Biometric Spoofing and Anti-Spoofing

Presentation Attack Detection

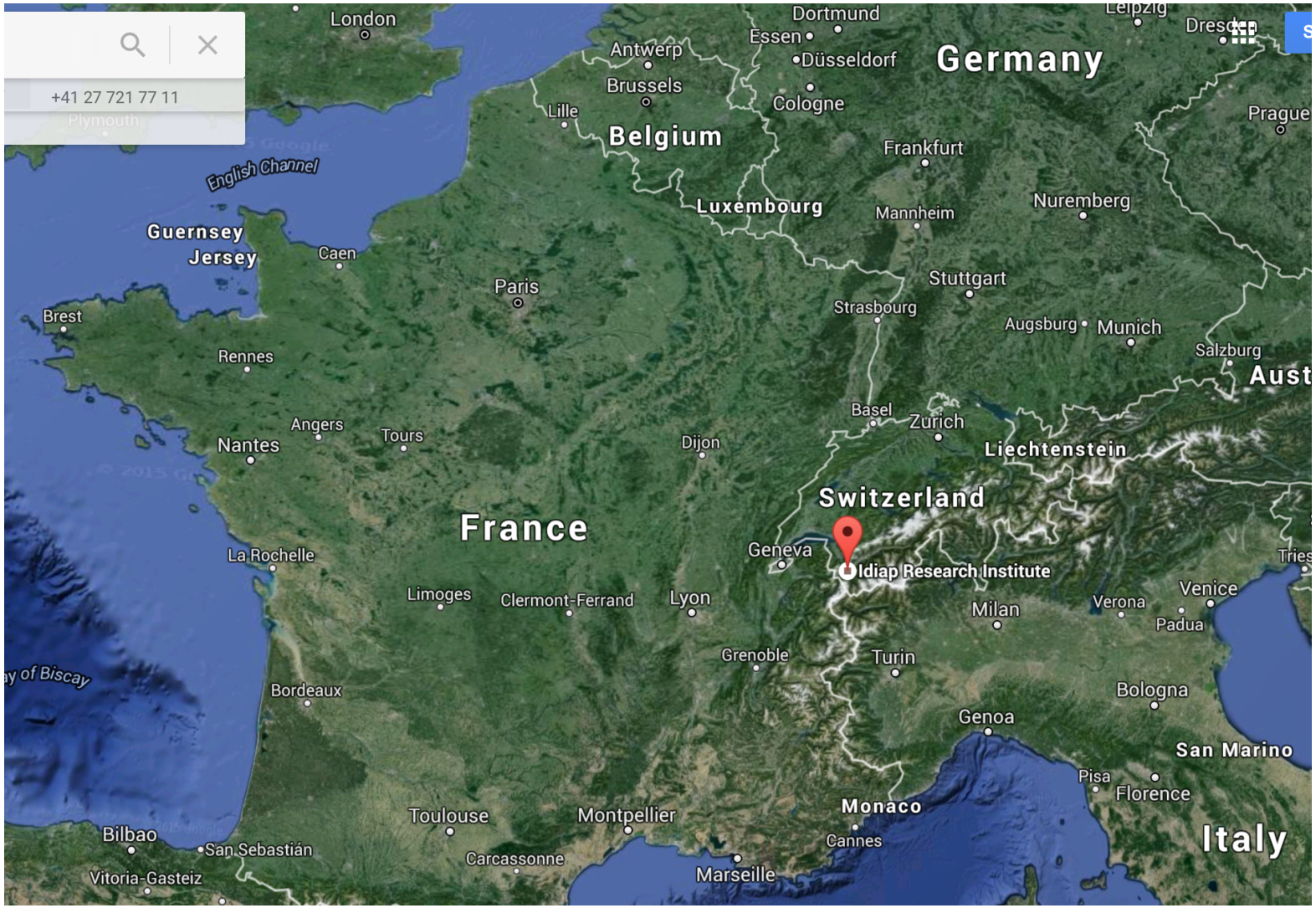
Sébastien Marcel
Head of the Biometrics Security and Privacy group
http://www.idiap.ch/~marcel

IAPR/IEEE Winter School on Biometrics,
Shenzhen,
China – Feb 1 2018

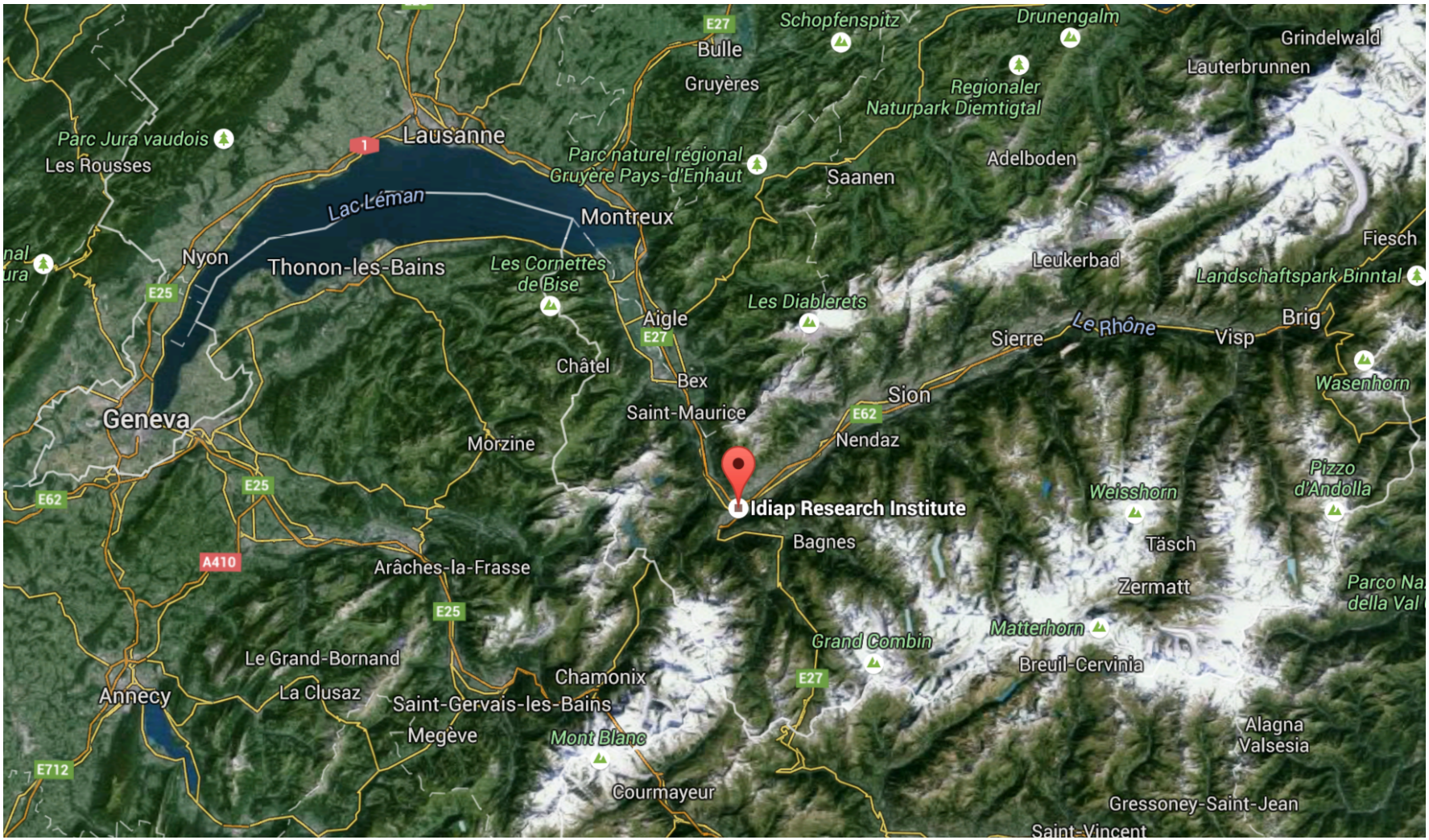
Outline

- Idiap
  - Where is Idiap ?
  - What is Idiap ?
- Introduction
  - Biometrics Security
  - Presentation Attacks in Movies
  - Presentation Attacks in reality
  - Definition
  - Importance
- Presentation Attacks
  - Seminal work
  - Presentation Attacks
  - Face PA
- Presentation Attack Detection
  - Presentation Attack Detection
  - Face PAD
- Performance evaluation
  - Biometrics and PAD
- The End

Where is Idiap ?



Where is Idiap ?



Where is Idiap ?

Altitude to ski ranges from 1400m to 3000m

What is Idiap ?

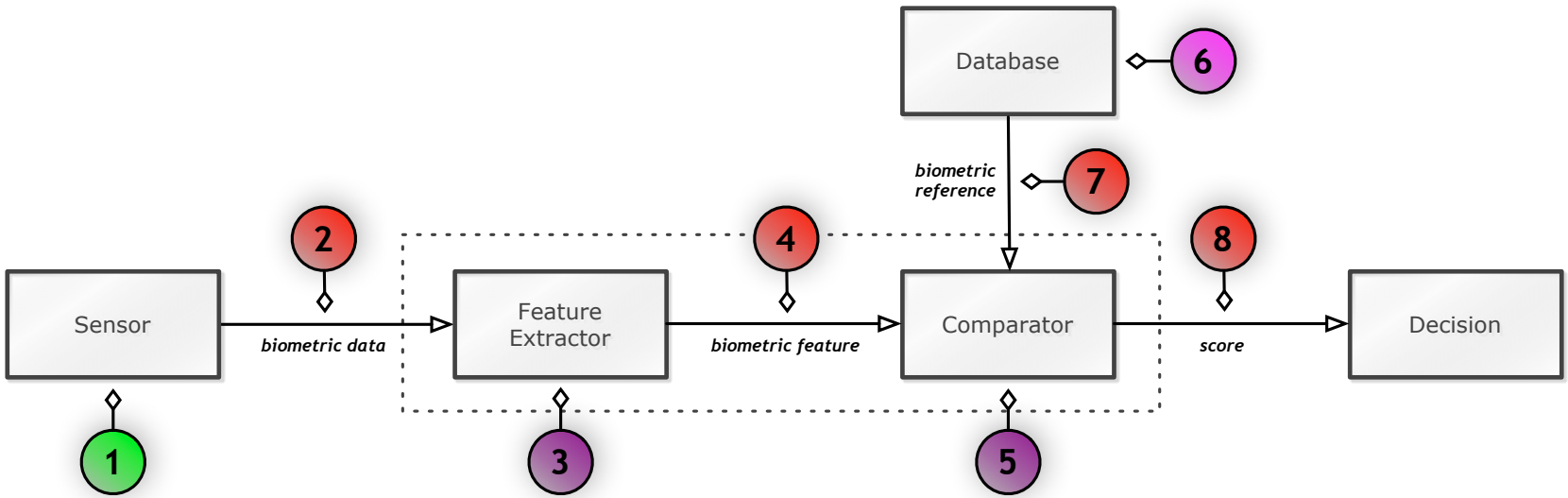
- Non-for-profit research institute founded in 1991
- Affiliated with École polytechnique fédérale de Lausanne (EPFL)
- Research, Education and Technology transfer
- 9 research groups in Human & Media Computing (computer vision, speech and audio, machine learning, ...) and one group on **Biometrics Security and Privacy**

For more information:

www.idiap.ch

Biometrics Security

A biometric system is vulnerable to attacks [1]

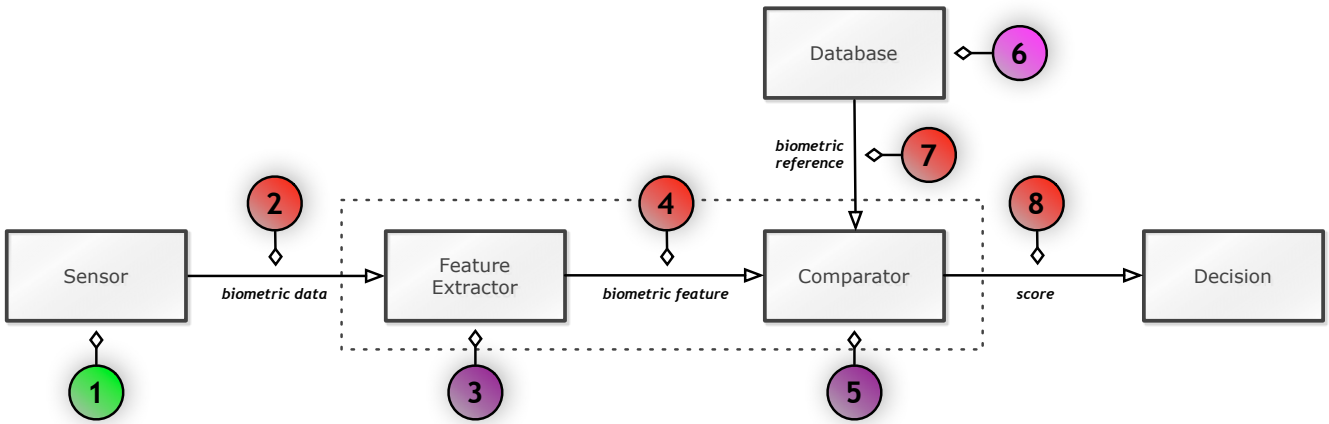


- Indirect attacks (**2-8**)
- Direct attacks (**1**)

[1] NK Ratha et al., *Enhancing security and privacy in biometrics-based authentication systems*, IBM Systems Journal, 40(3):614634, 2001

Biometrics Security

Indirect Attacks

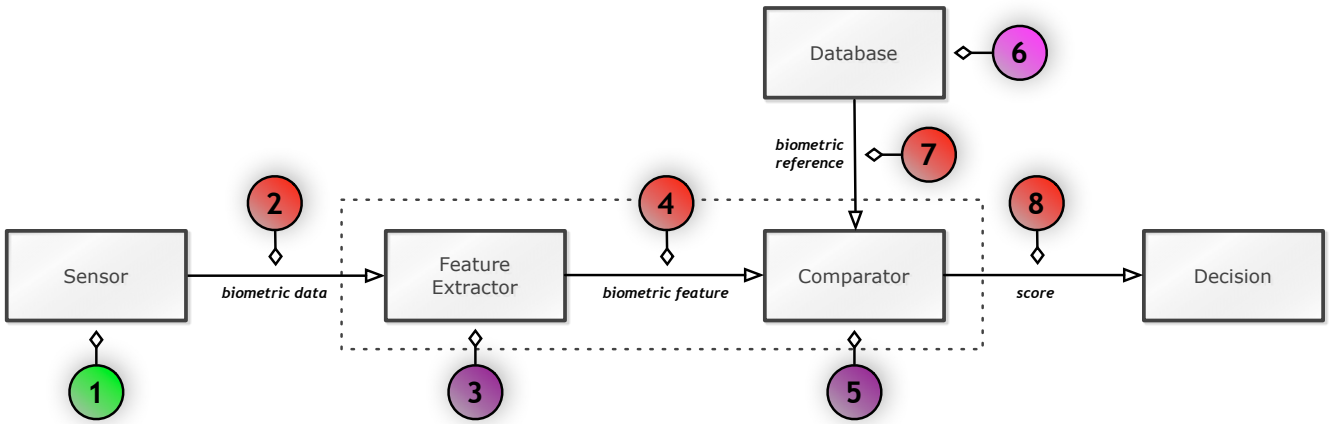


Indirect attacks are performed inside the system by:

- bypassing the feature extractor or the comparator (**3**, **5**),
- manipulating the biometric references in the biometric reference database (**6**),
- exploiting possible weak points in communication channels (**2**, **4**, **7**, **8**).

Biometrics Security

Direct Attacks



Direct attacks (**presentation/spoofing attacks**) are performed at the sensor level: the sensor is fooled and not replaced nor tampered.

In this lecture we are concerned with **presentation attacks**

Presentation Attacks in Movies

MacGyver - The Human Factor (S02E01 1986)

Using dust and jacket to simulate a hand on the hand print scanner !

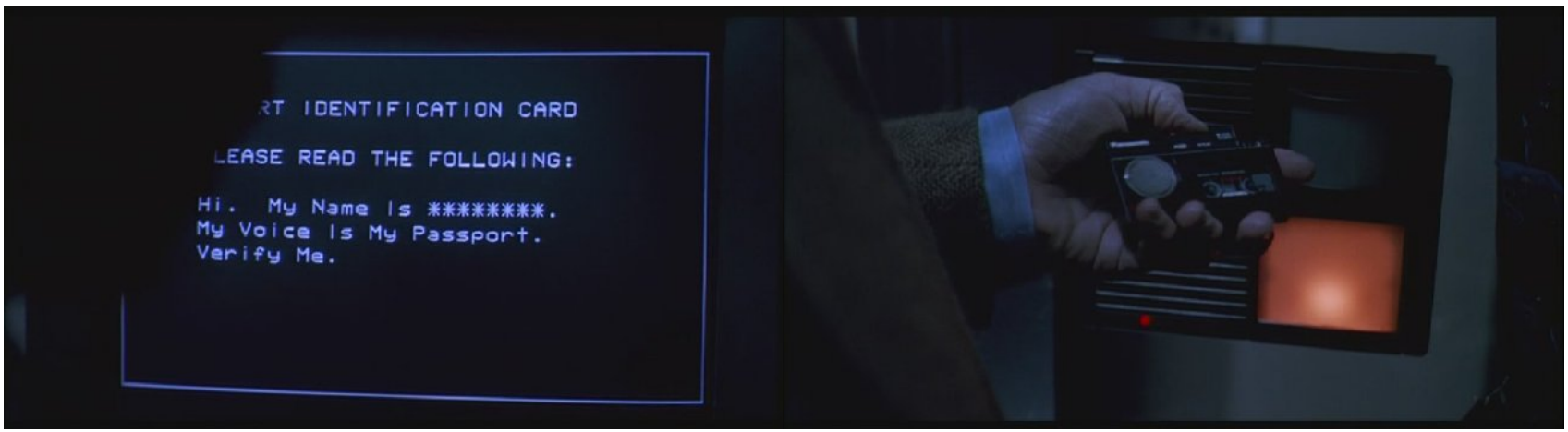
Presentation Attacks in Movies

MacGyver - The Human Factor (S02E01 1986)

1. scraped some plaster off the walls,
2. sprinkled the plaster dust over the palm print reader revealing the Colonels hand print,
3. laid a jacket down over the plaster hand print impression and lightly pressed down on the reader.

Presentation Attacks in Movies

Sneakers (1992)



Replay a voice recording in front of a speaker recognition system !

