



Biometrics system hacking in the age of the smart vehicle

Kevin2600 & Wesley Li

Who are we

Wesley Li (Data analyst & AI Security Researcher)

Kevin2600 (Hardware & Wireless Security Researcher)

Notable Achievements:

2018 After-Market Digital Key reversing (DEFCON 26)

2020 Tesla-Model3 NFC Keyfob relay attack (DEFCON 28)

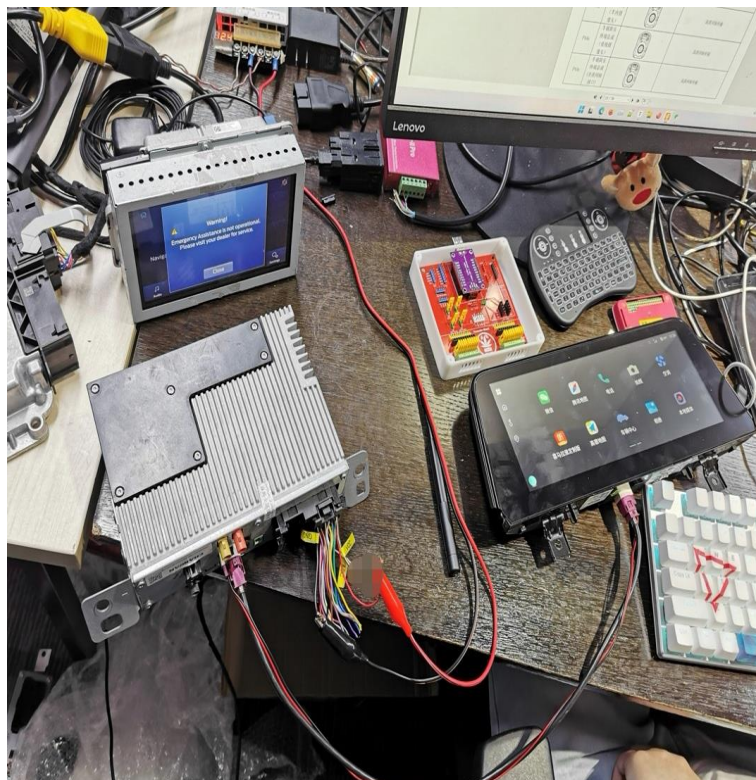
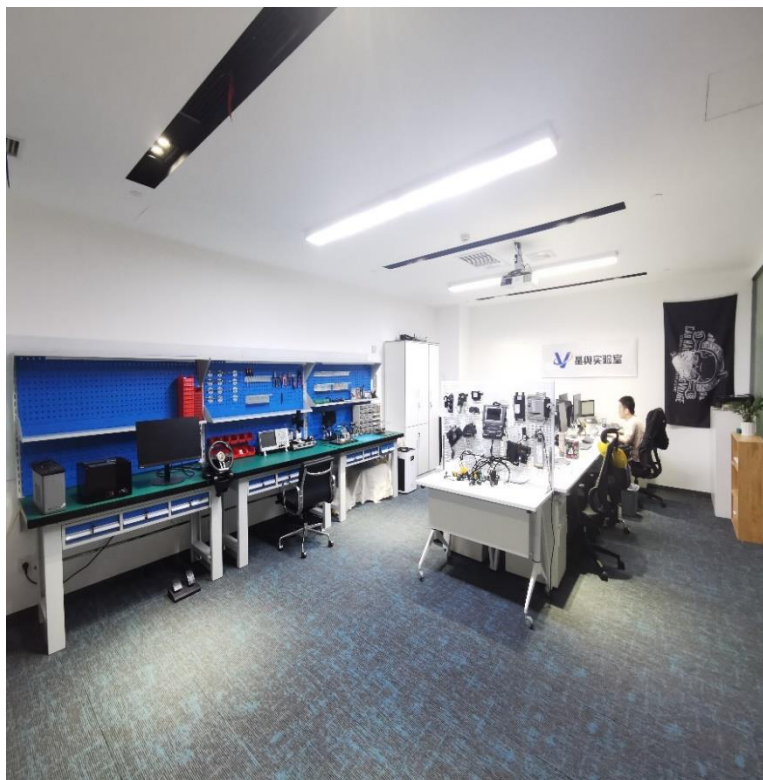
2021 Schneider-Electric EVlink Charging Station research (DEFCON 29)

2021 Rolling-Pwn attack research on Honda vehicles (rollingpwn.github.io/rolling-pwn)

2021 Bug on Model3/Y Made to the Tesla Hall of Fame (bugcrowd.com/QAX-StarV-Lab)



Star-V-Lab (星奥实验室)



Contents

Biometrics Authentication

Facial Recognition Spoofing

Speaker Recognition Spoofing

Biometrics Authentication



Multi-Factor Authentication (MFA)

Authentication using two or more factors to achieve authentication:

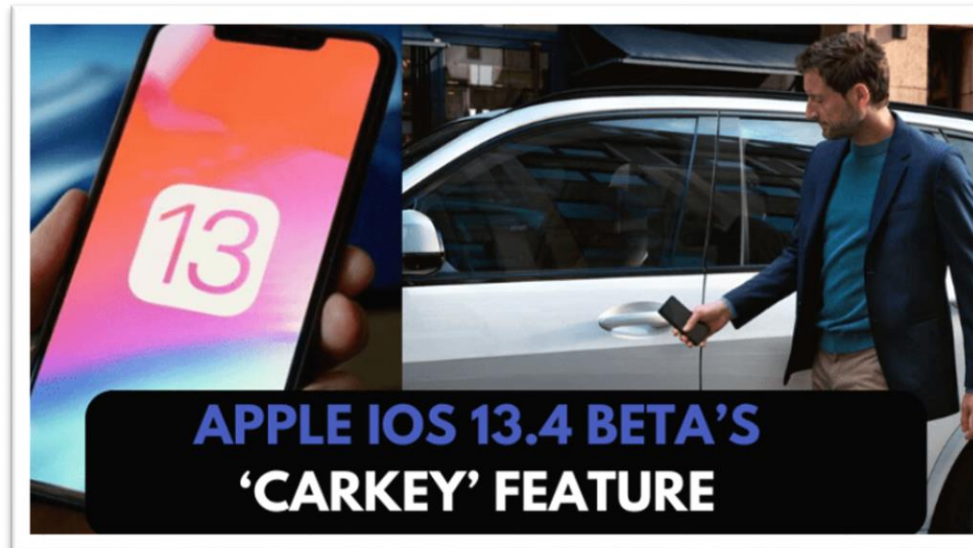
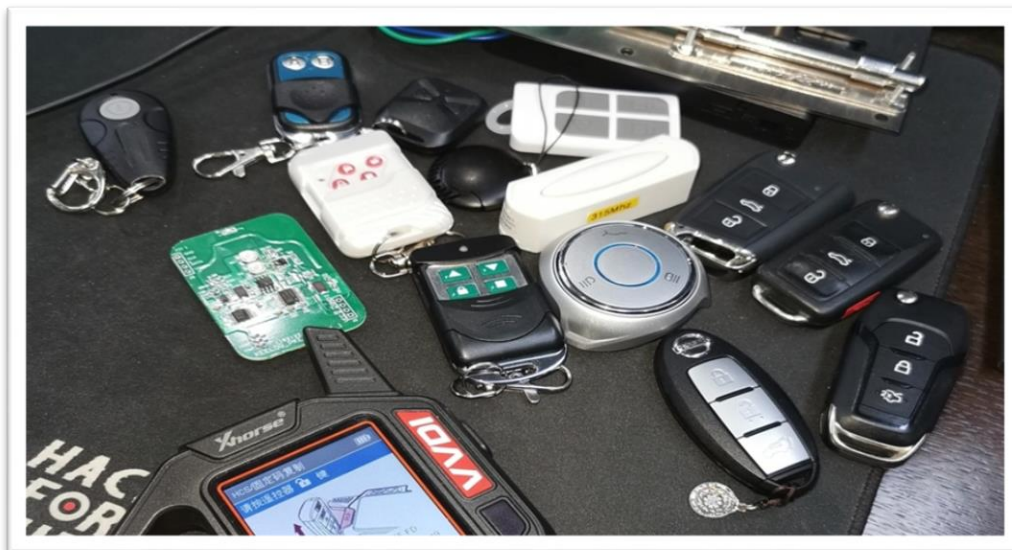
1: Something you are (Biometric; Fingerprints)

2: Something you have (Cryptographic identification device; Tokens)

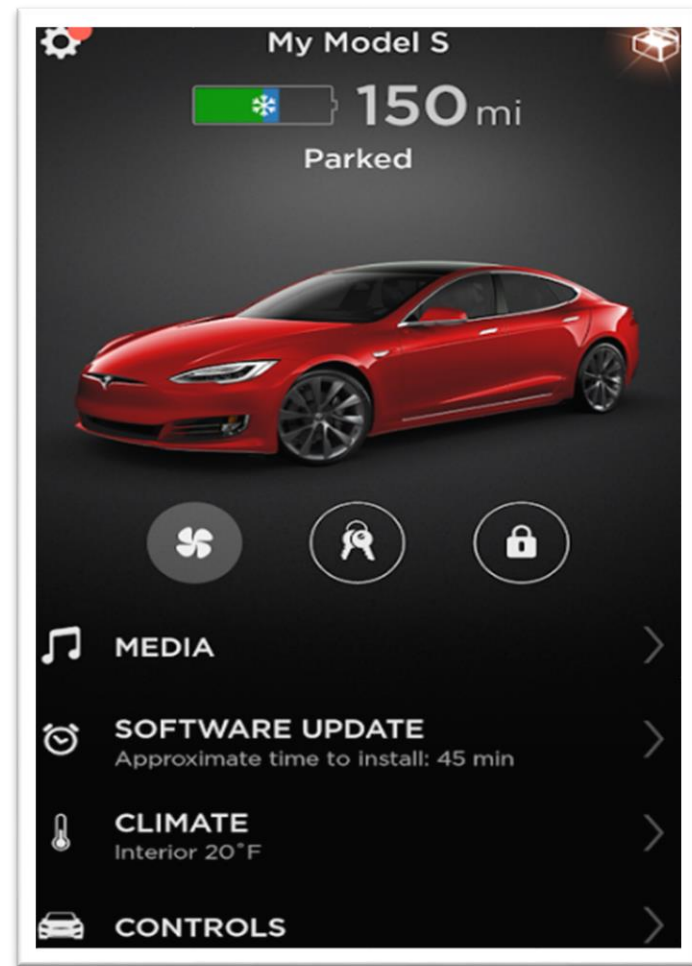
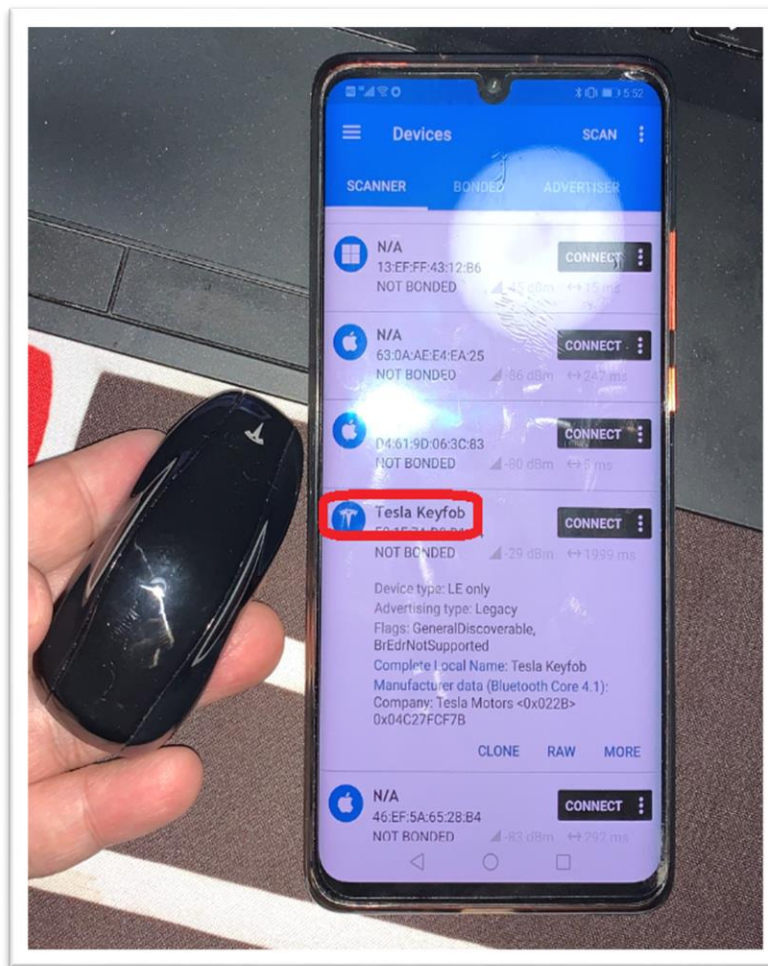
3: Something you know (Password; Personal identification number (PIN))

