BSIDES GOA SECURITY CONFERENCE
27th April 2K24
Planet Hollywood Resort, Goa

$whoami

SAGAR BHURE

Software Engineer | Lead at OWASP ML Top 10 | Blackhat Speaker | Mentor

Topic

Exploring Mobile Face Recognition SDKs Through Non-Deepfake Intrusions

Presentation Outline

- **Purpose**: Facial recognition, verifying liveness, integration with third-party SDKs.
- **Literature Review**: Addressing presentation attacks, deepfake threats, and other relevant studies.
- **Standard Processes**: Detailing system architecture and protocol flow in typical workflows.
- **Potential Pitfalls**: Identifying possible failure points and risks.
- **Experimental Analysis**: Investigating Android SDKs empirically.
- **Illustrative Example**: Step-by-step breakdown of an attack scenario.
- **Summary and Recommendations**: Concluding remarks and suggested actions.

Purpose

TLP:WHITE

Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

10 March 2021

PIN Number

210310-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Field Office**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors. This PIN was coordinated with DHS-CISA.

This PIN has been released TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Malicious Actors Almost Certainly Will Leverage Synthetic Content for Cyber and Foreign Influence Operations

Summary

Malicious actors almost certainly will leverage synthetic content for cyber and foreign influence operations in the next 12-18 months. Foreign actors are currently using synthetic content in their influence campaigns, and the FBI anticipates it will be increasingly used by foreign and criminal cyber actors for spearphishing and social engineering in an evolution of cyber operational tradecraft.

Explaining Synthetic Content

Purpose

Why are Deepfakes so dangerous?

Unlocking the Power of Perception: Beyond Deepfakes, into Fast vs. Slow Cognition!

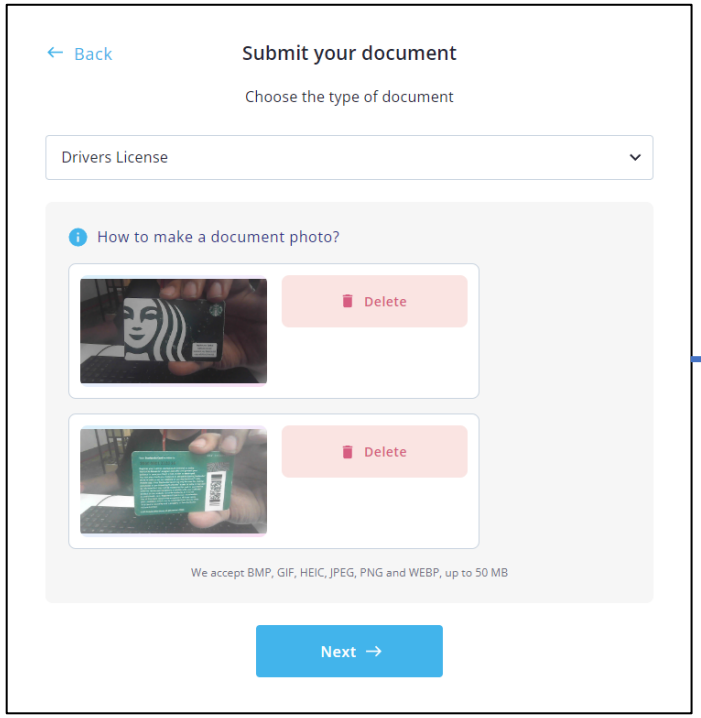
Defining terms…

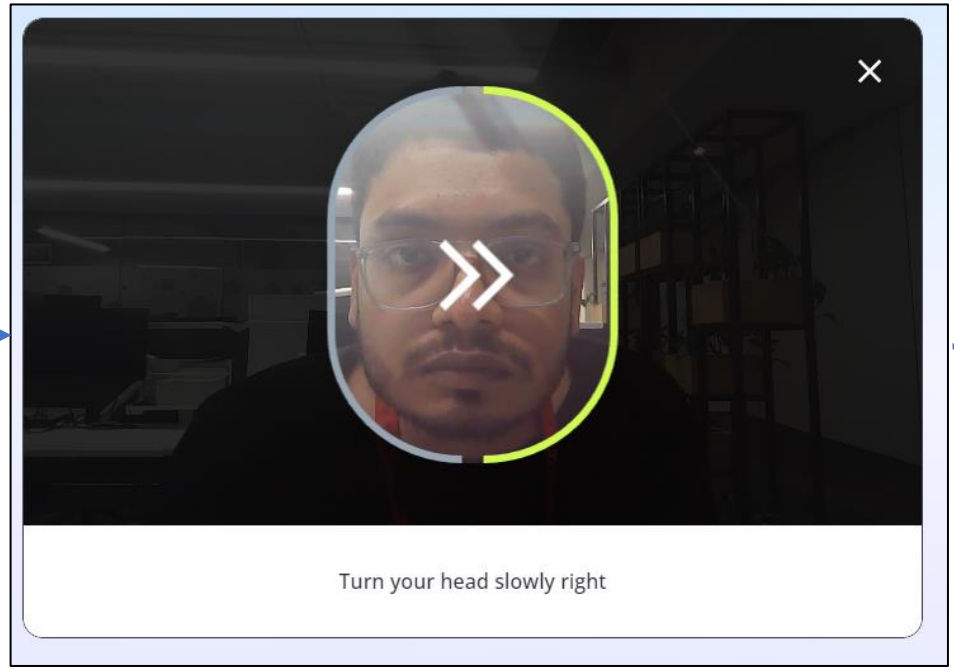
Synthetic Media - The Automated Art of Creating, Manipulating, and Modifying Data and Media.

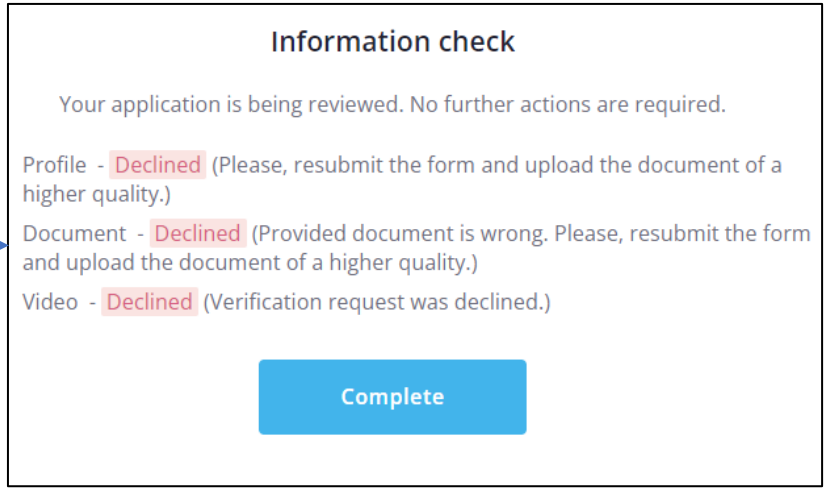
Document and Liveness Check

BSIDES GOA
Security by the Beach 2K24

Facial Recognition with Interactive Liveness Verification for Mobile Applications



