What is a Presentation Attack? And how do we detect it?

Christoph Busch, Claudia Nickel, Chris Stein, Raghu Ramachandra, Kiran Raja, Pankaj Wasnik, Martin Stokkenes, Marta Gomez-Barrero, Andreas Nautsch, Christian Rathgeb, Ulrich Scherhag, Ctirad Sousedik

Fraunhofer IGD, Germany

da/sec, Hochschule Darmstadt - CRISP, Germany

NBL, Norwegian University of Science and Technology - Gjøvik, Norway

Dan Panorama
Tel Aviv, January 16, 2018

CRISP
Center for Research
in Security and Privacy

NTNU

Research Projects

Thanks to the sponsors of this work

- da/sec@Hochschule Darmstadt
  Center for Research in Security and Privacy:
  - LOEWE/BMBF CRISP http://www.crisp-da.de/
  - LOEWE BioMobile http://www.christoph-busch.de/projects-biomobile.html
  - BMBF BioIndex http://www.christoph-busch.de/projects-bioindex.html
  - IARPA BATL http://www.christoph-busch.de/projects-batl.html

CRISP
Center for Research
in Security and Privacy

- NorwegianBiometricsLab@NTNU
  Norwegian University of Science and Technology - Gjøvik:
  - EU-FP7 INGRESS http://www.ingress-project.eu
  - EU-FP7 ORIGINS http://www.origins-project.eu
  - EU-FP7 PIDaaS http://www.pidaas.eu
  - IKTPLUSS SWAN http://nislab.no/biometrics_lab/swan

NTNU

What is a presentation attack?

What are Presentation Attacks?

We can learn from the James Bond movie

- 1971: Diamonds Are Forever …
  … and James Bond impersonates Peter Frank

Biometric Presentation Attacks

A new understanding of a

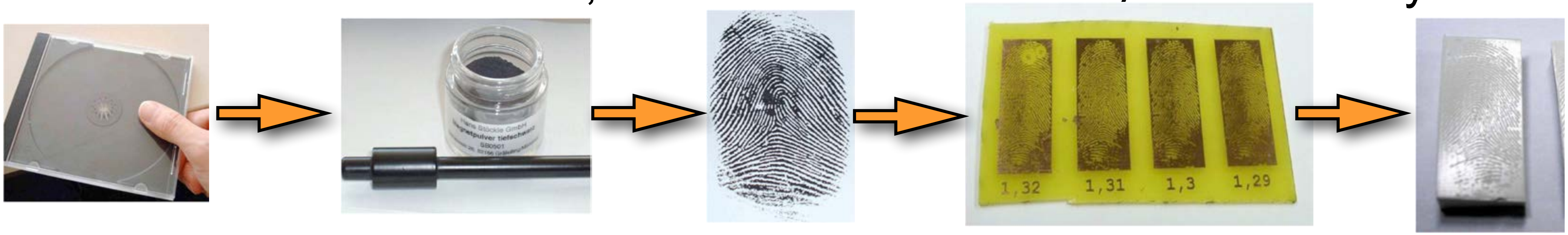
- Keyring - impersonating target victims that have the desired authorization

Image Source: c't magazine

Gummy Finger Production in 2000 !

Attack without support of the target victim

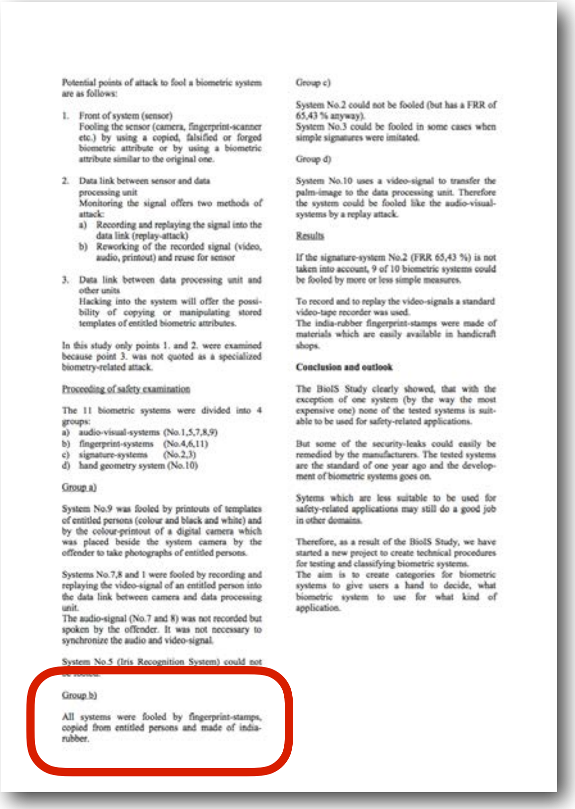
- Recording of a latent fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production of a circuit board
- Artefact with silicon, which will have flexibility and humidity



Gummy Finger Production in 2000 !

Reported in a publication by the German Federal Police

- Findings:
  - “*All systems were fooled by fingerprint-stamps, copied from entitled persons and made of india-rubber.*”



Potential points of attack to fool a biometric system are as follows:

1. Front of system (sensor)
   Fooling the sensor (camera, fingerprint-scanner etc.) by using a copied, falsified or forged biometric attribute or by using a biometric attribute similar to the original one.

2. Data link between sensor and data processing unit
   Monitoring the signal offers two methods of attack:
   a) Recording and replaying the signal into the data link (replay-attack)
   b) Reworking of the recorded signal (video, audio, printout) and reuse for sensor

3. Data link between data processing unit and other units
   Hacking into the system will offer the possibility of copying or manipulating stored templates of entitled biometric attributes.

In this study only points 1. and 2. were examined because point 3. was not quoted as a specialized biometry-related attack.

Proceeding of safety examination

The 11 biometric systems were divided into 4 groups:

a) audio-visual-systems (No.1,5,7,8,9)
b) fingerprint-systems (No.4,6,11)
c) signature-systems (No.2,3)
d) hand geometry system (No.10)

Group a)

System No.9 was fooled by printouts of templates of entitled persons (colour and black and white) and by the colour-printout of a digital camera which was placed beside the system camera by the offender to take photographs of entitled persons.

Systems No.7,8 and 1 were fooled by recording and replaying the video-signal of an entitled person into the data link between camera and data processing unit.
The audio-signal (No.7 and 8) was not recorded but spoken by the offender. It was not necessary to synchronize the audio and video-signal.

System No.5 (Iris Recognition System) could not be fooled.

Group b)

All systems were fooled by fingerprint-stamps, copied from entitled persons and made of india-rubber.

Group c)

System No.2 could not be fooled (but has a FRR of 65,43 % anyway).
System No.3 could be fooled in some cases when simple signatures were imitated.

Group d)

System No.10 uses a video-signal to transfer the palm-image to the data processing unit. Therefore the system could be fooled like the audio-visual-systems by a replay attack.

Results

If the signature-system No.2 (FRR 65,43 %) is not taken into account, 9 of 10 biometric systems could be fooled by more or less simple measures.

To record and to replay the video-signals a standard video-tape recorder was used.
The india-rubber fingerprint-stamps were made of materials which are easily available in handicraft shops.

Conclusion and outlook

The BioIS Study clearly showed, that with the exception of one system (by the way the most expensive one) none of the tested systems is suitable to be used for safety-related applications.

But some of the security-leaks could easily be remedied by the manufacturers. The tested systems are the standard of one year ago and the development of biometric systems goes on.

Sytems which are less suitable to be used for safety-related applications may still do a good job in other domains.

Therefore, as a result of the BioIS Study, we have started a new project to create technical procedures for testing and classifying biometric systems.
The aim is to create categories for biometric systems to give users a hand to decide, what biometric system to use for what kind of application.

[Zwiesele2000] A. Zwiesele et al. „BioIS Study - Comparative Study of Biometric Identification Systems“, In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, (2000)

Presentation Attack Detection

Impostor

- impersonation attack
  - positive access 1:1 (two factor application)
  - positive access 1:N (single factor application)
- finding a look-a-like
- making appearance similar to the reference
- artefact presentation

Image Source: http://upshout.net/game-of-thrones-make-up

For fingerprint recognition:
e.g. silicon artefact production

For face recognition:
e.g. find a look-a-like first and then consult a make-up-artist

Presentation Attack Detection

Impostor

- impersonation attack
  - positive access 1:1 (two factor application)
  - positive access 1:N (single factor application)
- finding a look-a-like
- making appearance similar to the reference
- artefact presentation

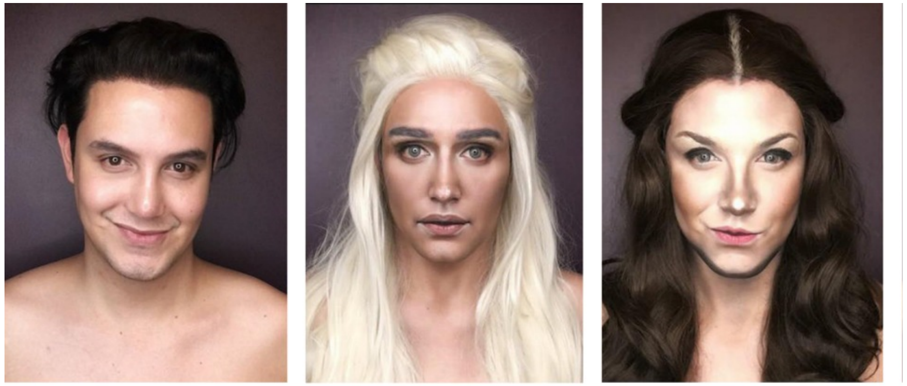
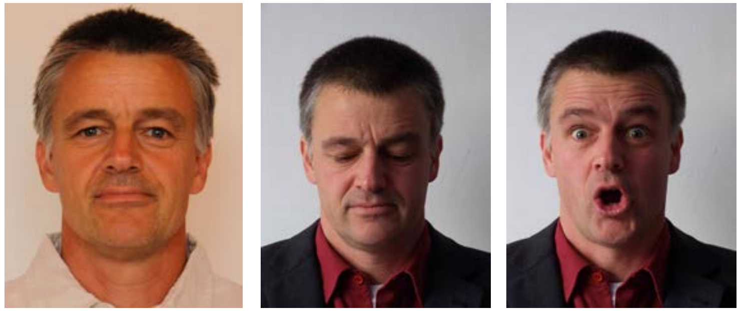


Image Source: http://upshout.net/game-of-thrones-make-up

Concealer

- evasion from recognition
  - negative 1:N identification (watchlist application)
- depart from standard pose



- evade face detection

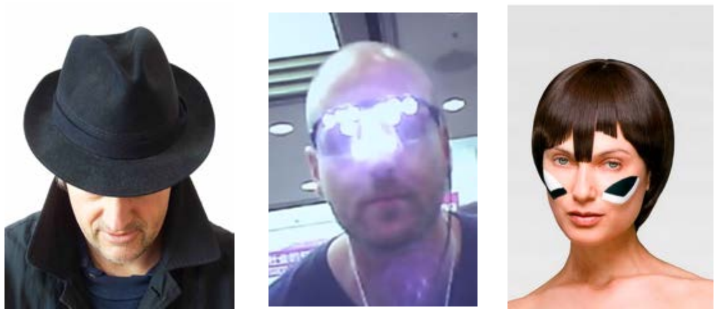


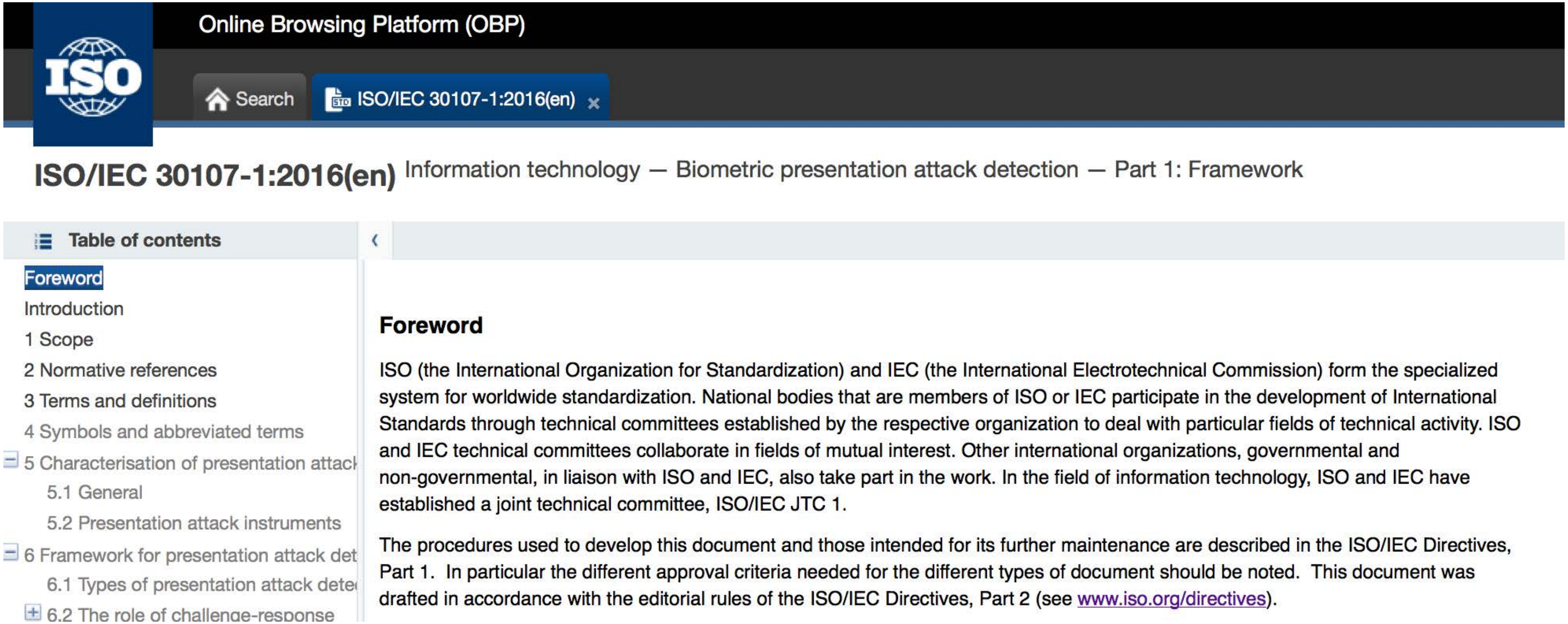
Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