Source: CNSSI 4009-2015 under multifactor authentication

Something you have



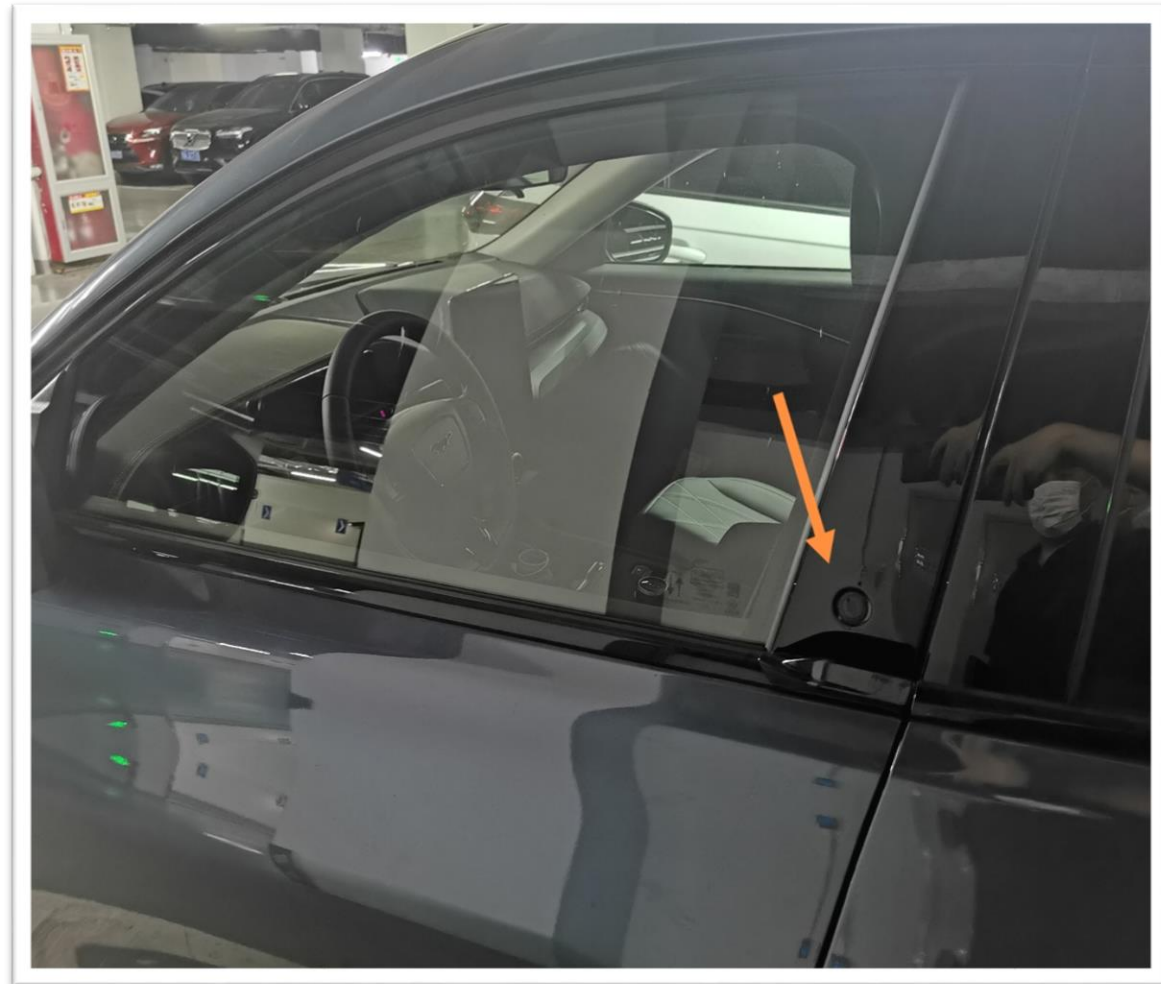
Something you have



Something you know



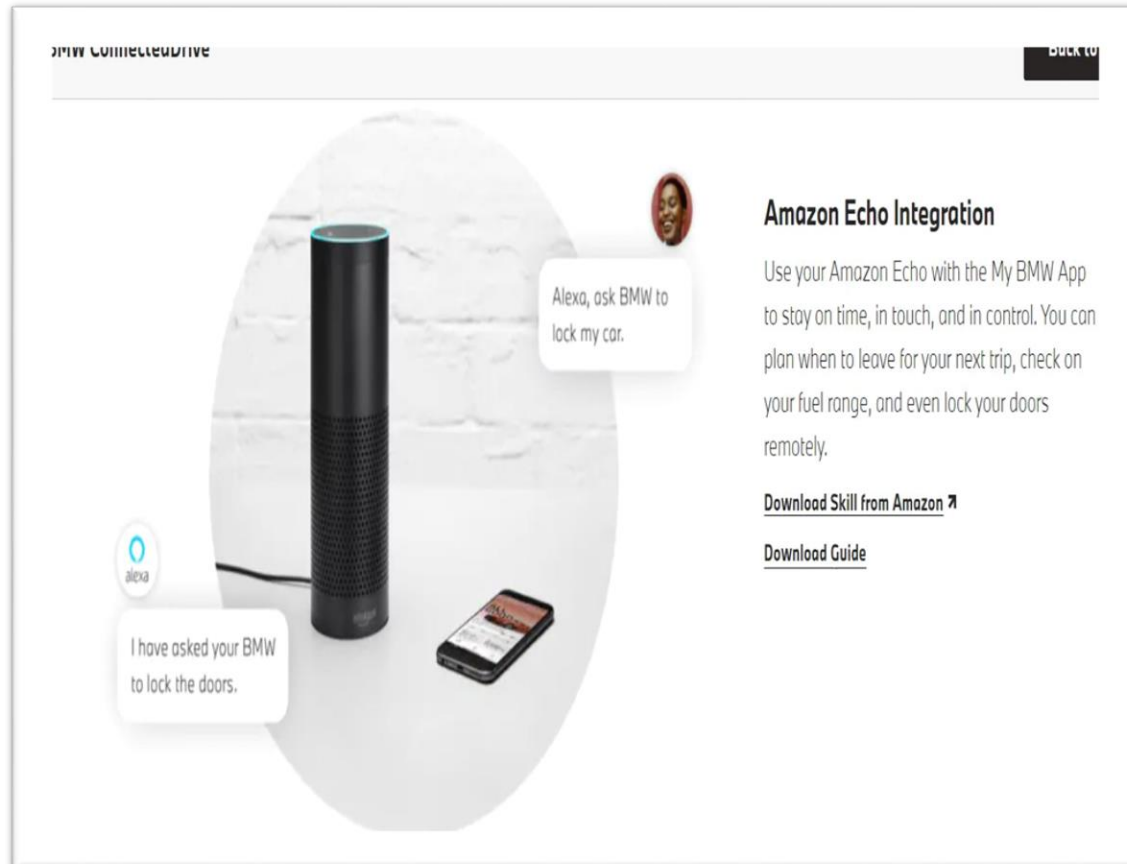
Something you are



Something you are



Something you are



The screenshot shows the BMW ConnectedDrive website. At the top left, it says "BMW ConnectedDrive" and at the top right, "BACK TO". The main content area features an Amazon Echo smart speaker and a smartphone. A speech bubble from the Echo says "Alexa, ask BMW to lock my car." and a response bubble from the phone says "I have asked your BMW to lock the doors." To the right of the image, the text reads: "Amazon Echo Integration Use your Amazon Echo with the My BMW App to stay on time, in touch, and in control. You can plan when to leave for your next trip, check on your fuel range, and even lock your doors remotely." Below this text are two links: "Download Skill from Amazon" and "Download Guide".

BMW ConnectedDrive

BACK TO

alexia

Alexa, ask BMW to lock my car.

I have asked your BMW to lock the doors.

Amazon Echo Integration

Use your Amazon Echo with the My BMW App to stay on time, in touch, and in control. You can plan when to leave for your next trip, check on your fuel range, and even lock your doors remotely.

[Download Skill from Amazon](#)

[Download Guide](#)



The advertisement features a dark grey Honda City 5th Gen car parked outdoors. In the foreground, a hand holds a smartphone displaying the My BMW app interface. The app screen shows a blue circular icon at the top, followed by the text "Tap or say 'Alexa'", and several menu items: "Start a list" (Add shopping items or things to do), "Create a reminder" (Remember things at a time or place), "Listen to music" (Play your favourite song or artist), and "Popular Skills" (including "Alexa, open Rajnikanth jokes" by Navvily & Ramona). A large white banner with blue and black text is overlaid on the bottom of the image, reading "HONDA CITY 5TH GEN ALEXA-POWERED CONNECTED CAR". In the bottom right corner, there is a blue circular logo with the white letters "HT".

HONDA CITY 5TH GEN

ALEXA-POWERED CONNECTED CAR



Speaker Recognition Spoofing

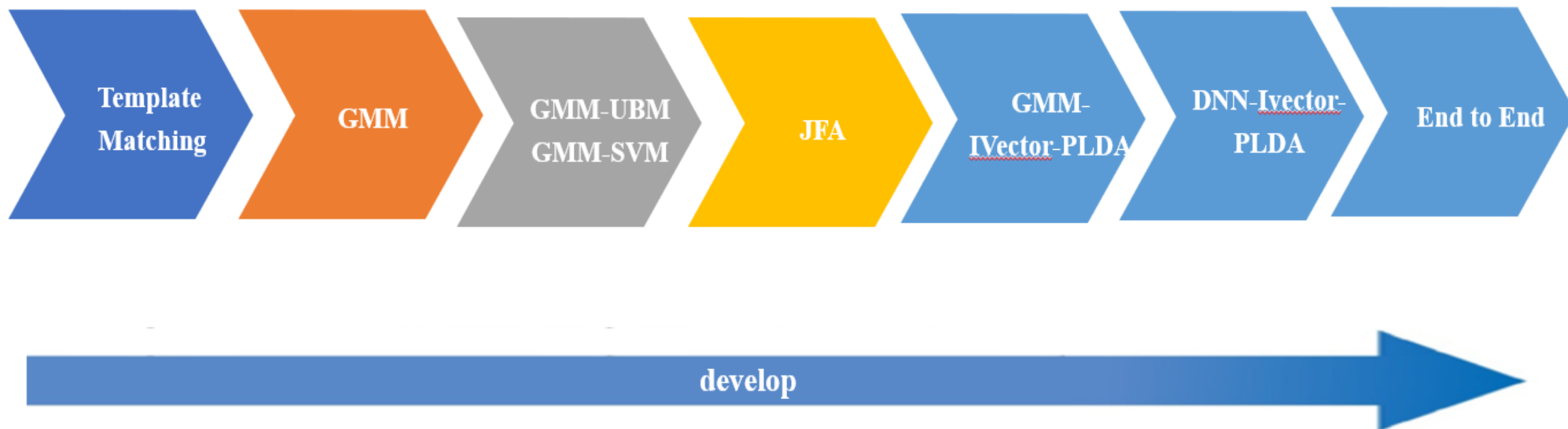


Speaker Recognition

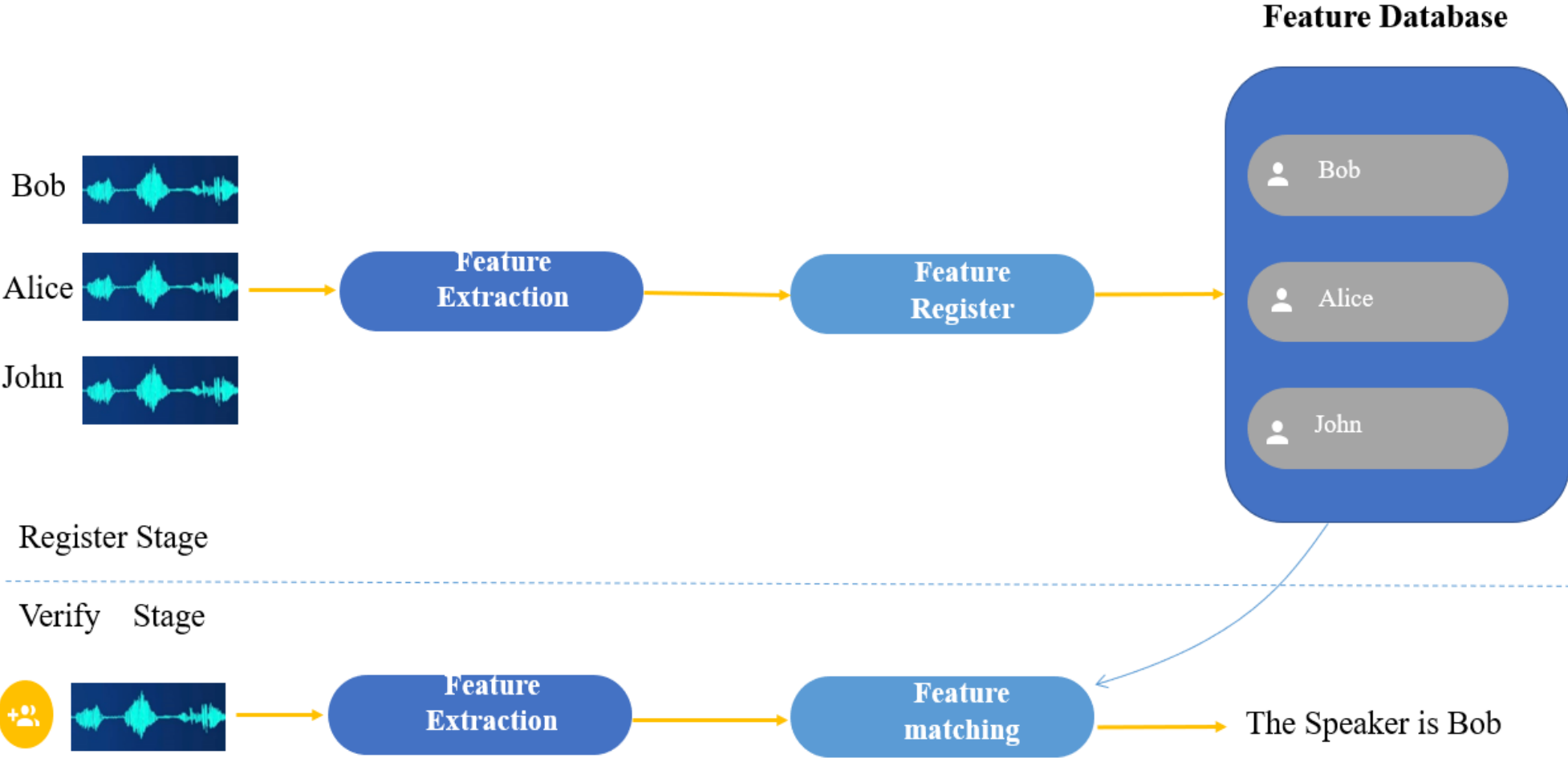
Speaker recognition is the identification of a person from characteristics of voices. It is used to answer the question "Who is speaking?" Recognizing the speaker can simplify the task of translating speech in systems that have been trained on specific voices or it can be used to authenticate or verify the identity of a speaker as part of a security process.

