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

Kévin Carta, André Huynh, Stéfane Mouille, Sébastien Brangoulo, Nadia El Mrabet and Claude Barral

kevin.carta@cabinet-louis-reynaud.fr

kevin.carta@emse.fr

MINES Saint-Étienne

Ad Usque Fidelis Cabinet Louis Reynaud

Agenda

1. **General introduction**
2. Introduction to biometrics, liveness detection and video attacks
3. Our experiments
4. Conclusion

Cabinet Louis Reynaud – CLR Labs

L'entreprise :

- Créée en 2017
- 7 collaborateurs
- Spécialisations :
  - Cybersécurité
  - Biométrie
  - Identité numérique
- Seul laboratoire agréé par l'ANSSI en région PACA

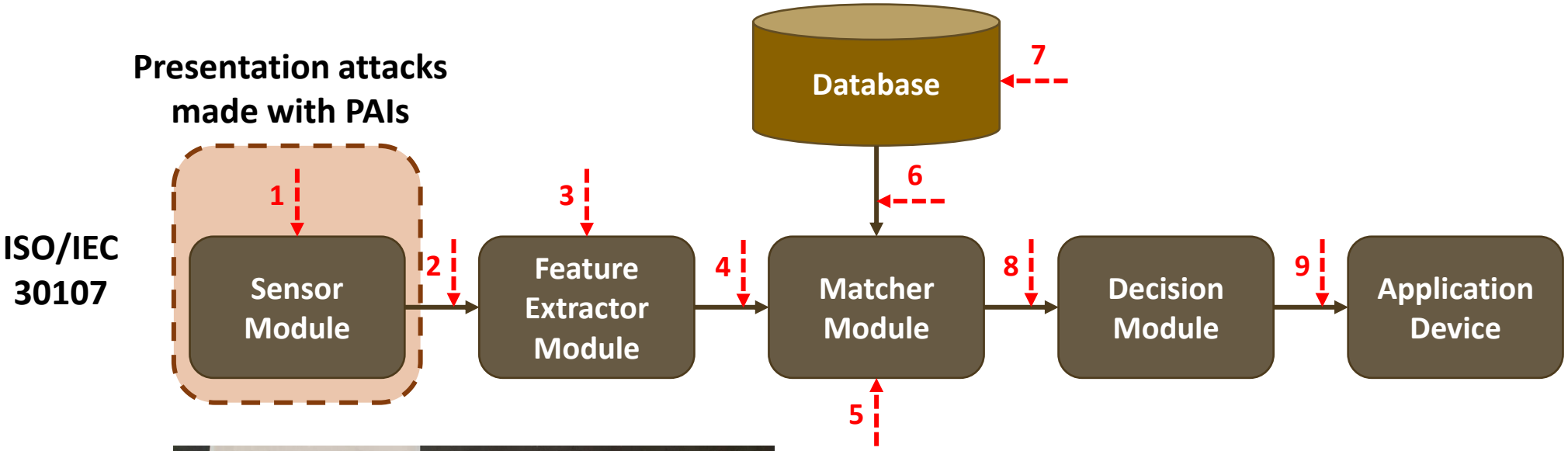
Quelques activités :

- Conseil et formation en cybersécurité
- Évaluation de systèmes de sécurité
- R&D :
  - Conception d'attaques au dessus de l'état de l'art
  - Conception et développement de produits innovants
- Collecte de données biométriques