Image Source: https://cvdazzle.com

Presentation Attack Detection - Framework

The international standard ISO/IEC 30107-1

- freely available in the ISO-Portal
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip



ISO/IEC 30107-1:2016(en) Information technology — Biometric presentation attack detection — Part 1: Framework

Table of contents

Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Symbols and abbreviated terms
5 Characterisation of presentation attacl
5.1 General
5.2 Presentation attack instruments
6 Framework for presentation attack det
6.1 Types of presentation attack dete
6.2 The role of challenge-response

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Presentation Attack Detection

Definitions in ISO/IEC 30107 PAD - Part 1: Framework

- **presentation attack**
  presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system
- **presentation attack detection (PAD)**
  automated determination of a presentation attack

Definitions in ISO/IEC 2382-37: Vocabulary
http://www.christoph-busch.de/standards.html

- **impostor**
  subversive biometric capture subject who attempts to being matched to someone else's biometric reference
- **identity concealer**
  subversive biometric capture subject who attempts to avoid being matched to their own biometric reference

Presentation Attack Detection

ISO/IEC 30107-1 - Definitions

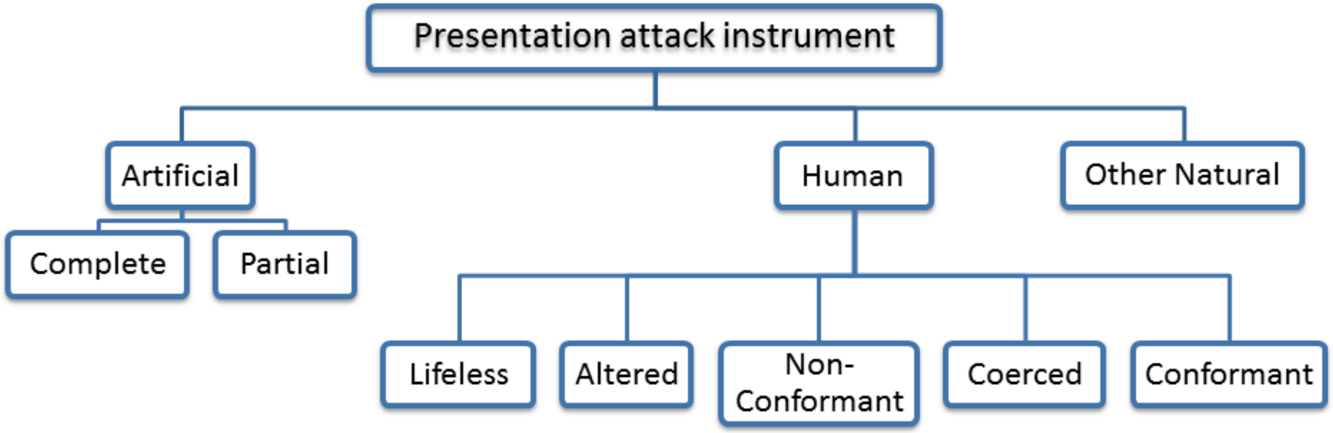
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

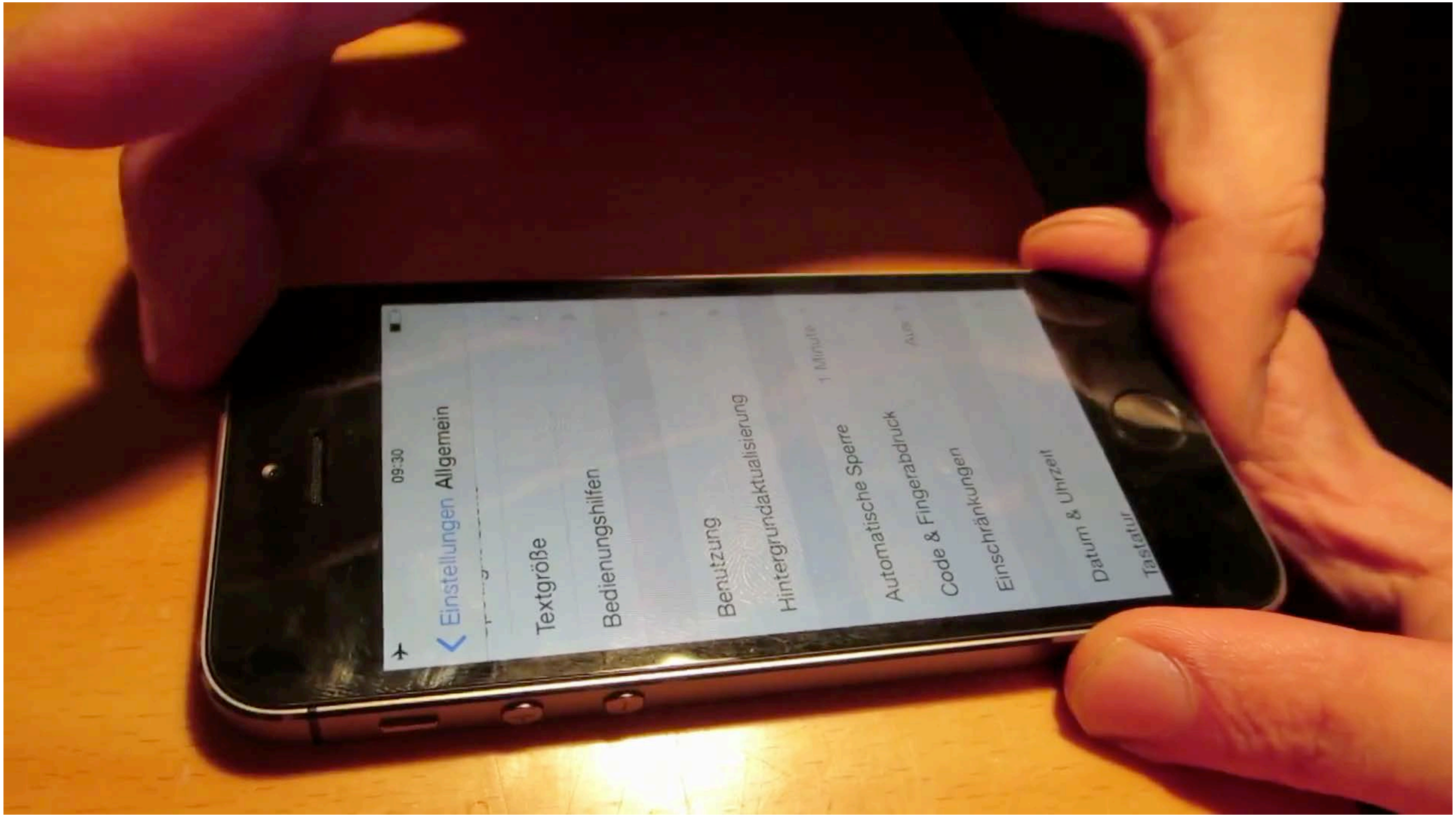
(Qualifying adjectives)



Source: ISO/IEC 30107-1

Presentation Attacks against the iPhone

Introduction of iPhone with Touch-ID in September 2013



Video Source: CCC, 2013

Fingerprint Capture Device Security

BSI Testing (www.bsi.bund.de)

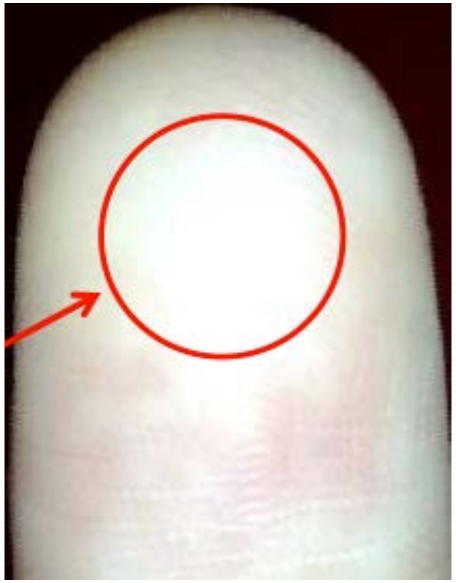
- evaluation with known artefacts
- development of new artefact species
    - BSI-Fake-Toolbox

Source: BSI

Fingerphoto Presentation Attack Detection

Finger recognition study - 2012/2013

- Observation
  - significant strong light reflection near the fingertip
  - from the cameras LED
- Reflection depends on
  - Shape of the finger
  - Consistency of the finger skin
  - Angle of the finger to the camera



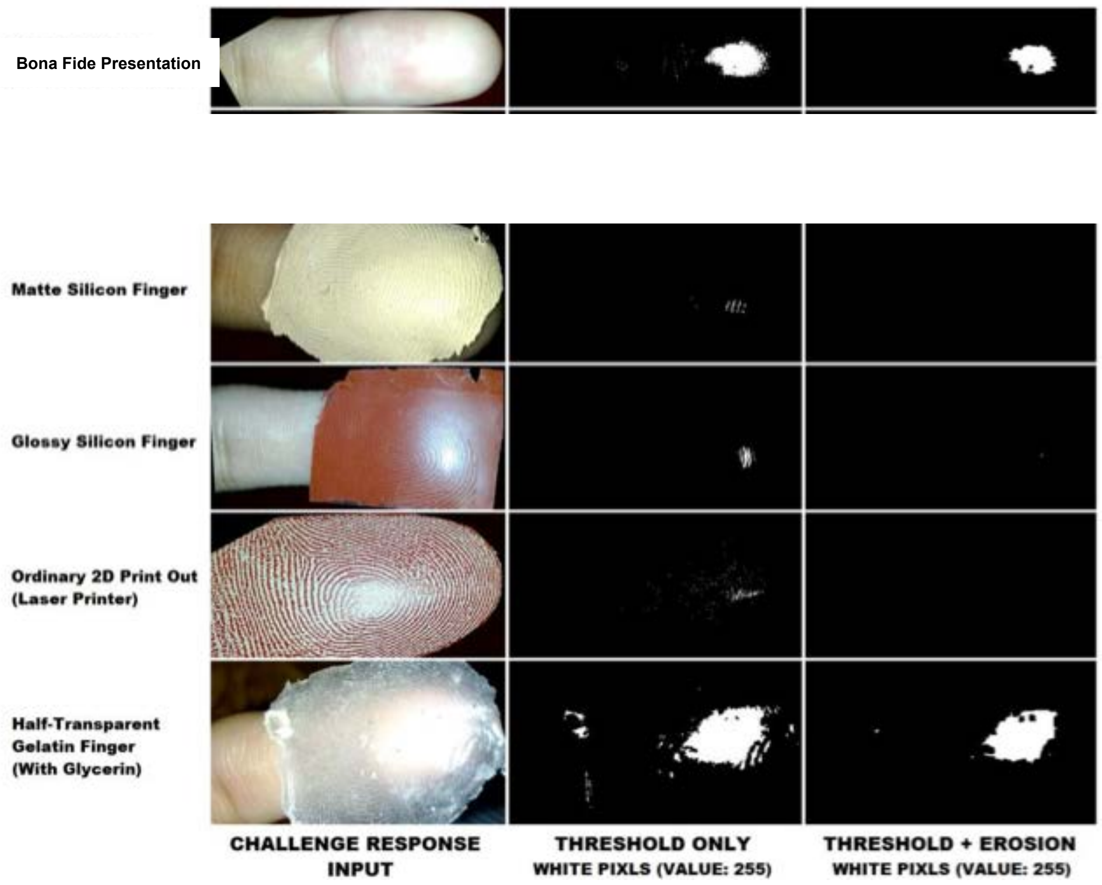
- Attack detection, as light reflection differs from artefacts to bona fide fingers

[SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG), (2013)

Fingerphoto Presentation Attack Detection

Finger recognition study - 2012/2013

- Results: Presentation Attack Detection (PAD)

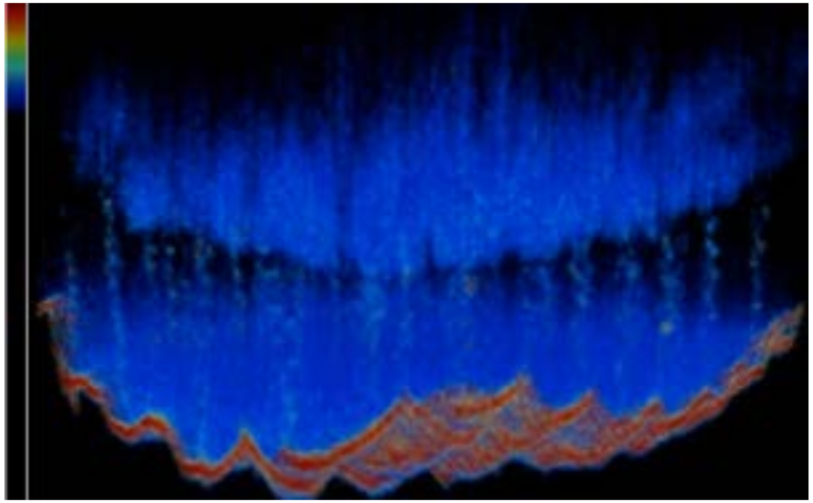


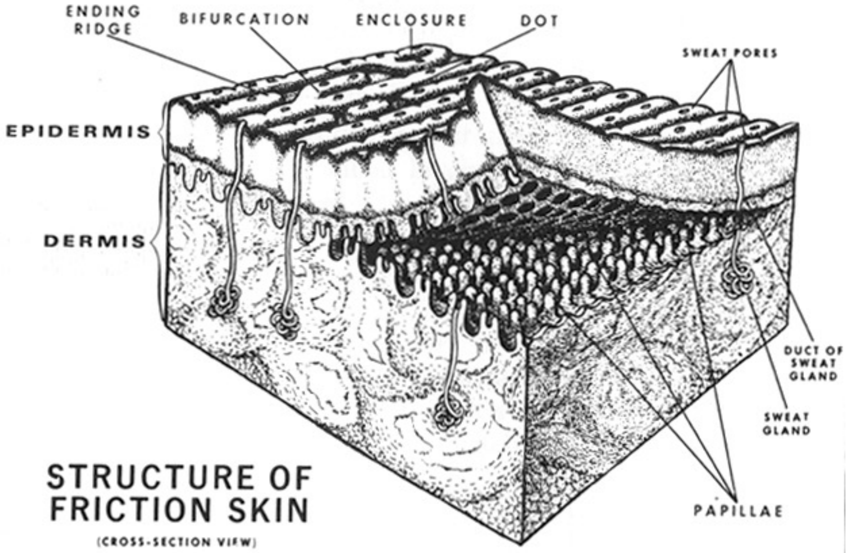
- Conclusion: Fingerphoto capture show better Presentation Attack Detection than capacitive sensors

Fingerprint Capture Device Security

Countermeasures

- Observation of the live skin properties
- Observation of the sweat glandes
- Sensor:
  - Optical Coherence Tomography (OCT)

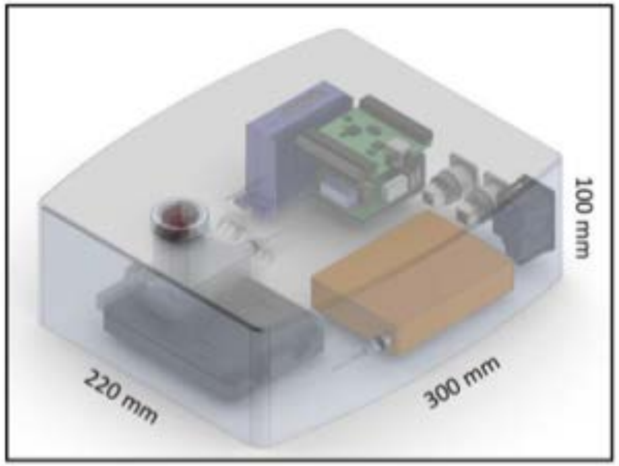




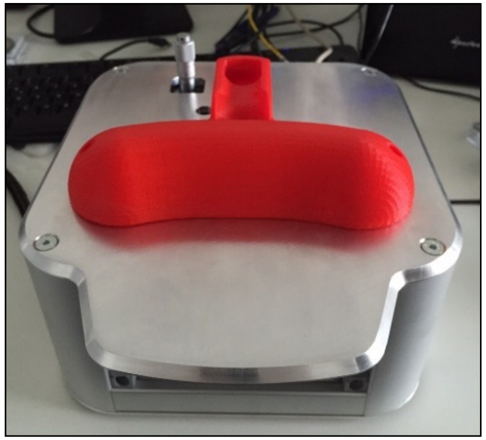
Fingerprint Capture Device Security

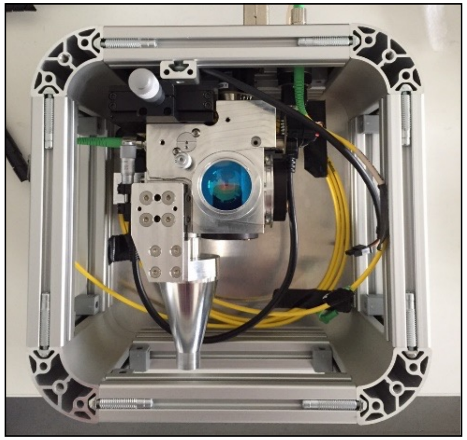
OCT

- at BSI-Germany
- Prototype for a high-end fingerprint sensor
- Requirements
  - PA robustness
  - Capture area: 20x20x6 mm
  - up to 3000 dpi
  - touchless scanning



Source: BSI



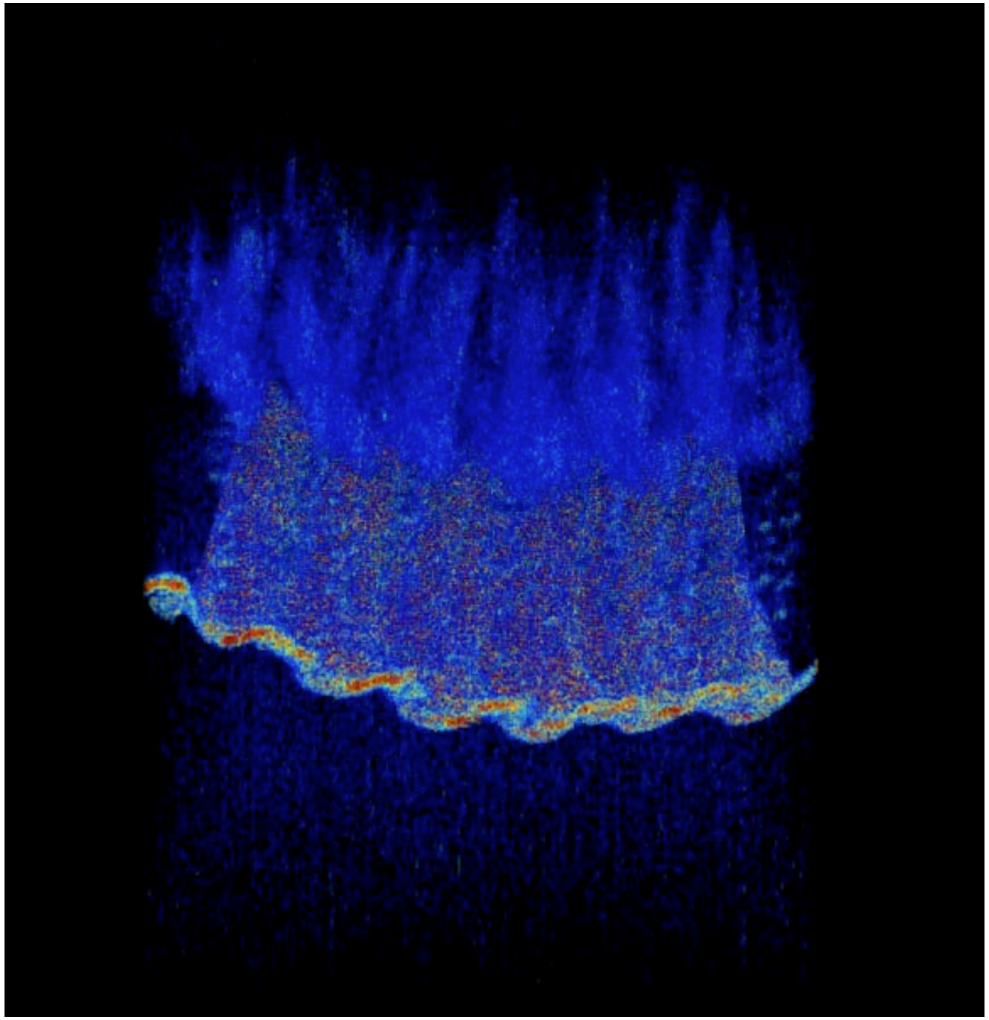


Source: BSI

Fingerprint Capture Device Security

OCT

- Visualization of sweat glands
  - good scan

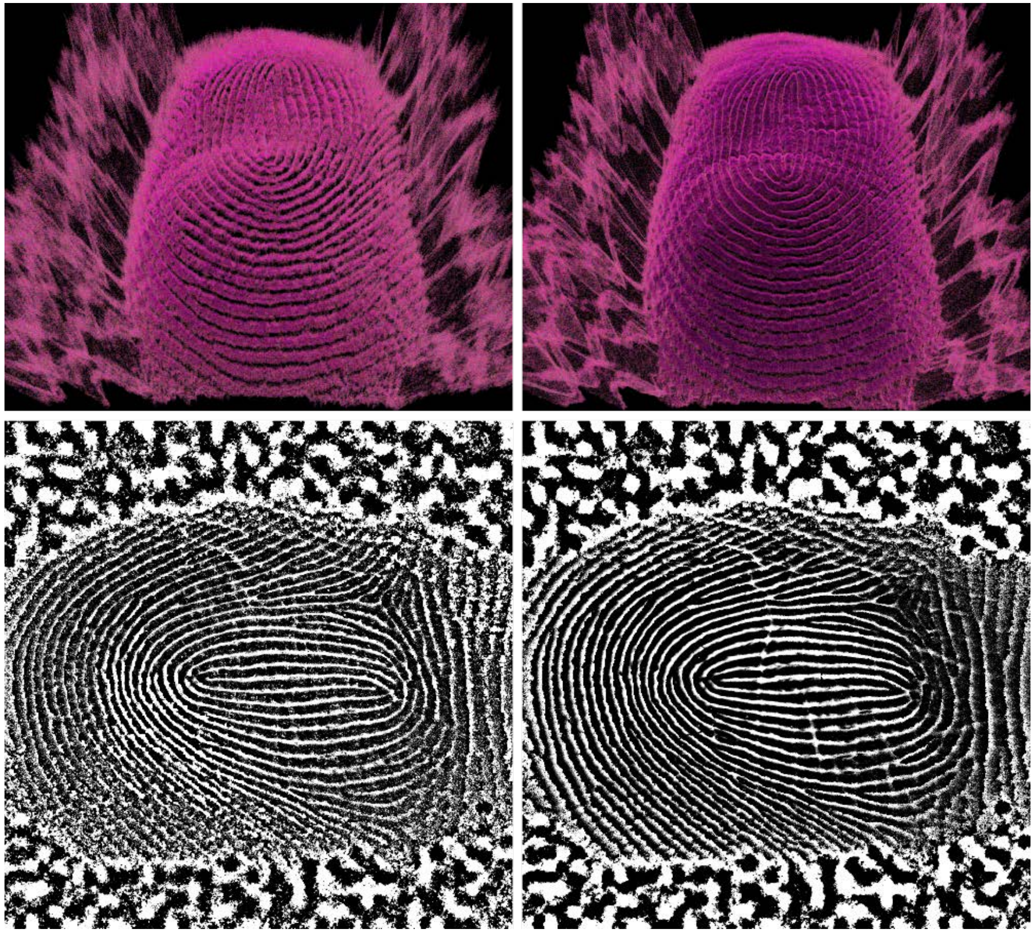


Source: C. Sousedik, NTNU, 2016

Fingerprint Capture Device Security

Comparing outer and inner fingerprint patterns

- Less than 2s (on GTX980)
  - detection of outer and inner layer
  - 2D projection



Internal fingerprint

Surface fingerprint

Source: BSI

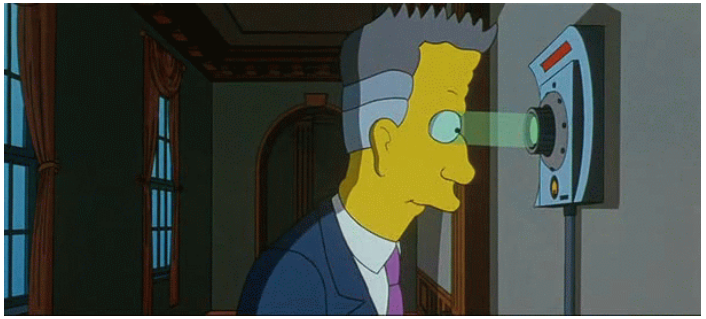
What about other modalities?