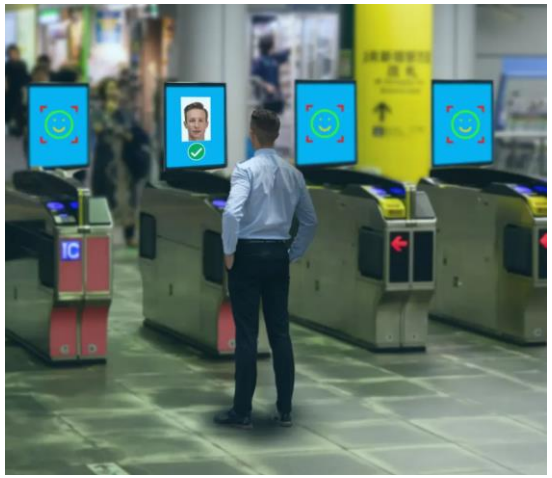




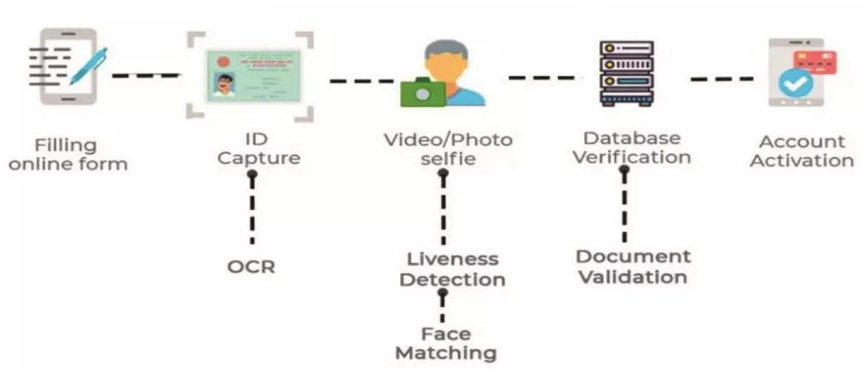
Use Cases

BSIDES GOA
Security by the Beach 2K24

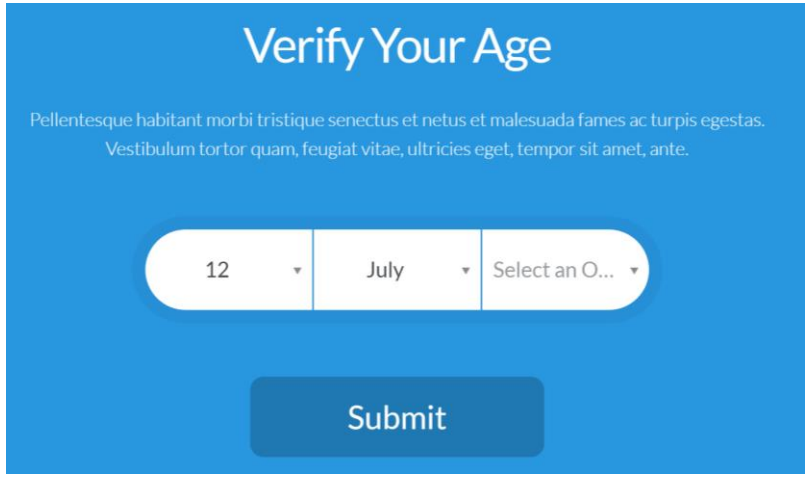
Airport and Immigration Security



Setup a new bank account



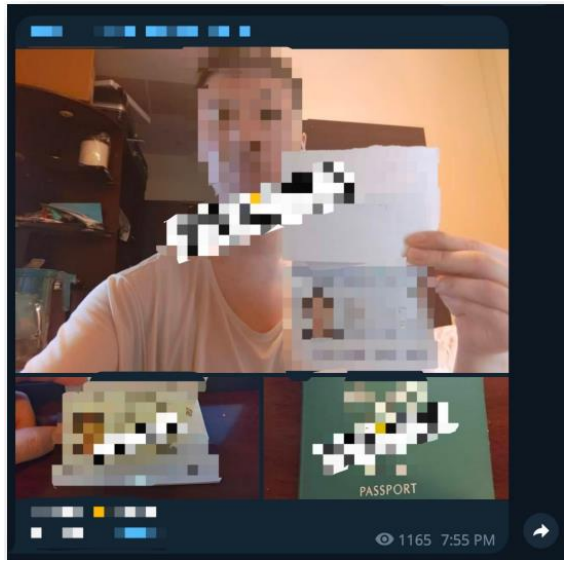
Age Verification In Game



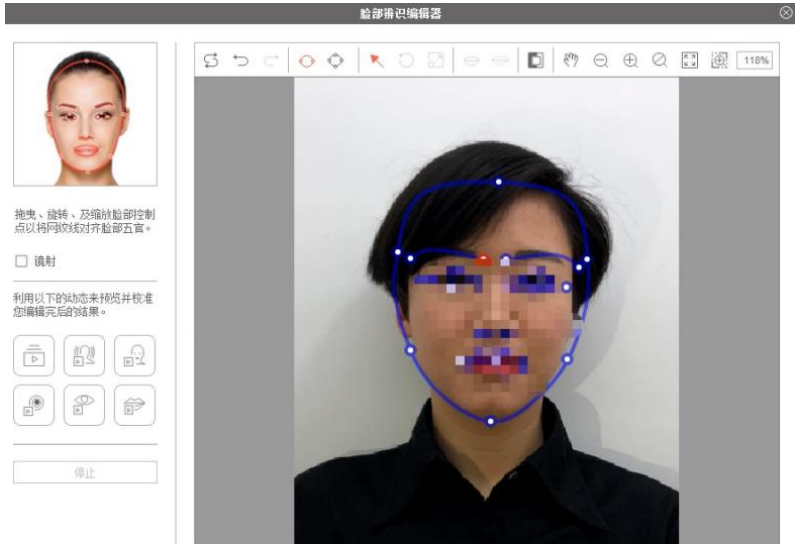
Black Market Sales of Hacking Kits

BOSIDESGOA
Security by the Beach 2K24

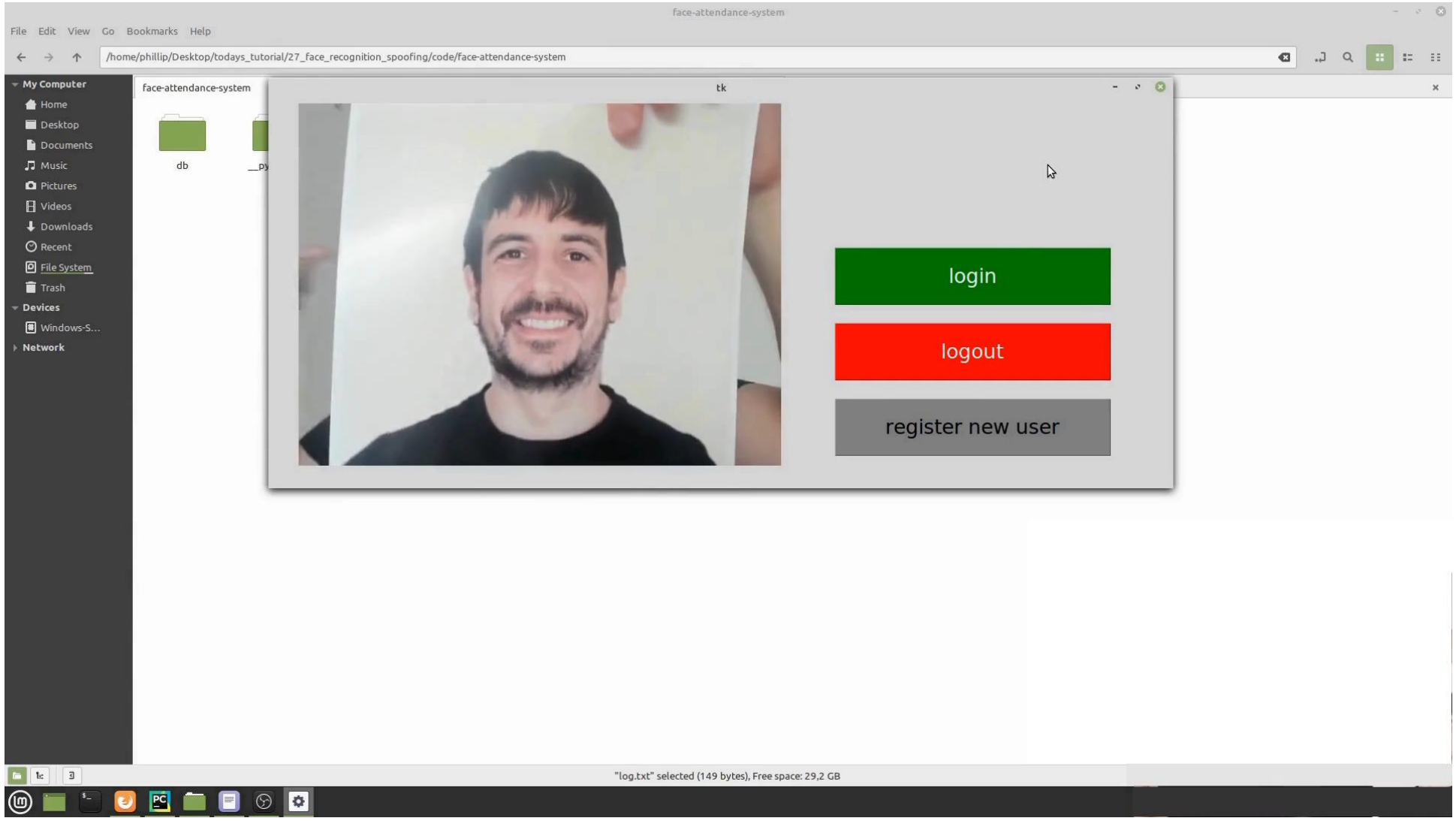
High-quality headshots for ID cards and passports