Agenda

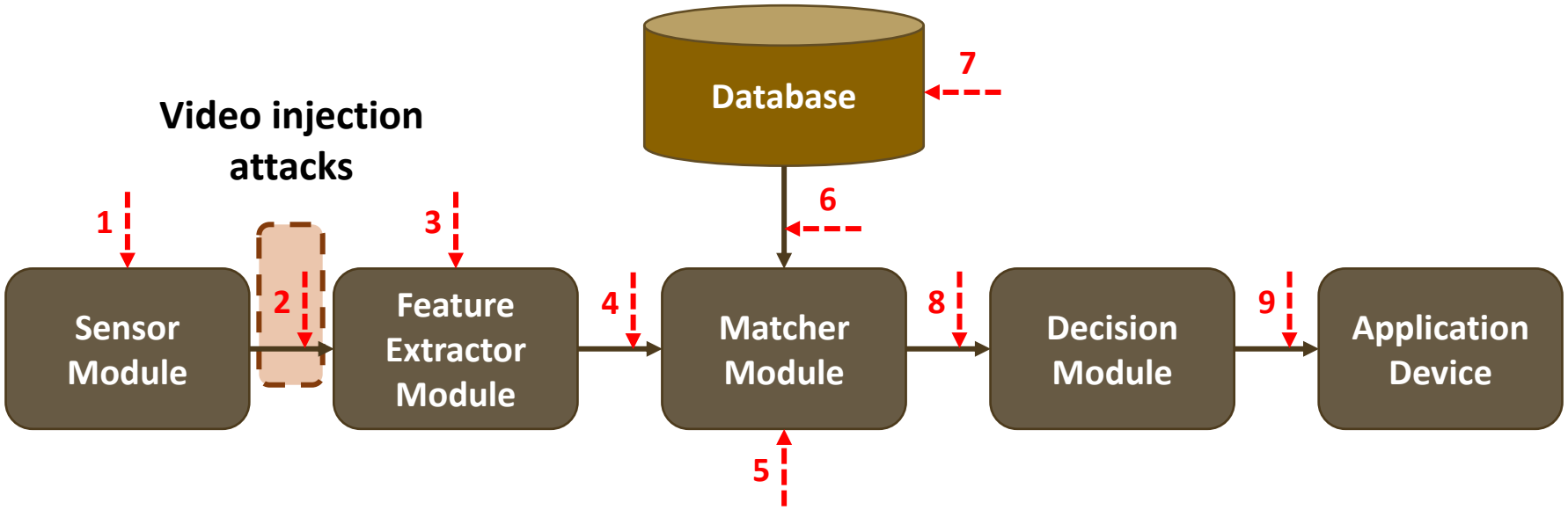
1. General introduction
2. **Introduction to biometrics, liveness detection and video attacks**
3. Our experiments
4. Conclusion