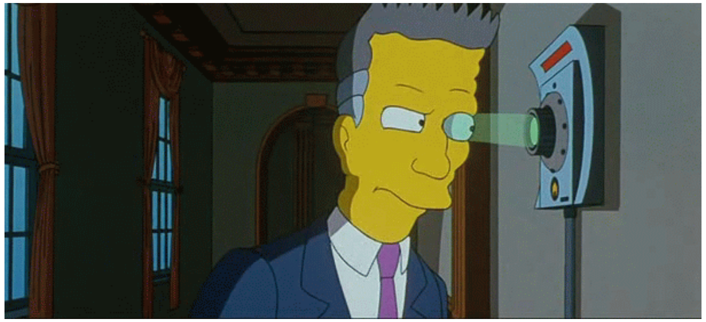
Presentation Attacks with Eye Artefacts

Eye Recognition Security

Presentation attacks

- in the Movie “The Simpsons” (2007)





PAD for Eye Recognition Security

Eye recognition study - 2015

- Presentation Attack Detection (PAD) videos on iPhone 5 S and Nokia 1020

- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information

PAD for Eye Recognition Security

Method based on Eulerian Video Magnification (EVM)

[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information",
in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem:

- **Attack presentation classification error rate (APCER)** *proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario*

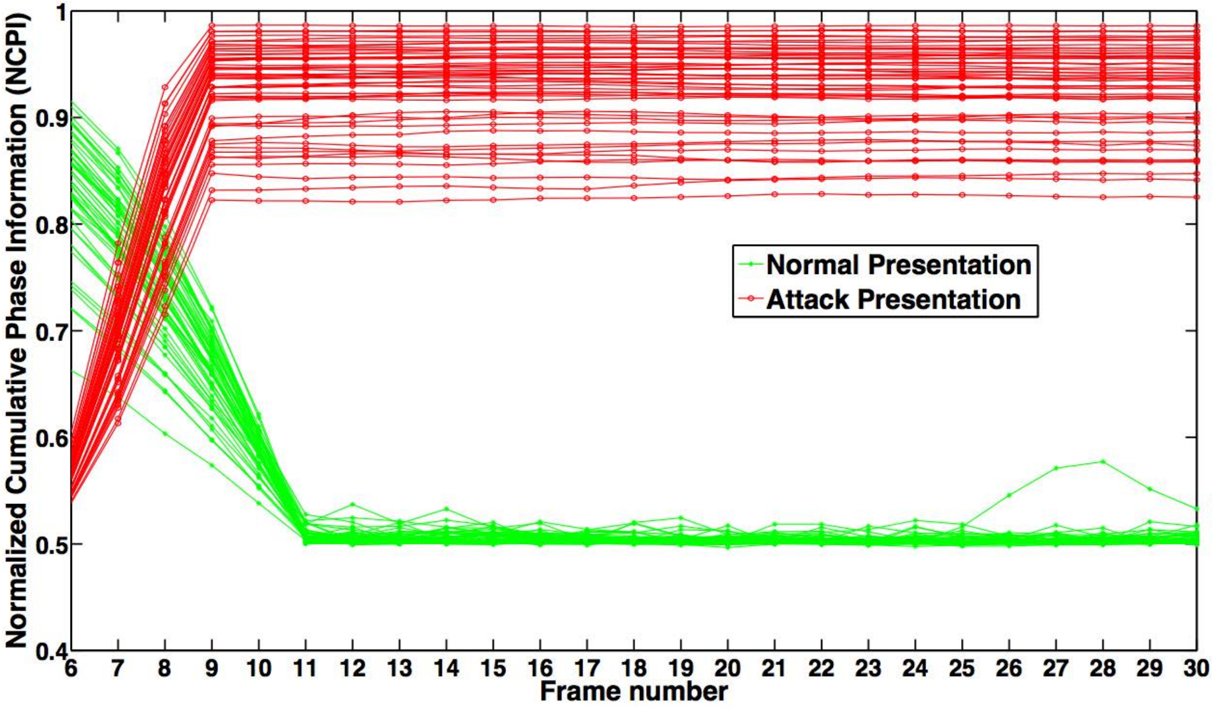
- **Bona fide presentation classification error rate (BPCER)** *proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario*

Source: ISO/IEC 30107-3

PAD for Eye Recognition Security

Eye recognition study - 2015

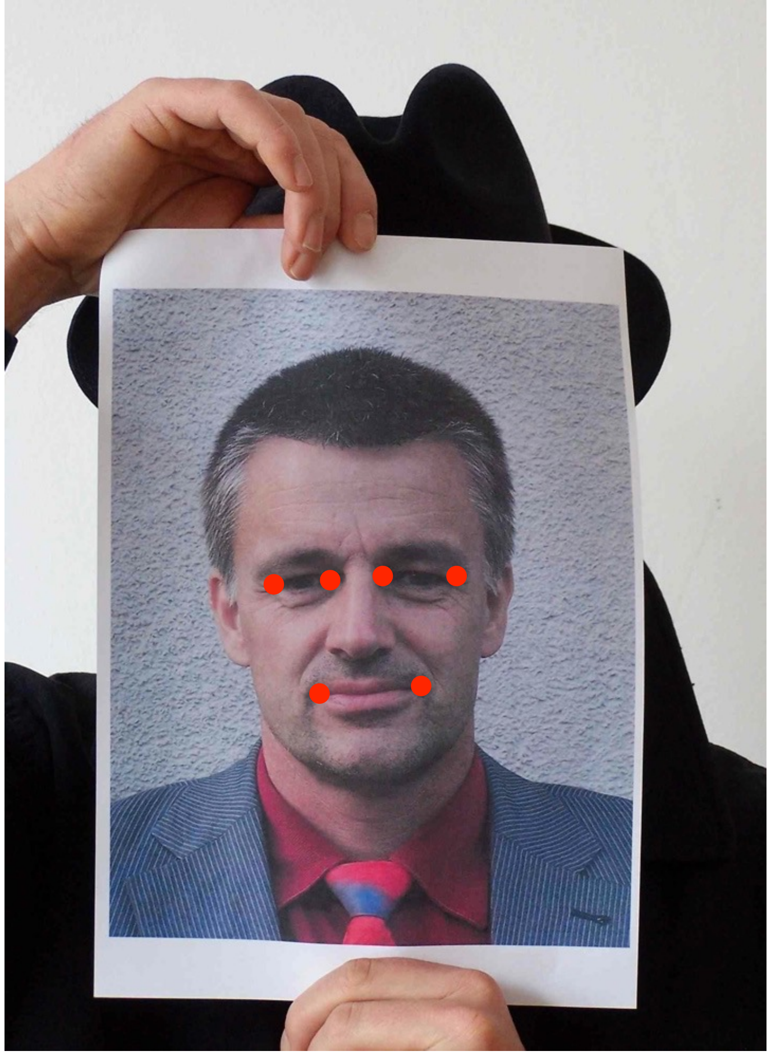
- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information
- Zero Error Rates:
  - APCER = 0 %
  - BPCER = 0 %



[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), (2015)

Widely used at borders is Face Recognition!
Presentation Attacks with Face Artefacts

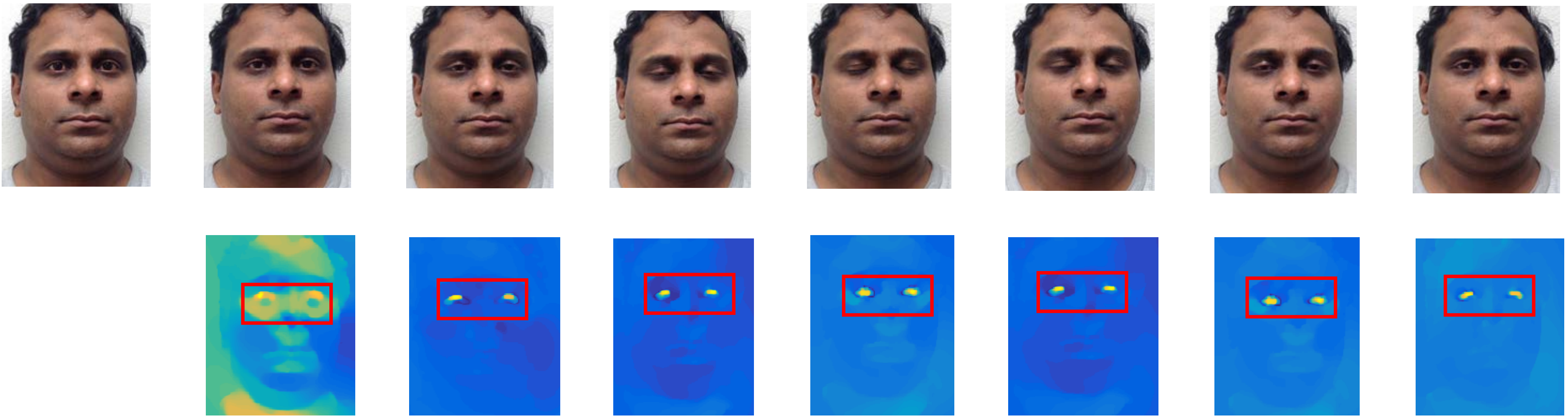
Face Presentation Attacks



Face Presentation Attack Detection

Hardware based

- Challenge Response
  - challenge the subject instructions and then compare the response to reference model for a bona fide behaviour
    - Instructions to the user to change head pose.
    - Reads user’s lips after playing audio tracks of words or numbers.
- Blink detection

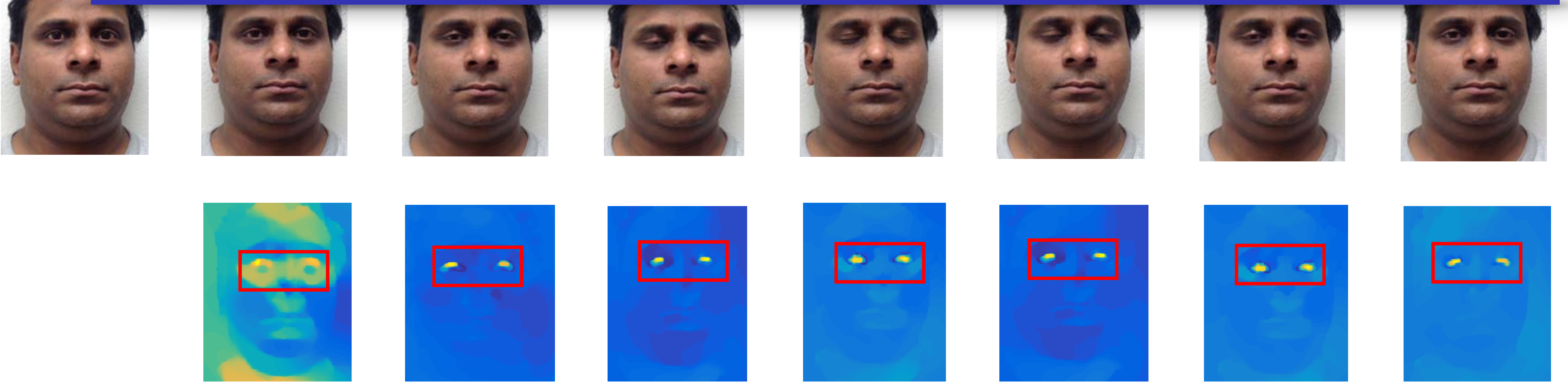


Face Presentation Attack Detection

Hardware based

- Challenge Response
  - challenge the subject instructions and then compare the response to reference model for a bona fide behaviour
    - Instructions to the user to change head pose
- B