Wikipedia

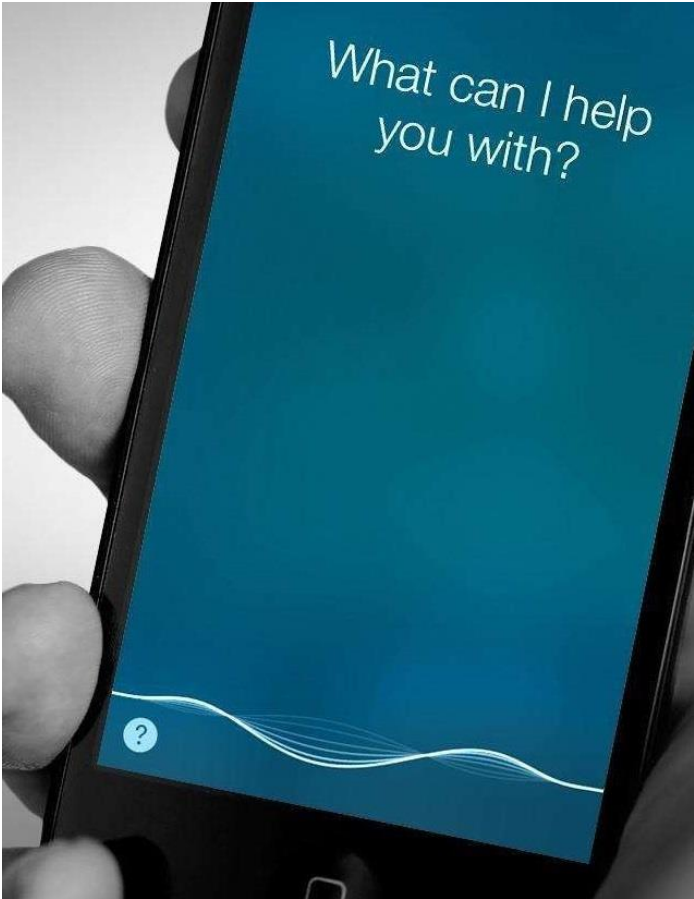
Speaker Recognition system 101



Speaker Recognition system 101



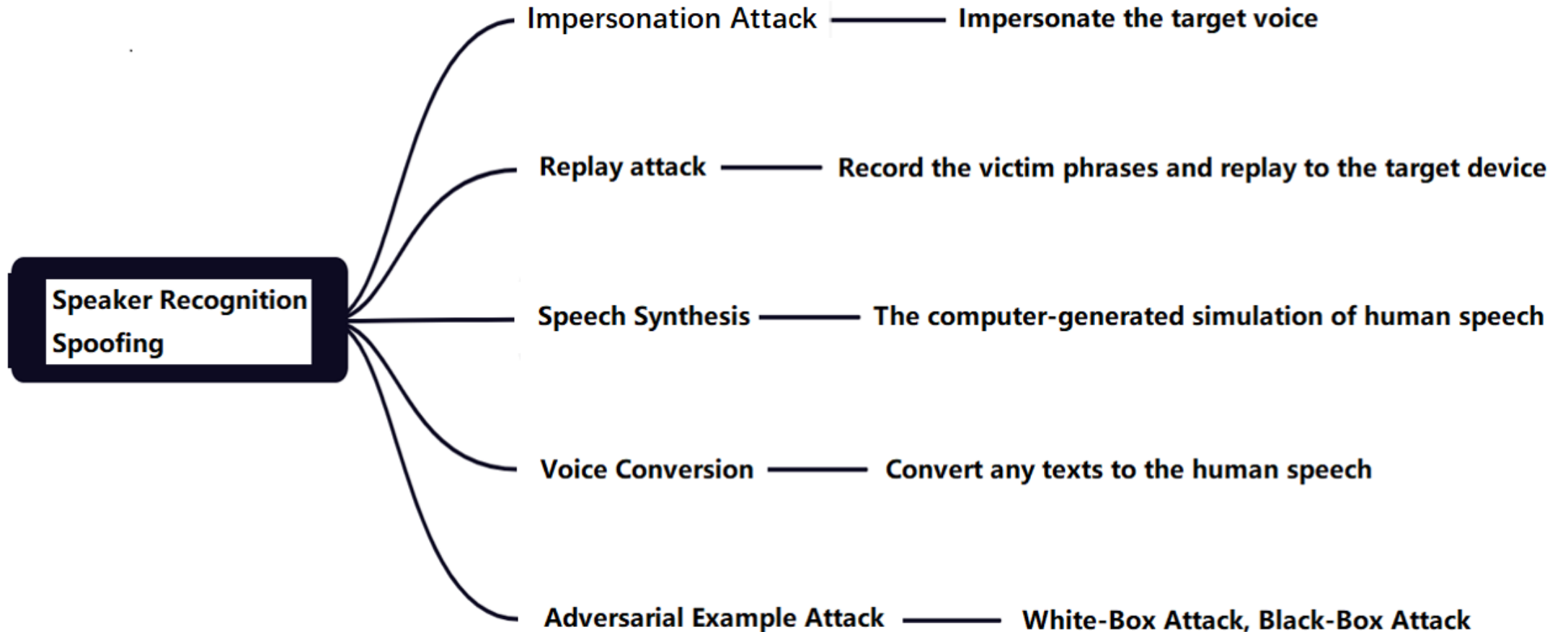
Speaker Recognition Applications



What Could Possibly Go Wrong ?

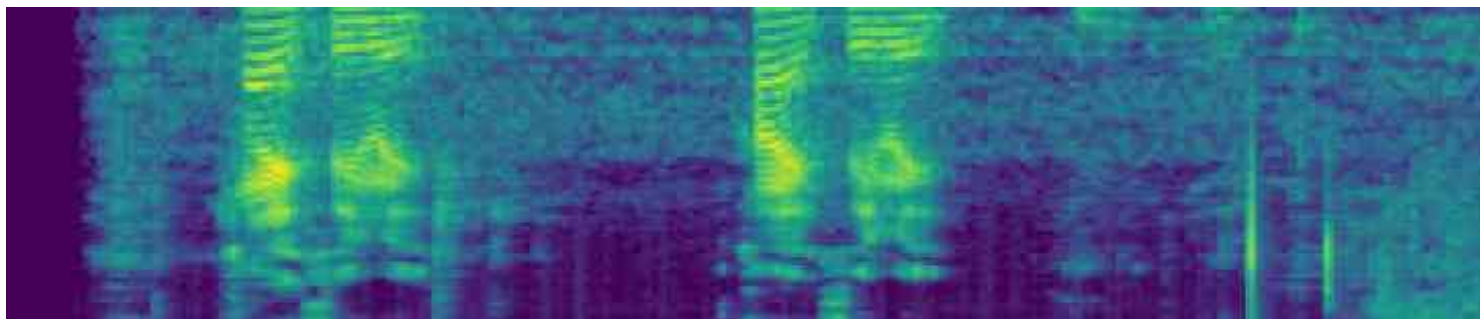


Speaker Recognition Spoofing Methodology

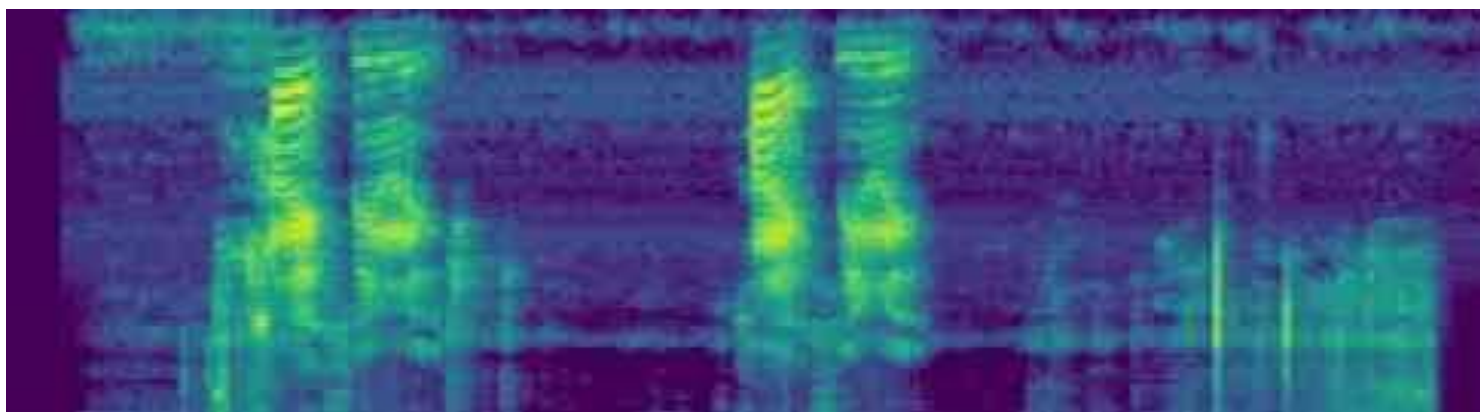


Speaker Recognition Replay Attack

Mel spectrogram of genuine voice data source



Mel spectrogram of replayed voice



Speaker Recognition Replay Attack (Stats App for Tesla)

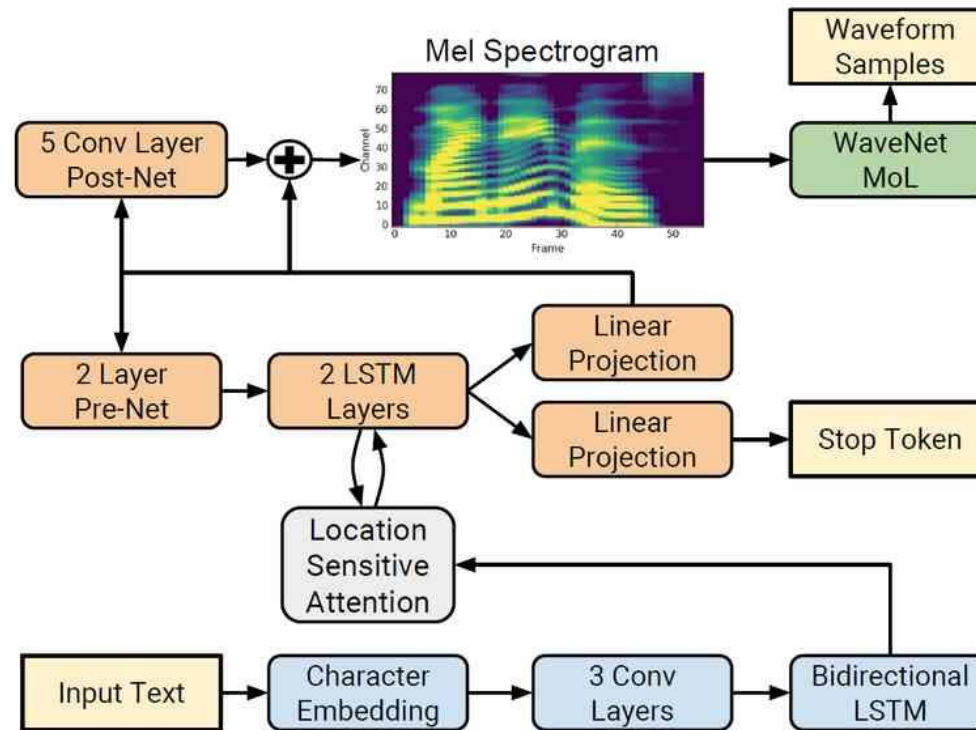
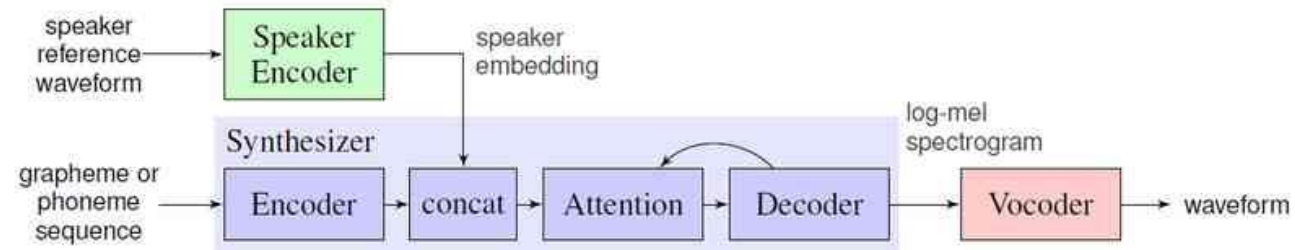


Speaker Recognition Replay Attack (Mystery App for Tesla)



Speaker Recognition
Replay Attack
Siri Unlock Tesla
星輿實驗室

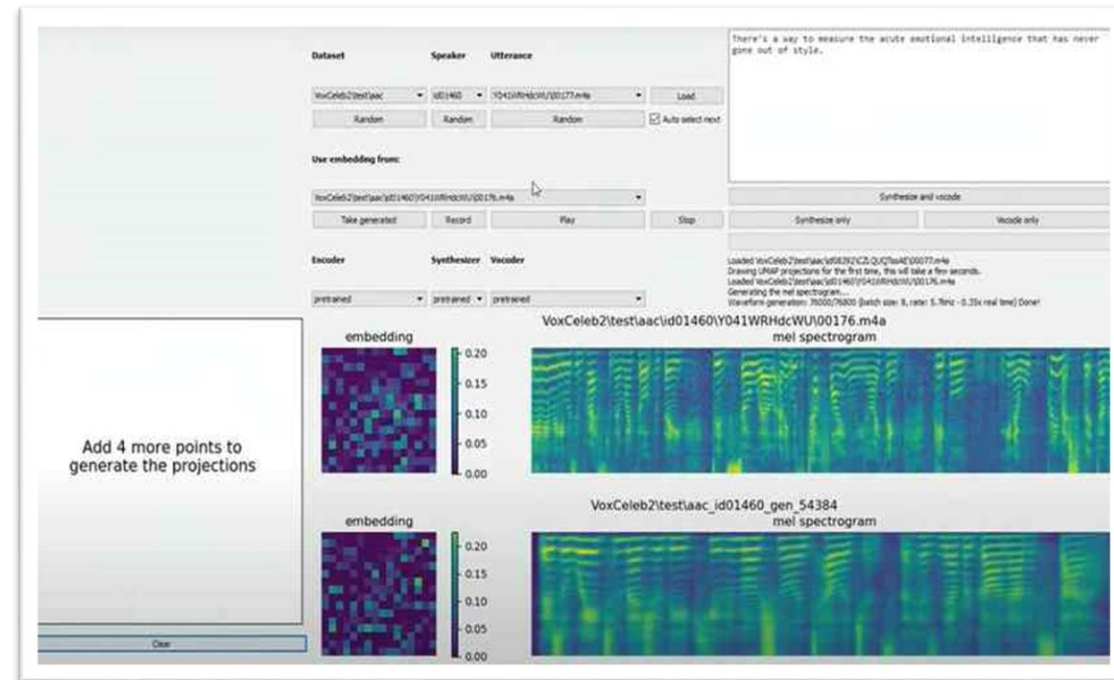
Speaker Recognition TTS (Text2Speech) attack