Biometrics are vulnerable by default



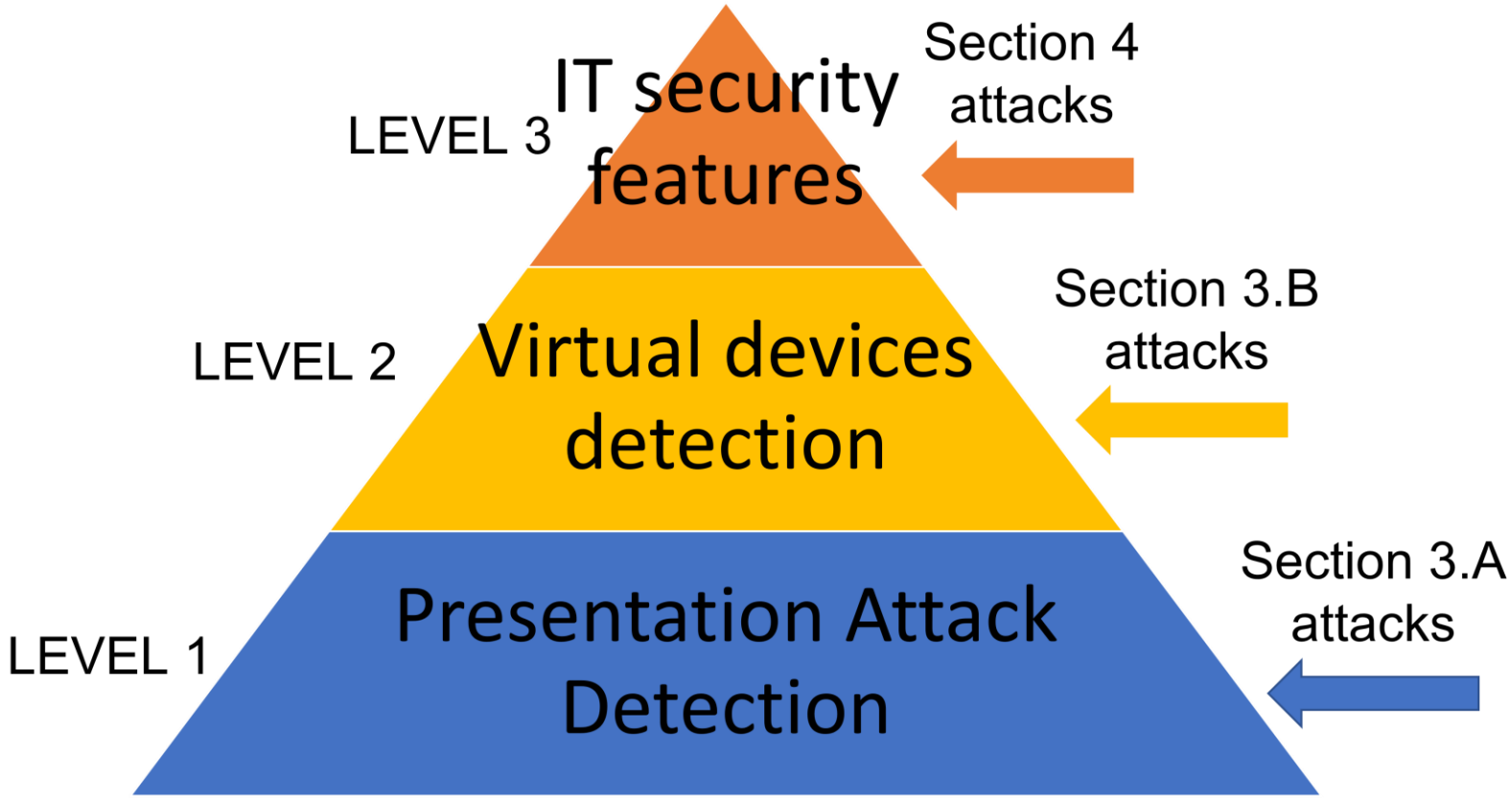
PAI: Presentation Attack Instrument

Biometrics are vulnerable by default



Video Injection Attacks are a real threat for remote identity verification systems (also called identity proofing systems) used by Qualified Trusted Services Providers or Organisation which need confidence in the identity of their customers (e.g., banks, insurances, governments, etc.).

Video Injection Attacks



Agenda

1. General introduction
2. Introduction to biometrics and liveness detection
3. **Our experiments**
4. Conclusion

The use case of our study: Unissey PAD

Unissey Presentation Attack Detection is a:

- Passive liveness detection system
- Deep-learning algorithm trained with legitimate and attacks datasets
- RGPP liveness detection system
- Certified system by two independent laboratories for conformity with ISO/IEC 30107 international standard at Level 2

The objective of our paper is to test if a state-of-the-art biometrics security system is able to detect video injection attacks

The use case of our study: Unissey PAD

- The Unissey system works with a portrait video (the user needs to put is face in a target in the center of the screen) of around 1s

Presentation attacks

- The first attacks that we have performed are Presentation Attacks to verify that the system deserves its certificates and is thus able to detect the most known presentation attacks and even the most accurate ones