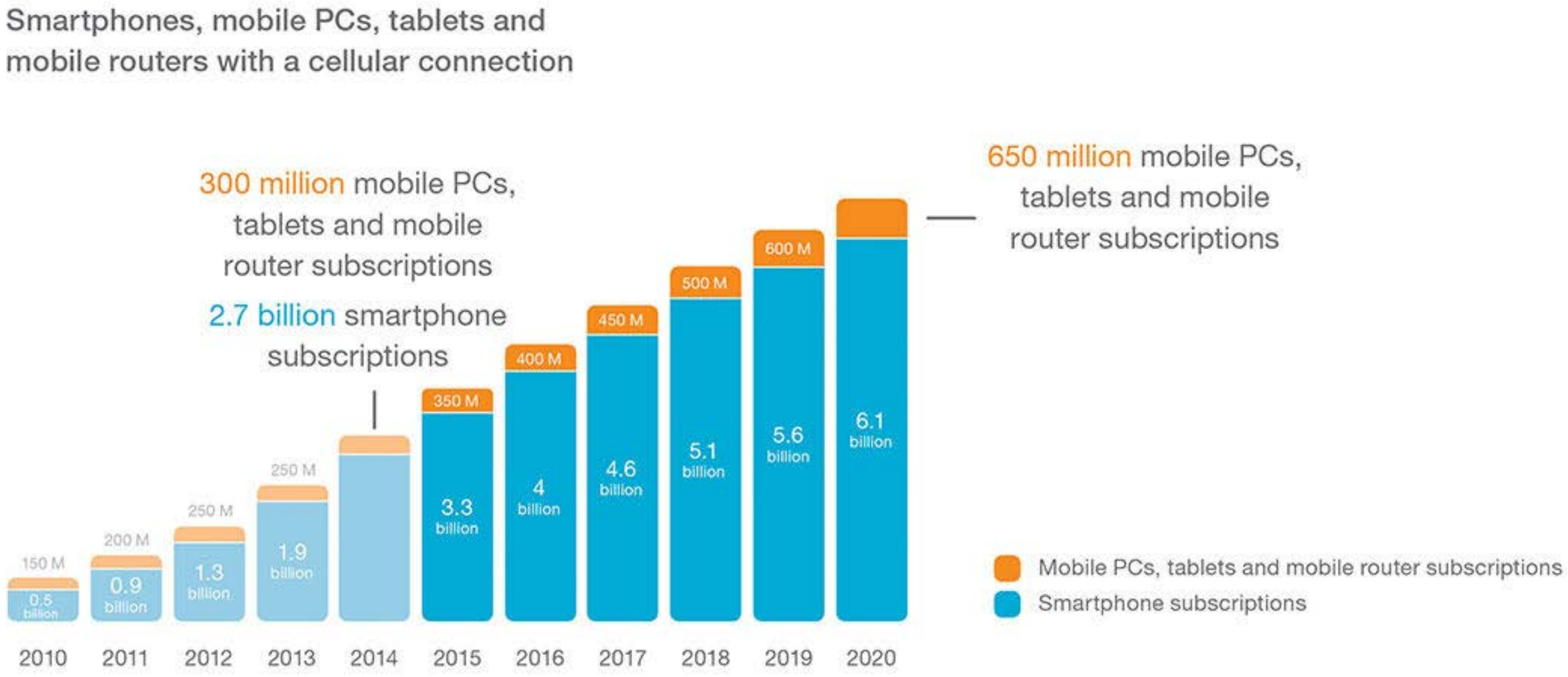
But today we have good displays to replay a video in high quality!



Face Recognition in unsupervised environments

Smartphone Deployment

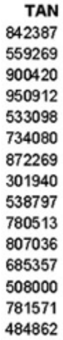
The Smartphone as personal device



Source: https://thenextweb.com/insider/2014/11/18/2020-90-worlds-population-aged-6-will-mobile-phone-report/

Access Control in the Banking Environment

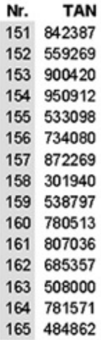
A European perspective



TAN
842387
559269
900420
950912
533098
734080
872269
301940
538797
780513
807036
685357
508000
781571
484862

...

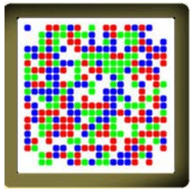
PHISHING ATTACKS START



Nr.	TAN
151	842387
152	559269
153	900420
154	950912
155	533098
156	734080
157	872269
158	301940
159	538797
160	780513
161	807036
162	685357
163	508000
164	781571
165	484862

...

bankID



vipps

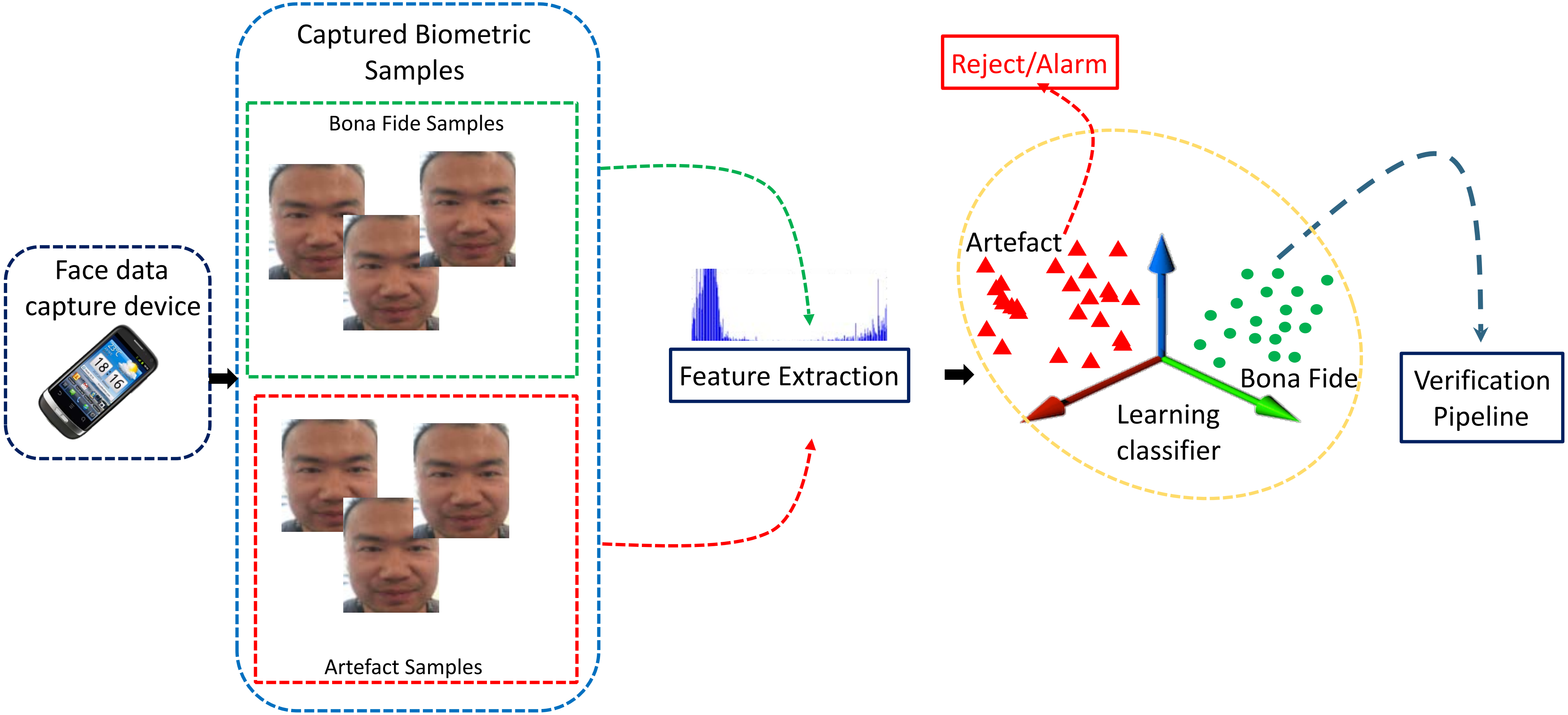
mobileTAN

TAN	1990
HBCI	1990
PHISHING ATTACKS START	2004
iTAN	2005
mobileTAN chipTAN	2006
bankID	2007
photoTAN	2012
touchID	2014
VIPPS	2015

Inspired by: BdB (2015)

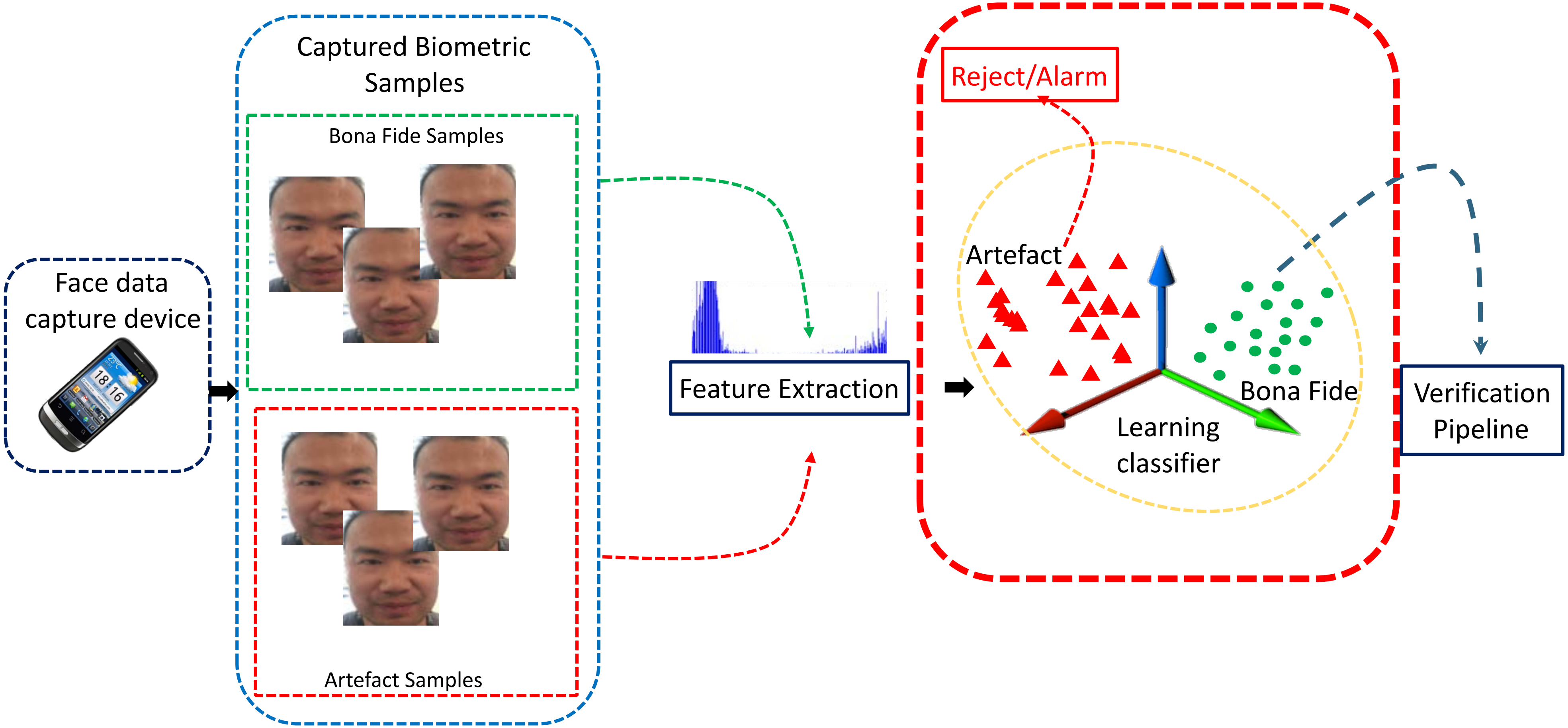
Smartphone - Presentation Attack Detection