Speaker Recognition TTS attack

MockingBird [<https://github.com/babysor/MockingBird>]

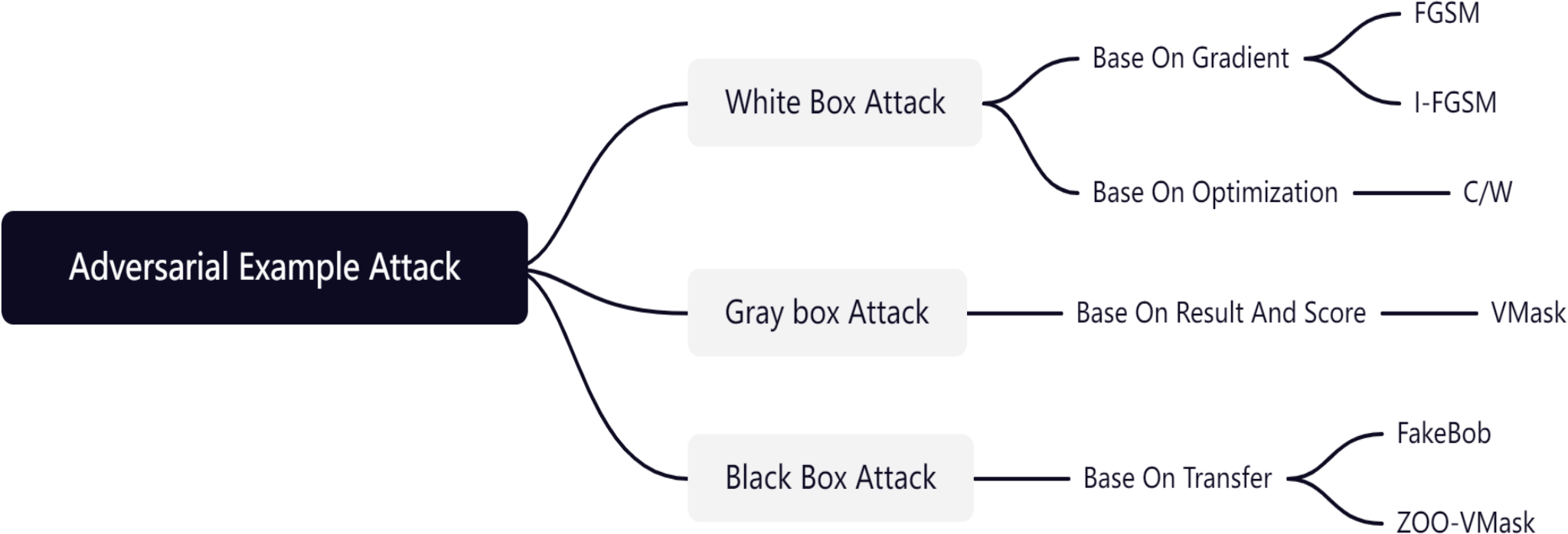
Real-Time-Voice-Cloning [<https://github.com/CorentinJ/Real-Time-Voice-Cloning>]



Speaker Recognition TTS attack



Adversarial Example Attack (Speaker Recognition)



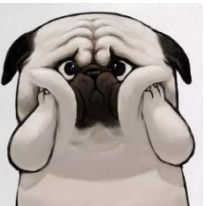
Adversarial Example Attack



Summary (Speaker Recognition Spoofing)

Recognition Procedure	Security Level	Spoofing Methods	Details
Fixed Vocabulary	Weak	Replay Attack, Speech Synthesis, Adversarial Example Attack	Easy to Attack
Fixed Vocabulary + Random Contents	Medium	Speech Synthesis, Adversarial Example Attack	By using the Fixed Vocabulary + Random Contents combination. It can prevent replay attack.
Random Contents	Strong	Speech Synthesis, Adversarial Example Attack	Hard to detect and more secure. But cost more system resources

Facial Recognition Spoofing

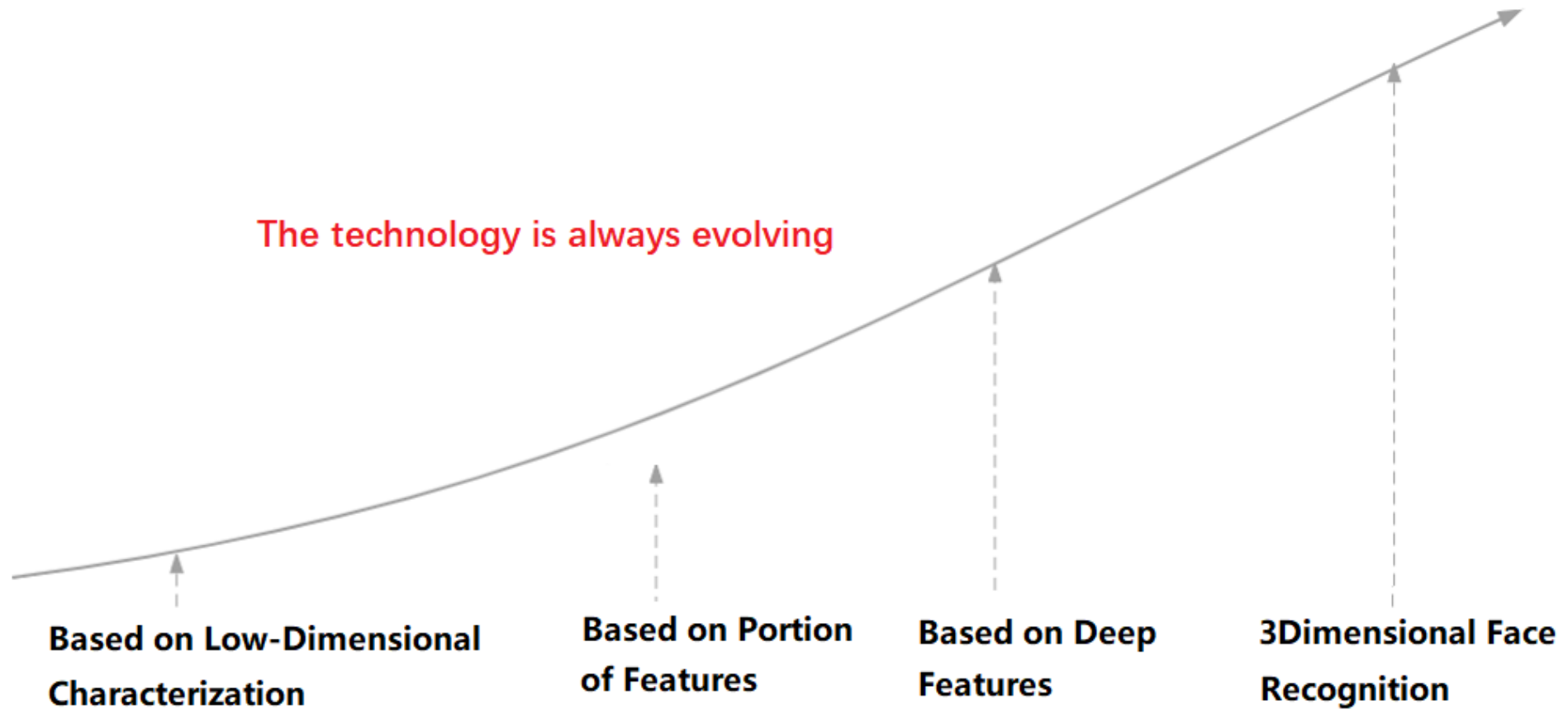


Facial Recognition

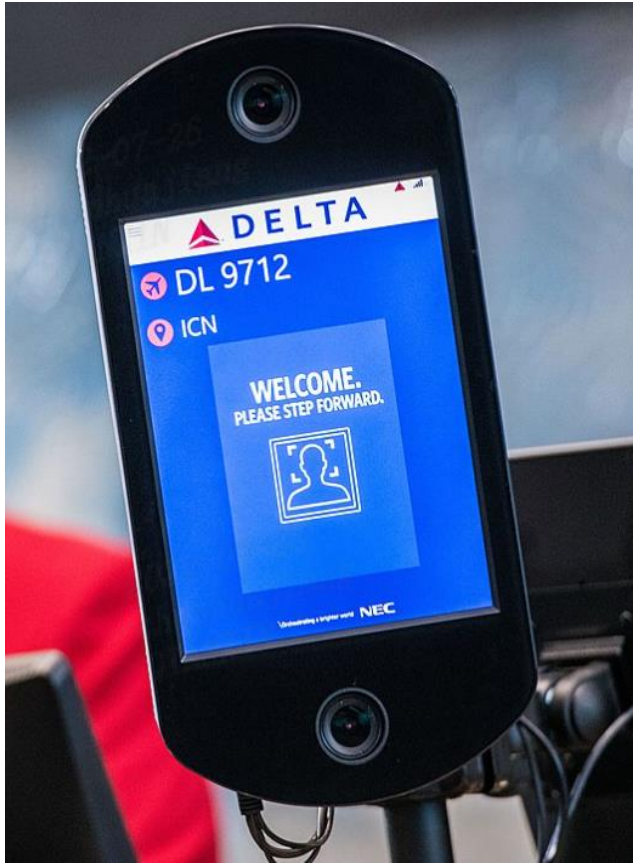
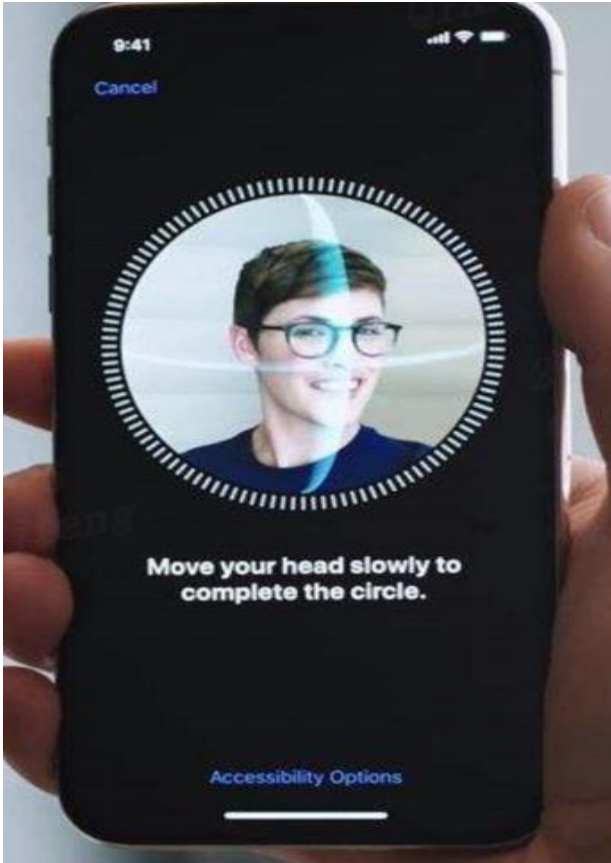
A technology capable of matching a human face from a digital image or a video frame against a database of faces, typically employed to authenticate users through ID verification services, works by pinpointing and measuring facial features from a given image