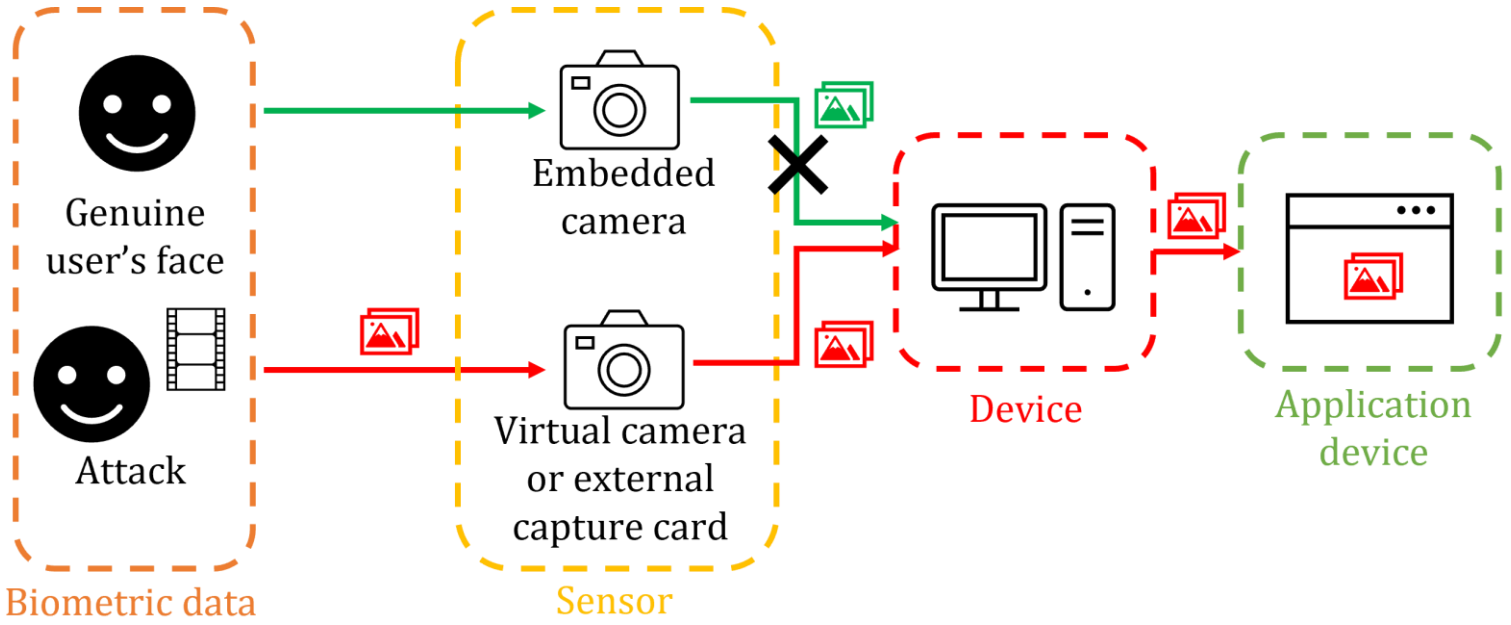
Results for Presentation attacks

- Each attack have been presented to the system 12 times (with 4 different cameras and 3 different lightning conditions)
- The success rate describes the success for bypassing the system

Attacks	Biometric source	Success rate
A photo printed	A photo	0/12 = 0%
A video displayed	A video	0/12 = 0%
A 3D rigid mask	A 3D face scan	0/12 = 0%
A 3D latex face mask	Face measurements	0/12 = 0%
A 3D silicone face mask	Face measurements	0/12 = 0%