- Augmenting the processing pipeline



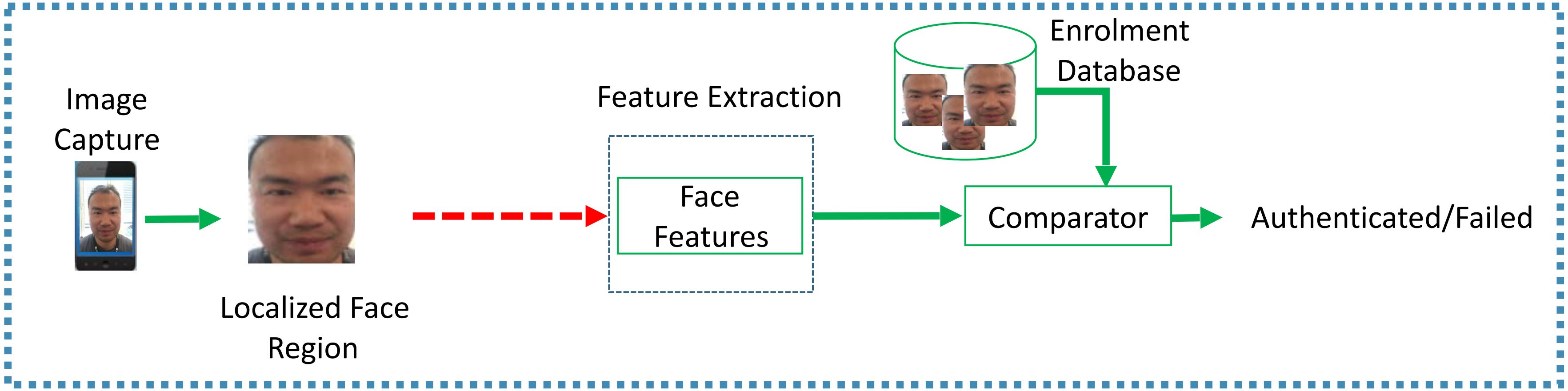
Smartphone - Face PAD

- Augmenting the processing pipeline



Smartphone - Face PAD

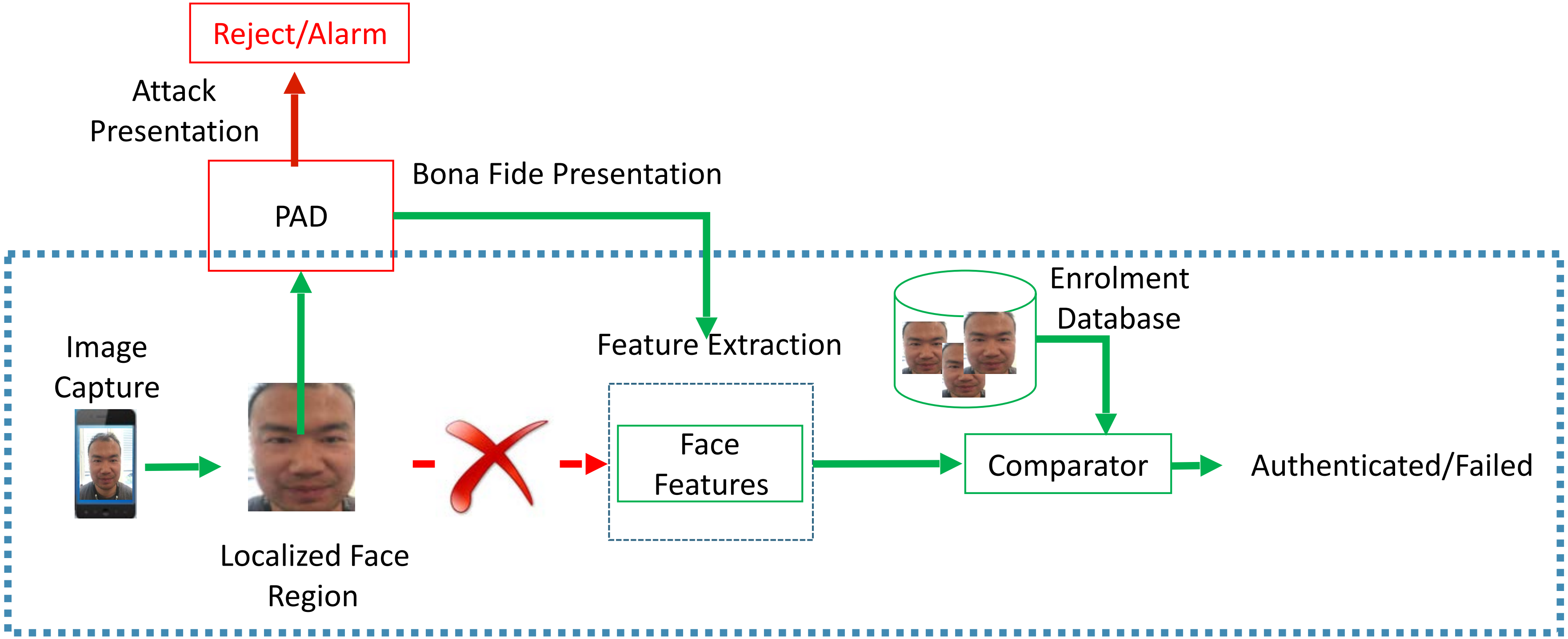
- Augmenting the processing pipeline



[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

Smartphone - Face PAD

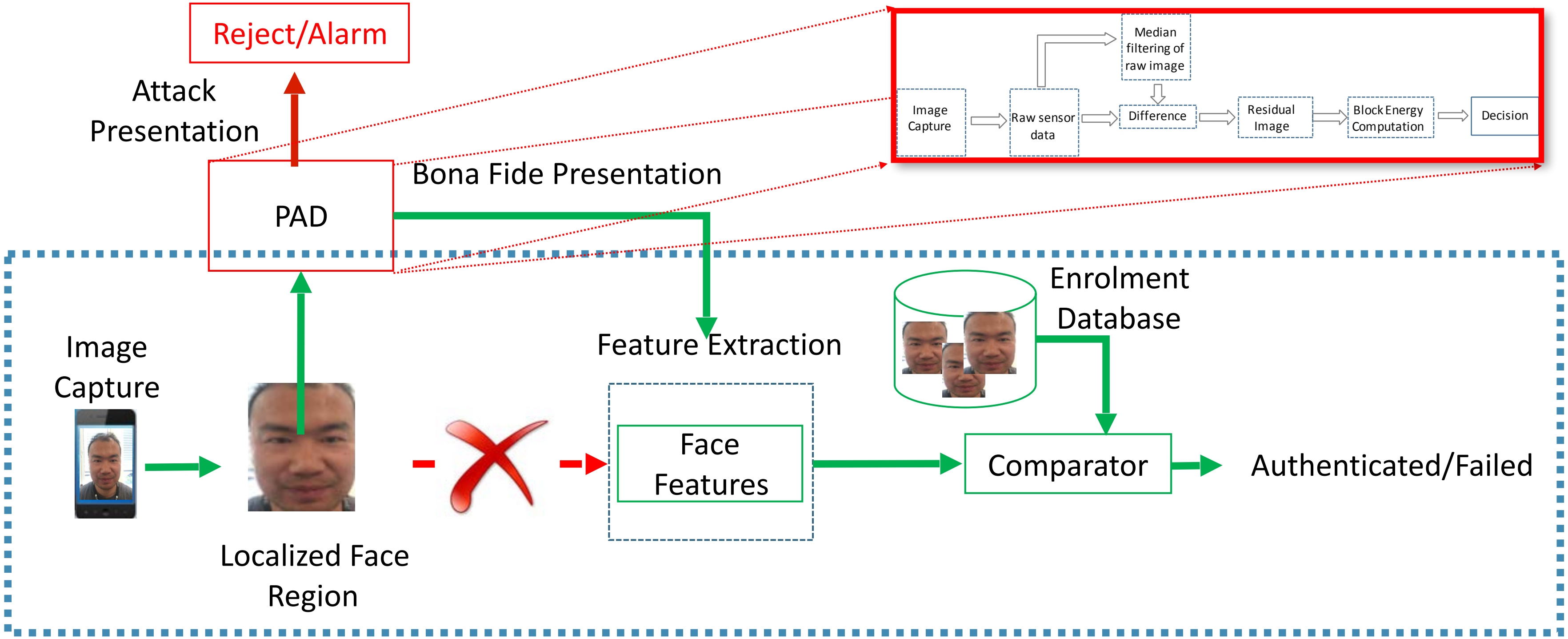
- Augmenting the processing pipeline



[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

Smartphone - Face PAD

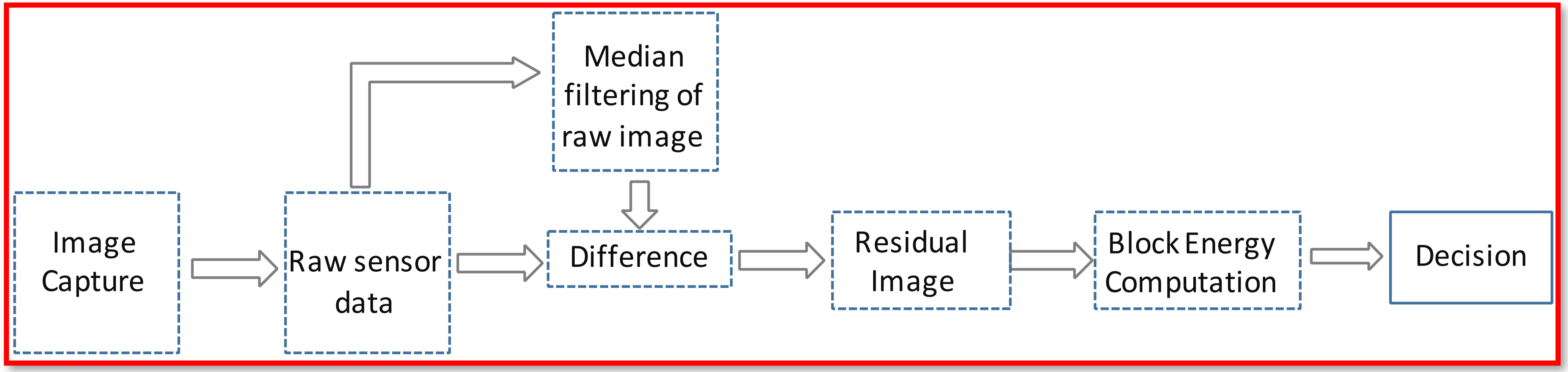
- Augmenting the processing pipeline



[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

Smartphone - Face PAD

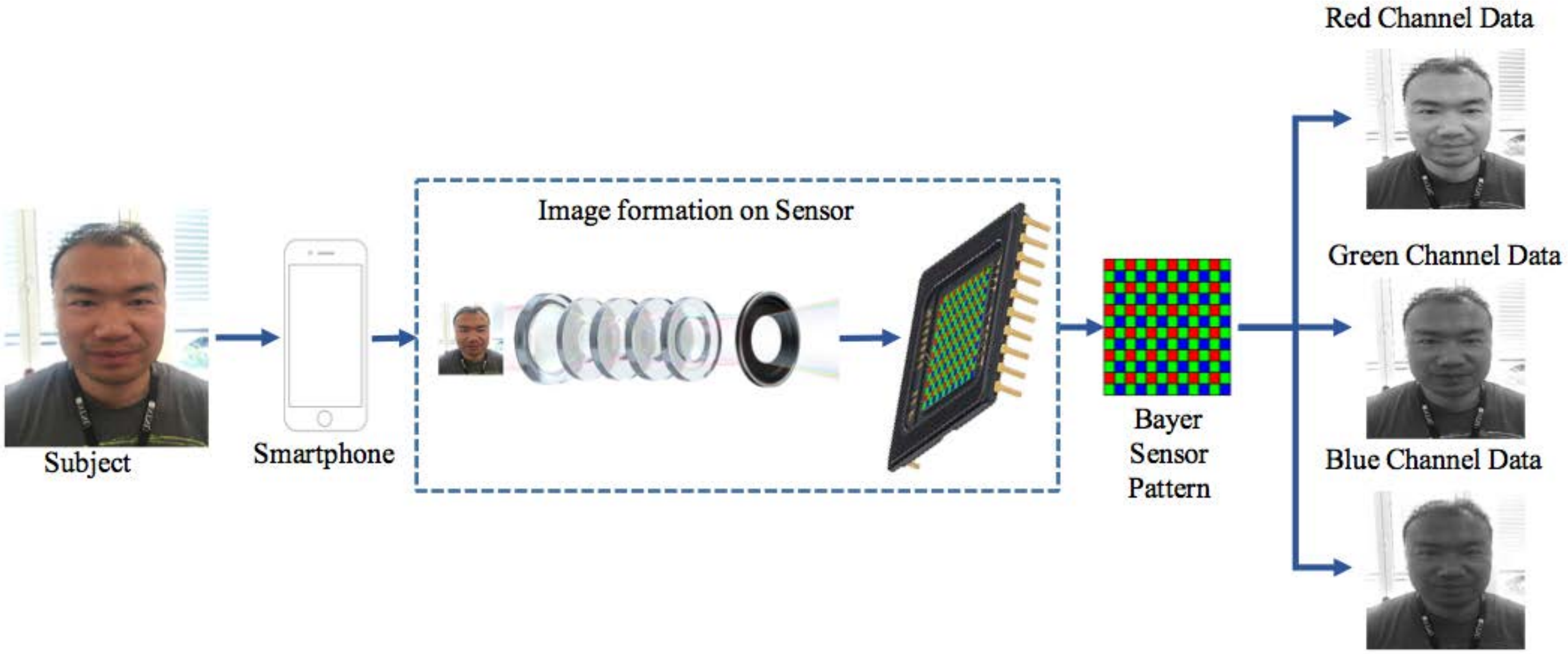
- The Presentation Attack Detection subsystem