Presentation Attacks in Movies

Sneakers (1992)

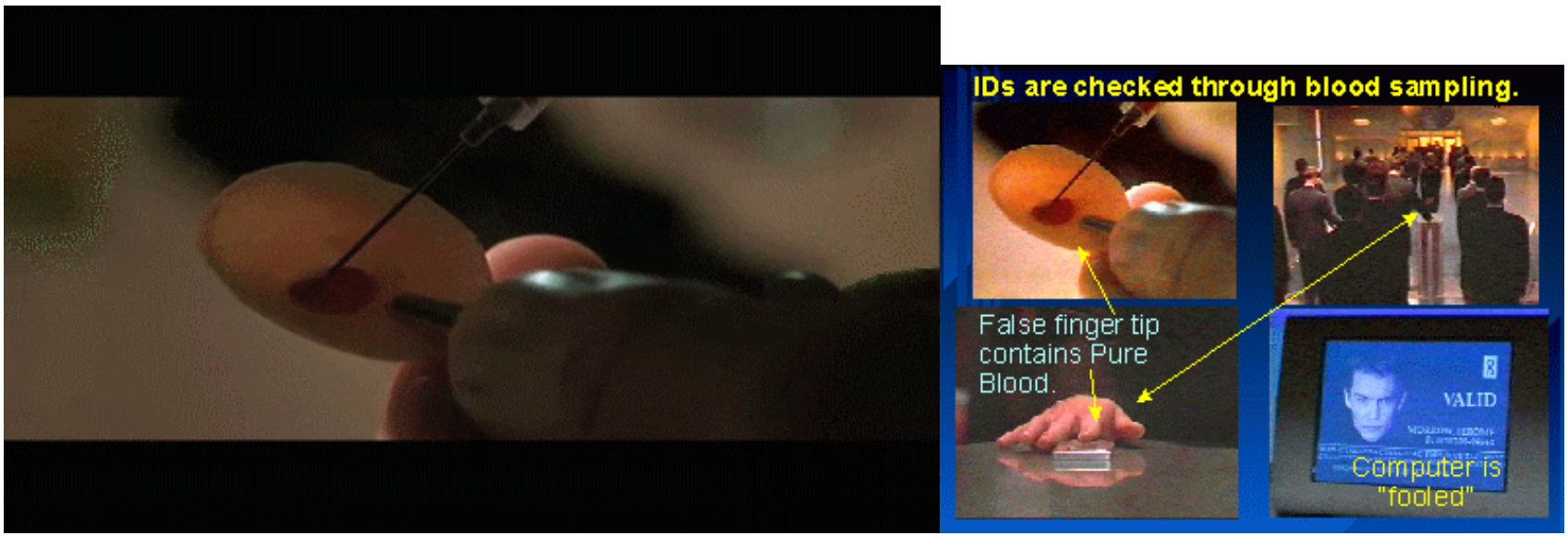
Presentation Attacks in Movies

Demolition Man (1993)

Present an eyeball in front of a iris scanner !

Presentation Attacks in Movies

GATTACA (1997)



Injecting blood samples in a false finger tip to fool DNA identification !

Presentation Attacks in Movies

Minority Report (2002)

Using eyeball-swapping surgery to avoid iris identification !

Presentation Attacks in Movies

X-Men 2 (2003)

High-tech iris spoofing !

Presentation Attacks in Movies

RED 2 (2013)

Iris spoofing (not retina) with a fake contact lens !

Presentation Attacks in reality

Bank robbery (2010)

Conrad Zdzierak used a silicon masks to pass himself off as a black character "SPFX The Player" during robberies !

Presentation Attacks in reality

Hong Kong - Vancouver (Jan 2011)

A passenger boarded a plane in Hong Kong with an old man mask and arrived in Canada !

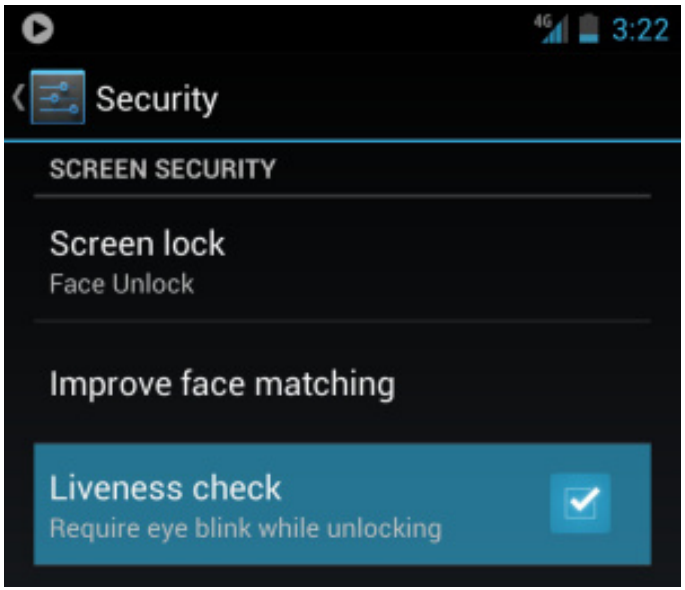
Presentation Attacks in reality

Android 4.0 (Nov 2011)

Android 4.0 Face UnLock feature spoofed by photograph

Presentation Attacks in reality

Android 4.1 (Jun 2012)



Liveness check (eye blink) introduced in Android 4.1

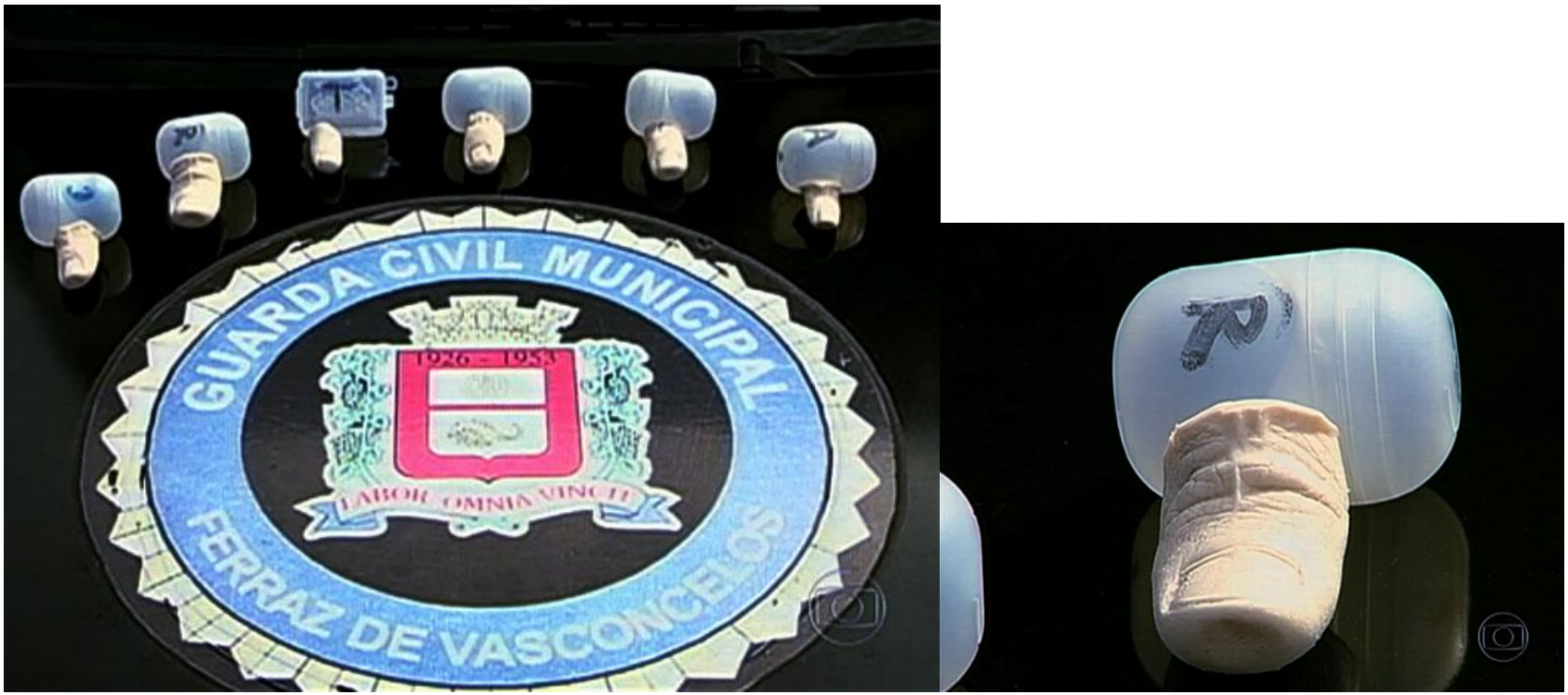
Presentation Attacks in reality

Bank robbery again (2012)

Burglars who robbed a cash-checking store in Queens disguised as cops !

Presentation Attacks in reality

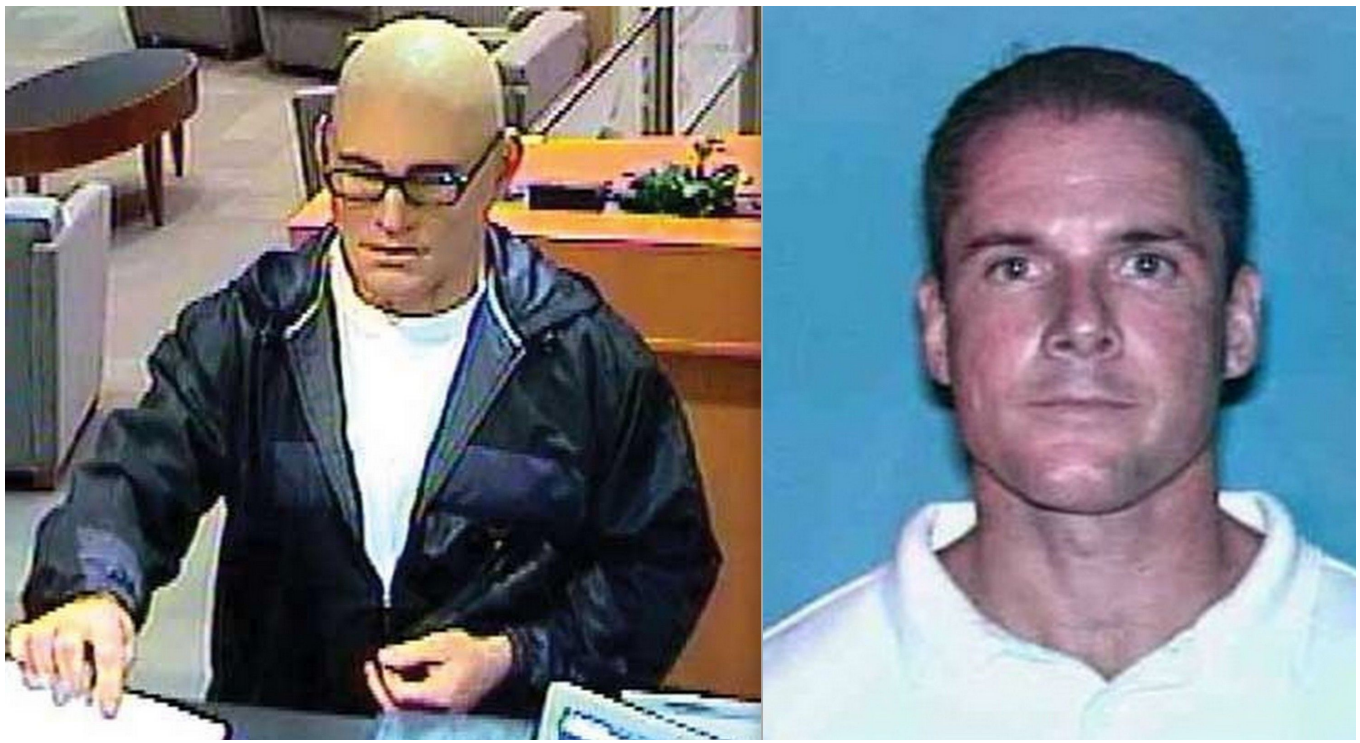
Brazil (March 2013)



Fake fingers used to fool Hospital clock-in scanner

Presentation Attacks in reality

More bank robbery (2013)



Steven Ray Milam robbed 11 banks in Texas with "SPFY The Handsome Guy" silicon mask

Presentation Attacks in reality

iPhone 5s - Touch ID (Sep 20 2013)

How many days will it take to spoof it ?

Presentation Attacks in reality

iPhone 5s - Touch ID (Sep 20 2013)

How many days will it take to spoof it ? 2 days !
iPhone 5s spoofed by the Chaos Computer Club (1st public ...)

Presentation Attacks in reality

iPhone 5s spoofed by CCC (Sep 21 2013)

http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid

Presentation Attacks in reality

Apple and fingerprints the full story

http://fingerchip.pagesperso-orange.fr/biometrics/types/fingerprint_apple.htm

Jean-François Mainguet (Sep 22 2013)

Presentation Attacks in reality

Finger-vein (Oct 2014)

Finger-vein commercial system spoofed by a piece of paper

Presentation Attacks in reality

Samsung Galaxy S8 Iris spoofed by CCC (May 23 2017)

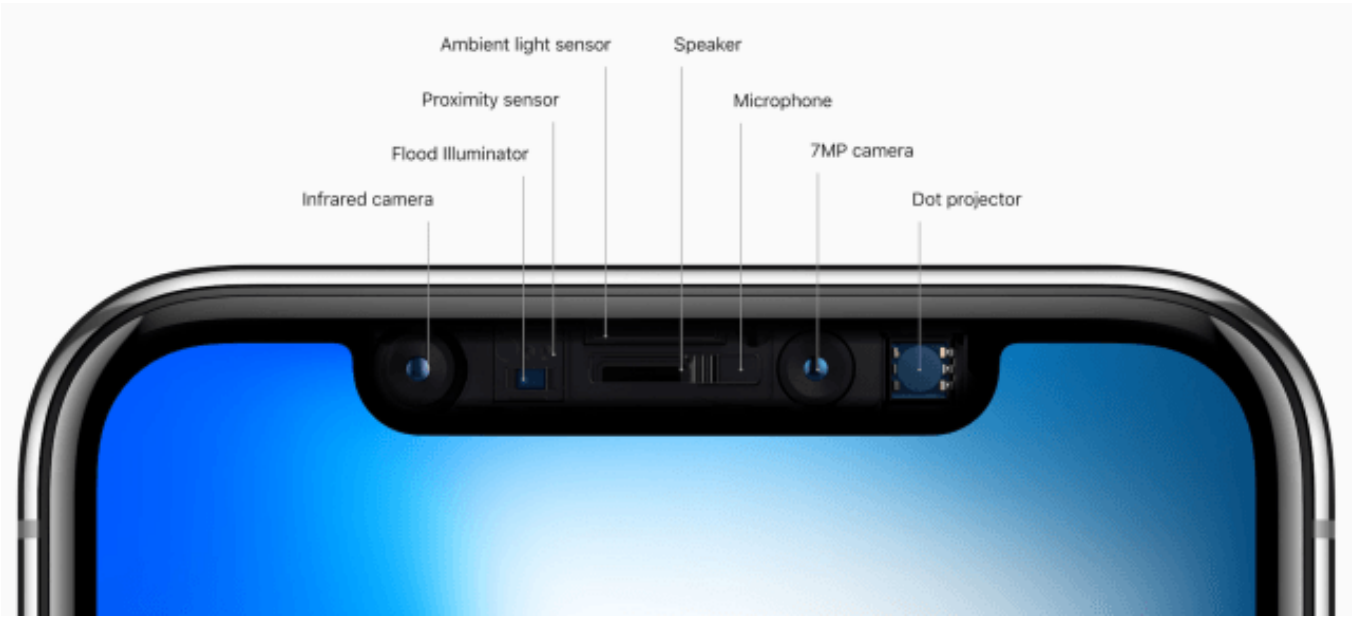
Presentation Attacks in reality

Samsung Galaxy S8 Iris spoofed by CCC (May 23 2017)

https://media.ccc.de/v/biometrie-s8-iris-en

Presentation Attacks in reality

iPhone X FaceID (Sep 2017)

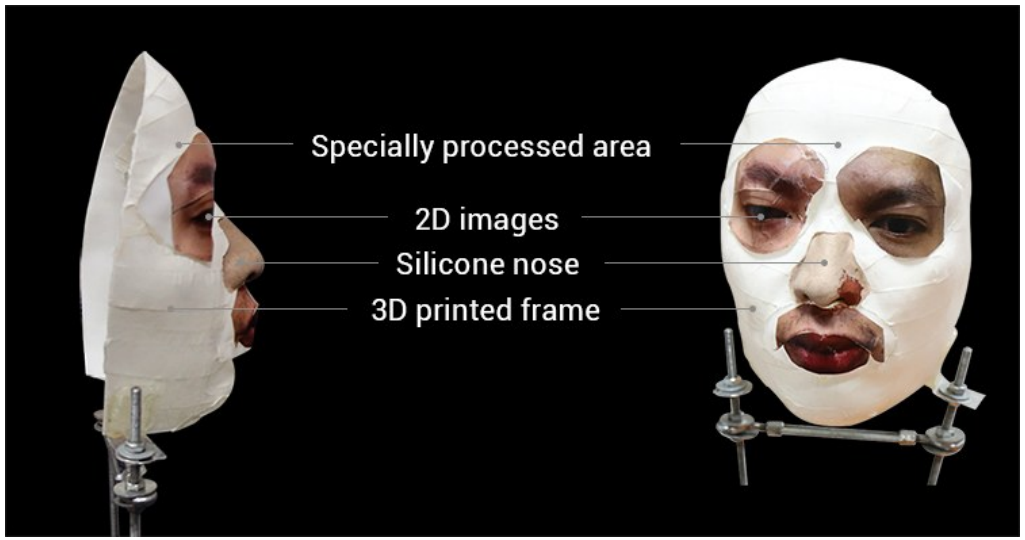


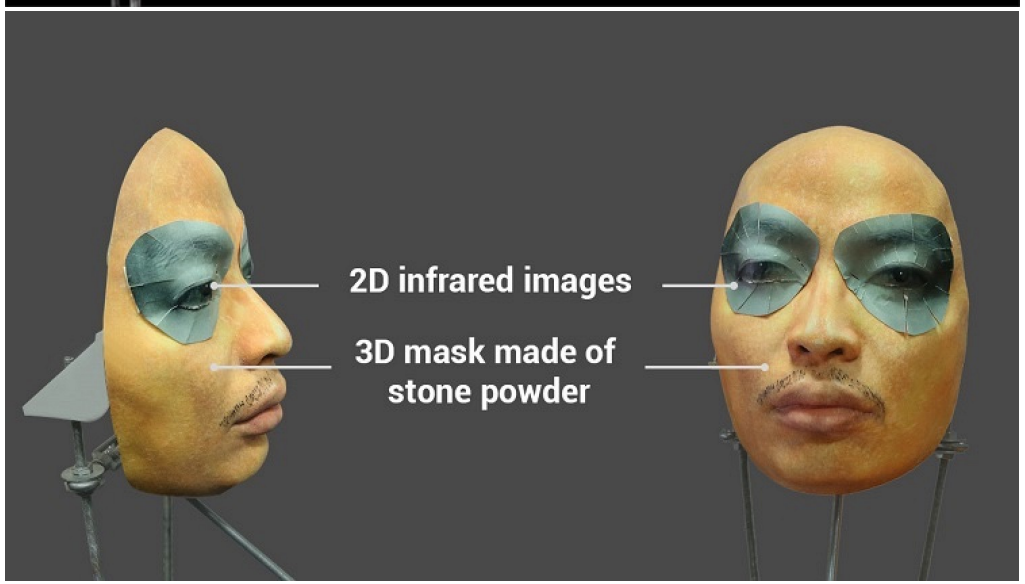
Presentation Attacks in reality

iPhone X FaceID robust to masks (Sep 2017)

Presentation Attacks in reality

iPhone X spoofed by Bkav (Nov 27 2017)





http://www.bkav.com

Definitions

Spoofing Attack

Outwitting a biometric sensor by presenting a counterfeit biometric evidence of a valid user[2]

Anti-Spoofing

Countermeasure to spoofing attack

No common terminology so far

spoofing, **evasion/concealment**, anti-spoofing, liveness detection, presentation attack, presentation attack detection, ...