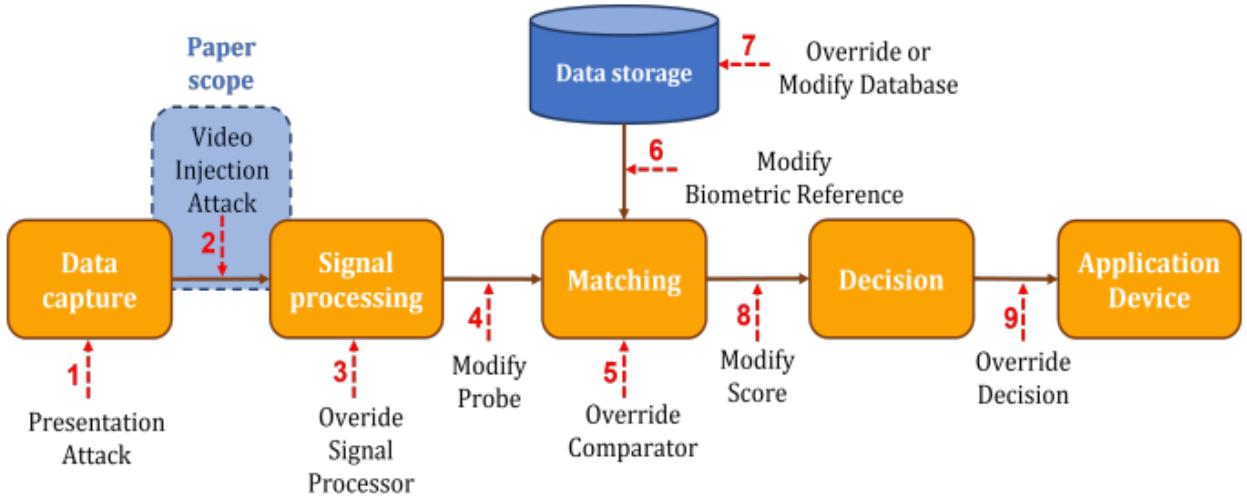
Guiding you through the creation of animated videos for evading facial recognition



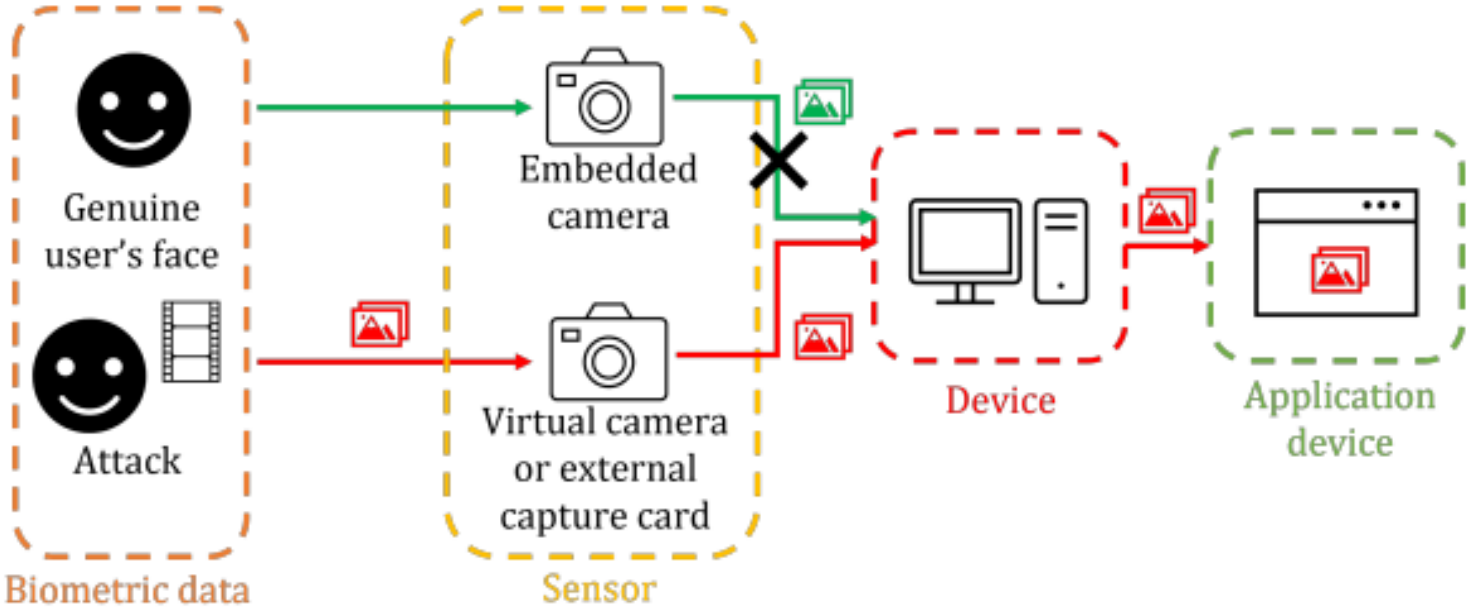
Face Spoofing: Presentation Attack



Video Injection Attack



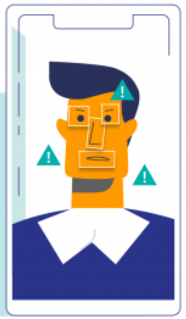
Video injection attack with a virtual camera



Reference: How video injection attacks can even challenge state-of-the-art Face Presentation Attack Detection Systems

Bypassing

1. The device on which the user undergoes the liveness check;



2. The internet connection on which the biometric data of the user reaches the server;

3. The server that checks the biometric data.

Deepfake reported Criminal Cases

Delhi

Dedicated laws on AI, Deepfake Need of the Hour: Advocate Pawan Duggal

Cyber criminals have evolved there methods in keeping with current tech advancements.

Coal India's retd official loses Rs 40K after he gets deep-fake video call from ex-colleague asking for money

George Poikayil

Published: July 17, 2023 02:21 PM IST | Updated: July 17, 2023 05:11 PM IST

Kerala man loses ₹40k to AI-enabled deep-fake fraud

By Vishnu Varma

Read this news in brief form

Jul 18, 2023 01:01 AM IST

Play to Win

Deepfake scam: Company loses over Rs 200 crore after fake video call from 'CFO'

The employees that attended this conference call were instructed to make 15 transfers totaling $25.5 million to five different Hong Kong Bank accounts.