Wikipedia

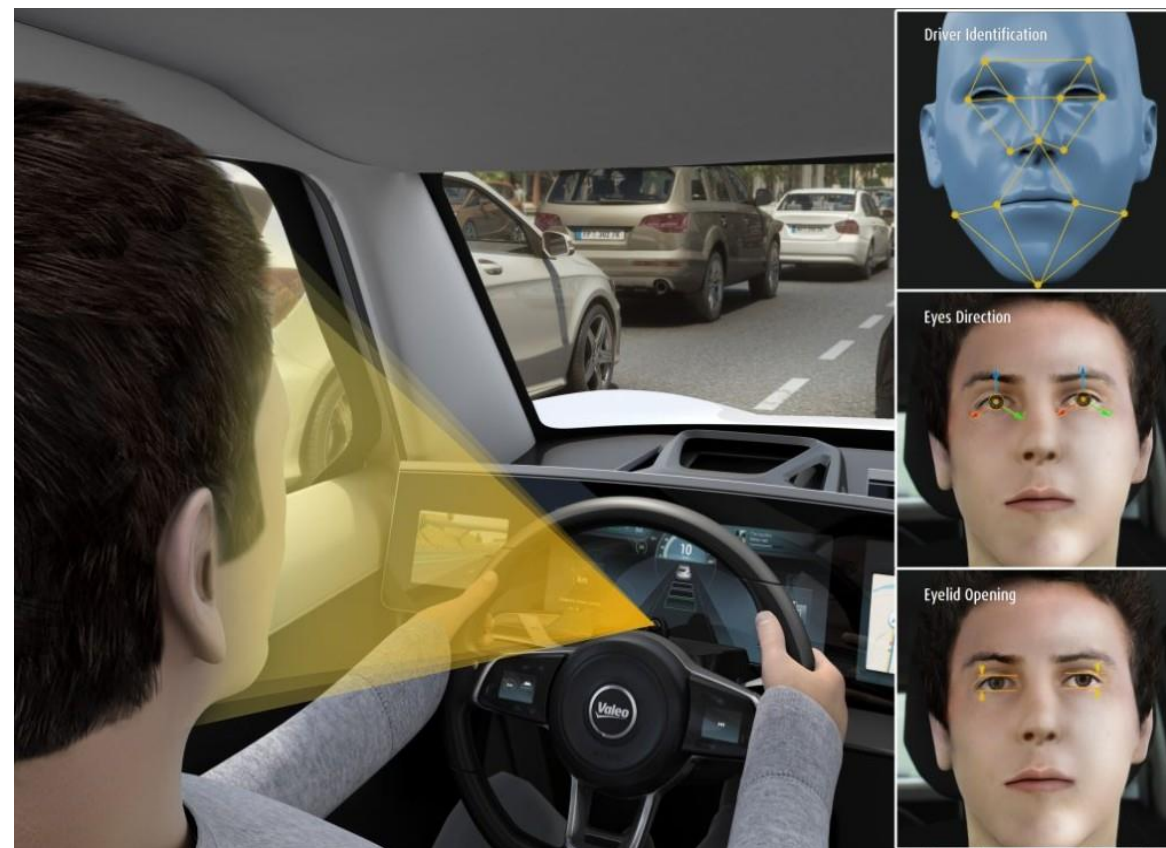
Facial Recognition Roadmap



Facial Recognition Applications



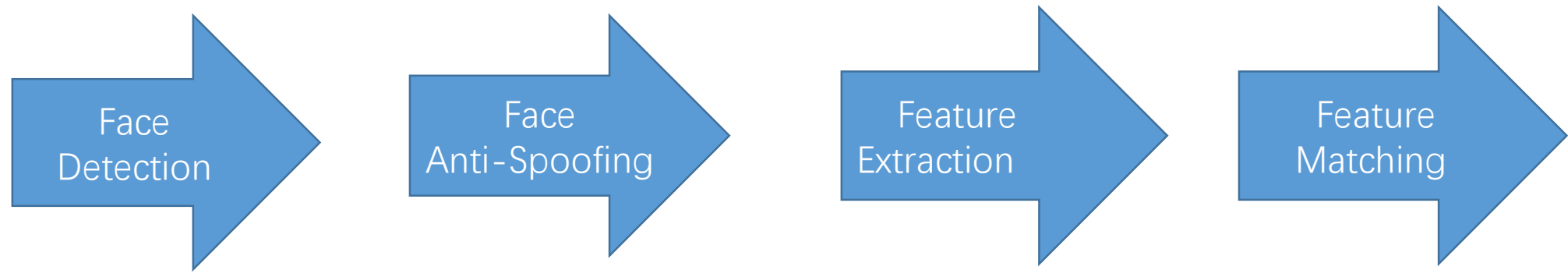
Facial Recognition Applications



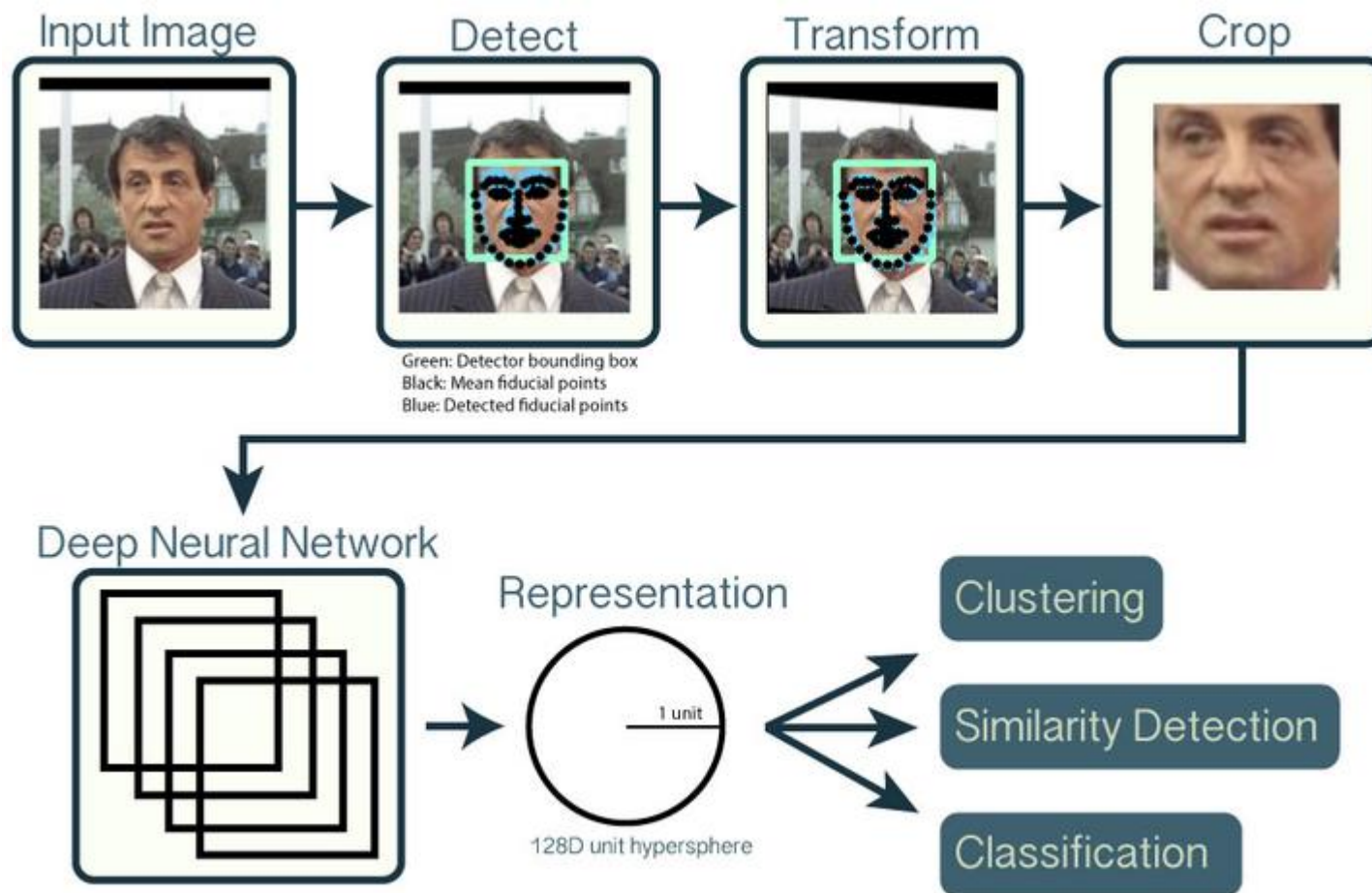
Facial Recognition Applications



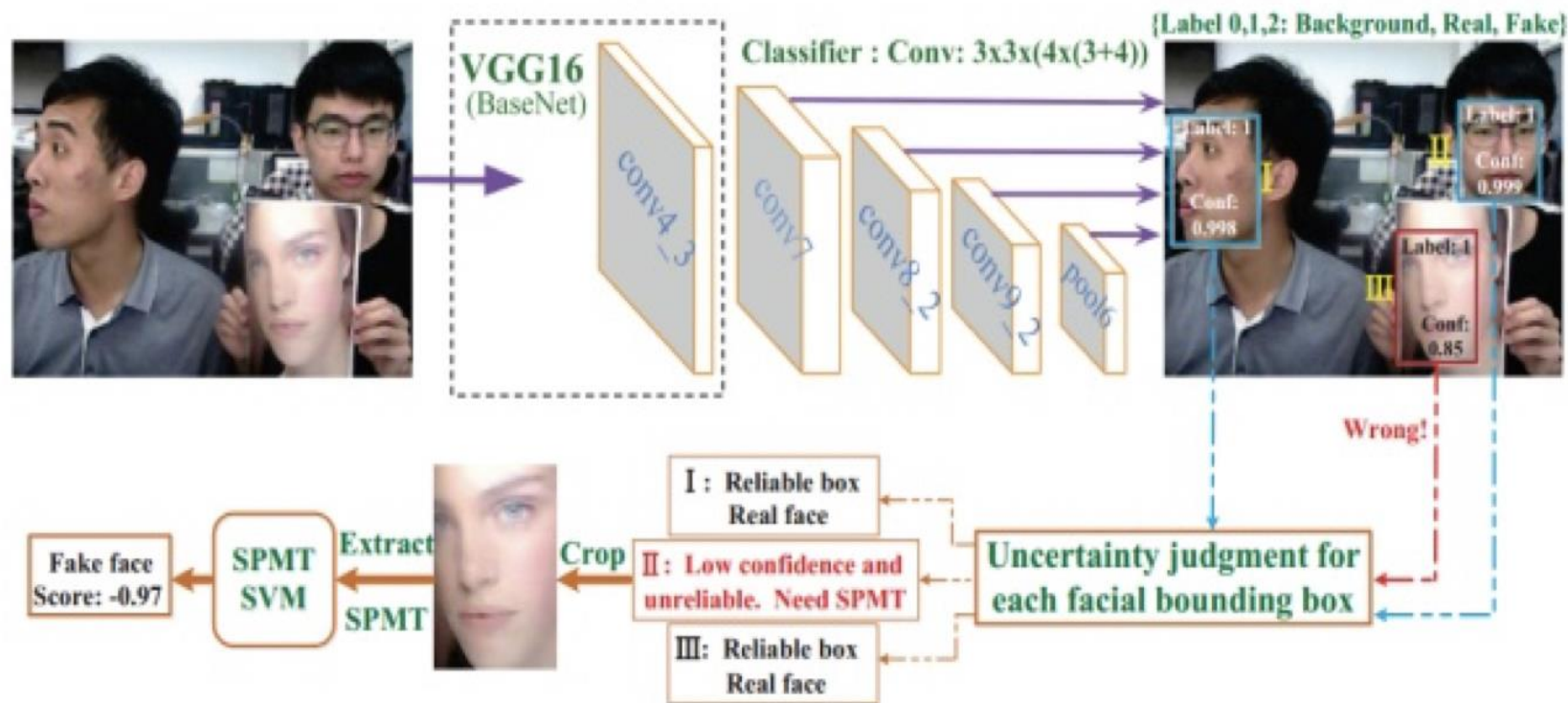
Facial Recognition Procedure



Facial Recognition Procedure



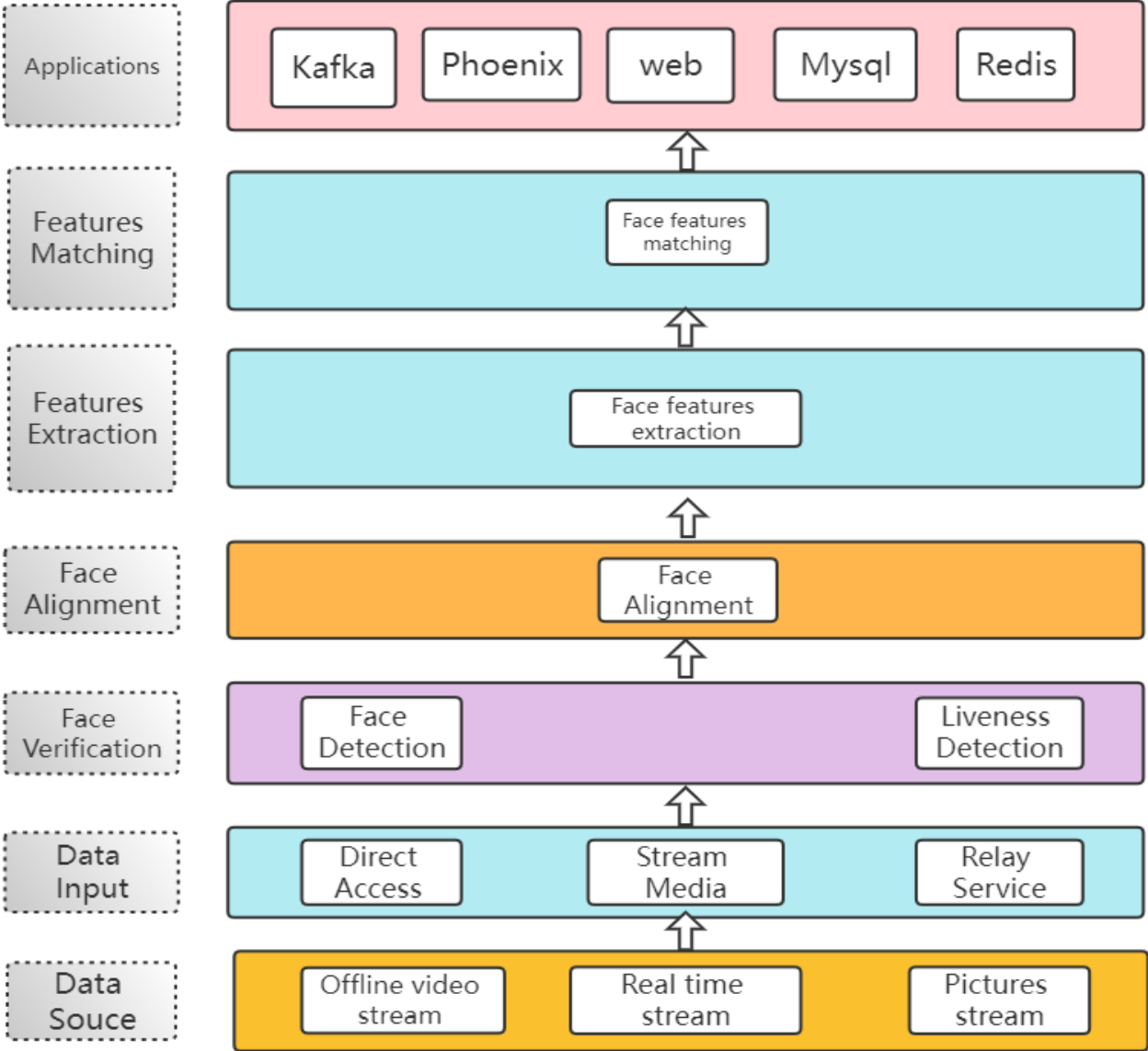
Facial Recognition Procedure



texture + SSD or binocular depth[10]