[2] K. A. Nixon et al. *Spoof Detection Schemes; Handbook of Biometrics*, 2008

Definition by ISO [3]

Presentation Attack – PA

presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

methods: artefact, mutilations, replay, ...

goals: impersonation or not being recognized (concealment)

Normal (Bona Fide) Presentation

interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system

in short anything which is not a PA !

Presentation Attack Instrument – PAI

biometric characteristic or object used in a presentation attack

eg. artefacts, dead bodies, altered fingerprints, ...

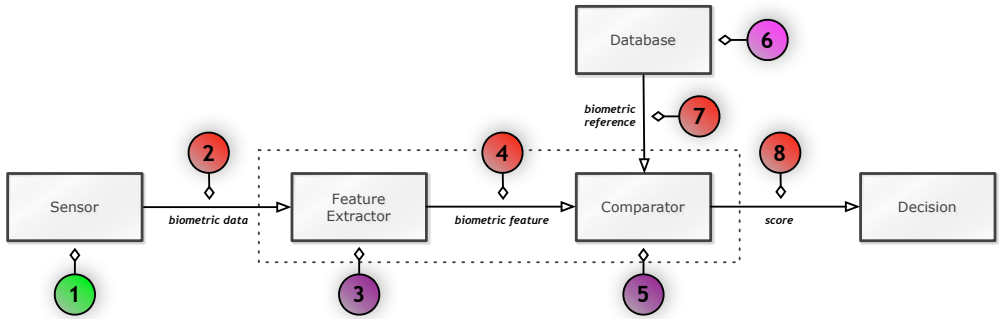
Presentation Attack Detection – PAD

automated determination of a presentation attack

[3] ISO/IEC 30107-1:2016, *Biometric presentation attack detection – part 1*, 2016

Importance

Presentation Attack is a major threat



because it can be created and performed by anyone with no specific skills in computer science

Importance

Funding programs/projects

- EU TABULA RASA "Trusted Biometrics under Spoofing Attacks" (2010-2014)

  www.tabularasa-euproject.org

- EU BEAT "Biometrics Evaluation and Testing" (2012-2016)

  www.beat-eu.org

- CH/VS: Swiss Center for Biometrics Research and Testing (2014–)

  www.biometrics-center.ch

- NO: SWAN "Secure Access Control Over Wide Area Network" (2016-2019)

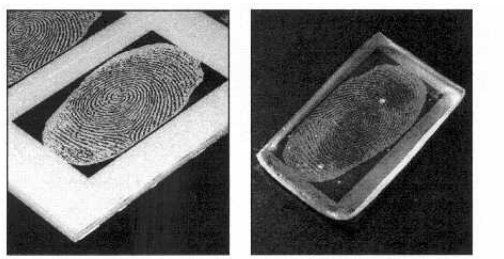
  www.ntnu.edu/iik/swan

- US: IARPA Odin Thor/Loki red team approach (2017-2020)

  www.iarpa.gov/index.php/research-programs/odin

Seminal work

"Gummy Fingers" [4]



(a) The mold for gummy fingers (b) Gummy finger

Figure 4.5 Photographs of the outside appearance of the mold and a *gummy* finger. The *gummy* finger was produced from a residual fingerprint on a glass plate, enhancing it with a cyanoacrylate adhesive

Figure 4.6 The Fingerprint image of the *gummy* finger, which was displayed by the system with Device H (equipped with a capacitive sensor).

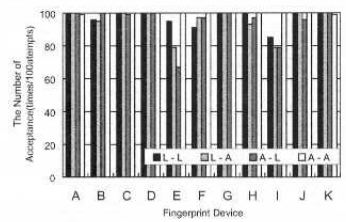
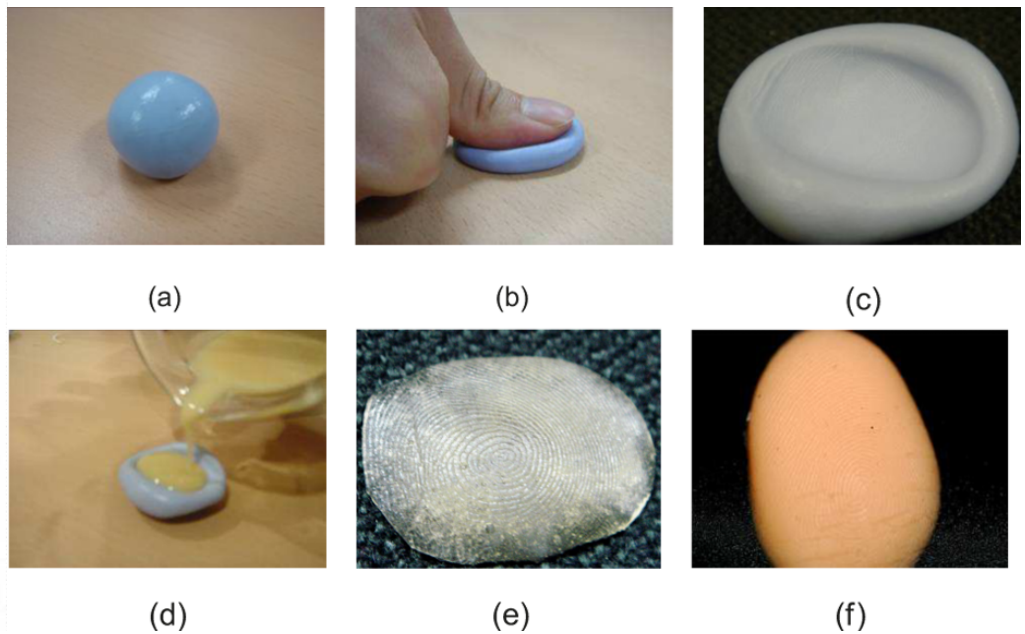


Figure 4.7 Average number of acceptance for each device, in terms of *gummy* fingers which were cloned from residual fingerprints. Here, the subject is one person.



Gelatin fake fingers to spoof 11 fingerprint biometric systems

[4] T. Matsumoto et al., *Impact of Artificial Gummy Fingers on Fingerprint Systems*, SPIE 4677, Optical Security and Counterfeit Deterrence Techniques IV, 275, 2002, (http://cryptome.org/gummy.htm

Seminal work

Prior work with Fake Fingerprints

T. van der Putte and J. Keuning *Biometrical Fingerprint Recognition Don't Get Your Fingers Burned*, Conference on smart card research and advanced applications, 289-303, 2001 (`http://cryptome.org/fake-prints.htm`)

M. Kàkona *Biometrics: yes or no?*, 2001 (`http://home.i.cz/kakl/biometrics/Biometricsyesorno.htm`)

L. Thalheim et al. *Body Check: Biometric Access Protection Devices and their Programs Put to the Test*, 2002

Seminal work

Black Hat 2009 [5]

Printed photo to spoof face recognition systems on 3 laptops

[5] D. Nguyen et al., *Your Face Is NOT Your Password*, 2009

Seminal work

Black Hat 2009

Printed photo to spoof face recognition systems on 3 laptops:

- Asus (F6S Series, X80 Series): Asus SmartLogin ver 1.0.0005
- Toshiba (L310, M300): Toshiba Face Recognition ver 2.0.2.32
- Lenovo (Y410, Y430): Lenovo Veriface III

Presentation Attacks

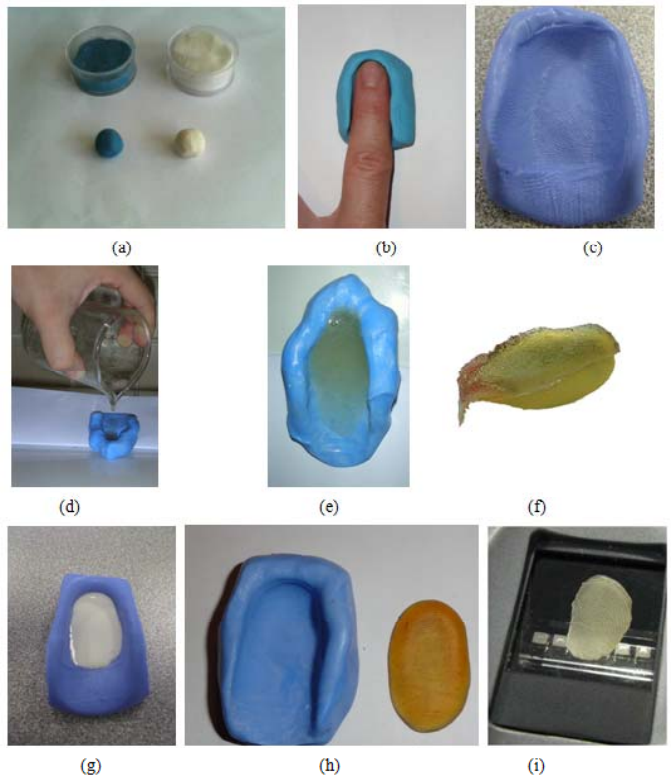
Fingerprint PA

Presenting a fake fingerprint to a capture device

Acknowledgement: Gian Luca Marcialis and Fabio Roli @ UNICA

Presentation Attacks

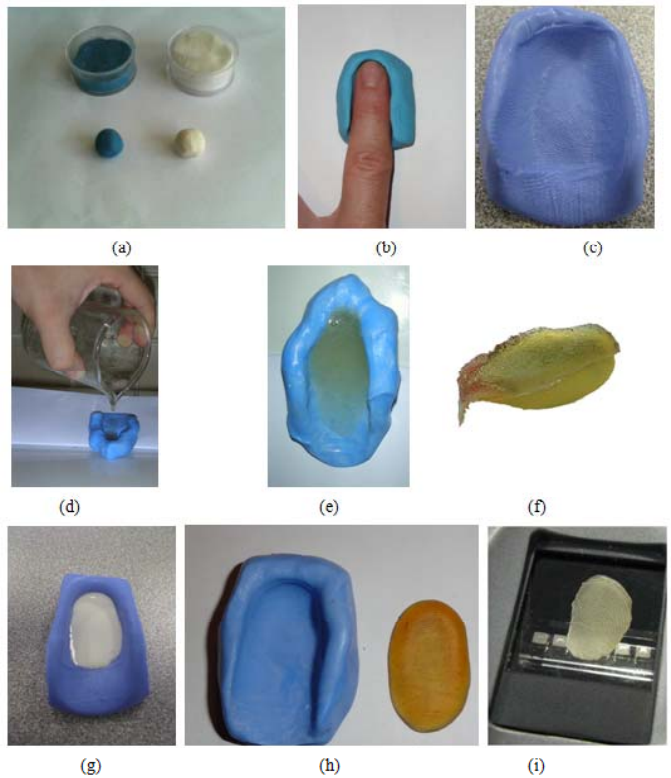
Fingerprint PA: latex/silicone PAI (with cooperation)



Prepare a silicone mold (a, b and c)

Presentation Attacks

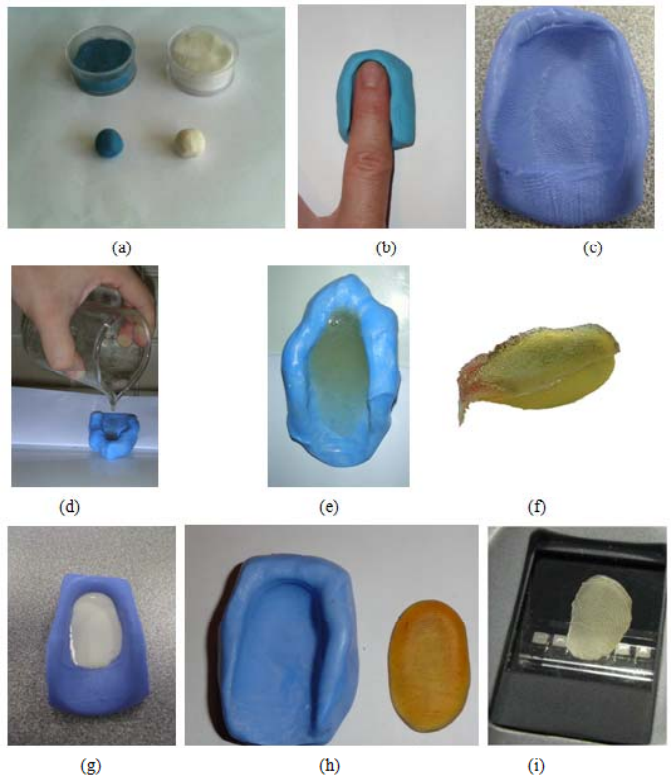
Fingerprint PA: latex/silicone PAI (with cooperation)



Prepare fake with liquid latex (d, e and f)

Presentation Attacks

Fingerprint PA: latex/silicone PAI (with cooperation)



Use fake (g, i and j)

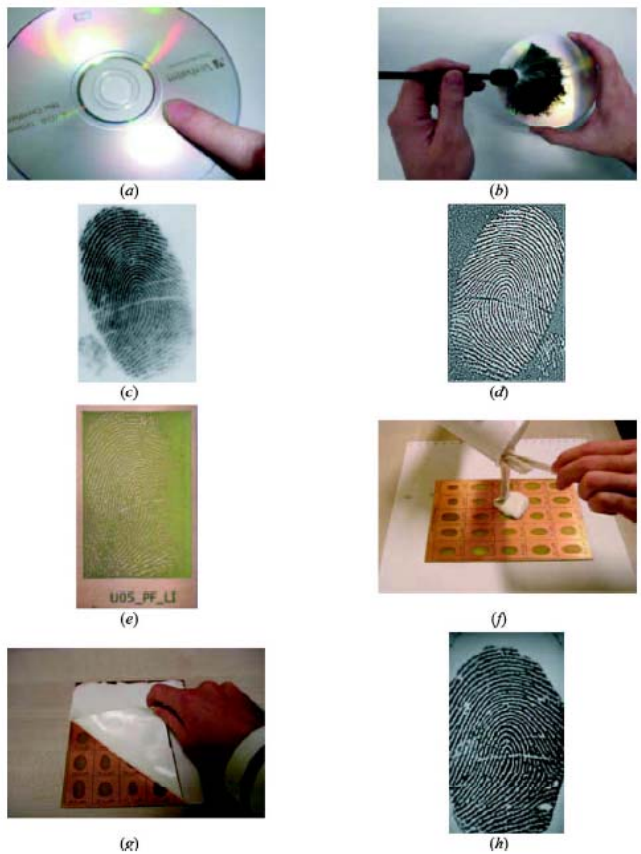
Presentation Attacks

Fingerprint PA: wood glue PAI (with cooperation)

Same recipe but with hot glue and wood glue !