Priya Singh

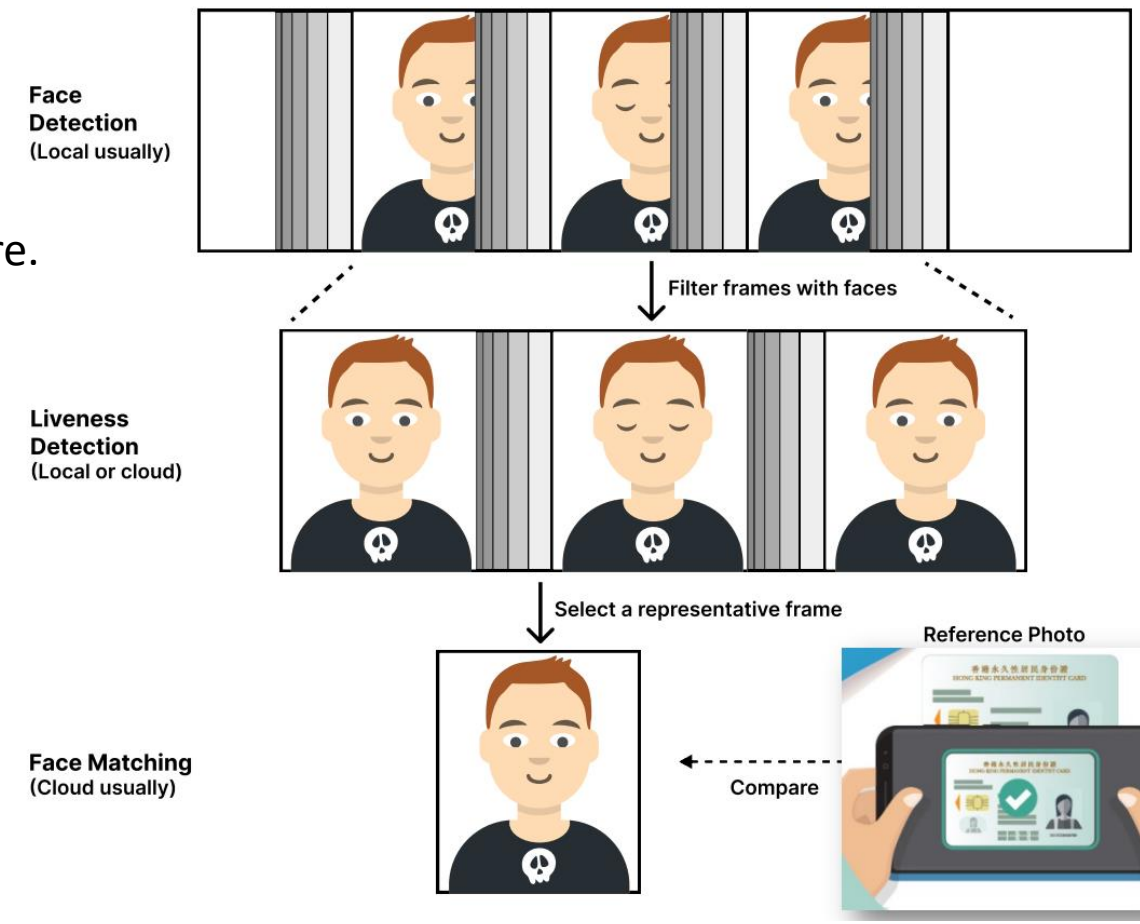
Updated Feb 05, 2024, 12:40 PM IST

Man gets caught in deepfake trap, almost ends life; among first such cases in India

ET Online • Last Updated: Nov 30, 2023, 11:05:00 AM IST

FOLLOW US SHARE FONT SIZE SAVE PRINT COMMENT

Liveness Detection SDK Workflow



- **Face Detection and Localization**
  Ensuring high-quality, accurately positioned facial data capture.

- **Liveness Verification**
  Confirming the presence of a live person to prevent spoofing attempts.

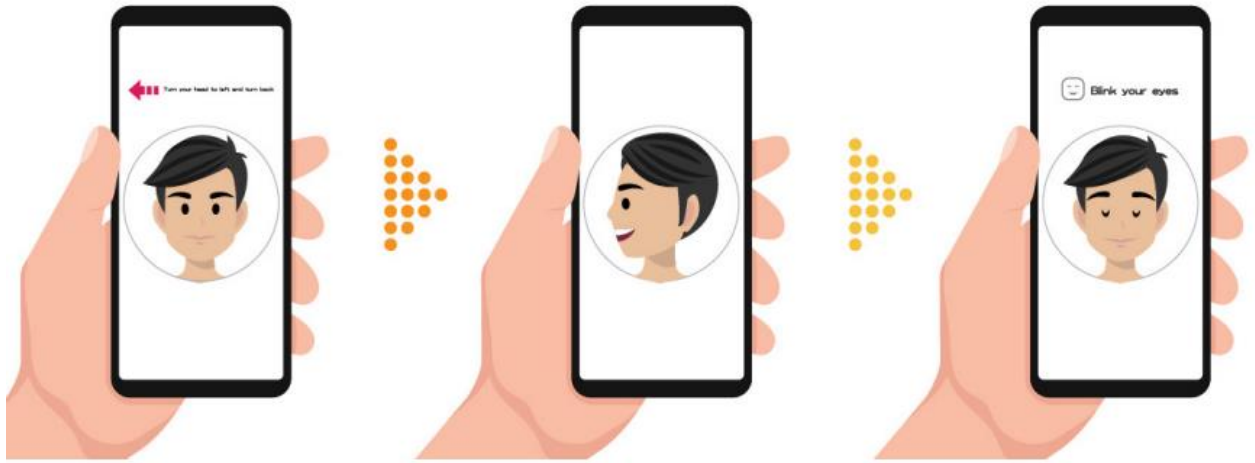
- **Facial Matching**
  Comparing the captured frame with:
  - Photos from previously scanned ID cards
  - Data from authoritative databases for authentication purposes.

Liveness Detection

Static Liveness Detection
Image-based
aka ‘Passive Liveness’

* Image source: https://www.thalesgroup.com

Interactive Liveness Detection
Video-based
aka ‘Active Liveness’

