 腾讯

腾讯安全玄武实验室
TENCENT SECURITY XUANWU LAB