Presentation Attacks

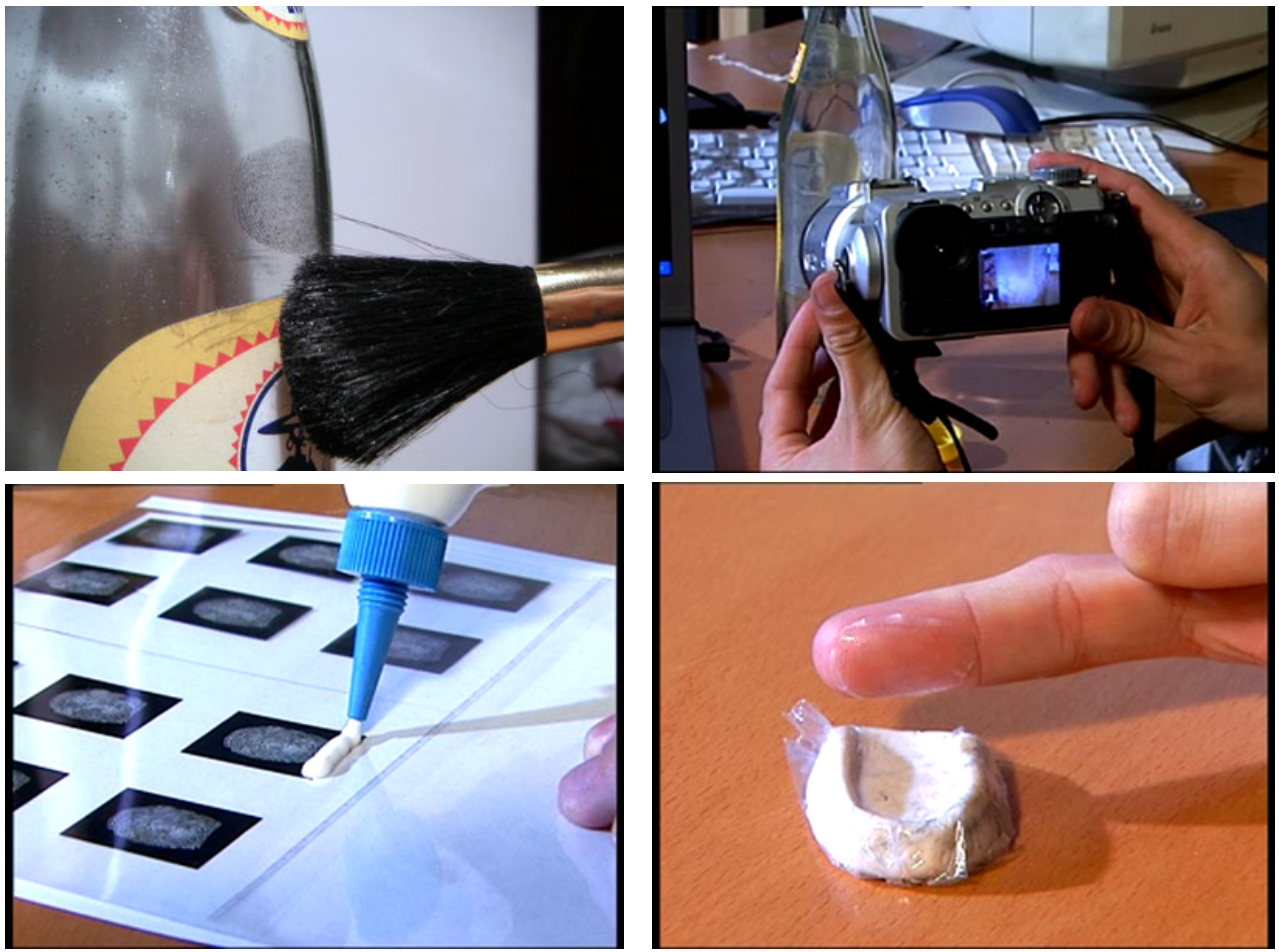
Fingerprint PA: latex/silicone PAI (without cooperation)



The lifted latent fingerprint is printed on a PCB (Printed Circuit Board) to serve as a mold

Presentation Attacks

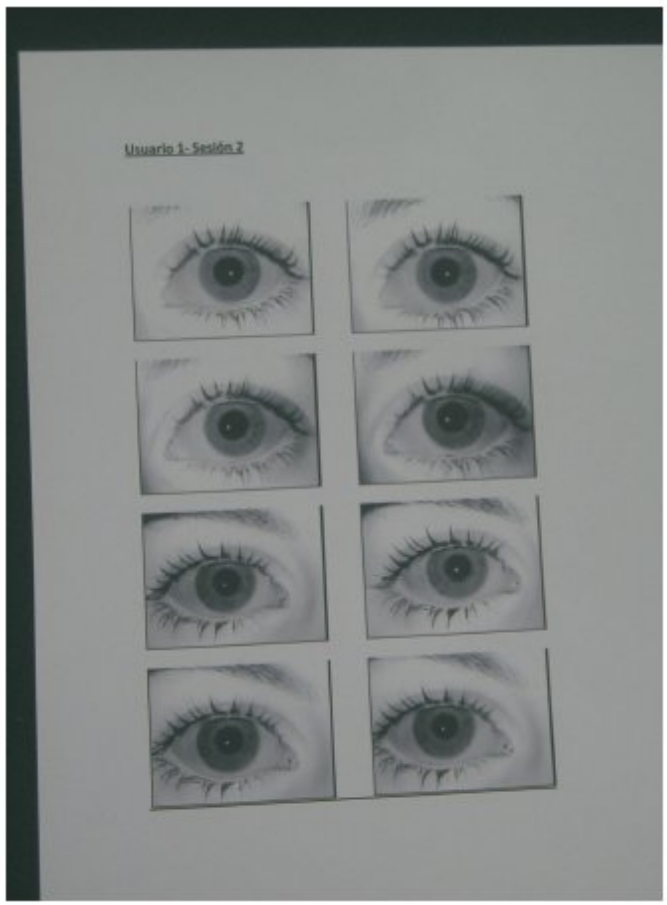
Fingerprint PA: wood glue PAI (without cooperation)



CCC vs iPhone5s: http://dasalte.ccc.de/biometrie/fingerabdruck_kopieren?language=en

Presentation Attacks

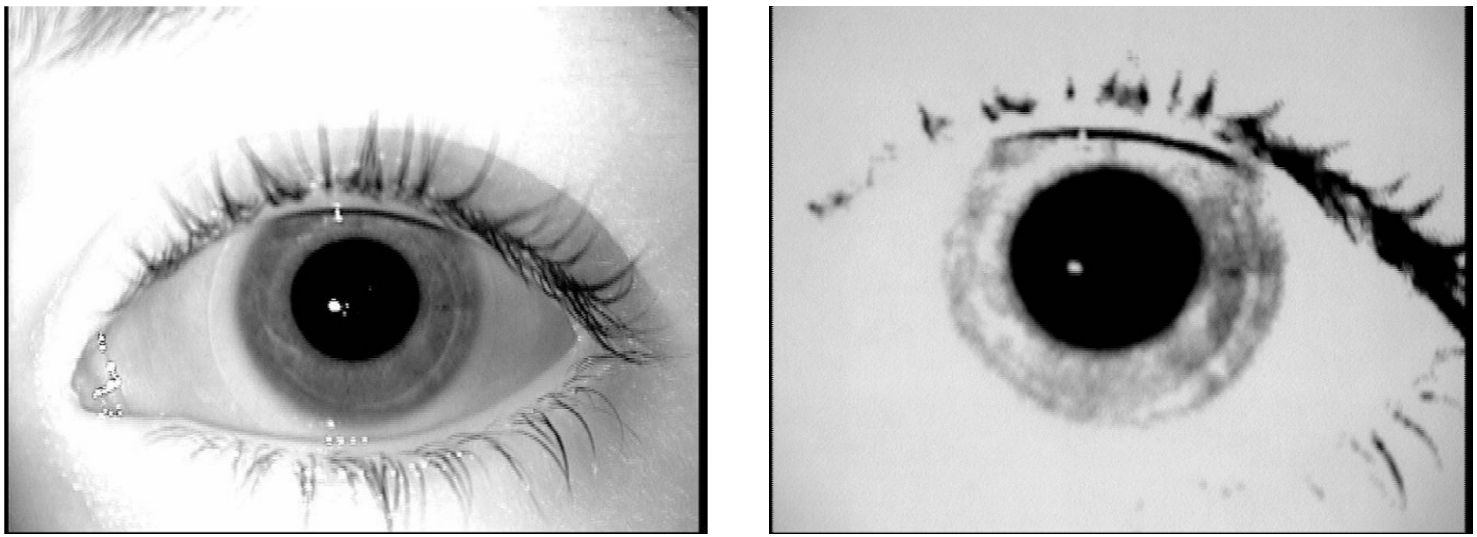
Iris PA: printed paper PAI



High quality paper and inkjet printer

Presentation Attacks

Iris PA: printed paper PAI



Real Iris (left) vs Fake Iris (right)

Acknowledgement: Julian Fierrez @ UAM

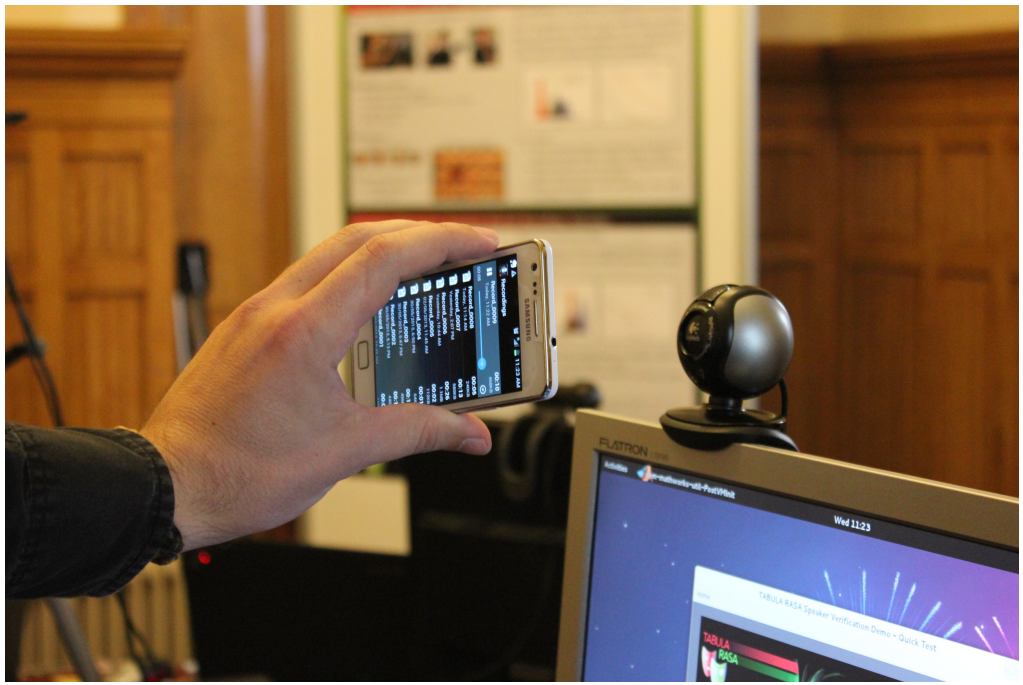
Presentation Attacks

2D face PA: printed paper PAI

Same recipe for photo and video attacks with a mobile phone or a tablet

Presentation Attacks

Voice PA – replay PAI [6]



Playback of a voice recording, a synthesised speech or a converted voice in front of a microphone

Acknowledgement: Nicholas Evans @ EURECOM

[6] "On the vulnerability of speaker verification to realistic voice spoofing", S. Ergunay, E. Khoury, A. Lazaridis, and S. Marcel, BTAS 2015.

Presentation Attacks

Voice PA: replay PAI

Original voice of target speaker (rec on HQ mic)
Playback with laptop (rec on laptop)
Playback with iPhone (rec on laptop)
Playback with Samsung (rec on laptop)

Voice PA: voice synthesis PAI

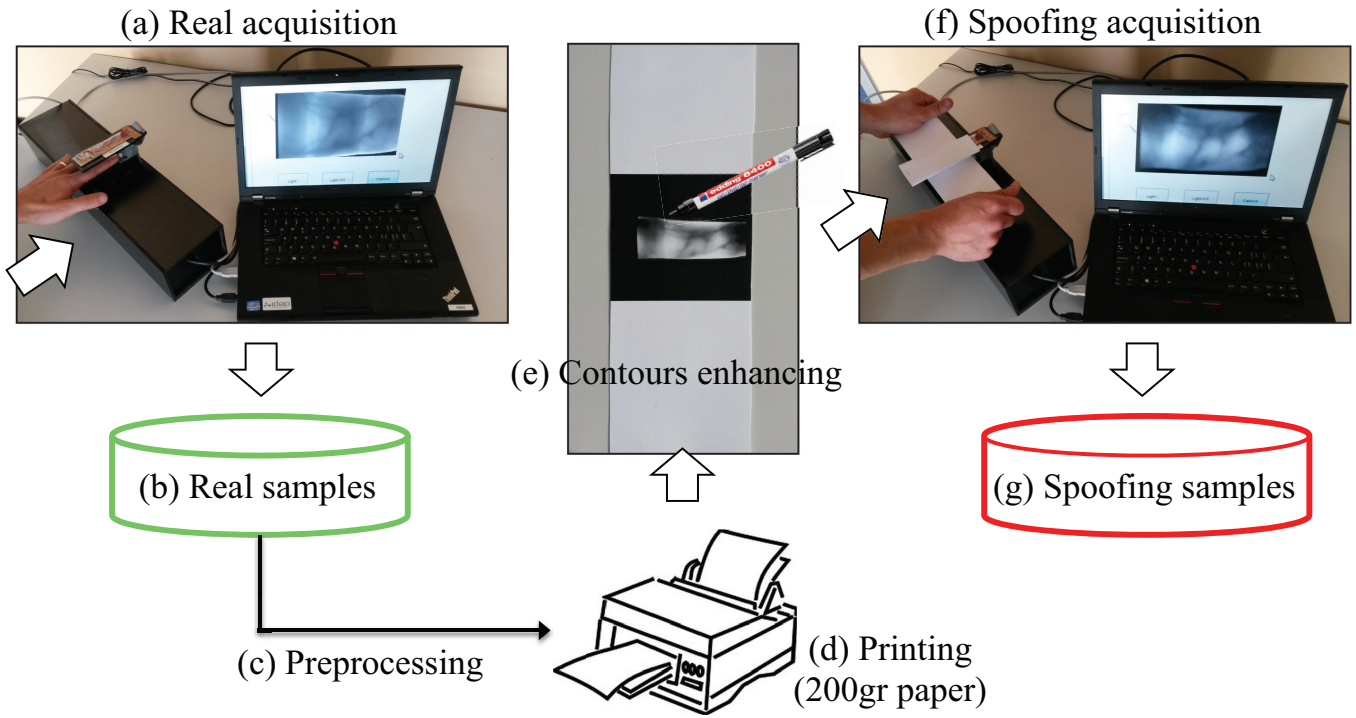
Voice of target speaker synthesized
Playback with laptop (rec on laptop)

Voice PA: voice conversion PAI

Original voice of source speaker (rec on laptop)
Voice of target speaker converted from source speaker
Playback with laptop (rec on laptop)

Presentation Attacks

Fingervein PA: printer paper PAI[7]

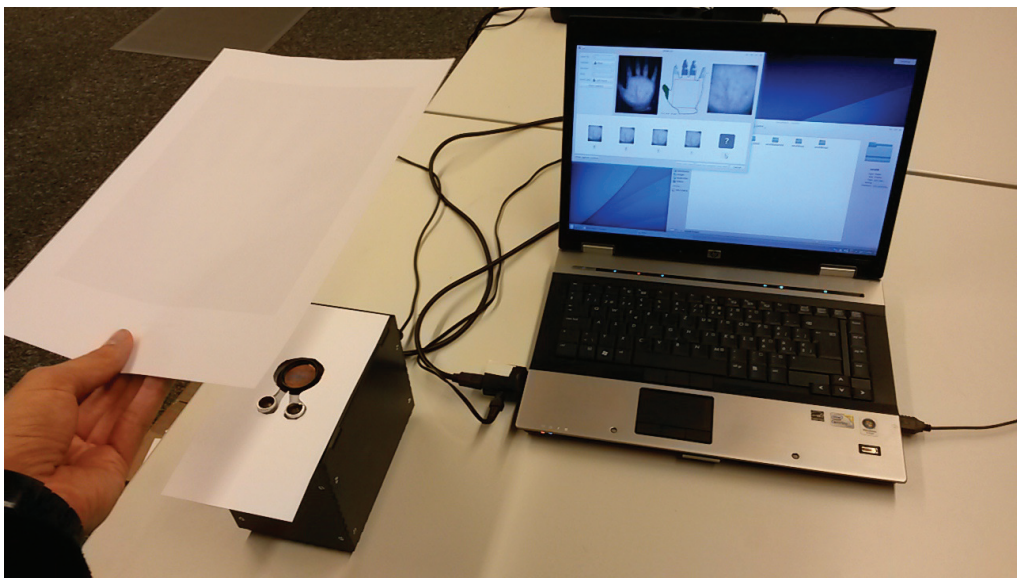


with paper

[7] "On the vulnerability of finger vein recognition to spoofing", P. Tome, M. Vanoni, and S. Marcel, IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2014.

Presentation Attacks

Palmvein PA: printed paper PAI[8]



with paper

[8] "On the vulnerability to palm vein recognition to spoofing attacks", P. Tome and S. Marcel, International Conference on Biometrics (ICB), 2015.

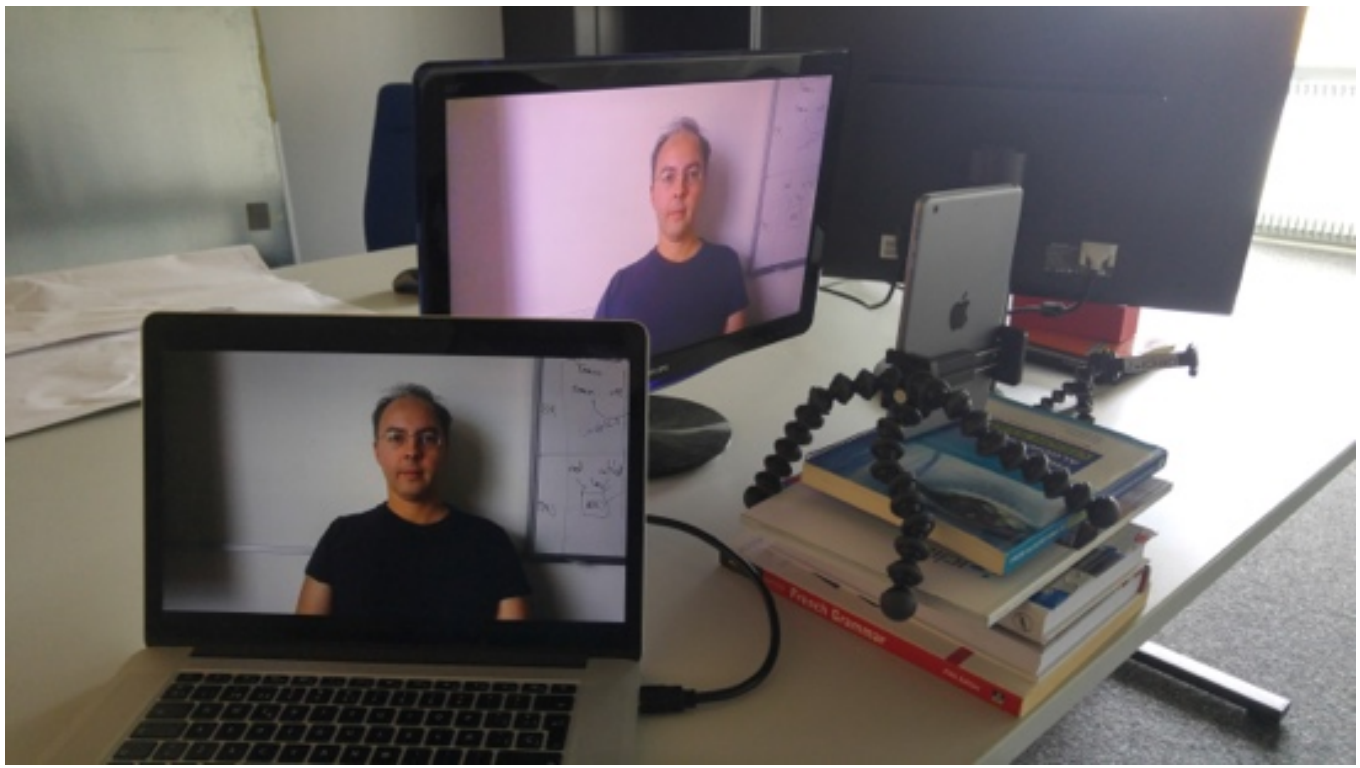
Presentation Attacks

2D face PA: printed paper PAI [9]

[9] "Counter-Measures to Photo Attacks in Face Recognition: a public database and a baseline", A. Anjos and S. Marcel, IJCB, 2011.