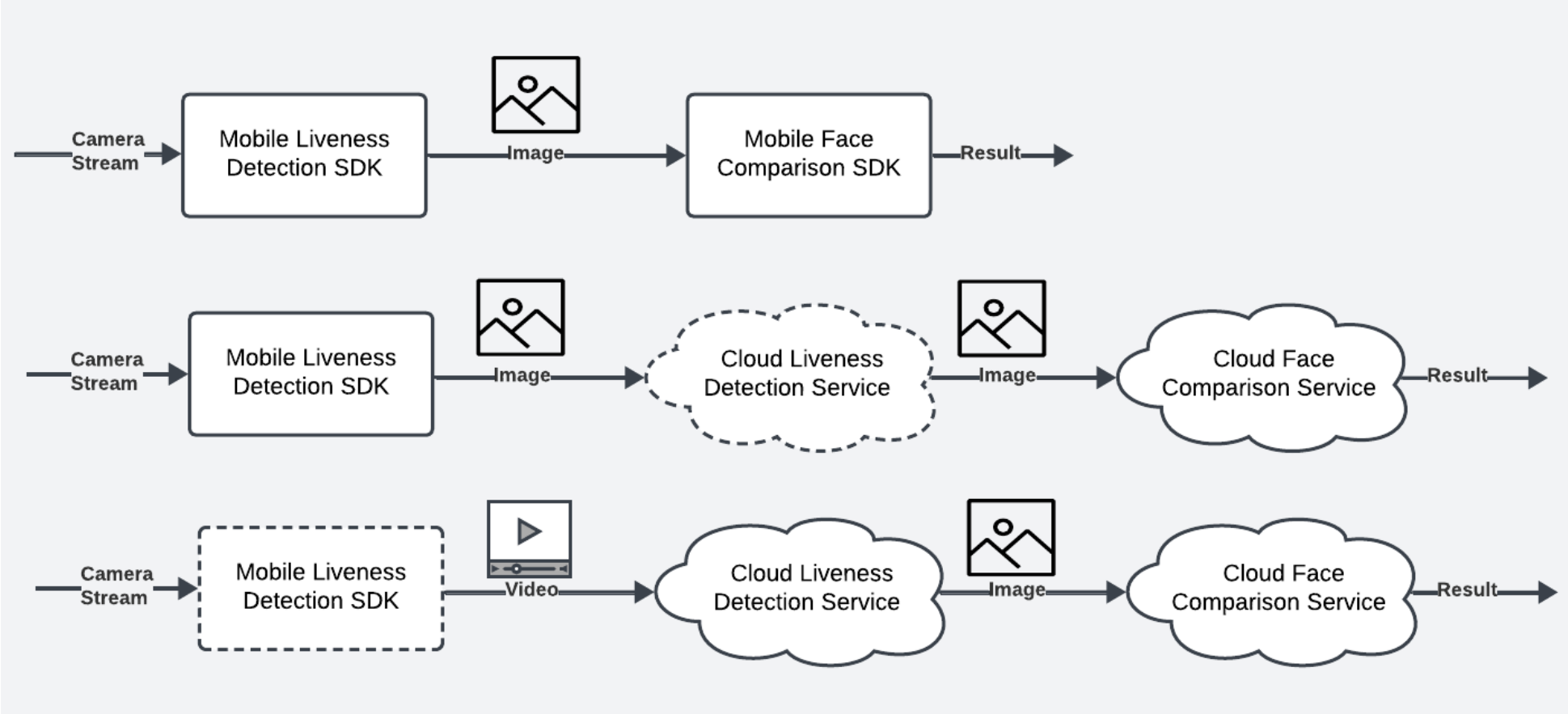


Liveness Detection Architecture

Pure Local
More common in non-end user devices

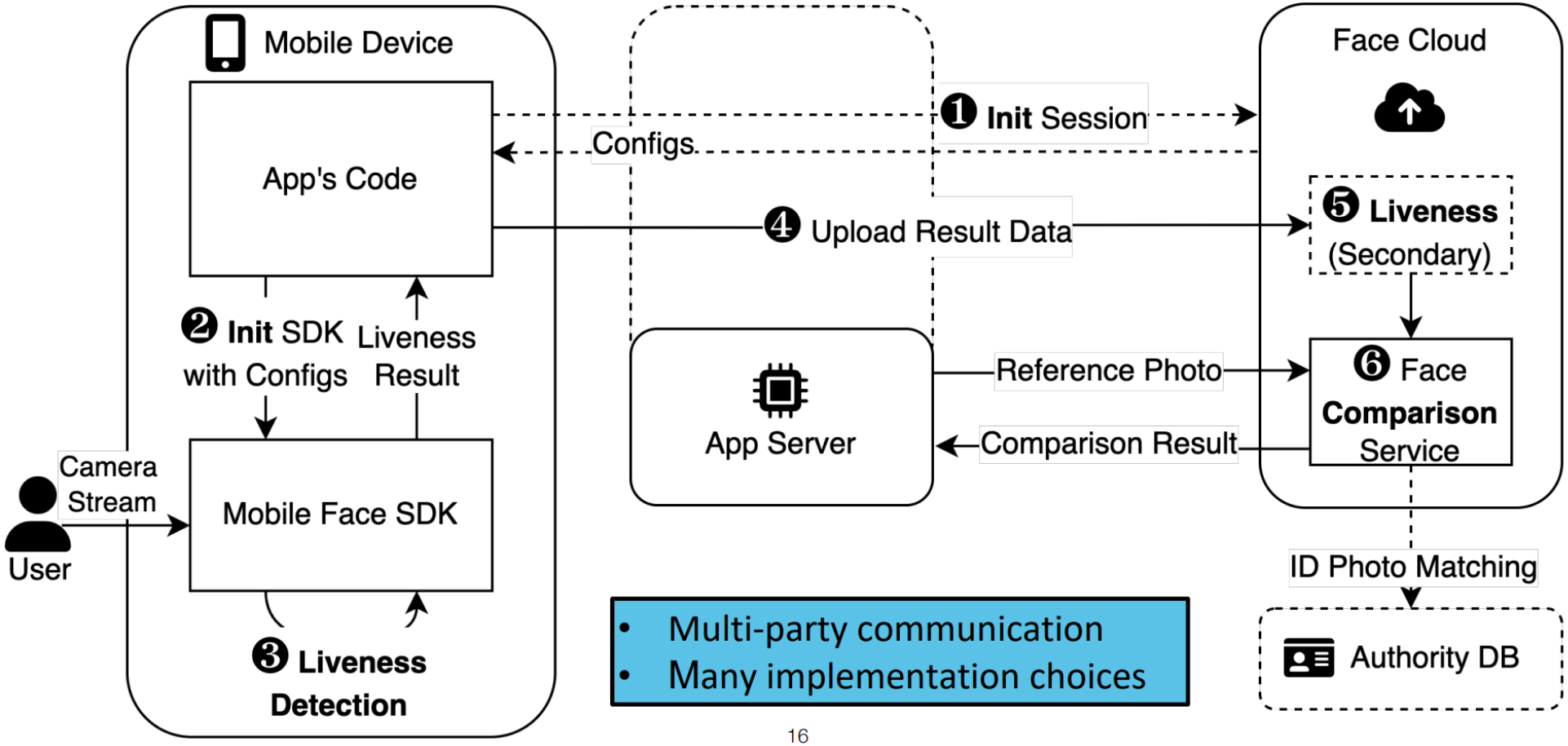
Local-Cloud Mixed
Most popular in mobile apps