https://blog.csdn.net/SIGAI_CSDN

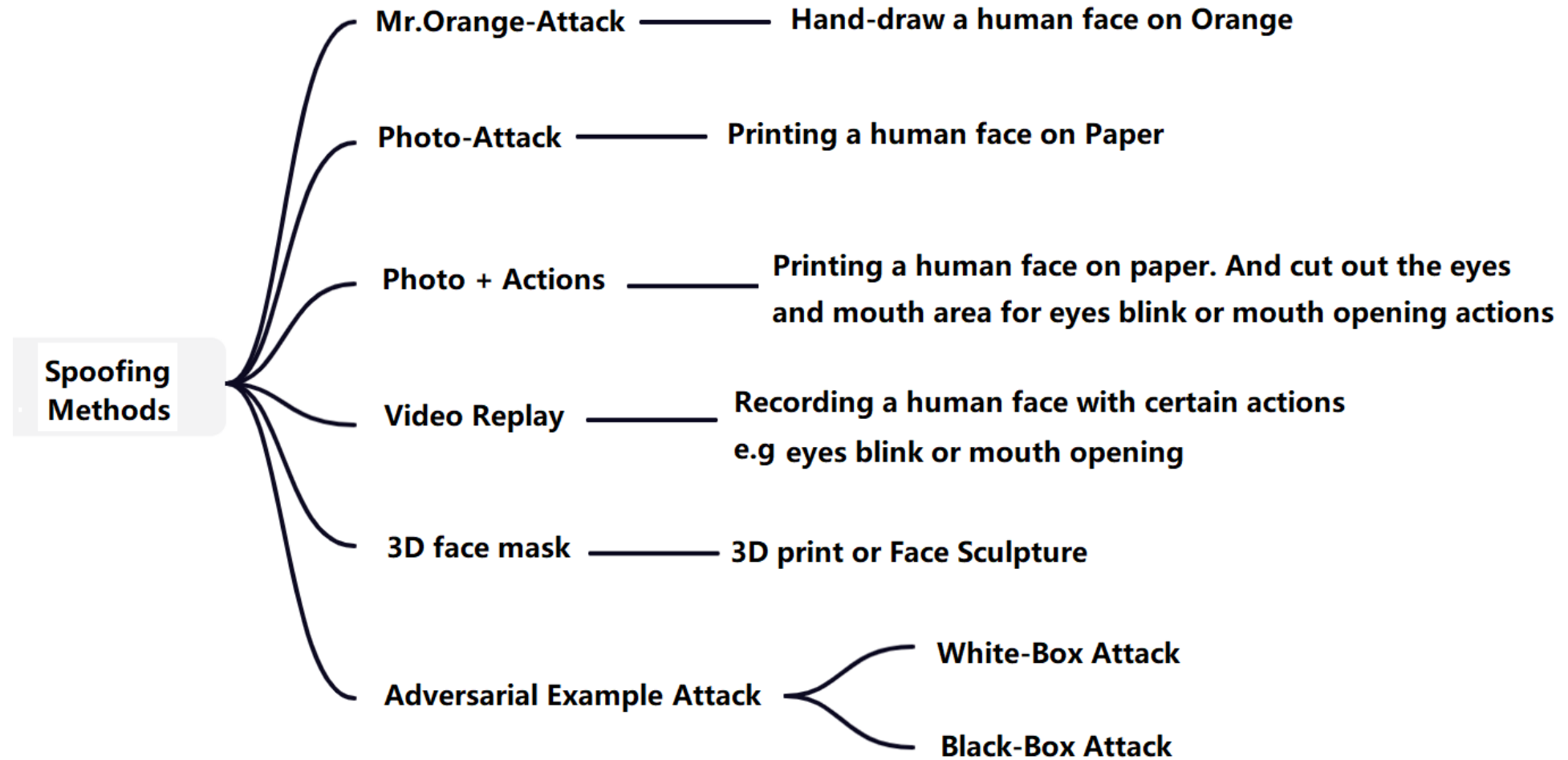
Facial Recognition Structure



What Could Possibly Go Wrong ?



Facial Recognition Spoofing Methodology



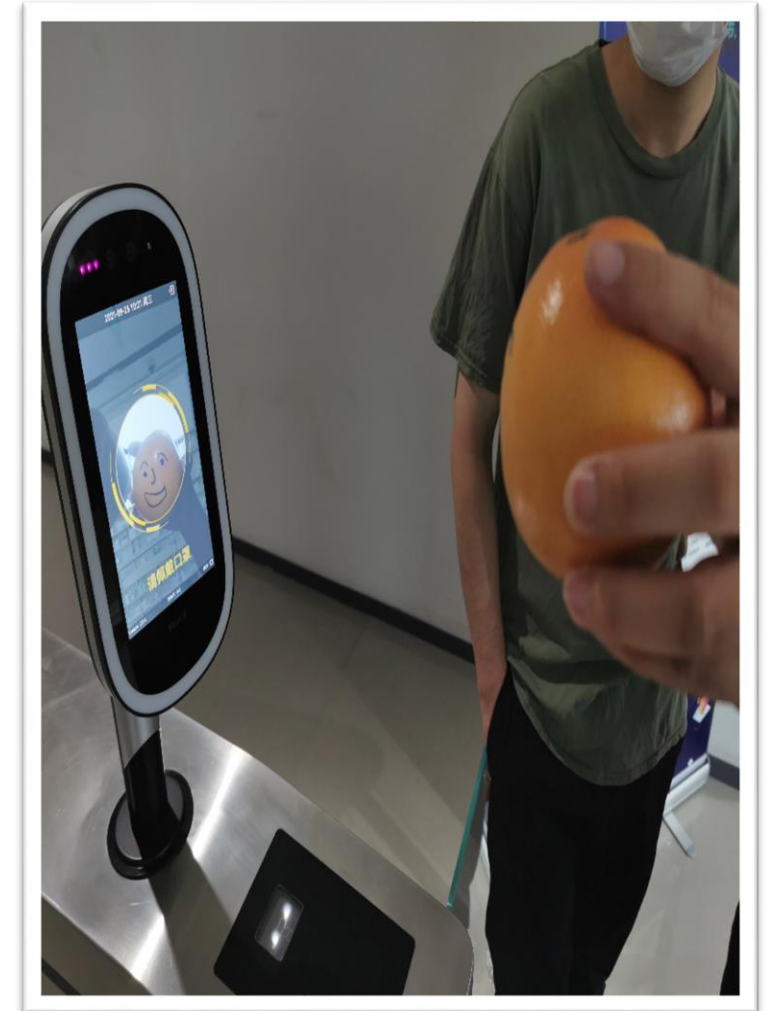
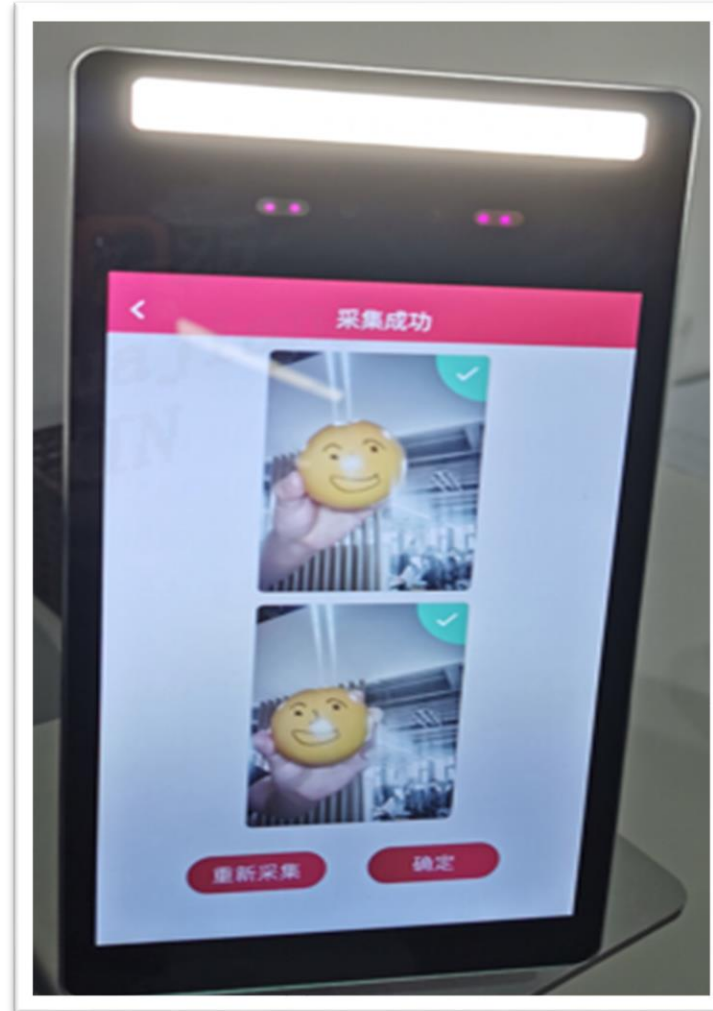
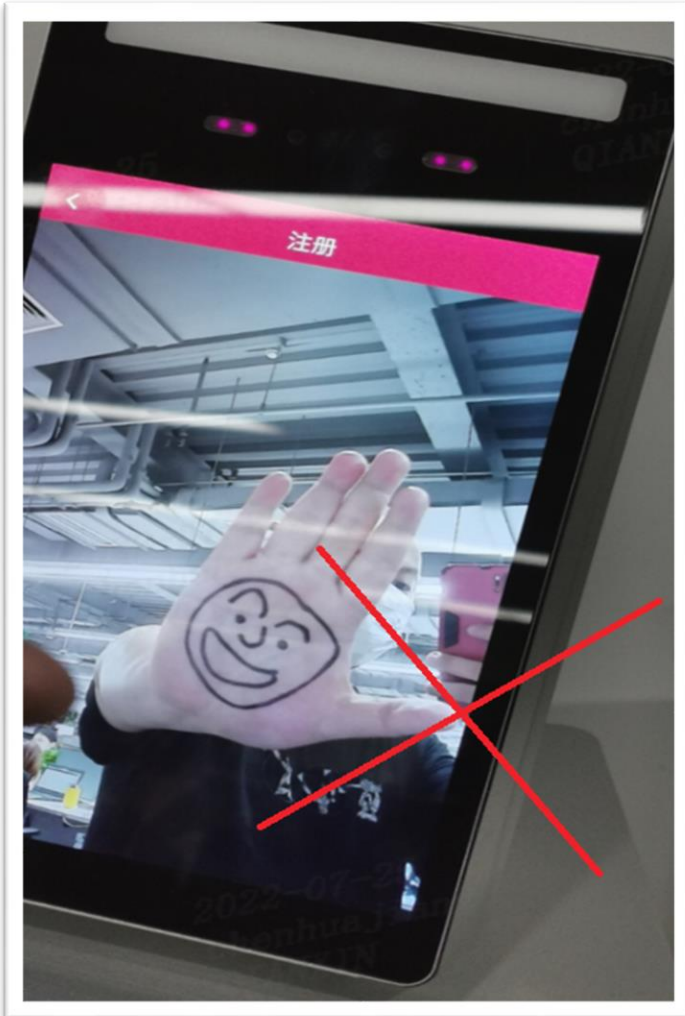
Face Photo Attack – Hive Box



Mr. Orange Attack



Mr.Orange Attack



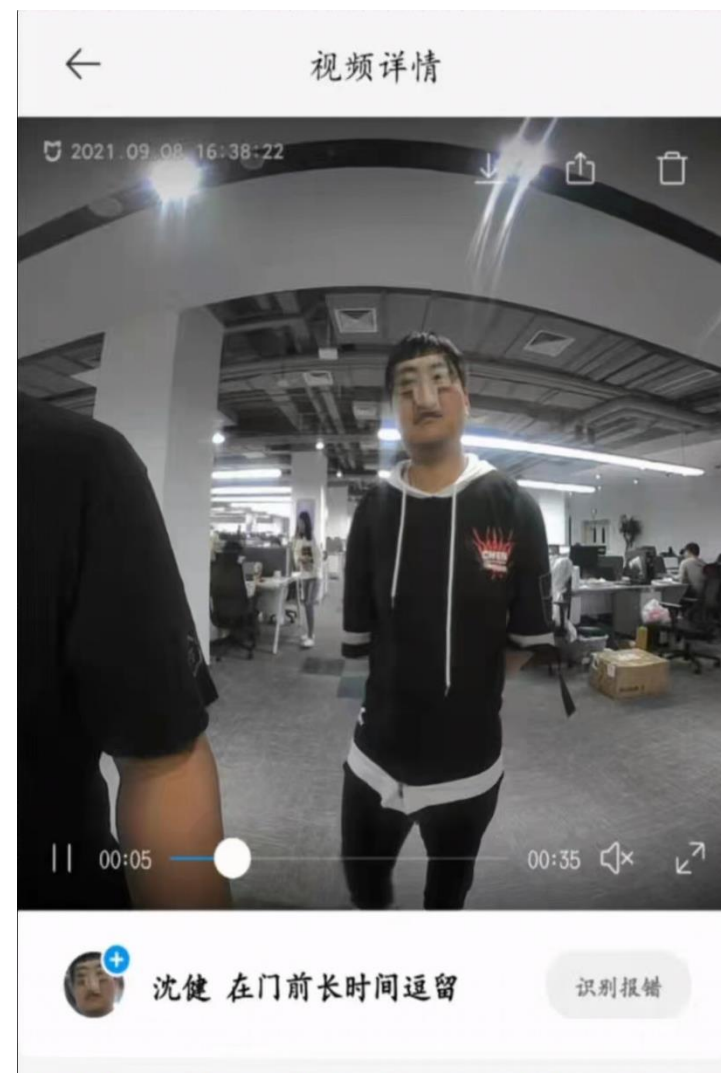
Mr.Orange Attack – Xiaomi Smart Lock



Face Photo Attack – Xiaomi Smart Lock



Face Photo Attack – Xiaomi Smart Lock



Face Anti-Spoofing



Face under IrDA for human



Face under IrDA on Paper



Face under IrDA on Mobile

Face Anti-Spoofing



Face Sculpture Attack



Face Sculpture Attack – Huawei P30 Pro



Adversarial Example Attack (Face Recognition)