Presentation Attacks

2D face PA: photo/video screen PAI [10]



[10] "The REPLAY-MOBILE Face Presentation-Attack Database", A. Costa-Pazo and al., BioSig, 2016.

Presentation Attacks

2D face PA: biometric data (print/photo/video PAI)

Why one is real (Bona Fide) or fake (PA) ?

Presentation Attacks

2D face PA: biometric data (print/photo/video PAI)

Why one is real (Bona Fide) or fake (PA) ?

All are fakes: print (left), iPhone (middle) and iPad (right) !

Acknowledgement: Andre Anjos @ IDIAP

Presentation Attacks

2D face PA: printed paper PAI

PA with printed paper exhibits:

- Reduced image texture
- Printer halftoning artifacts
- Mechanical artifacts (horizontal lines)
- No local motion (e.g., eye blinks)
- Borders of image may be visible

Presentation Attacks

2D face PA: biometric data (print/photo/video PAI)

Why one is real (Bona Fide) or fake (PA) ?

Presentation Attacks

2D face PA: biometric data (print/photo/video PAI)

Why one is real (Bona Fide) or fake (PA) ?

All are Bona Fide !

Acknowledgement: Andre Anjos @ IDIAP

Presentation Attacks

2D face PA: biometric data (print/photo/video PAI)

These as PAs!

Presentation Attacks

2D face PA: photo/video replay PAI

PA with an electronic screen exhibits:

- Blurred image texture
- Reduced color diversity
- Moiré effect

Presentation Attacks

2D face PA: 3D (rigid) mask PAI [11]

Hard resin composite in full 24-bit color !

Acknowledgement: Nesli Erdogmus @ IDIAP

[11] "Spoofing Face Recognition with 3D Masks", N. Erdogmus and S. Marcel, IEEE Transactions on Information Forensics and Security, 9(7):1084–1097, 2014.

Presentation Attacks

2D face PA: 3D (rigid) mask PAI

Cost: $\sim$ USD 300

Presentation Attacks

2D face PA: 3D (rigid) mask PAI

1 frontal and 2 profile pictures

http://www.thatsmyface.com

Presentation Attacks

2D face PA: 3D (paper) mask PAI

Cost: $\sim$ USD 25 – but not effective

Presentation Attacks

2D face PA: 3D (ridid) mask PAI

PA with 3D (rigid) mask exhibits:

- vivid colors
- no facial motion (no lips or eye movement)

Presentation Attacks

2D face PA: 3D (rigid) mask with holes PAI

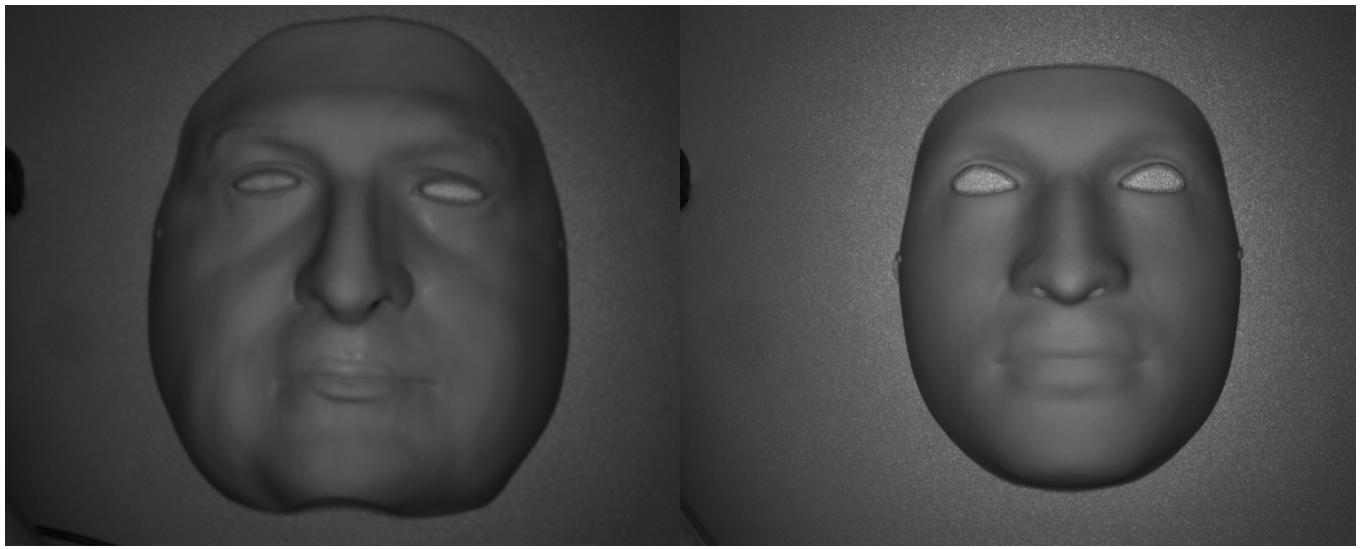
Cost: $\sim$ USD 400

Presentation Attacks

2D face PA: 3D (ridid) mask with holes PAI

PA with 3D (rigid) mask with holes exhibits:

- vivid colors
- no facial motion
- no texture in NIR



Presentation Attacks

2D face PA: 3D (ridid) mask with holes PAI

PA with 3D (rigid) mask don't absorb heat (much):

- thermal imaging

Presentation Attacks

2D/3D face PA: 3D silicone masks PAI

Cost: $\sim$ USD 800

Presentation Attacks

2D/3D face PA: 3D silicone custom masks PAI

Cost: starting USD 3'000

Presentation Attacks

2D/3D face PA: 3D silicone masks PAI [12]

PA with 3D silicone mask exhibits:

- skin-like appearance and reflexion
- facial motion

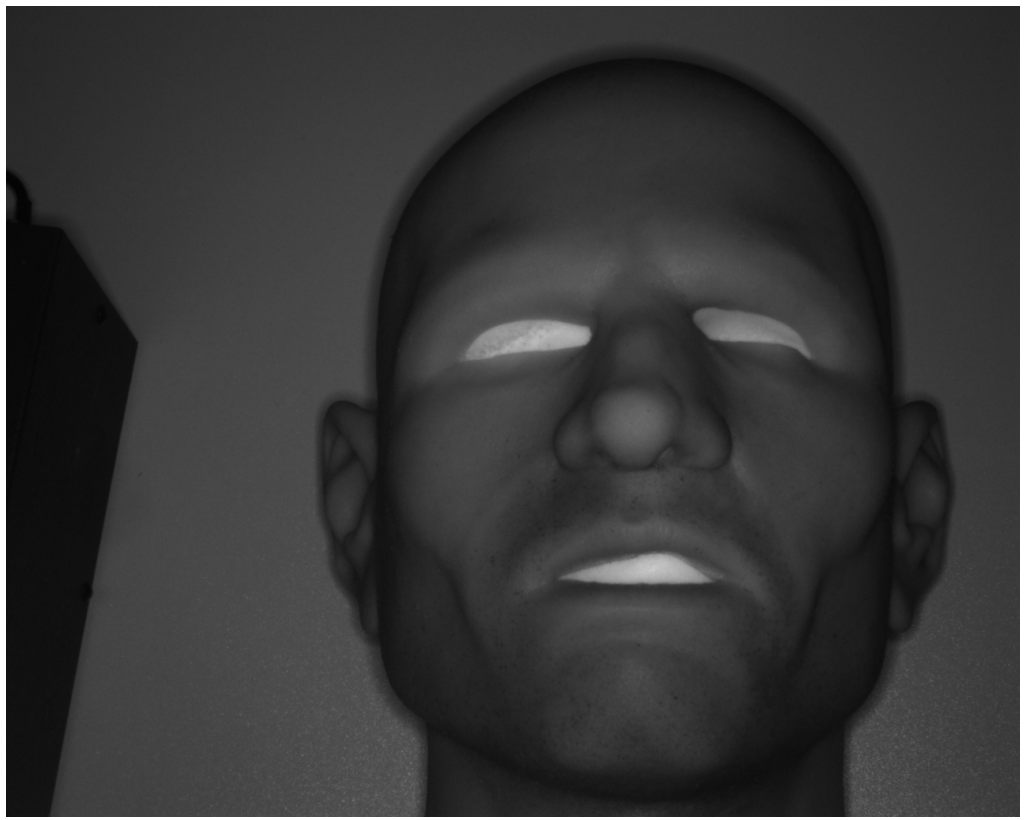
[12] "What you cant see can help you extended-range imaging for 3D-mask presentation attack detection", S. Battacharjee and al., BioSig, 2017.

Presentation Attacks

2D/3D face PA: 3D silicone masks PAI [13]

PA with 3D silicone mask exhibits:

- texture in NIR



[13] "What you cant see can help you extended-range imaging for 3D-mask presentation attack detection", S. Battacharjee and al., BioSig, 2017.

Presentation Attacks

2D/3D face PA: 3D silicone masks PAI [14]

PA with 3D silicone mask exhibits:

- thermal imaging ?

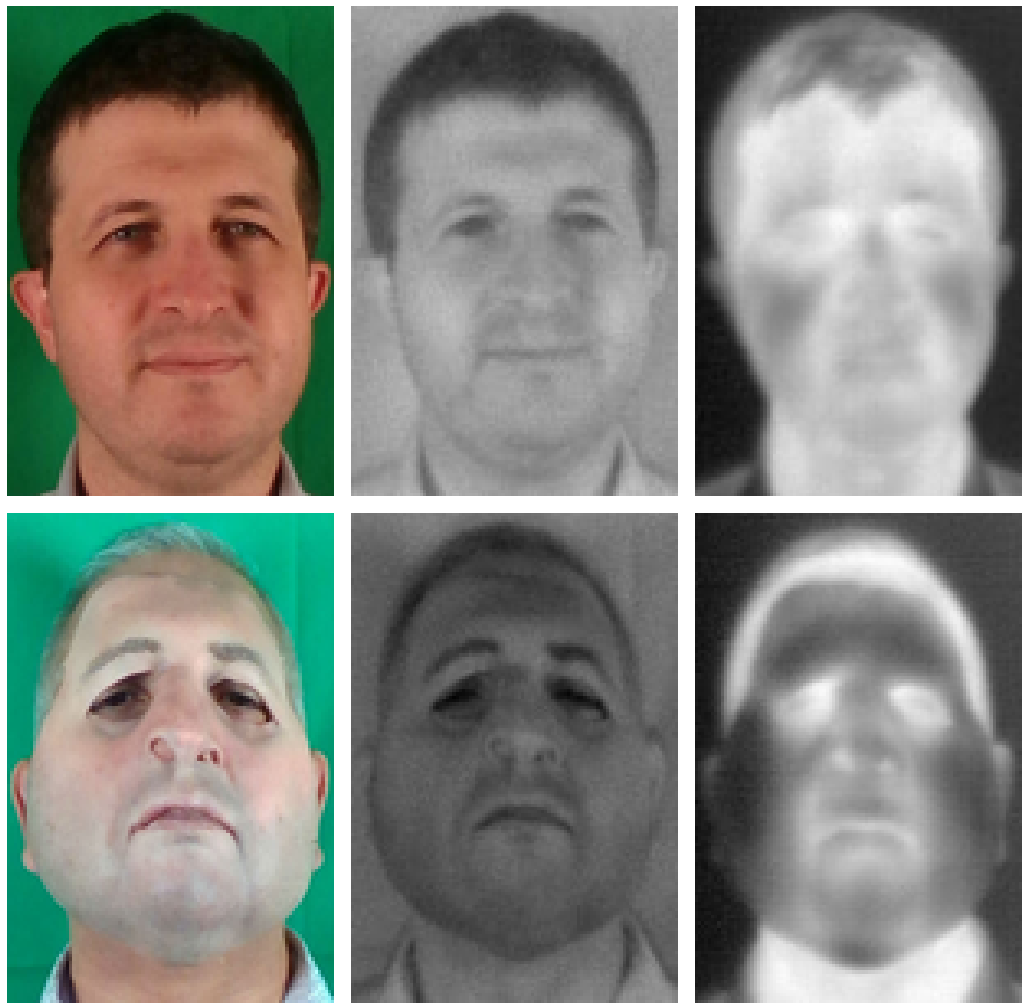
Silicone absorbs heat !

[14] "What you cant see can help you extended-range imaging for 3D-mask presentation attack detection", S. Battacharjee and al., BioSig, 2017.

Presentation Attacks

2D/3D face PA: 3D silicone masks PAI

PA with 3D silicone mask exhibits thermal imaging:



Presentation Attacks

2D/3D face PA: make-up PAI

Presentation Attacks

2D/3D face PA: make-up PAI

PA with make-up exhibits:

- skin-like appearance and reflexion in VIS and NIR
- facial motion
- thermal imaging ?

Presentation Attacks

2D Face PA: a morphed face PAI [15]

It was shown that:

- 2 COTS face recognition system are matching correctly identities A and B against the morphed face (A+B),
- giving to the citizens the possibility of providing a printed face photo poses serious concerns in terms of security.

Also a test organized by FRONTEX demonstrated that a human expert can be easily fooled.

[15] "The magic passport", M. Ferrara, A. Franco, D. Maltoni, IJCB 2014

Presentation Attacks

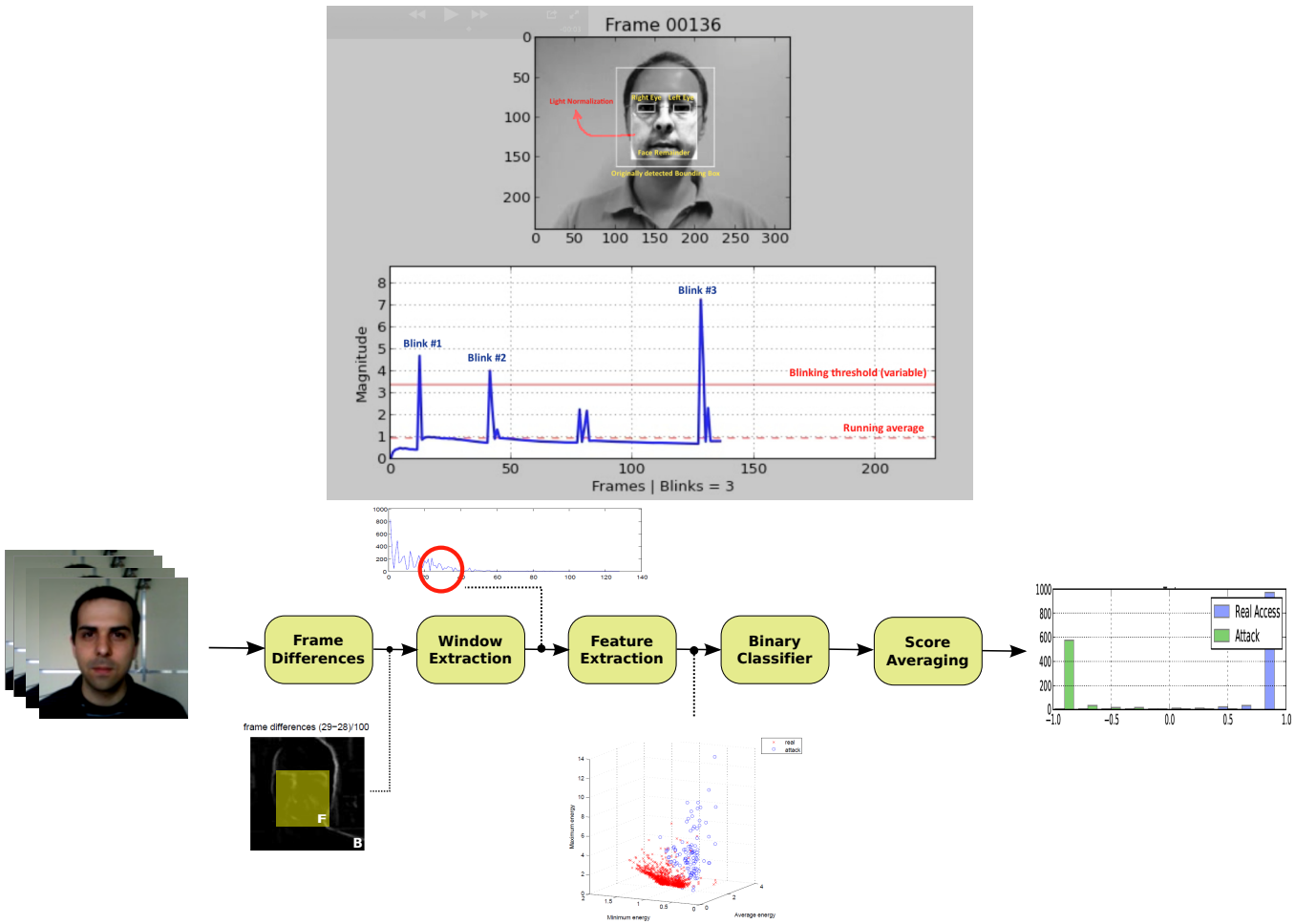
2D Face PA: a morphed face PAI

PA with morphing exhibits:

- symmetric features
- smooth texture
- morphing artefacts

Presentation Attack Detection

Face PAD[16]

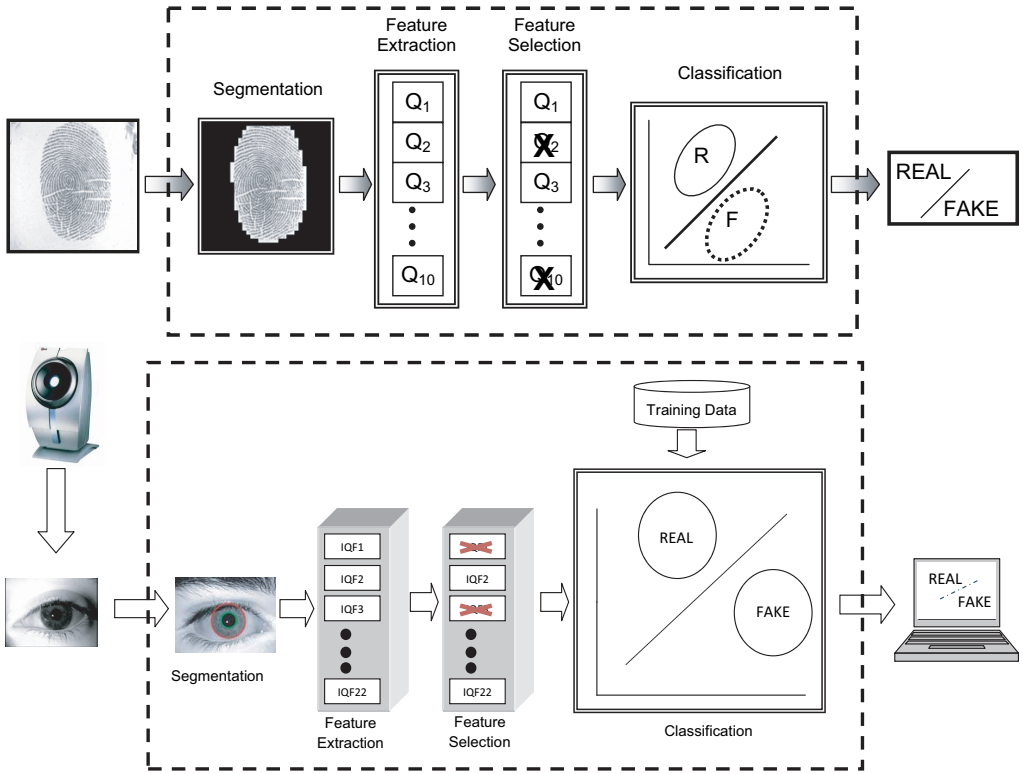


using eye blinking or motion

[16] "Motion-Based Counter-Measures to Photo Attacks in Face Recognition", A. Anjos and S. Marcel, IET Biometrics, 2013.