Pure Cloud
In some mobile apps

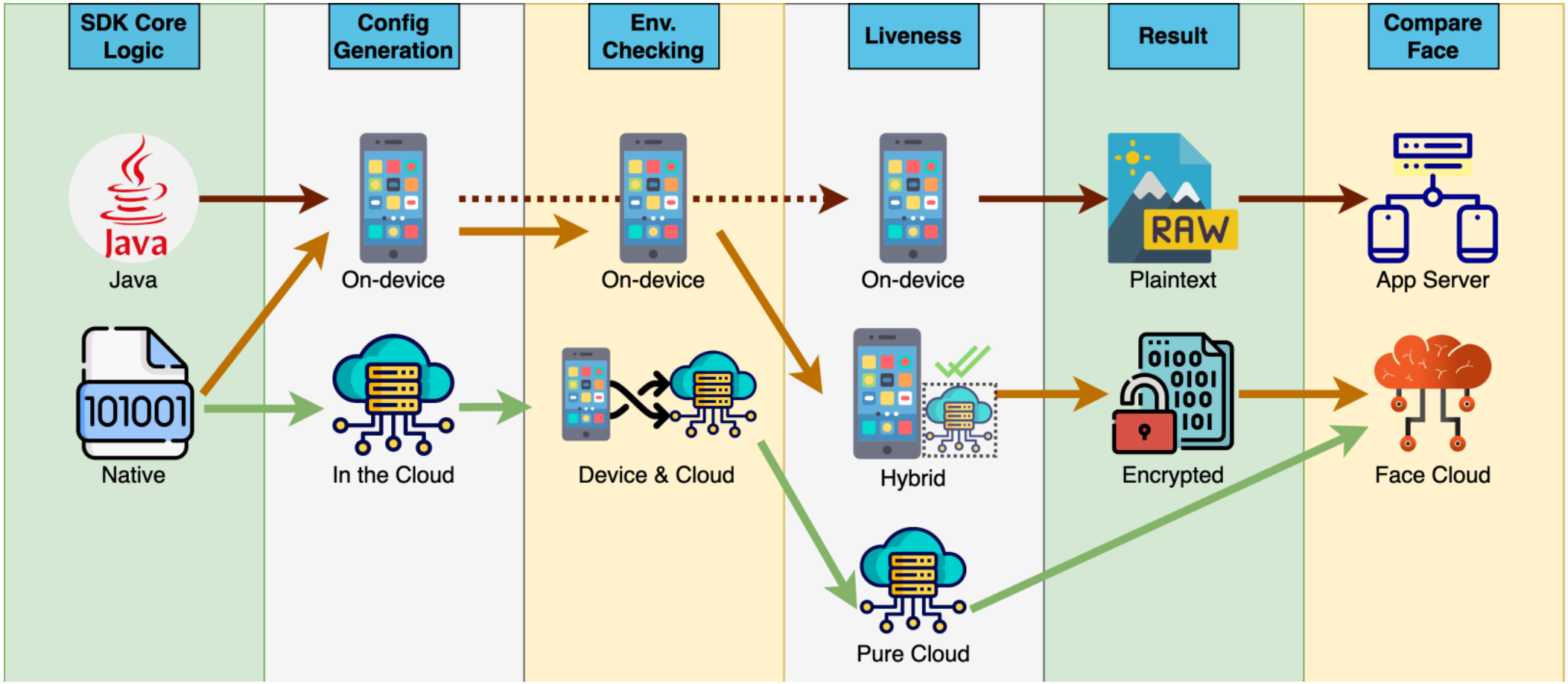


Threat model: attacker has total control of his mobile device (rooted)
Any operation performed on the client cannot be trusted

Liveness Workflow



Implementation Choices



Liveness Workflow

Attacker owns:

Victim's Photo(s), a device with full control

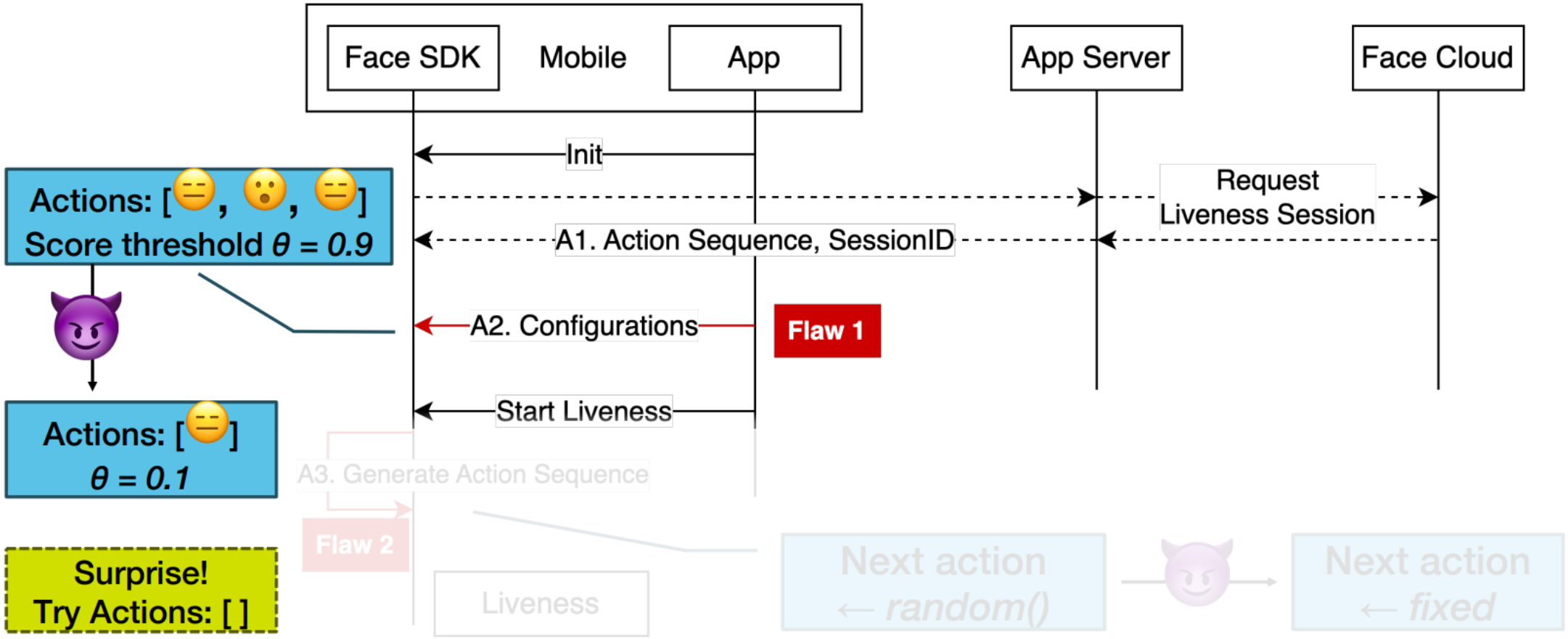
Goal:

Spoof Face Recognition, Identify as the victim

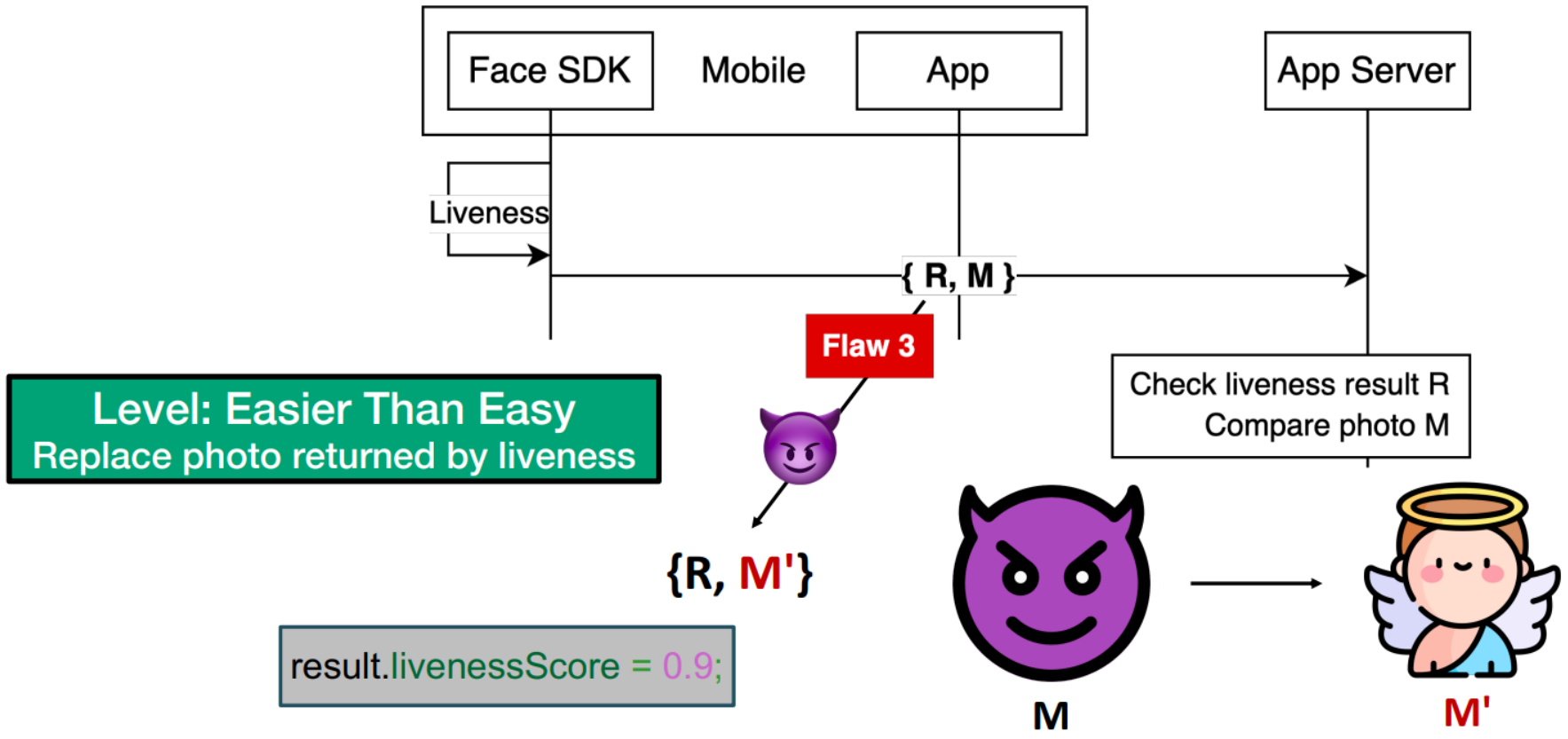
How:

Bypass/Deceive Liveness & Upload victim's photo

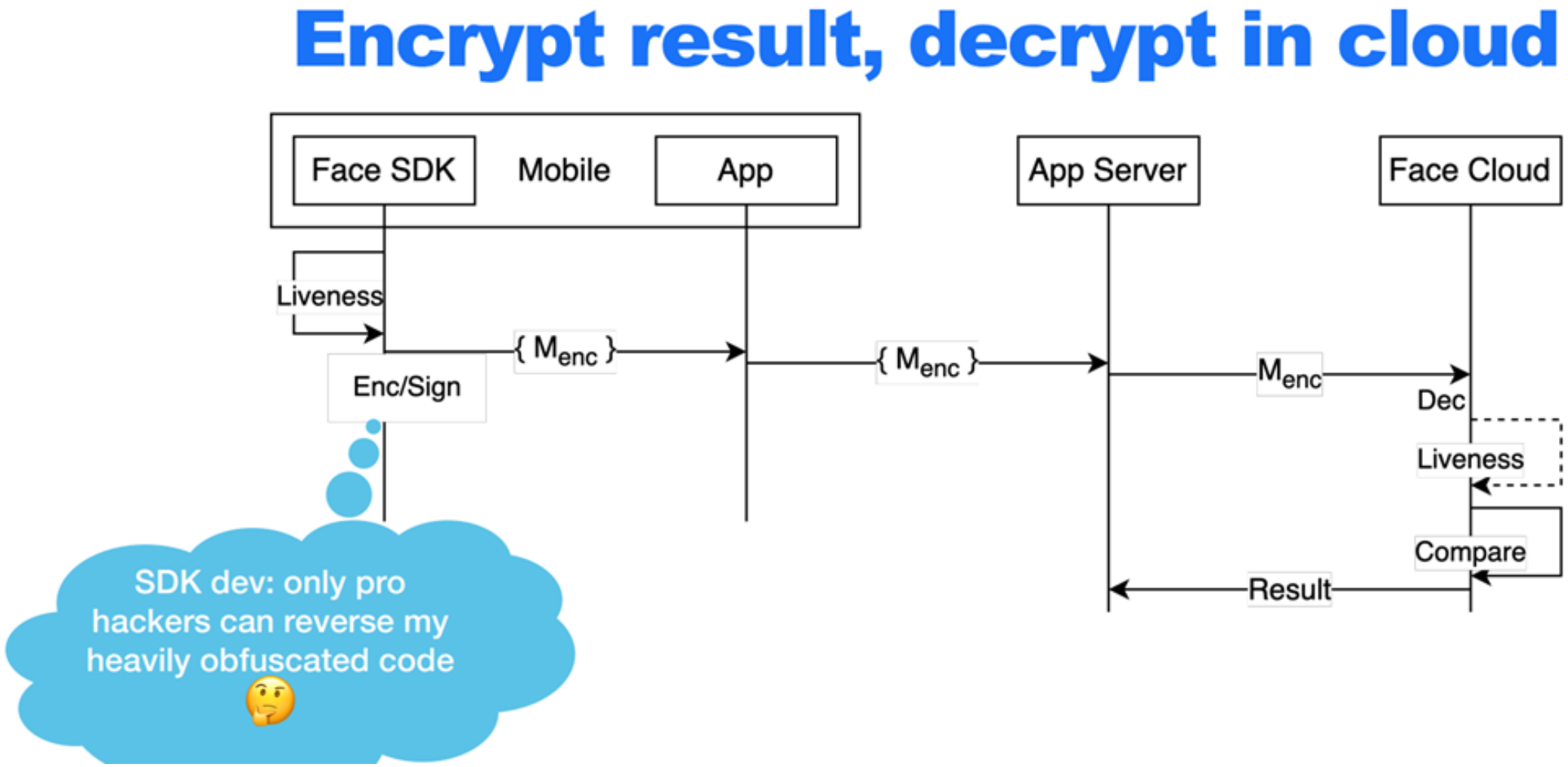
Pitfalls: Initialization Stage



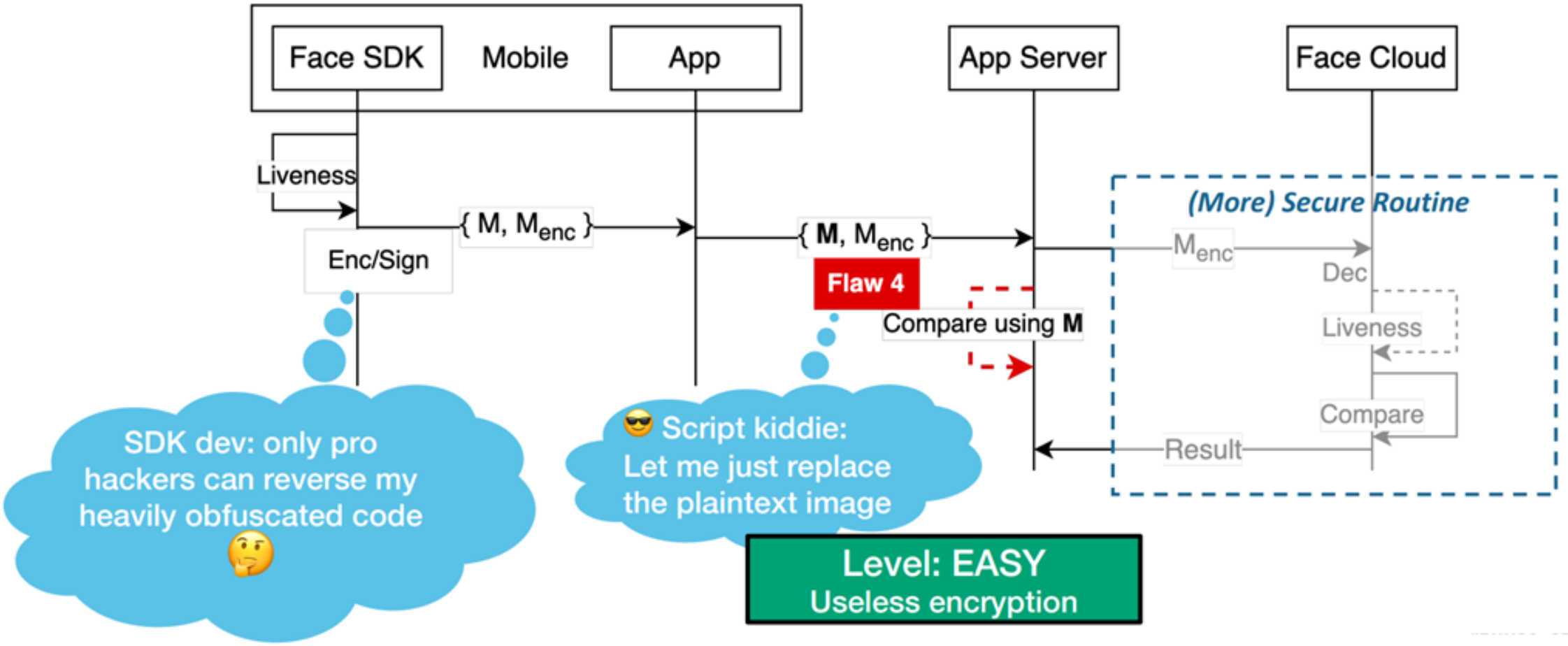
Pitfalls: Result passing



Pitfalls: Result passing



Pitfalls: Result passing



Some Cliche Mistakes

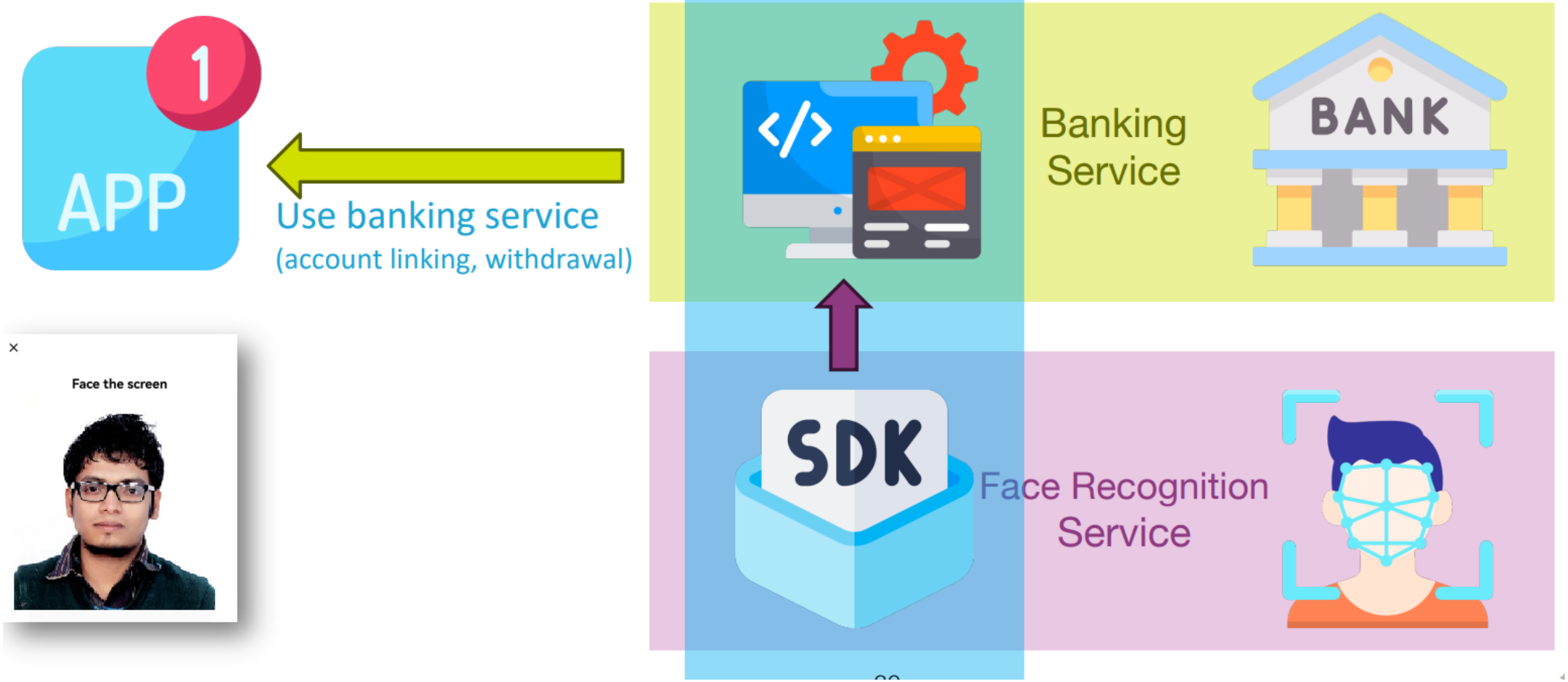
BSIDES GOA
Security by the Beach 2K24

Insecure file storage

```
67 /* loaded from: classes2.dex */
68 public class LiveDetectActivity extends Activity implements Camera.AutoFocusCallback,
69     private static String aG = FileUtils.getSdcardPath() + "/DCIM/";
70     private static String aH = FileUtils.getSdcardPath() + "/DCIM/pic/pic1.jpg";
71     private static String aI = FileUtils.getSdcardPath() + "/DCIM/pic/pic2.jpg";
72     private static String aJ = FileUtils.getSdcardPath() + "/DCIM/pic/pic3.jpg";
73     private static String aK = "bestPic.jpg";
74     private static String aL = "bestPic1.jpg";
75     private static String aM = "bestPic2.jpg";
76     private static String aN = "shakePic.jpg";
77     private static String aO = "nodPic.jpg";
78     private static String aP = "gazePic.jpg";
79     private static String aQ = "blinkPic.jpg";
80     private static String aR = "openMouthPic.jpg";
```

No UI hijacking protection

Case Study


1
APP
Use banking service
(account linking, withdrawal)
Banking
Service
BANK
Face the screen
SDK
Face Recognition
Service

Hacker Master Plan

Recon

- Is the app packed?
- Which face SDK?
- Collect SDK package
- Read SDK docs

Target Localization

- Decompile the SDK to locate hooking target
- Defeat anti-debugging
- Locate target in app