[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

Smartphone - Face PAD

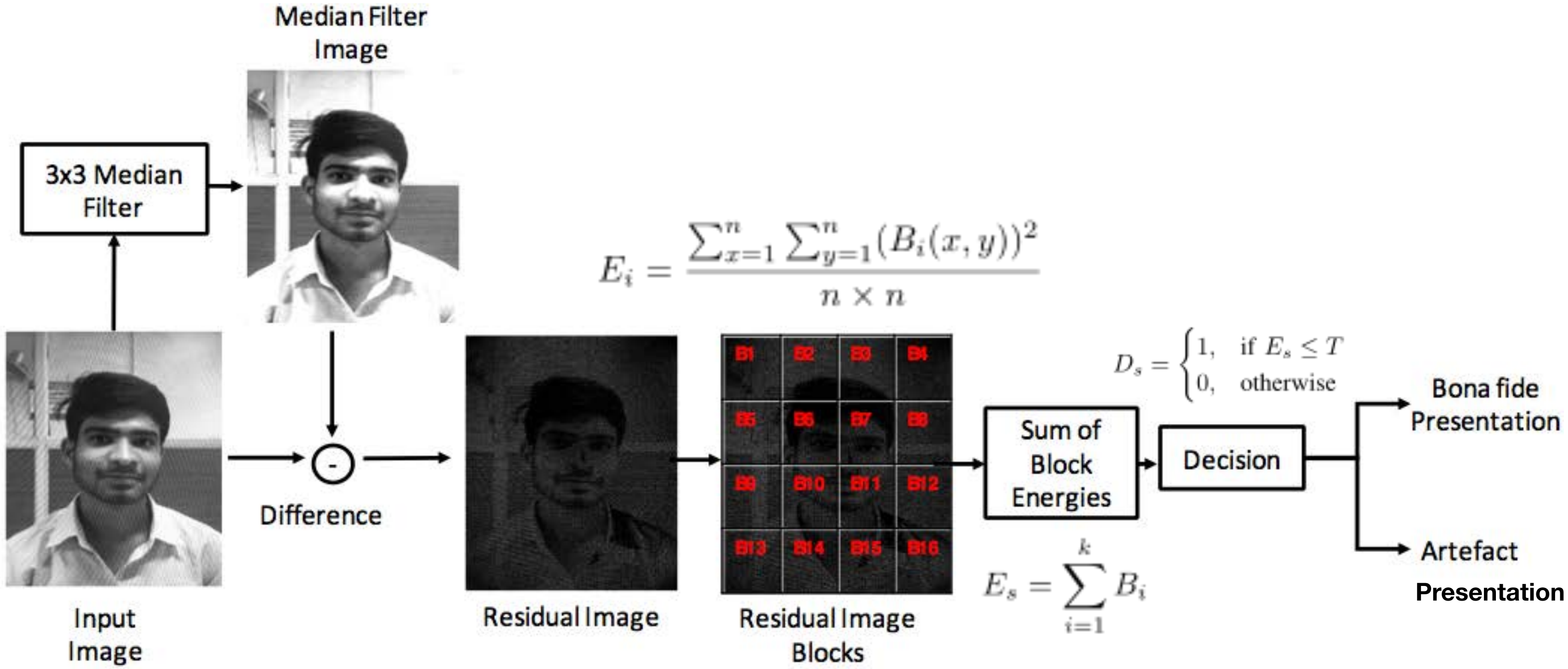
- The biometric sample



[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

Smartphone - Face PAD

- Channel based processing



$$E_i = \frac{\sum_{x=1}^{n} \sum_{y=1}^{n} (B_i(x,y))^2}{n \times n}$$

$$D_s = \begin{cases} 1, & \text{if } E_s \leq T \\ 0, & \text{otherwise} \end{cases}$$

$$E_s = \sum_{i=1}^{k} B_i$$

[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

Smartphone - Face PAD

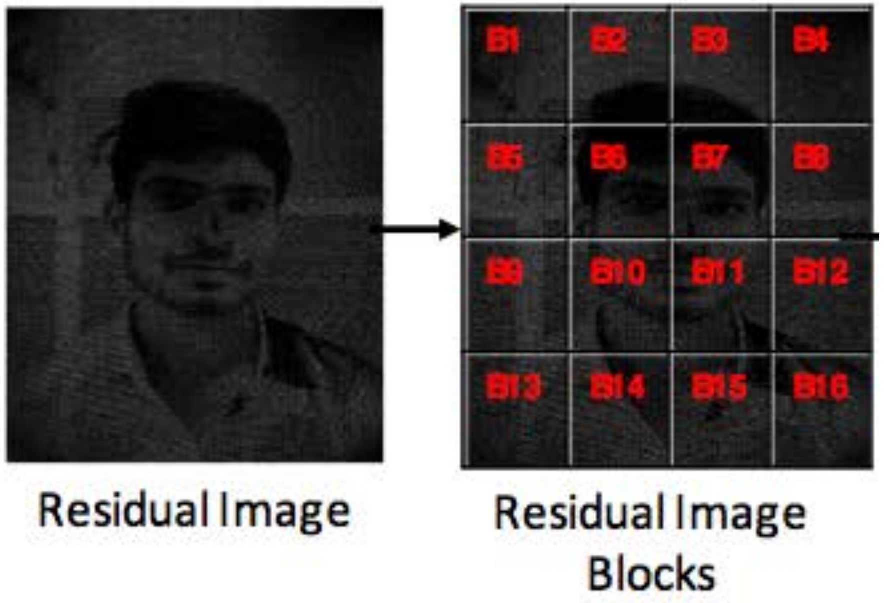
- Residual image computation

$$E_i = \frac{\sum_{x=1}^{n} \sum_{y=1}^{n} (B_i(x,y))^2}{n \times n}$$

$$E_s = \sum_{i=1}^{k} B_i$$

$$D_s = \begin{cases} 1, & \text{if } E_s \leq T \\ 0, & \text{otherwise} \end{cases}$$

$$D = \begin{cases} 1, & \text{if } majority\{D_r, D_g, D_b\} = 1 \\ 0, & \text{otherwise} \end{cases}$$

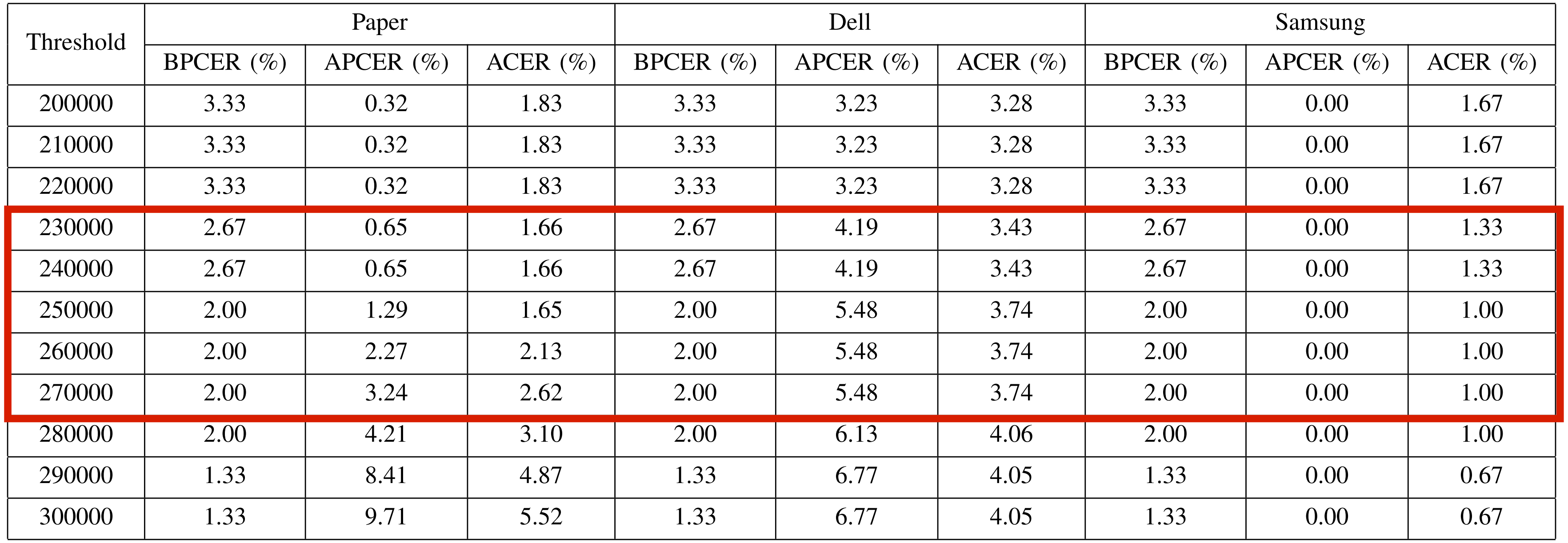


[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

Smartphone PAD – Results Majority Voting

Classification Error Rates

- Error rates for different thresholds of with majority voting on all three channels



Threshold	Paper			Dell			Samsung		
	BPCER (%)	APCER (%)	ACER (%)	BPCER (%)	APCER (%)	ACER (%)	BPCER (%)	APCER (%)	ACER (%)
200000	3.33	0.32	1.83	3.33	3.23	3.28	3.33	0.00	1.67
210000	3.33	0.32	1.83	3.33	3.23	3.28	3.33	0.00	1.67
220000	3.33	0.32	1.83	3.33	3.23	3.28	3.33	0.00	1.67
230000	2.67	0.65	1.66	2.67	4.19	3.43	2.67	0.00	1.33
240000	2.67	0.65	1.66	2.67	4.19	3.43	2.67	0.00	1.33
250000	2.00	1.29	1.65	2.00	5.48	3.74	2.00	0.00	1.00
260000	2.00	2.27	2.13	2.00	5.48	3.74	2.00	0.00	1.00
270000	2.00	3.24	2.62	2.00	5.48	3.74	2.00	0.00	1.00
280000	2.00	4.21	3.10	2.00	6.13	4.06	2.00	0.00	1.00
290000	1.33	8.41	4.87	1.33	6.77	4.05	1.33	0.00	0.67
300000	1.33	9.71	5.52	1.33	6.77	4.05	1.33	0.00	0.67

[Wasnik2016] P. Wasnik, K. Raja, R. Raghavendra, and C. Busch. “Presentation attack detection in face biometric systems using raw sensor data from smartphones”. In Proc. 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), (2016)

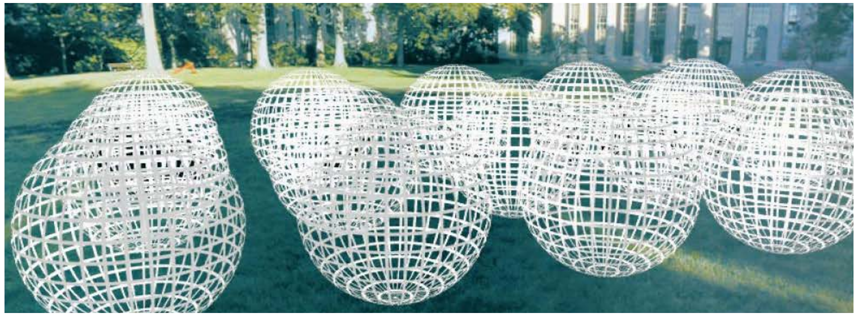
PAD – based on Depth Information

Light-field camera recently proposed for PAD

- panoptic or directional camera

Why light-field camera?

- Multiple focus/depth images in one shot.
- No need to adjust the lens to set focus.
- Portable and hand-held, low cost.