Presentation Attack Detection

Fingerprint/Iris PAD[17]

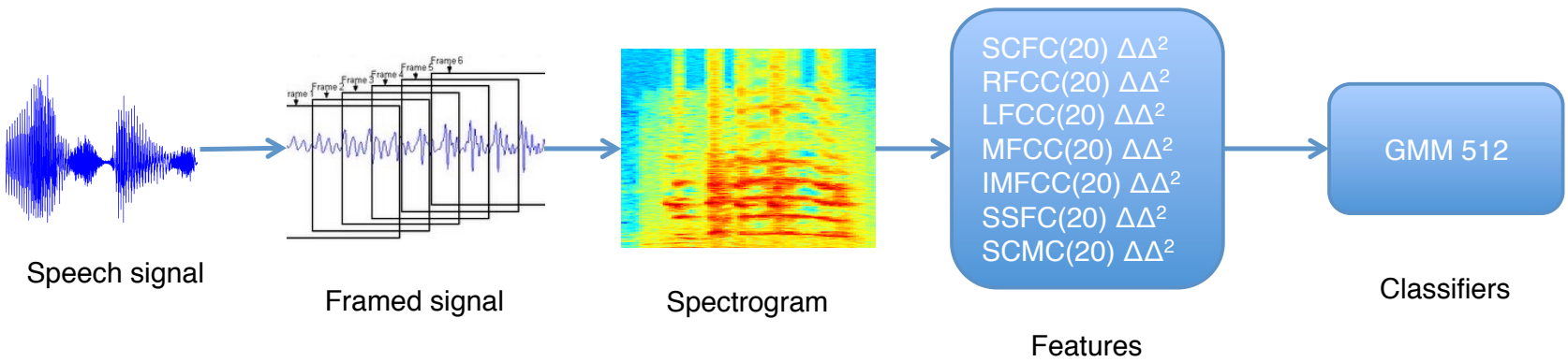


using generic image quality measures

[17] "Image quality assessment for fake biometric detection: Application to iris, fingerprint and face recognition", J. Galbally, S. Marcel, and J. Fierrez, IEEE Transactions on Image Processing, 23(2):710–724, 2014.

Presentation Attack Detection

Voice PAD[18]

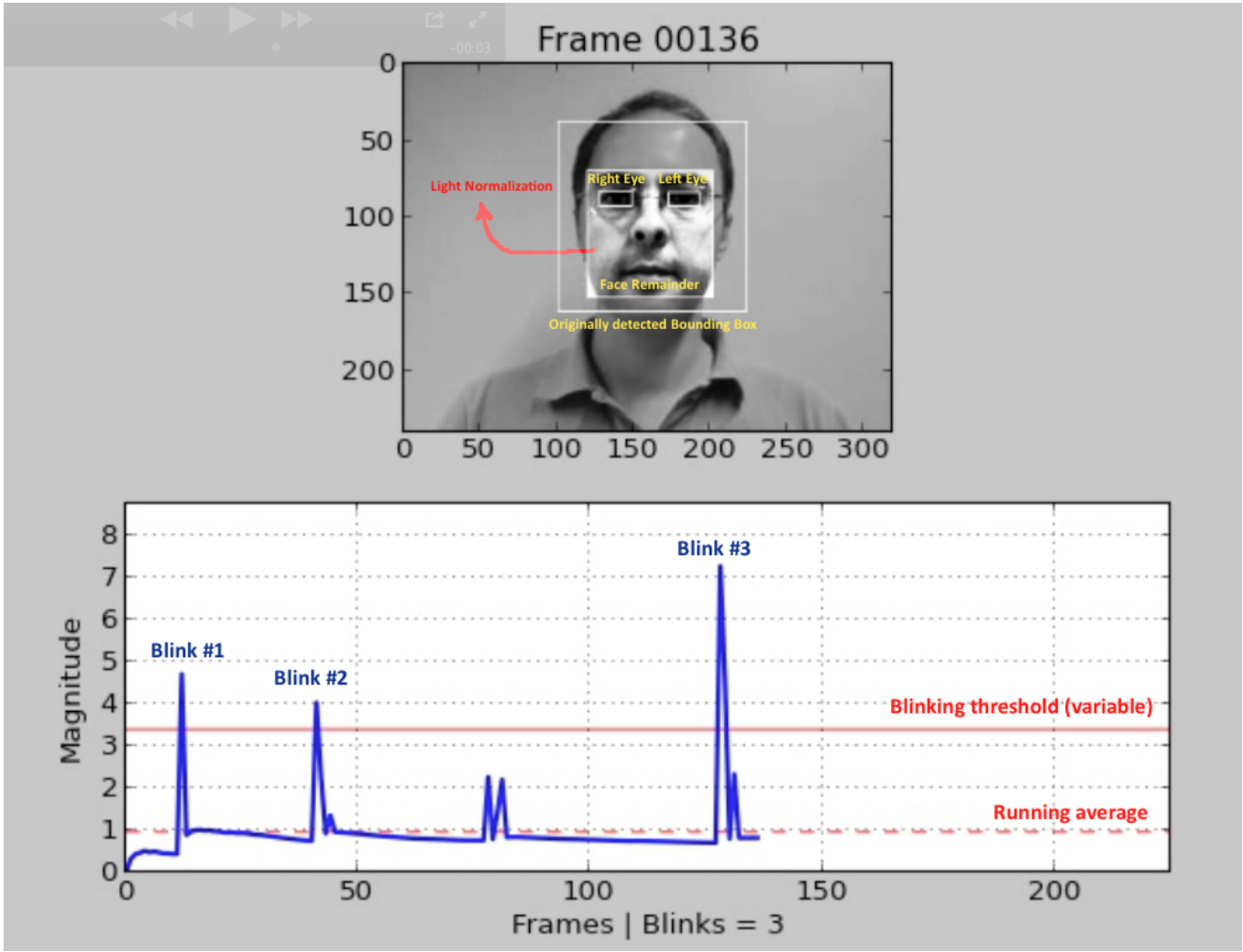


using cepstral-based features

[18] "Joint operation of voice biometrics and presentation attack detection", P. Korshunov and S. Marcel, International Conference on Biometrics: Theory, Applications and Systems, 2016.

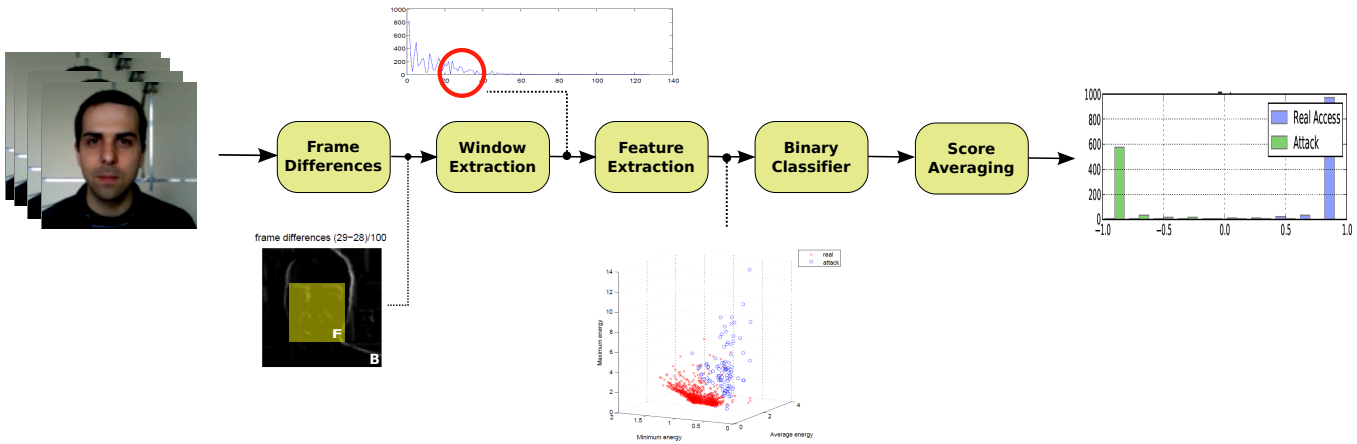
Face PAD

Eye-blinking



Face PAD

Motion[19]

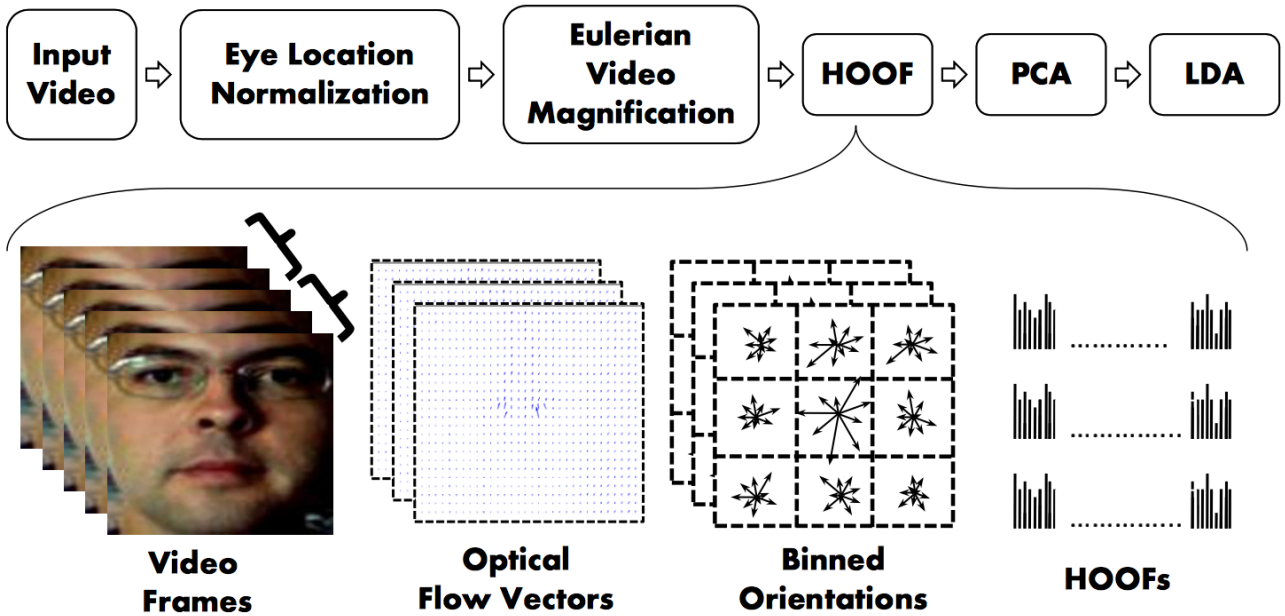


- use statistics of optical-flow between consecutive frames to detect print-attacks
- HTER (Half-Total Error Rate) on test data: 1.52%

[19] "Motion-Based Counter-Measures to Photo Attacks in Face Recognition", A. Anjos and S. Marcel, IET Biometrics, 2013.

Face PAD

Motion [20]

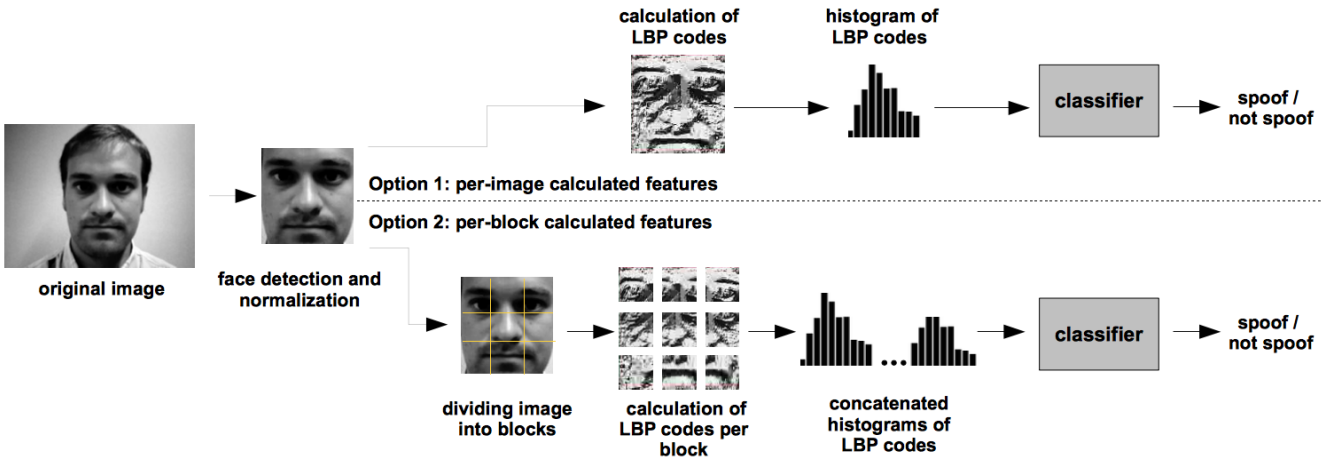


- use LBP and optical-flow to detect print-attacks and replay-attacks
- HTER: Print-attacks: 0% Replay-attacks: 1.25%

[20] "Computationally efficient face spoofing detection with motion magnification", Bharadwaj et al., CVPR, 2013.

Face PAD

Texture analysis [21]



- use LBP in 3 dimensions (LBP-TOP) to differentiate between real and spoof face presentations
- HTER (Print and Replay attacks): 15%

[21] "On the effectiveness of local binary patterns (LBP) in face anti-spoofing", Chingovska et al., BioSig, 2012.

Face PAD

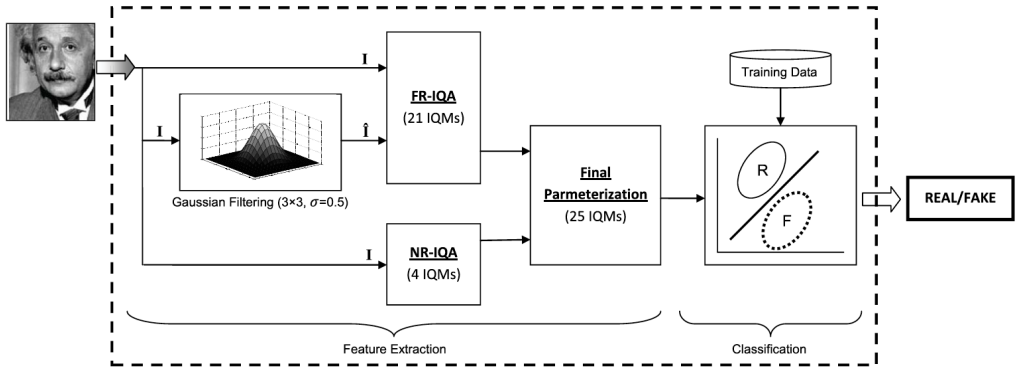
Frequency analysis [22]

- use LBP to detect the presence of moiré patterns
- HTER on Replay-attack: 6%

[22] "Live face video vs. spoof face video: use of moiré patterns to detect replay video attacks", Patel et al., ICB, 2015.