Attack

- Dump and inspect data
- Process victim's photo to match to format
- Replace the data

Empirical Research

Face SDK	Interact Mode	Native Library	Action Generation	Configurable	Env. Checking	Liveness Location	Liveness Results	Matching Location	UI Included	Easiest Possible Attack
A	actions	✓	—	$\theta, \mathbb{A}$	N	L	$\{r, M, M_{enc}\}$	C, S	✗	*Result Replacement*
A′	actions	✓	L	$\theta, \mathbb{A}$	N	L	M_{sign}	C	✗	*Result Replacement*
B	flashing	✓	C	$\varnothing$	N, C	L	M_{enc}	C	✓	—
B′	static	✓	—	$\varnothing$	N, C	C	—	C	✓	—
C	actions	✓	C	$\theta_s, \mathbb{A}_s$	N, C	$L \wedge C$	$\{M_{enc}, E_{enc}\}$	C	✓	—
E	actions	✓	L	θ	N	L	M	S	✗	*Result Replacement*
F	actions	✓	C	$\theta_s, \mathbb{A}_s$	N, C	$L \wedge C$	?	C	✓	—
D	actions	✓	L	$\theta, \mathbb{A}$	N	L	M	S	✗	*Result Replacement*
G	actions	✓	C	$\varnothing$	N, C	$L \wedge C$	M_{sign}	C	✓	—
H	actions	✗	C	$\varnothing$	J	L	M	C	✓	*Result Replacement*
I	actions	✓	—	$\theta_s, \mathbb{A}_s$	J	L	M	S	✓	*Result Replacement*
J	static	✗	—	$\varnothing$	✗	C	—	C	✓	—
K	actions	✗	fixed	$\varnothing$	✗	L	$\{M_{enc}, M\}$	S	✓	*Result Replacement*
L	static	✓	—	$\varnothing$	✗	L	r	L, S	✗	*Result Replacement*
M	actions	✓	?	θ	✗	L	$\{r, M_{enc}\}$	L, S	✗	—
N	static	✓	—	θ	✗	L	r	L, S	✗	*Result Replacement*
O	actions	✗	L	$\mathbb{A}$	✗	C	—	C	✗	*Video Forgery*
P	actions	✓	L	$\mathbb{A}$	✗	L	$\{r, M_{sign}\}$	S	✗	*Result Replacement*

Catastrophic

Less secure

Good practice

11 out of 18 *face SDKs* have insecure design or implementation

Wanna get in touch?

linkedin.in/in/sagarbhure
www.sagarbhure.com

BSIDES GOA

Security by the Beach 2K24

THANK YOU