ALL the attacks have been detected by the system

Simple video injection attacks



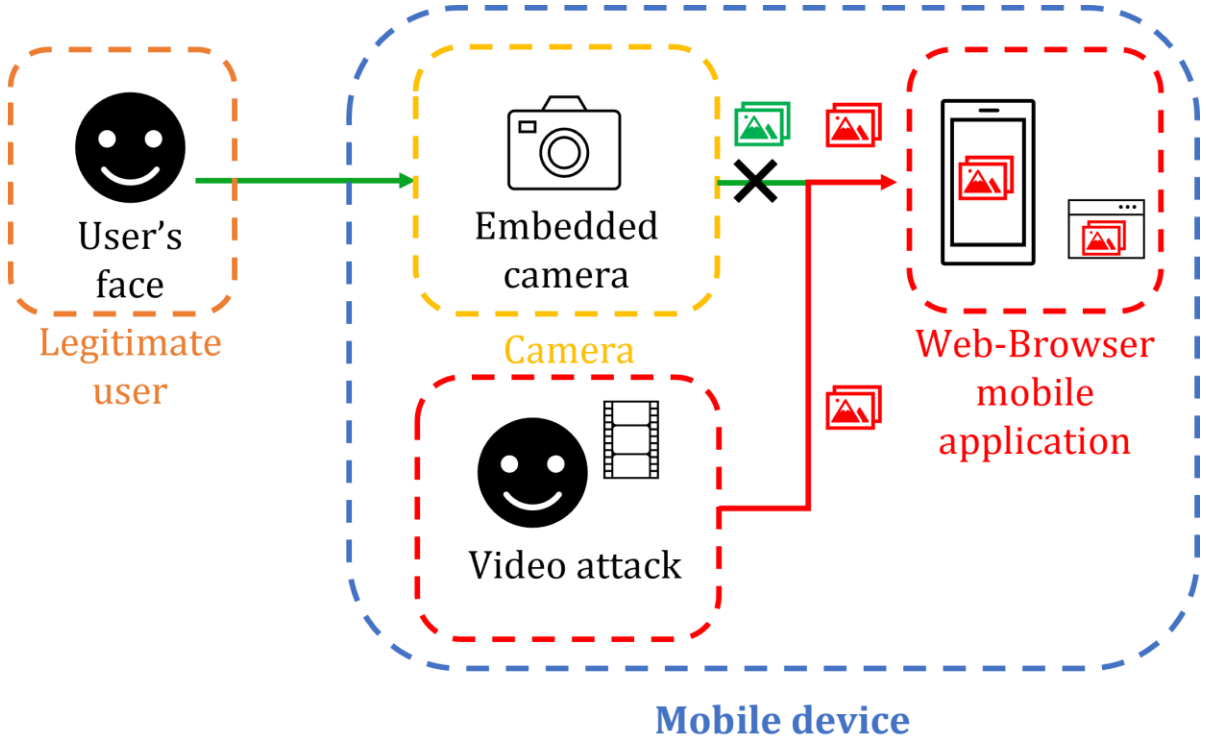
Results for simple video injection attacks

- Unissey is supposed to have a detection system for virtual devices
- The video used is a simple portrait video
- We have used 4 virtual devices: 3 virtual cameras (OBS, Manycam and Akvcam) and 1 capture card (Camlink)

Web-browser (OS)	OBS	Manycam	Akvcam	Camlink
Chrome (Win10)	**Detected**	**Detected**	*Incompatible*	**Detected**
Edge (Win10)	**Detected**	**Detected**	*Incompatible*	**Detected**
Opera Win10)	**Detected**	**Detected**	*Incompatible*	**Detected**
Firefox (Linux)	**Detected**	*Incompatible*	**Detected**	*Incompatible*
Chromium (Linux)	**Detected**	*Incompatible*	**Detected**	*Incompatible*