Face PAD

Image Quality Analysis [23]



- use 25 well known image quality measures for gray-level images to train a 2-class classifier

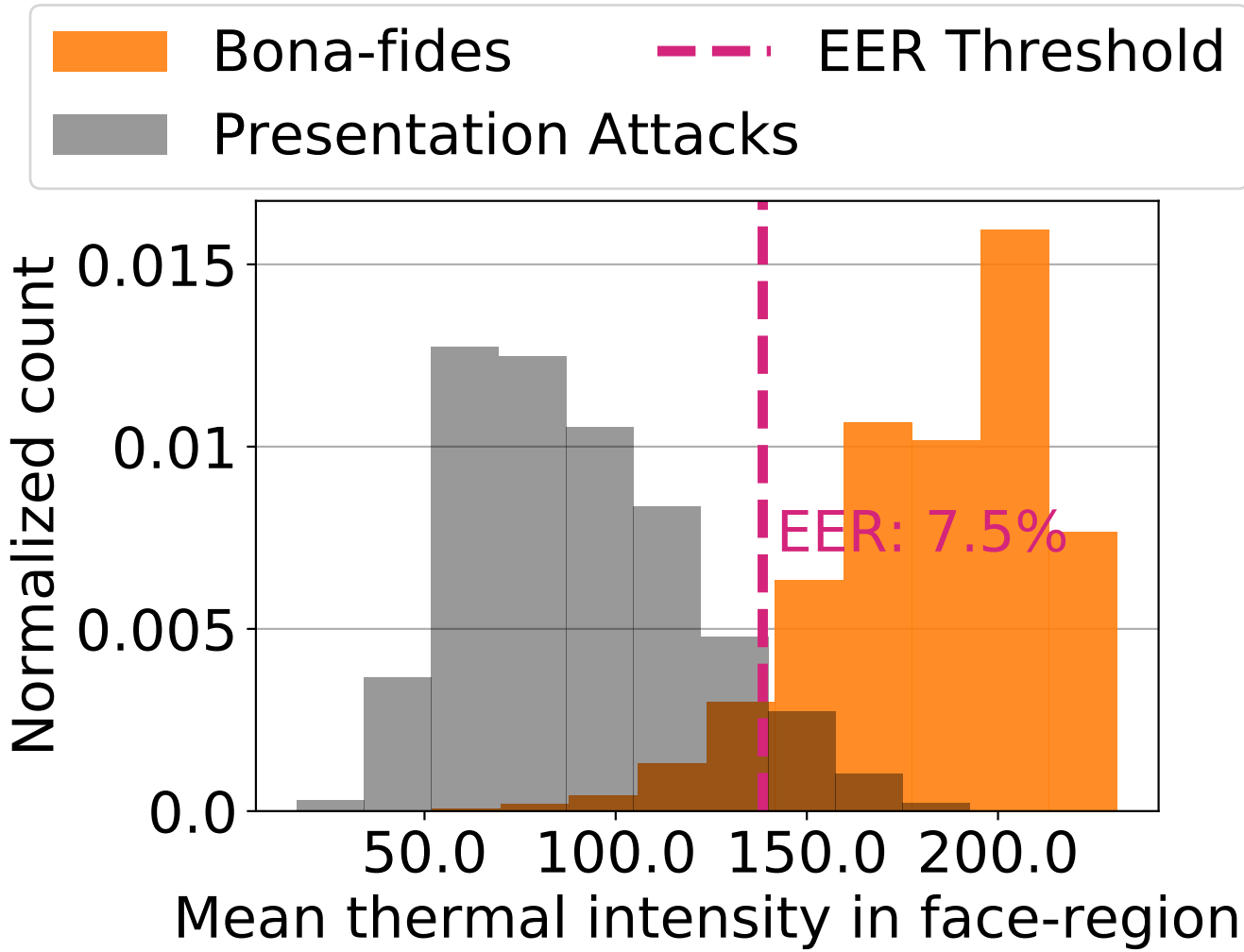
1	FR	MSE	Mean Squared Error	[29]	$MSE(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})^2$
2	FR	PSNR	Peak Signal to Noise Ratio	[30]	$PSNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\max(\mathbf{I}^2)}{MSE(\mathbf{I},\hat{\mathbf{I}})})$
3	FR	SNR	Signal to Noise Ratio	[31]	$SNR(\mathbf{I},\hat{\mathbf{I}}) = 10\log(\frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{N\cdot M\cdot MSE(\mathbf{I},\hat{\mathbf{I}})})$
4	FR	SC	Structural Content	[32]	$SC(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j})^2}{\sum_{i=1}^{N}\sum_{j=1}^{M}(\hat{\mathbf{I}}_{i,j})^2}$
5	FR	MD	Maximum Difference	[32]	$MD(\mathbf{I},\hat{\mathbf{I}}) = \max\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert$
6	FR	AD	Average Difference	[32]	$AD(\mathbf{I},\hat{\mathbf{I}}) = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}(\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j})$
7	FR	NAE	Normalized Absolute Error	[32]	$NAE(\mathbf{I},\hat{\mathbf{I}}) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}-\hat{\mathbf{I}}_{i,j}\rvert}{\sum_{i=1}^{N}\sum_{j=1}^{M}\lvert\mathbf{I}_{i,j}\rvert}$

- HTER: Replay-attack: 15.4%

[23] "Image quality assessment for fake biometric detection: application to iris, fingerprint, and face recognition", Galbally et al. , IEEE TIP, 2014.

Face PAD

Thermal (unpublished)



Face PAD

Open source (face) PAD framework

Open source tools to run comparable and reproducible generic PAD experiments

http://pythonhosted.org/bob.pad.base

eg. face PAD with native support for Replay Attack, Replay Mobile and MSU MFSD

source code: https://gitlab.idiap.ch/bob/bob.pad.face
doc: https://www.idiap.ch/software/bob/docs/bob/bob.pad.face/master/index.html

based on the Bob signal-processing and machine learning toolbox

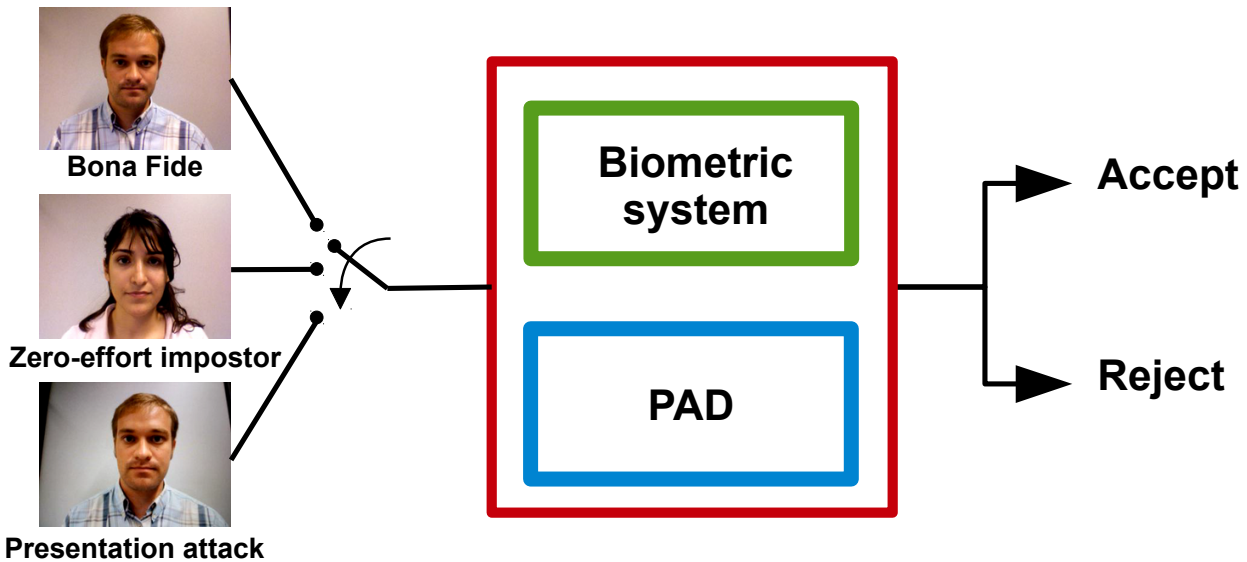
https://www.idiap.ch/software/bob/

Biometrics and PAD

Bona Fide, Zero Effort Impostor and PA

Biometrics and PAD

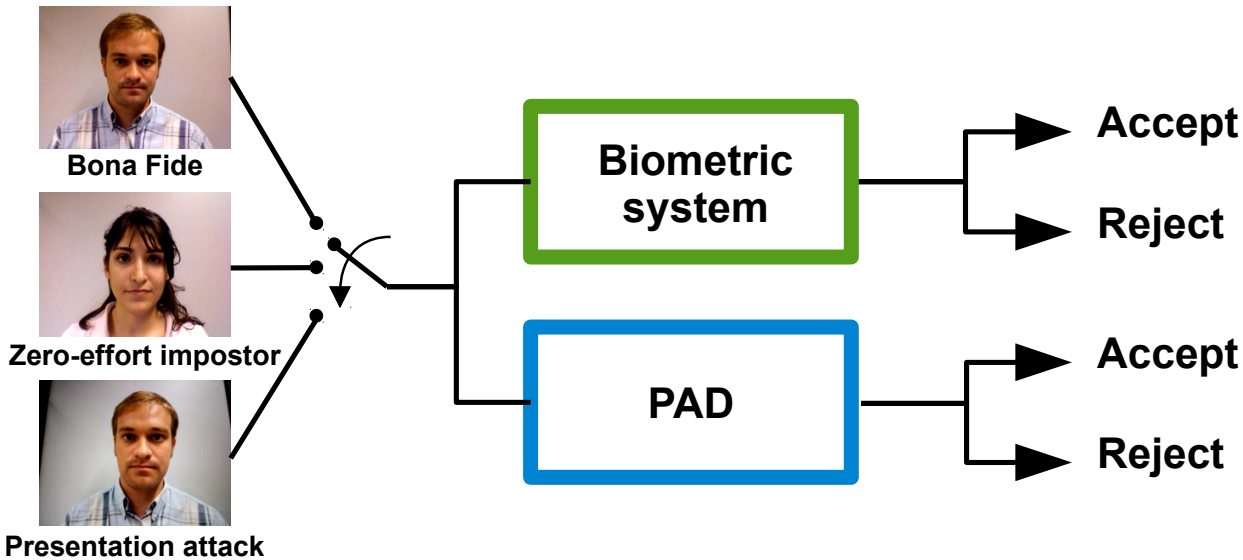
Two separate components



- A biometric sub-system
- A PAD sub-system

Biometrics and PAD

Two separate components

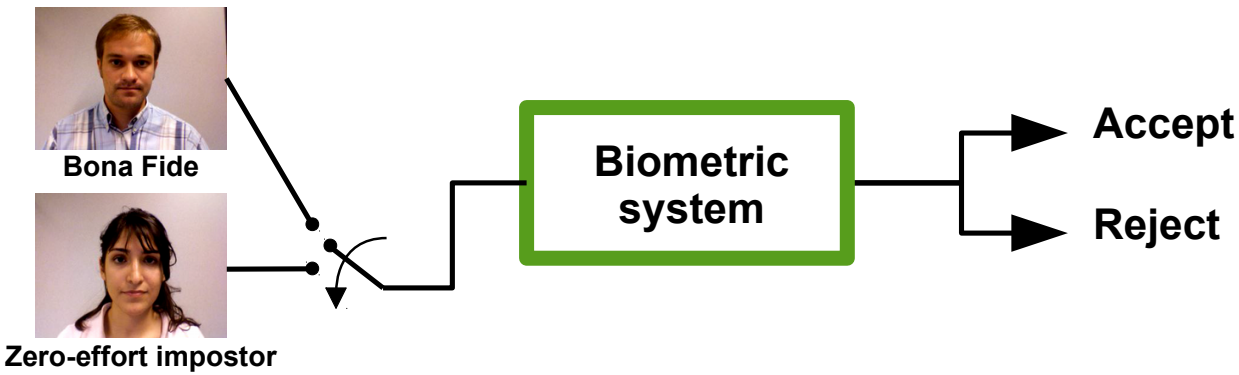


Overall

- Accept: genuine and bona fide
- Reject: zero-effort impostor and presentation attack

Biometrics and PAD

Biometric sub-system: a binary classifier

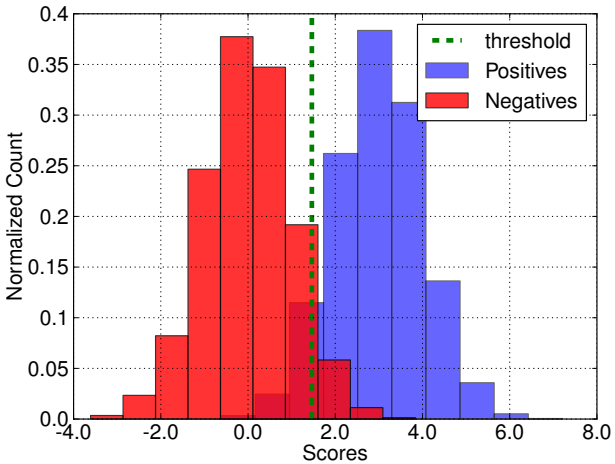


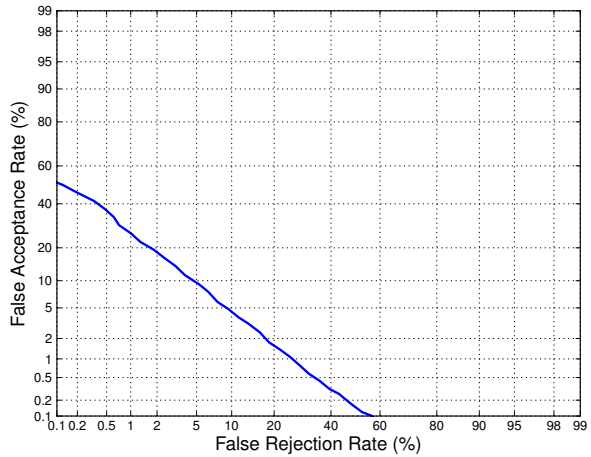
We measure 2 errors:

- False Match Rate (FMR): zero-effort impostors incorrectly matched as genuines – also referred to as False Acceptance Rate (FAR)
- False Non-Match Rate (FNMR): genuines not matched – also referred to as False Rejection Rate (FRR)

Biometrics and PAD

Biometric sub-system: a binary classifier



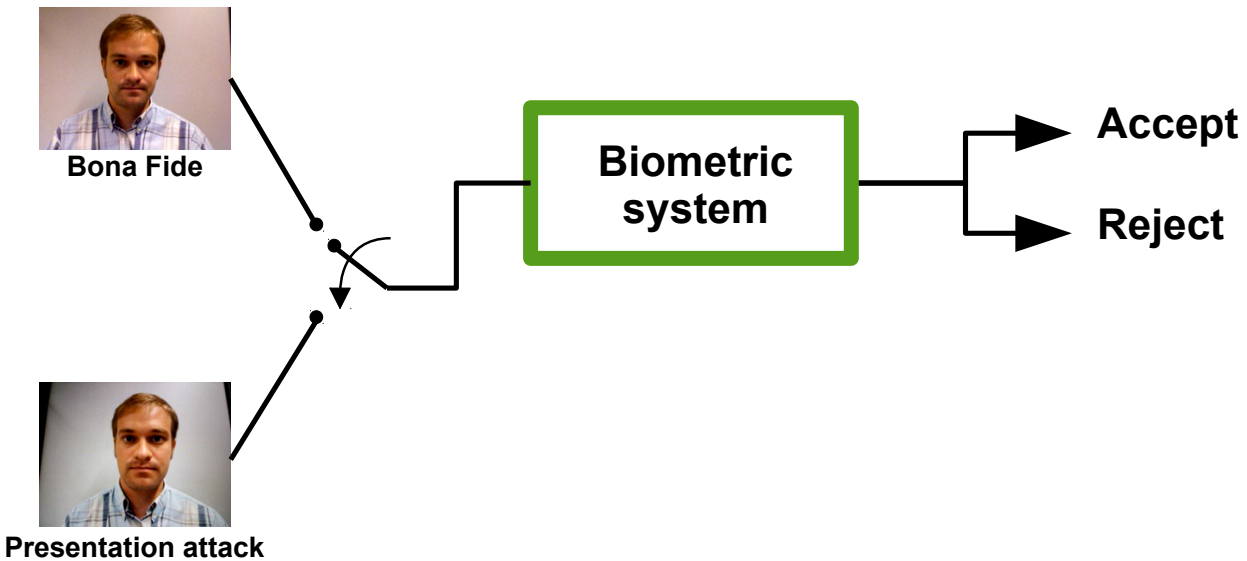


We measure 2 errors:

- False Match Rate (FMR): zero-effort impostors incorrectly matched as genuines – also referred to as False Acceptance Rate (FAR)
- False Non-Match Rate (FNMR): genuines not matched – also referred to as False Rejection Rate (FRR)

Biometrics and PAD

Biometric sub-system: a binary classifier

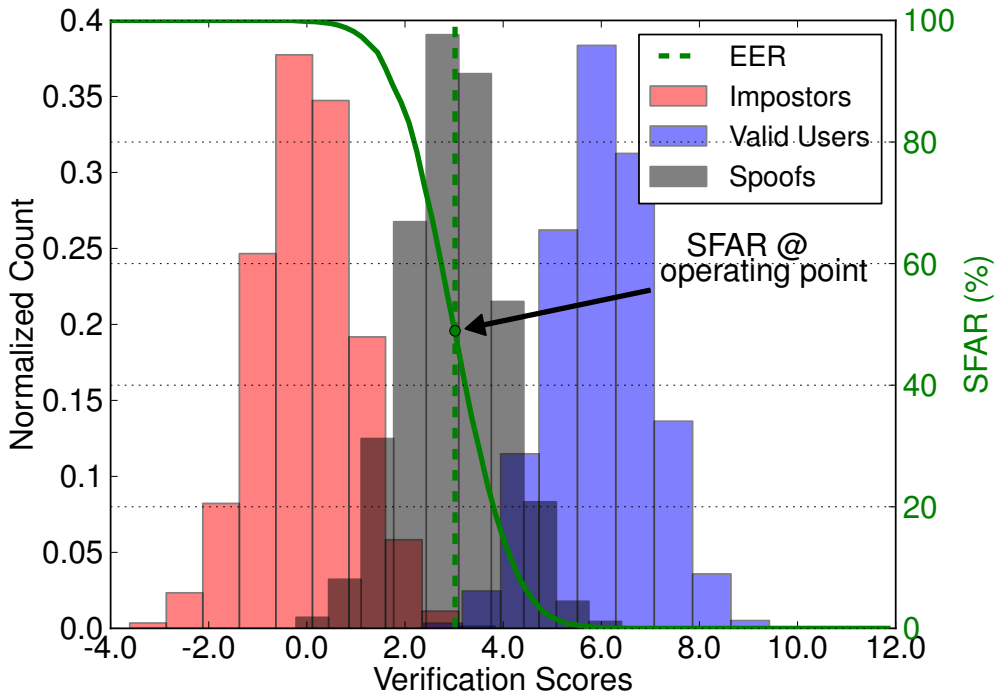


We measure the vulnerability as:

- Impostor Attack Presentation Match Rate (IAPMR): PAs which are accepted as genuine samples – also referred to as Spoofing False Accept Rate (SFAR)