"panda"

57.7% confidence

+ ϵ



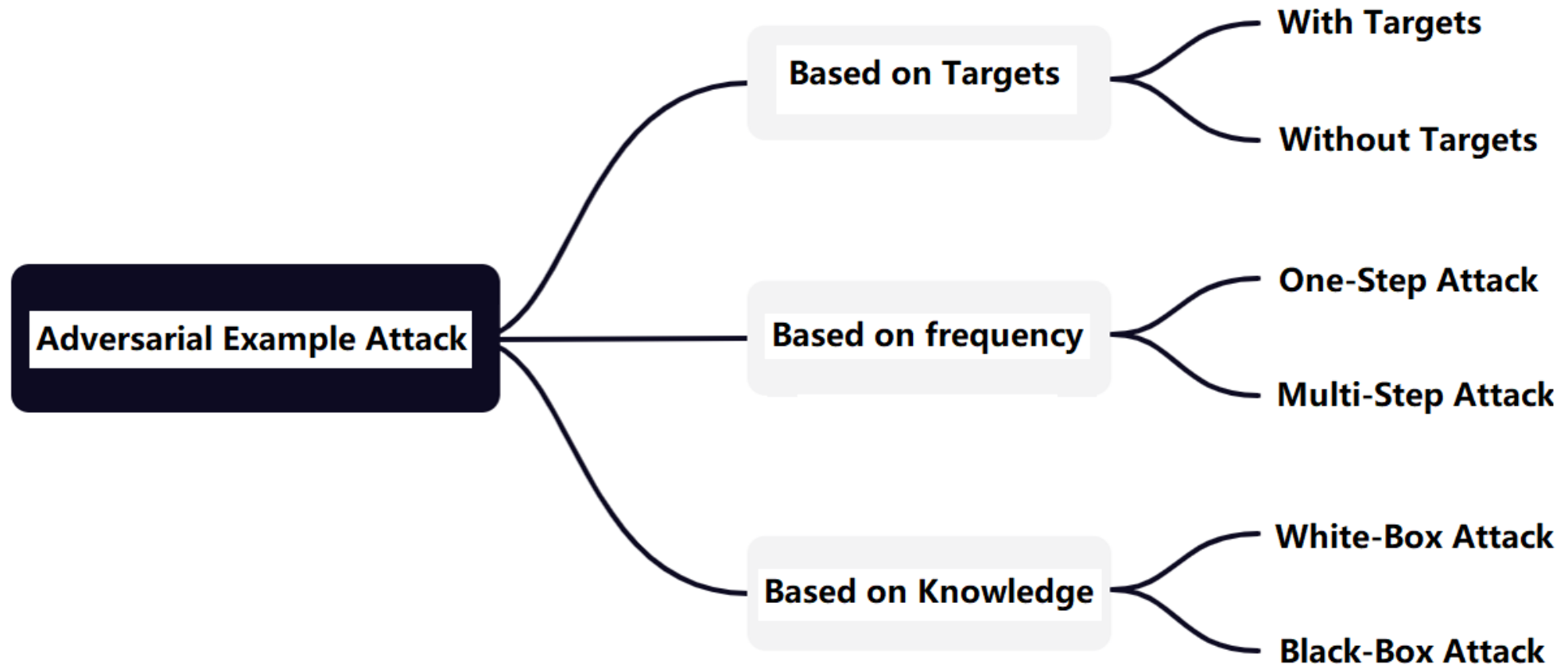
=



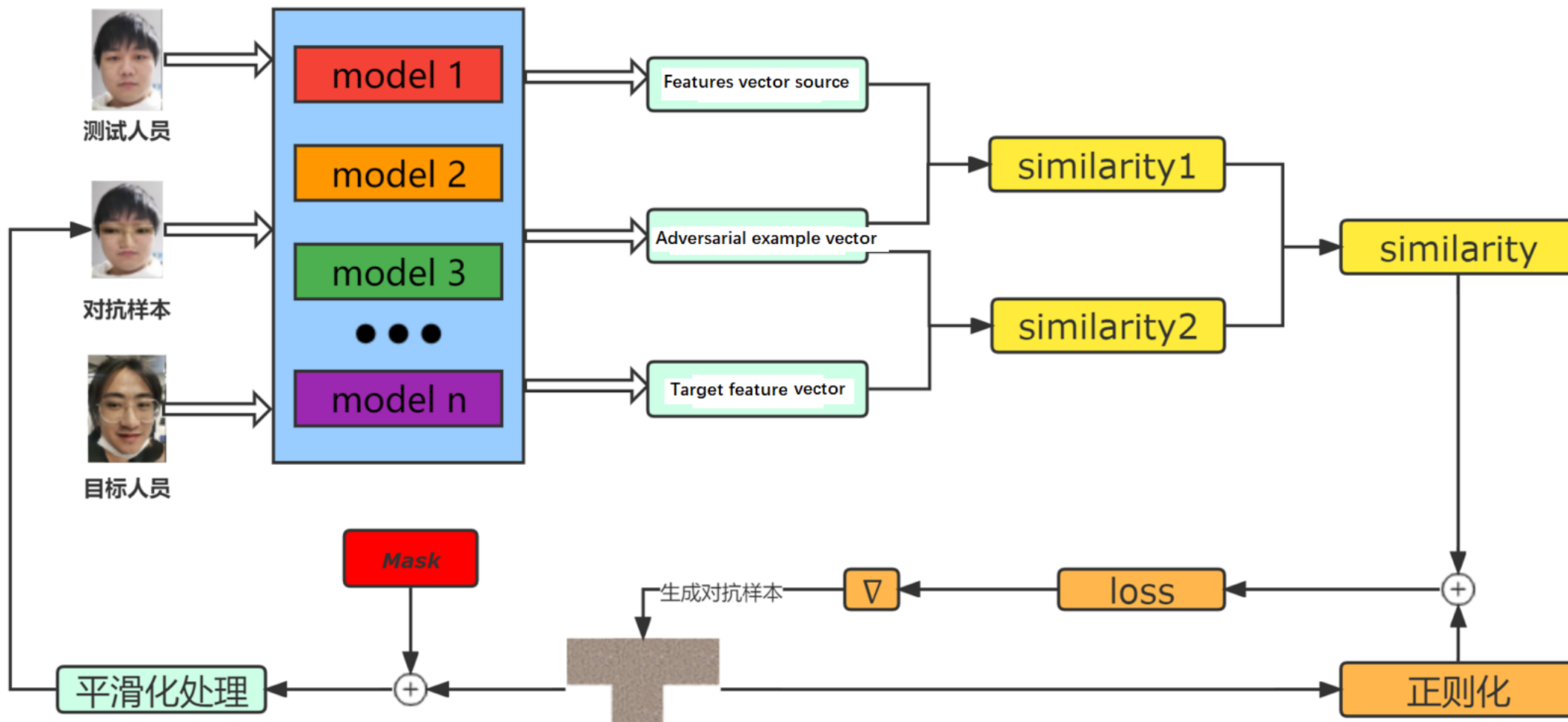
"gibbon"

99.3% confidence

Adversarial Example Attack (Face Recognition)



Adversarial Example Attack (Face Recognition)



Perturbation Area Selection



adv_hat



adv_glasses



adv_patch



adv_makeup

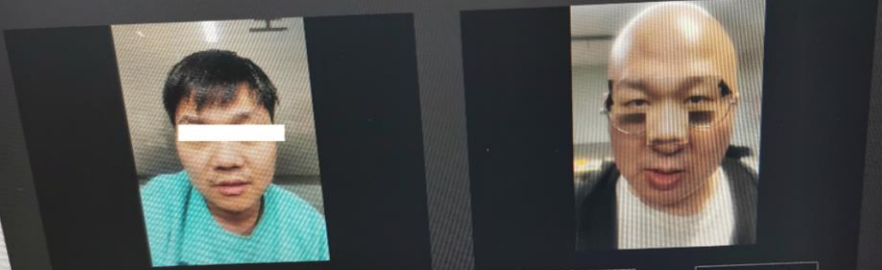


ours

Adversarial Example Attack Comparison

功能演示

相似度 73%
同一个人的可能性较低



URL上传 或 本地上传

Request

- 第一张图片类型:
 - 生活照
 - 带水印证件照
- 第二张图片类型:
 - 生活照
 - 带水印证件照
- 第一张活体检测控制:
 - 不进行检测
 - 一般的活体要求
- 第二张活体检测控制:
 - 不进行检测
 - 一般的活体要求

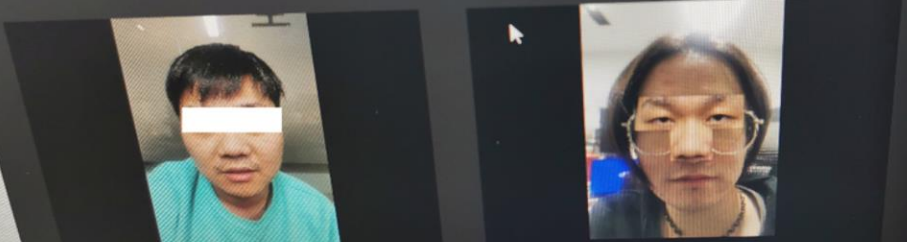
Response

```
{  
  "image": "图片1的Base64编码",  
  "image_type": "BASE64",  
  "face_type": "LIVE",  
  "liveness_control": "NDN"  
}
```

图片文件支持PNG、JPG、JPEG、BMP，图片大小不超过2M，人脸对比只可对比图片中主体部分。
本功能演示使用人脸检测接口对图片进行了初步处理。

功能演示

相似度 89%
同一个人的可能性较高



URL上传 或 本地上传

Request

- 第一张图片类型:
 - 生活照
 - 带水印证件照
- 第二张图片类型:
 - 生活照
 - 带水印证件照
- 第一张活体检测控制:
 - 不进行检测
 - 一般的活体要求
- 第二张活体检测控制:
 - 不进行检测
 - 一般的活体要求

Response

```
{  
  "image": "图片1的Base64编码",  
  "image_type": "BASE64",  
  "face_type": "LIVE",  
  "liveness_control": "NONE"  
}
```

图片文件支持PNG、JPG、JPEG、BMP，图片大小不超过2M，人脸对比只可对比图片中主体部分。
本功能演示使用人脸检测接口对图片进行了初步处理。

Adversarial Example Attack – Huawei P30 Pro



Adversarial Example Attack – Weltmeister Car

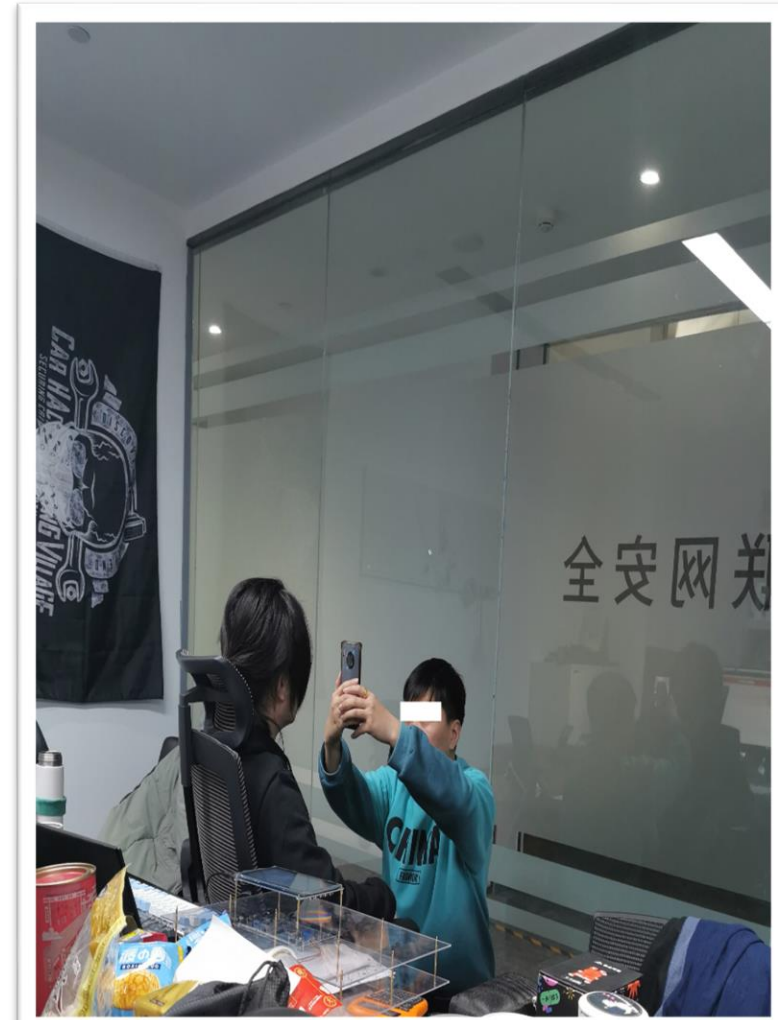


人脸识别欺骗 - 星輿实验室

Adversarial Example Attack – Mystery Car ;)



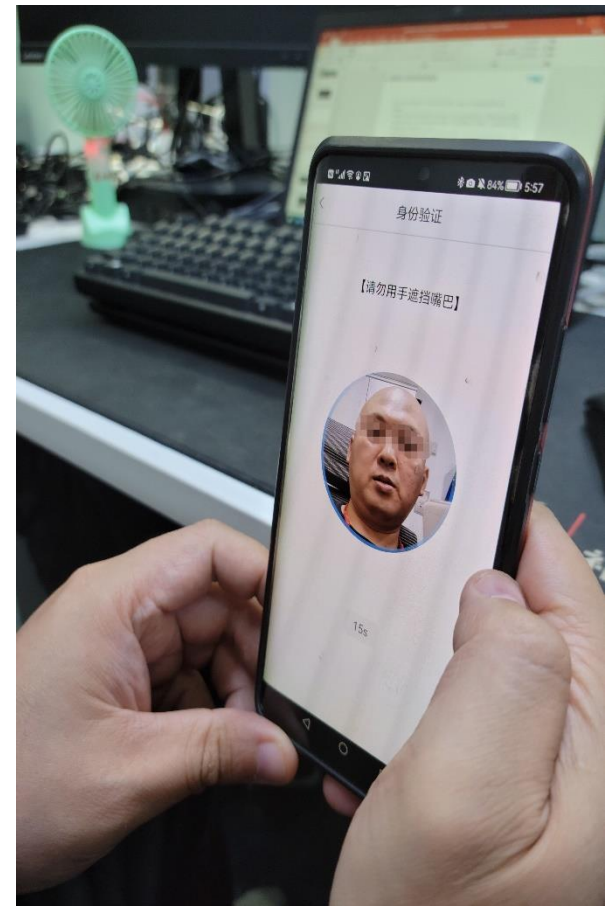
Features Replace Attack



Features Replace Attack – Xiaomi Note9



Features Replace Attack – Bank App (Failed Attempt)