ALL the attacks have been detected by the system

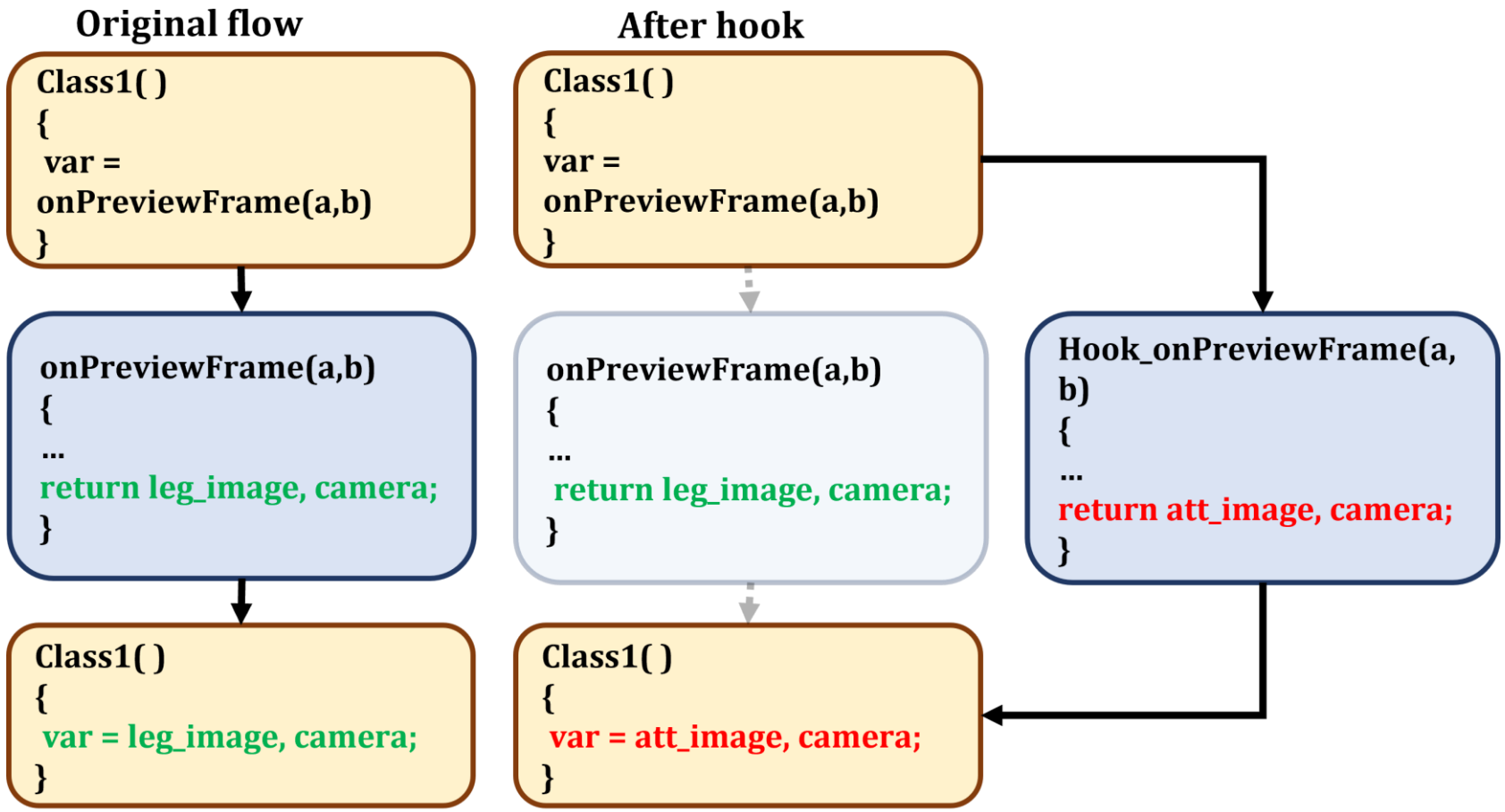
A more elaborated video injection attack



Needed materials

- A rooted Android device (see how to root a smartphone in the paper)
- A web browser mobile application
- Frida: the tool which enables the hook process (see next slide)
- A Javascript file containing the injection script (see how to write the injection script in the paper)

Hook process



Video injection attacks performed

- Attack 1: a simple portrait photo
- Attack 2: Face reenactment (with Avatarify). It consists in giving some « movements » to a portrait photograph.
- Attack 3: Low quality deepfake (Reface)
- Attack 4: a simple face video
- Attack 5: High quality deepfake (DeepfaceLab)

Attack 3

Attack 5

Deepfake attacks

Results for elaborated injection attack

- Each injection attack have been performed with four different subjects (2 women and 2 men) of different ages
- The word *success* describes the success for bypassing the system

Attacks	Victim 1	Victim 2	Victim 3	Victim 4
Simple photo	Success	Success	Success	Success
Face reenactment	Success	Success	Success	Success
LQ deepfake	Success	Success	Success	Success
Simple video	Success	Success	Success	Success
HQ deepfake	Success	Success	Success	Success

ALL the attacks have fooled the system

Agenda

1. General introduction
2. Introduction to biometrics and liveness detection
3. Our experiments
4. **Conclusion**

Conclusion

- Video injection attacks are a real threat for biometric systems where the data capture system is under the control of the user
- This threat highly concerns remote identity verification systems
- There is a real need to develop video injection attacks detection systems as smartphones and computer can’t be considered as trustworthy
- In our next work, we will focus on new countermeasures to overcome this new breach

Thanks for your attention

Questions ?