Biometrics and PAD

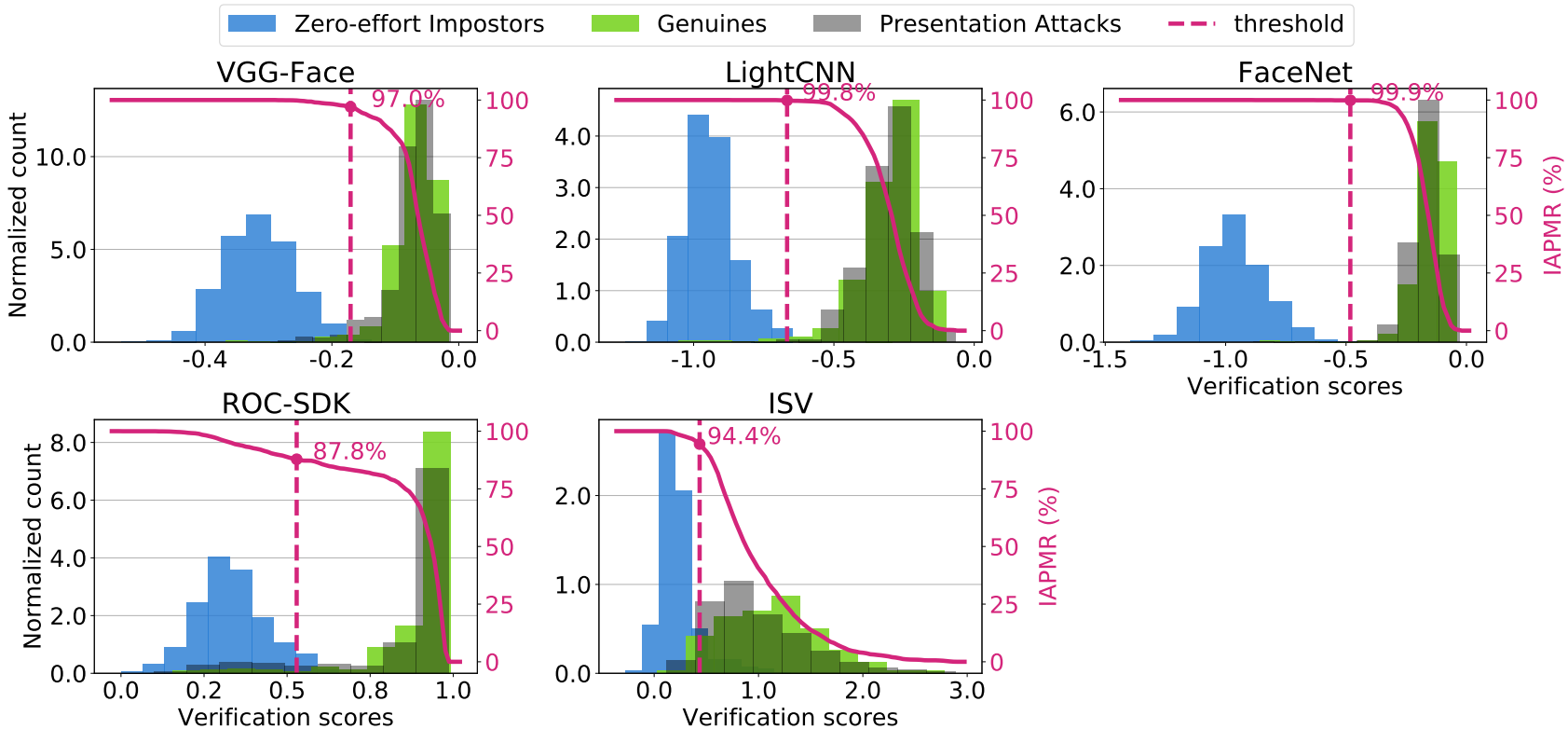
Biometric sub-system: a binary classifier



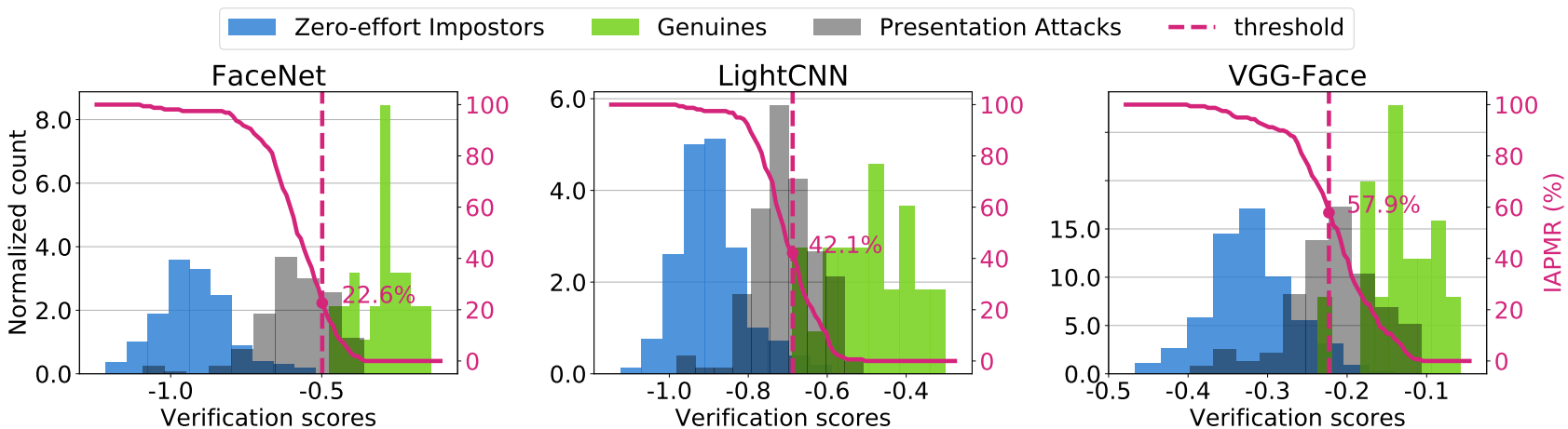
We measure the vulnerability as:

- Impostor Attack Presentation Match Rate (IAPMR): PAs which are accepted as genuine samples – also referred to as Spoofing False Accept Rate (SFAR)

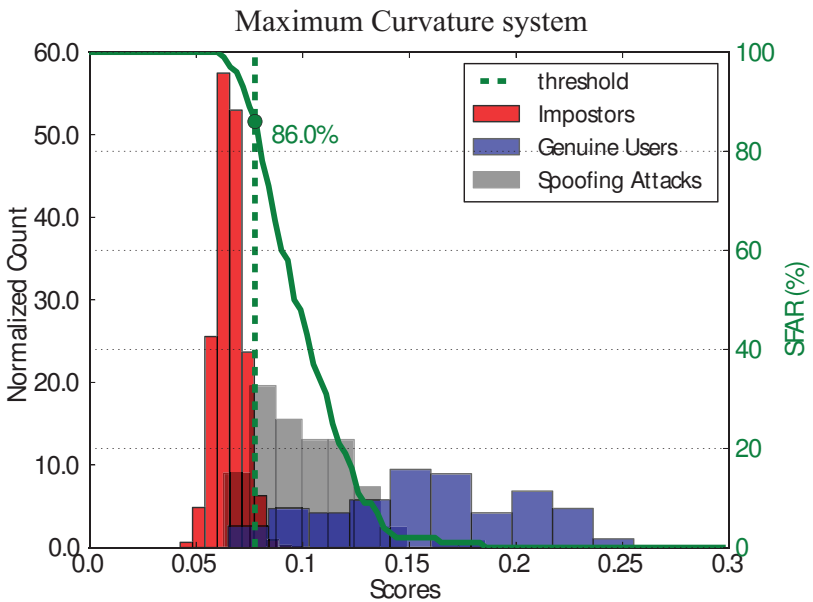
IAPMR Deep Face Recognition (print and replay PA)

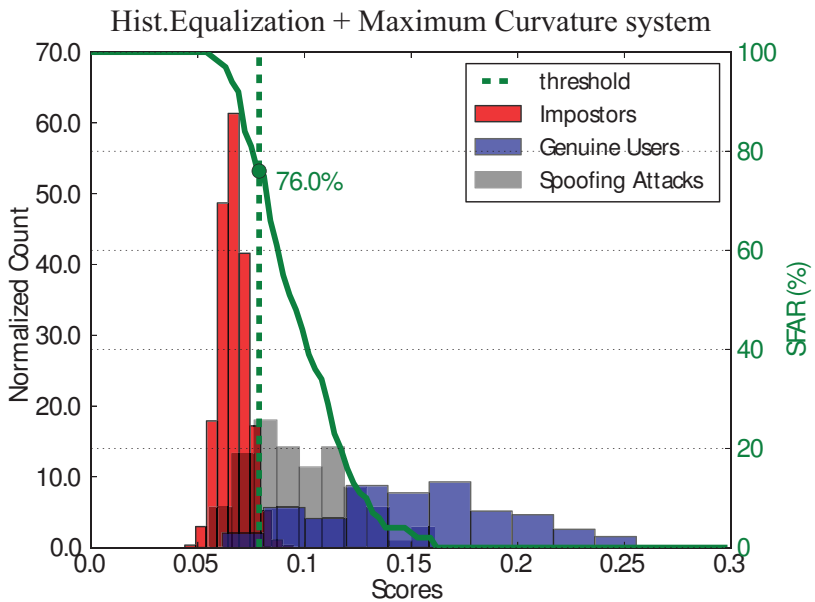


IAPMR Deep Face Recognition (silicone masks PA)



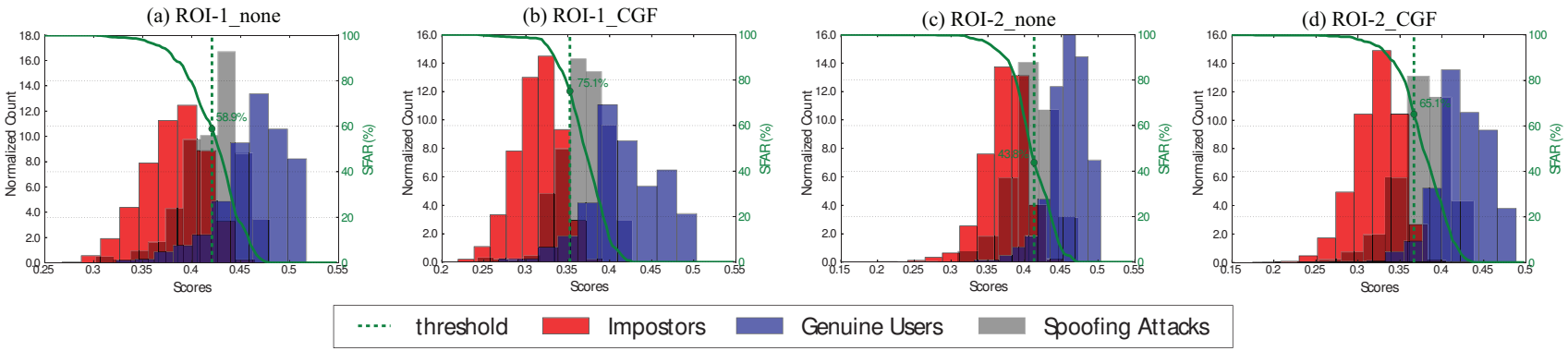
IAPMR Fingervein





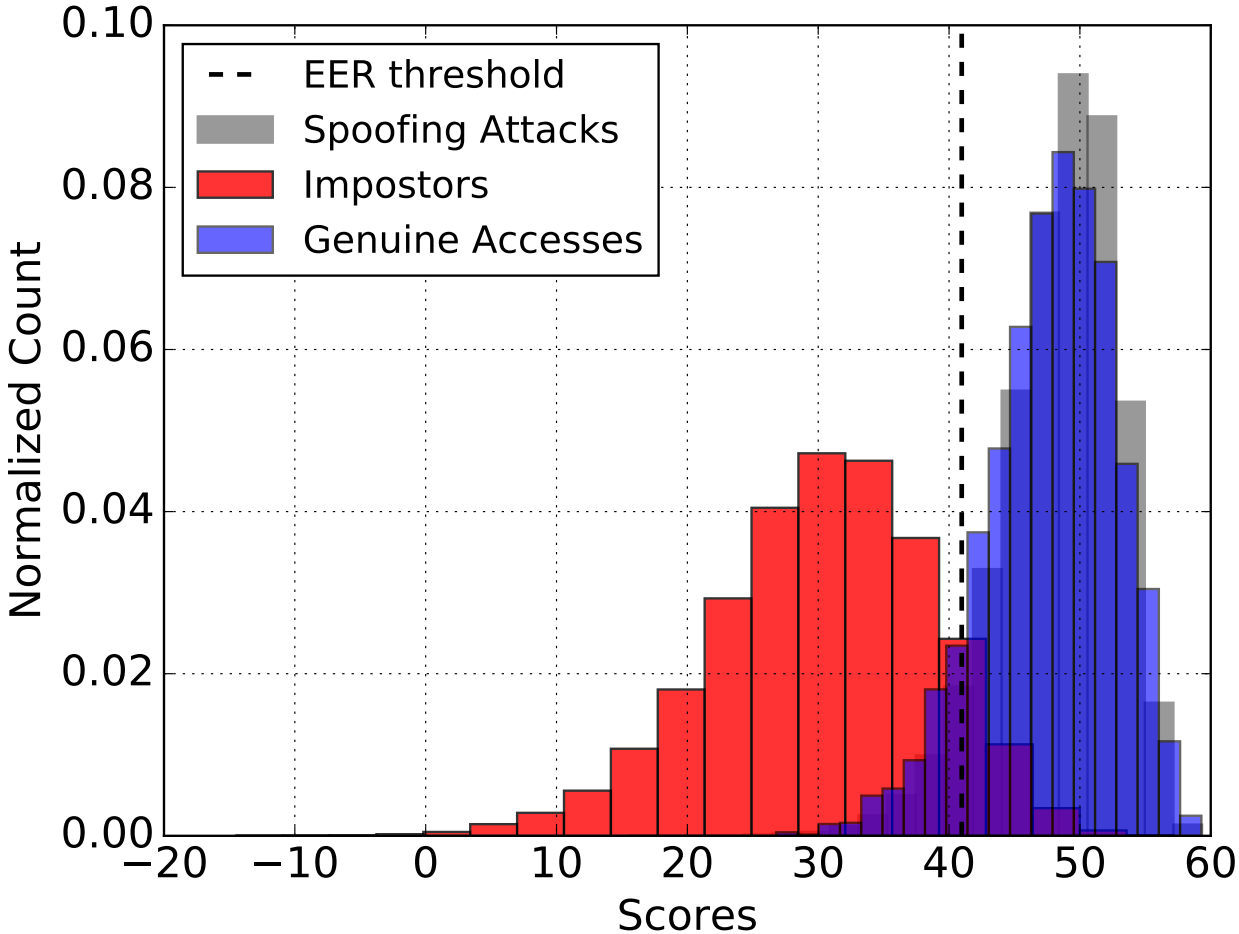
Biometrics and PAD

IAPMR Palmvein



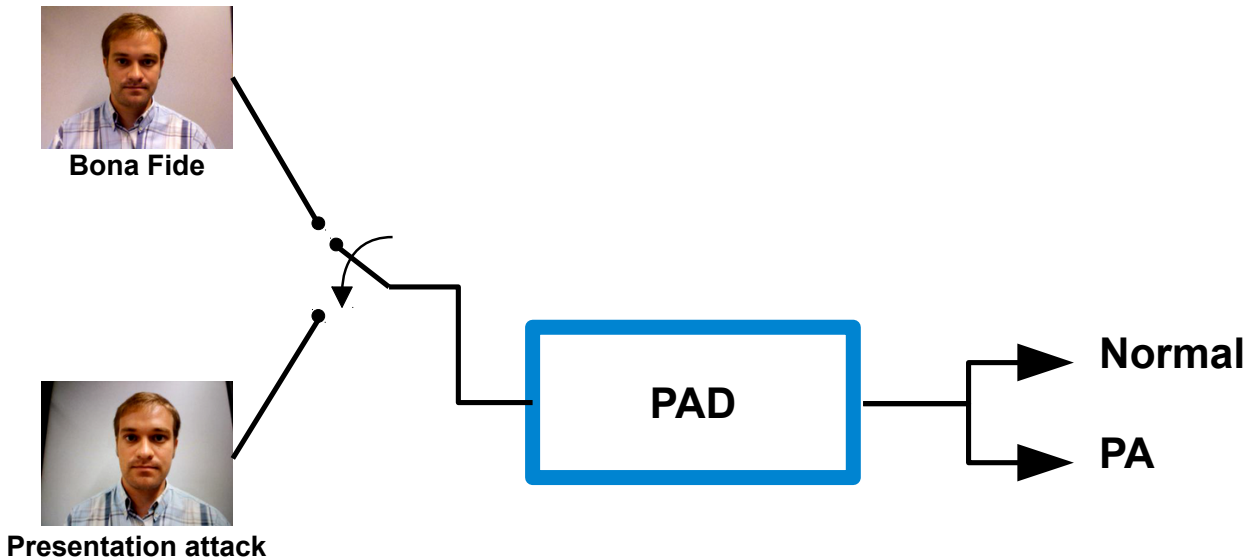
Biometrics and PAD

IAPMR Voice



Biometrics and PAD

PAD sub-system: a binary classifier



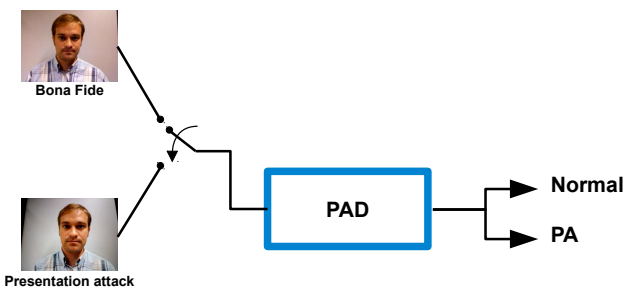
We measure 2 errors:

- Attack Presentation Classification Error Rate (APCER): PAs incorrectly classified as normal presentations
- Normal Presentation Classification Error Rate (NPCER): normal presentations incorrectly classified as PAs

Biometrics and PAD

PAD methods

- software-based: biometric data from the sensor is analysed to discriminate bona fide vs PA (eg. motion, texture)
- hardware-based: an additional sensor is used and its data analysed to discriminate bona fide vs PA (eg. temperature, pulse)
- challenge-response: the user interacts with the system (eg. prompted text in face/speaker recognition)



Some literature

Book

Handbook of Biometric Anti-Spoofing,
Sébastien Marcel, Mark S. Nixon and Stan Z. Li (Eds.)
Fingerprint, Iris, Face, Voice, Gait and MultiModal Anti-Spoofing
http://link.springer.com/book/10.1007/978-1-4471-6524-8

Transactions on Information Forensics and Security (TIFS)

Special Issue on Biometric Spoofing and Countermeasures
14 contributions relating to ocular, face, and voice modalities in addition to studies involving multiple biometric traits
http://ieeexplore.ieee.org/document/7060794/

IEEE Signal Processing Magazine

Special Issue on Biometric Security and Privacy
http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7192815

Thank you for your attention

Acknowledgements

Secure Access Control Over Wide Area Network (SWAN)

https://www.ntnu.edu/aimt/swan

IARPA ODIN BATL

ODIN

Swiss Center for Biometrics Research and Testing

www.biometrics-center.ch