Thresholds Value Attack – Mystery Car ;)



Thresholds Value Attack – Mystery Car ;)



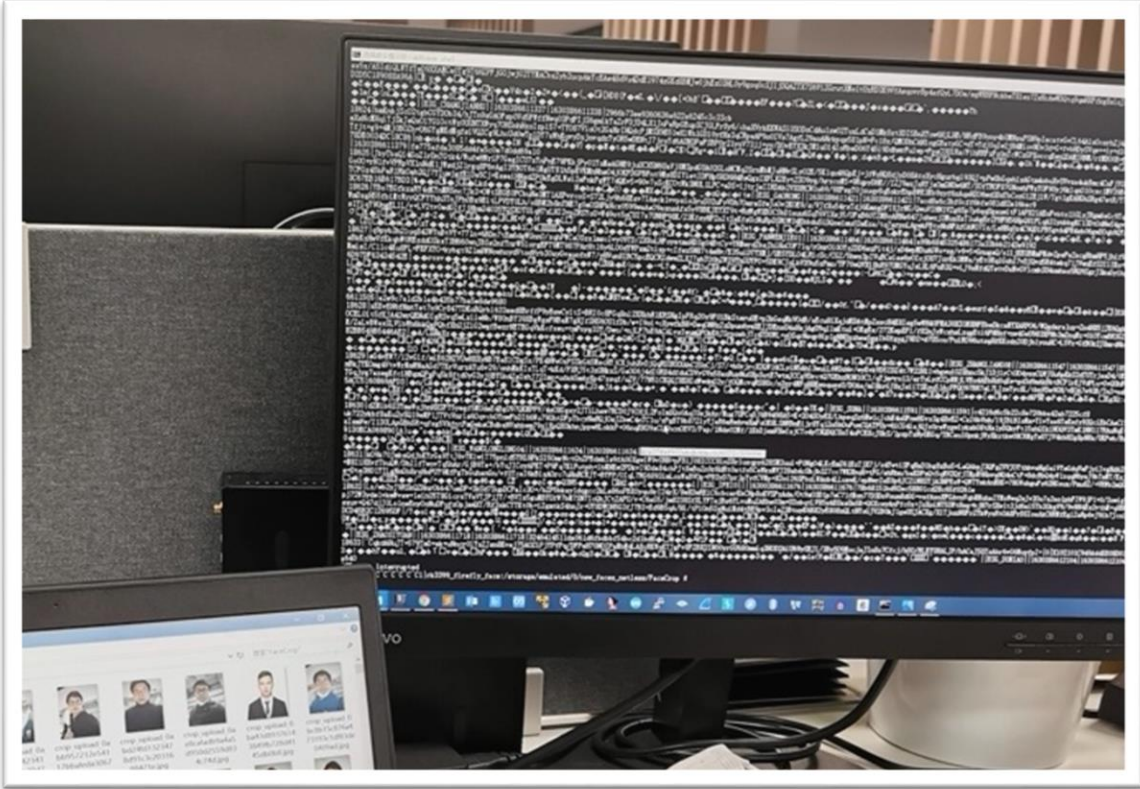
Thresholds Value Attack – Mystery Car ;)



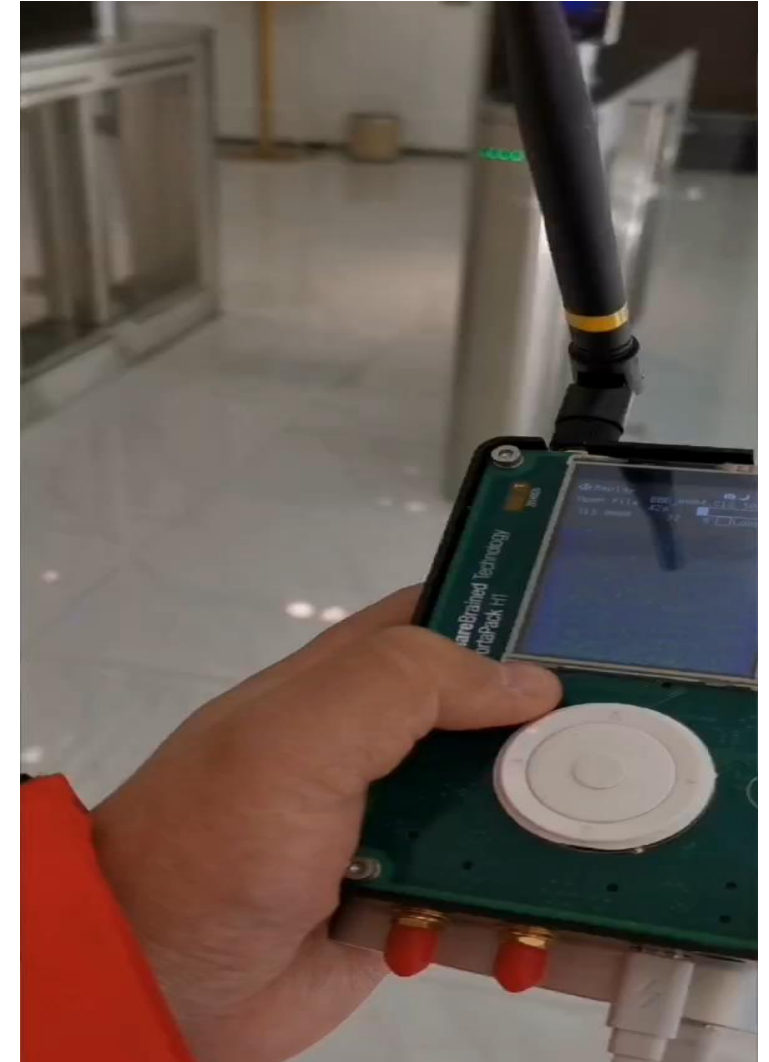
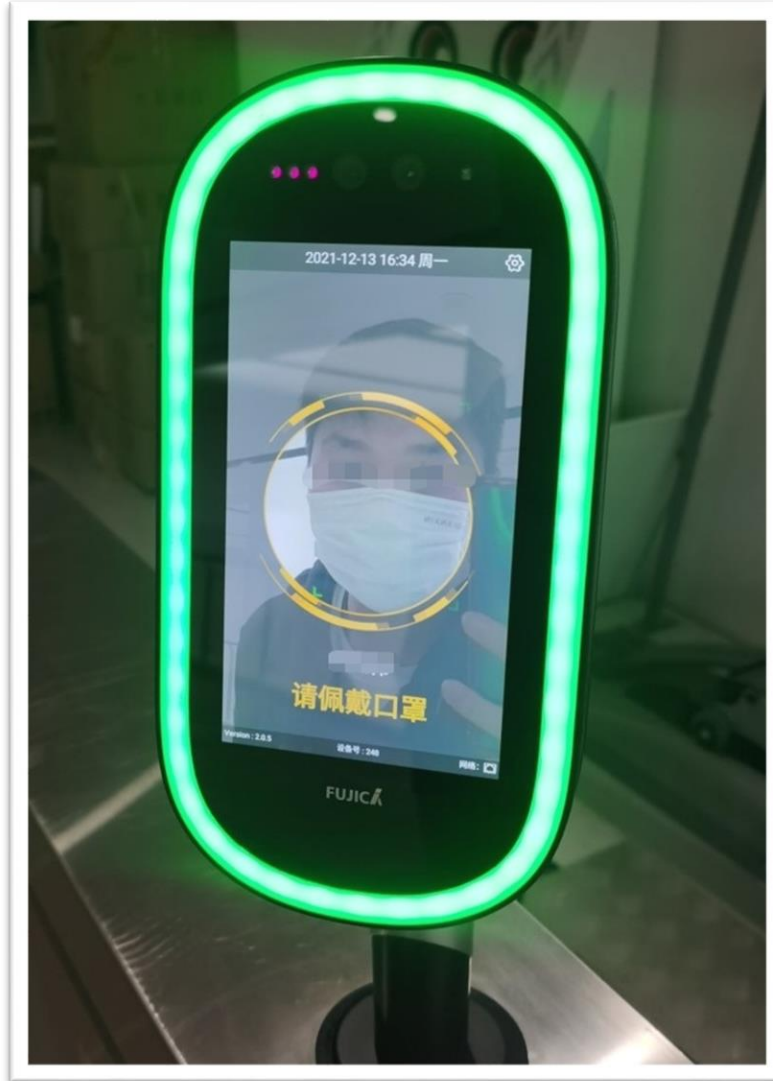
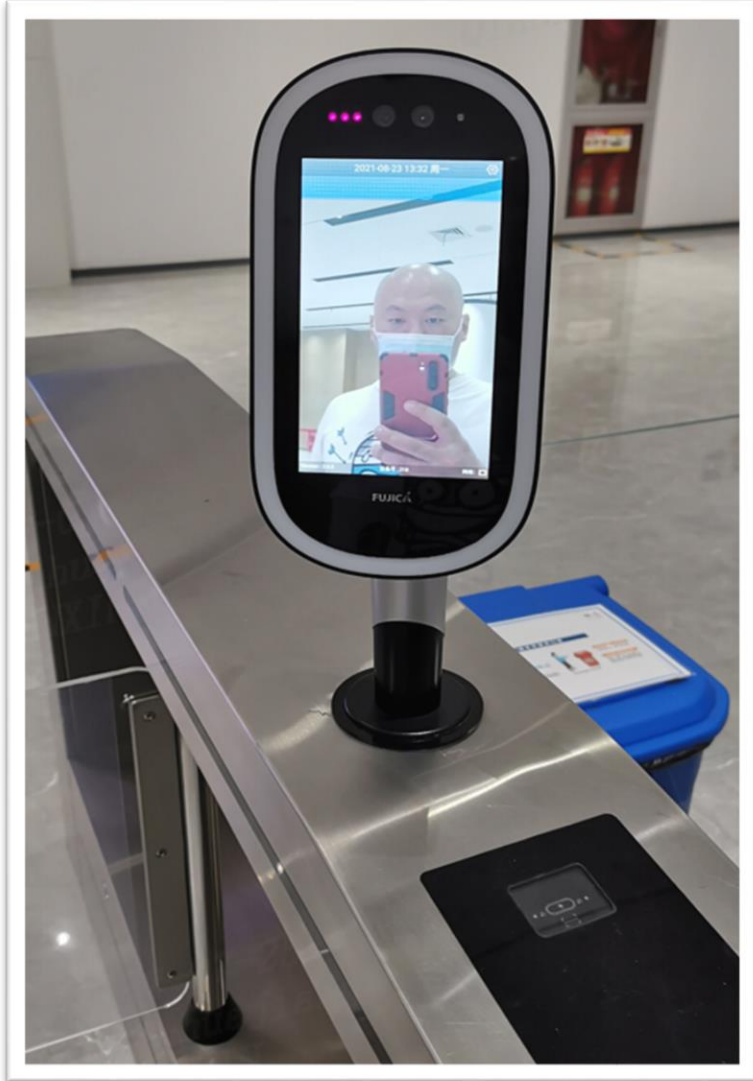
Thresholds Value Attack – Mystery Car ;)



Features Value Attack – Mystery system ;)



Extra Functions Attack – Access Control



Summary (Facial Recognition Spoofing)

Recognition Procedure	Security Level	Spoofing Methods	Details
Face Detection	Weak	Mr.Orange Attack Face photo Attack Face Sculpture Attack ..	The main task is to detect faces, no defense against various spoofing methods
Face Anti-Spoofing	Strong	Features Replace Attack Adversarial Example Attack	The most important security stage of the face recognition. It is possible use a plain photo to break the 2D face recognition system without it.
Feature Extraction & Matching	Medium	Features Value Attack Thresholds Value Attack	By adjusting the face features model to enhance the Adversarial Example, in order to break the face recognition system

Reference

Facial Recognition Spoofing

<https://cmusatyalab.github.io/openface/>

<https://zhuanlan.zhihu.com/p/43480539>

https://www.sohu.com/a/449050750_610671

A Dataset and Benchmark for Large-scale Multi-modal Face Anti-spoofing

D Sztahó, G Szaszák, A Beke. Deep learning methods in speaker recognition: a review

Stepan Komkov, Aleksandr Petiushko. AdvHat: Real-world adversarial attack on ArcFace Face ID system

Naveed Akhtar, Ajmal Mian. Threat of Adversarial Attacks on Deep Learning in Computer Vision: A Survey

Speaker Recognition Spoofing

<https://www.jianshu.com/p/19d34b19517b>

https://zhuanlan.zhihu.com/p/67563275?ivk_sa=1024320u

Zhongxin Bai, Xiao-Lei Zhang. Speaker Recognition Based on Deep Learning: An Overview

Zhaoxi Mu, Xinyu Yang, Yizhuo Dong. Review of end-to-end speech synthesis technology based on deep learning

Rohan Kumar Das¹, Xiaohai Tian¹, Tomi Kinnunen² and Haizhou Li. The Attacker's Perspective on Automatic Speaker Verification: An Overview

Guangke Chen, Sen Chen, Lingling Fan, Xiaoning Du, Zhe Zhao, Fu Song, Yang Liu. Who is Real Bob? Adversarial Attacks on Speaker Recognition Systems



HITBSecConf
2022 Singapore

Thank You



#HITB2022SIN