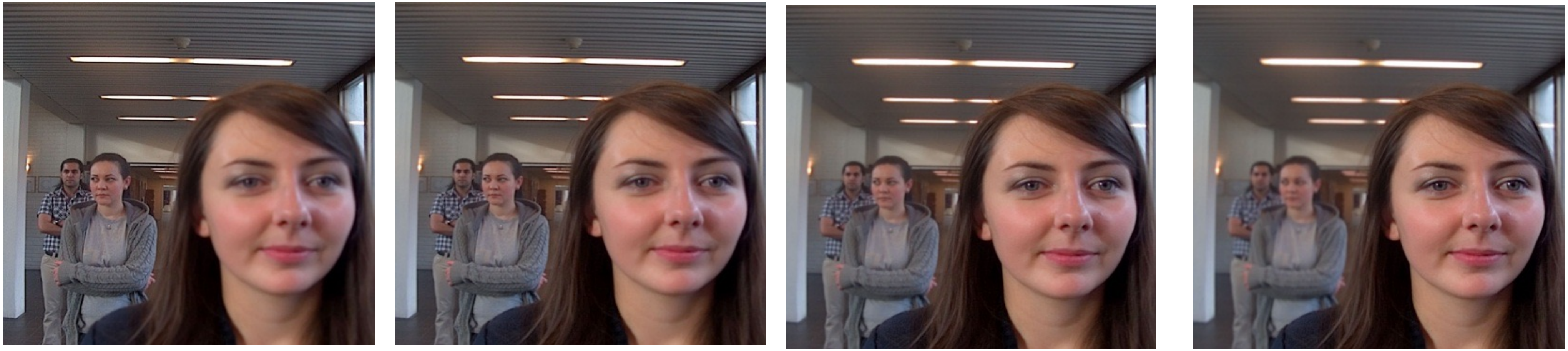
$P(\theta, \phi, \lambda, t, Vx, Vy, Vz)$

Raytrix

[Raghu2015] R. Raghavendra, K.B. Raja, and C. Busch: "Presentation Attack Detection for Face Recognition using Light Field Camera", in IEEE Transactions on Image Processing, vol. 24, no. 3, pp. 1060–1075, (2015)

PAD – based on Depth Information

Example of light-field imaging (LYTRO)

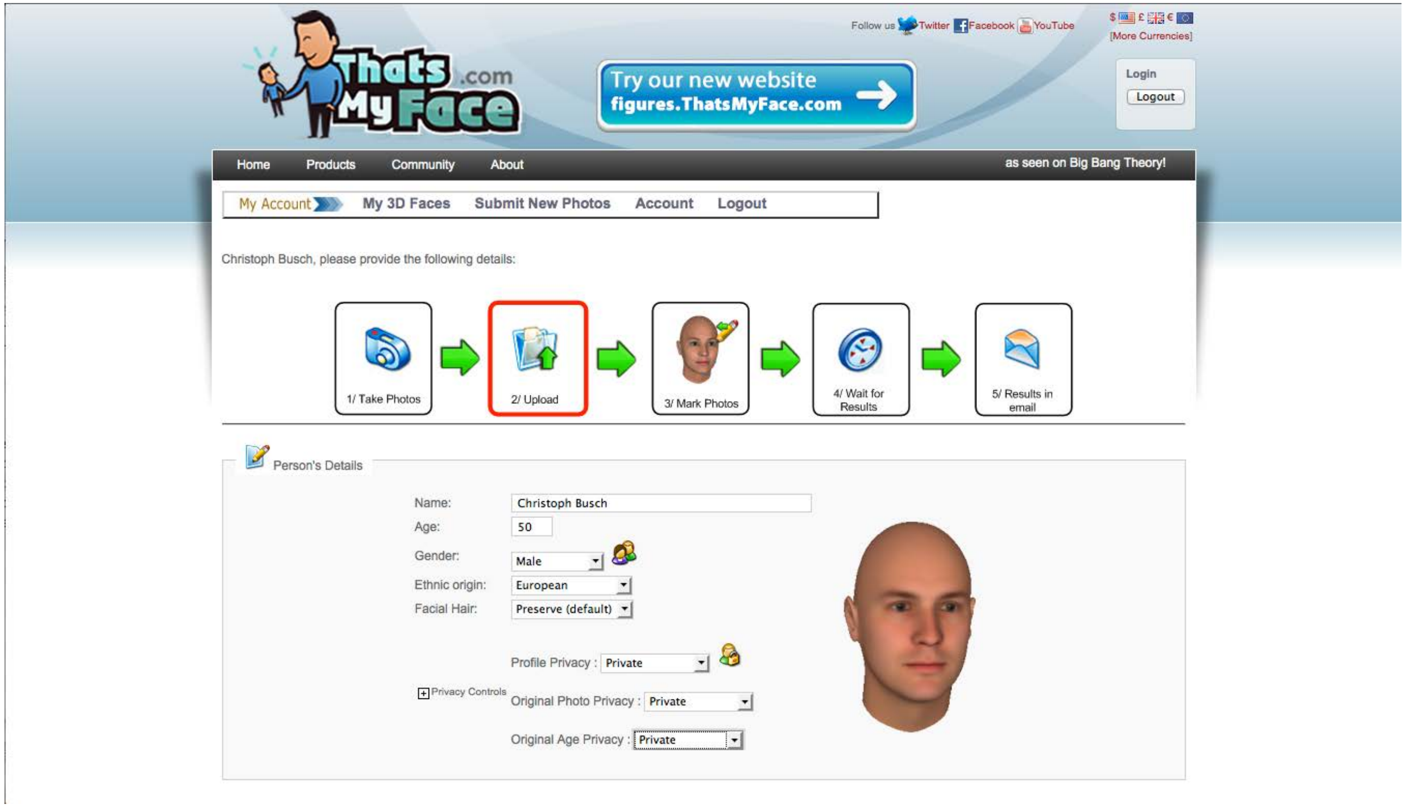


[Raghu2015] R. Raghavendra, K.B. Raja, and C. Busch: "Presentation Attack Detection for Face Recognition using Light Field Camera", in IEEE Transactions on Image Processing, vol. 24, no. 3, pp. 1060–1075, (2015)

3D Face Mask Production

Attack again without support of an enroled individual

- Frontal and profile photos are uploaded
- 3D face dataset rendered and produced



Christoph Busch, please provide the following details:

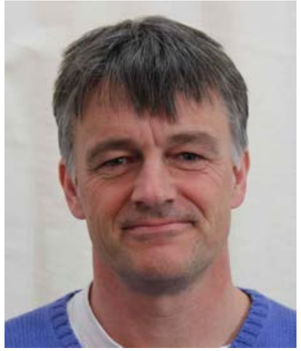
1/ Take Photos → 2/ Upload → 3/ Mark Photos → 4/ Wait for Results → 5/ Results in email

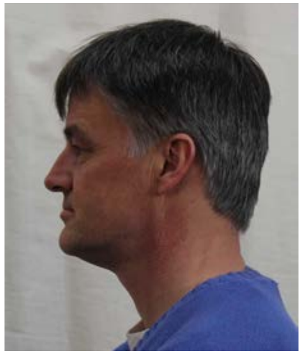
Person's Details

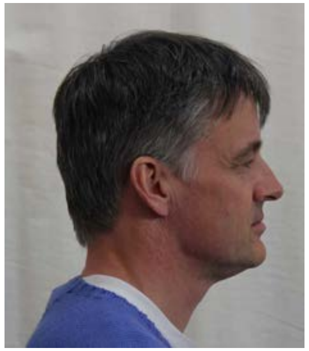
Name:	Christoph Busch
Age:	50
Gender:	Male
Ethnic origin:	European
Facial Hair:	Preserve (default)

Privacy Controls

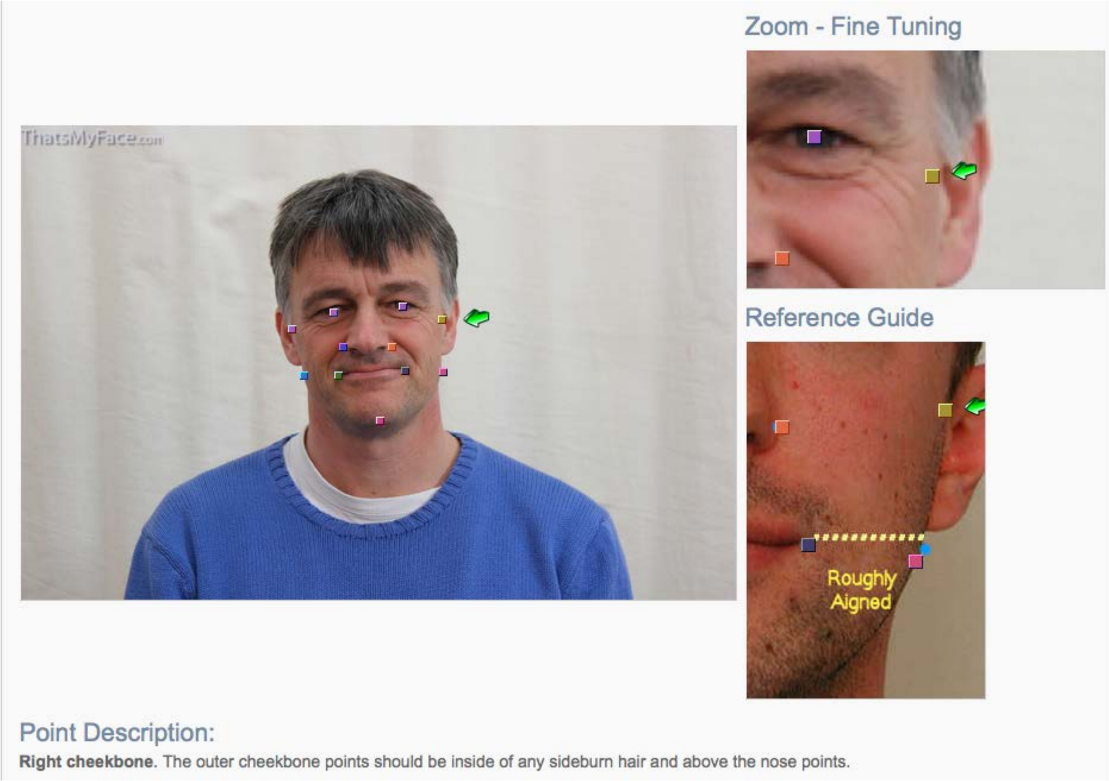
Profile Privacy :	Private
Original Photo Privacy :	Private
Original Age Privacy :	Private







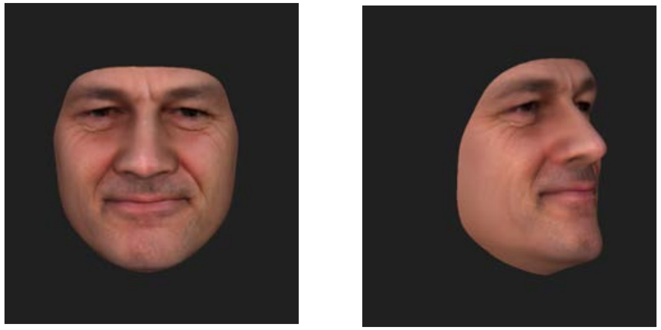
3D Face Mask Production



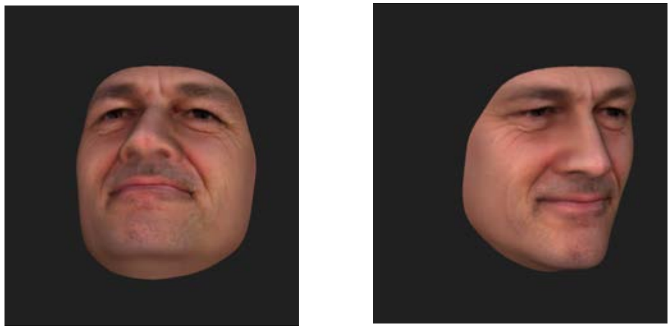
Point Description:

Right cheekbone. The outer cheekbone points should be inside of any sideburn hair and above the nose points.

3D-reconstruction



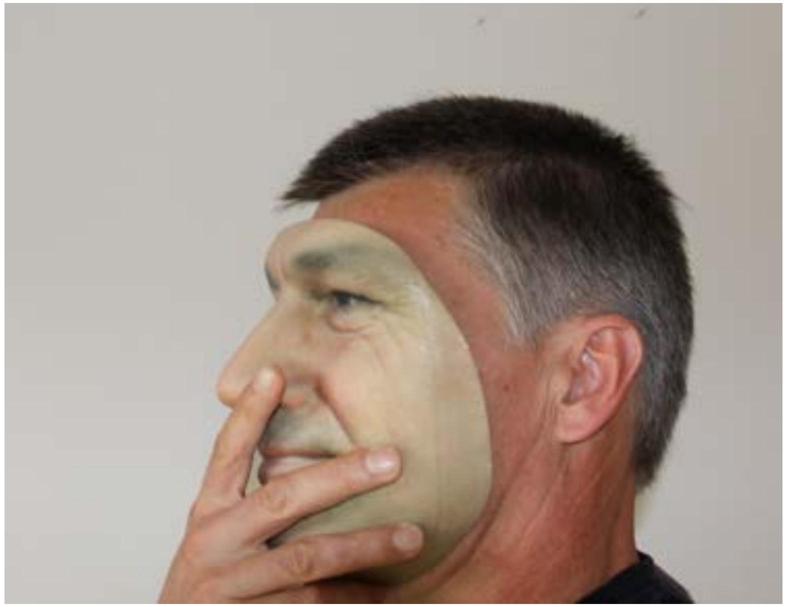
mask production preview (“beautified”):

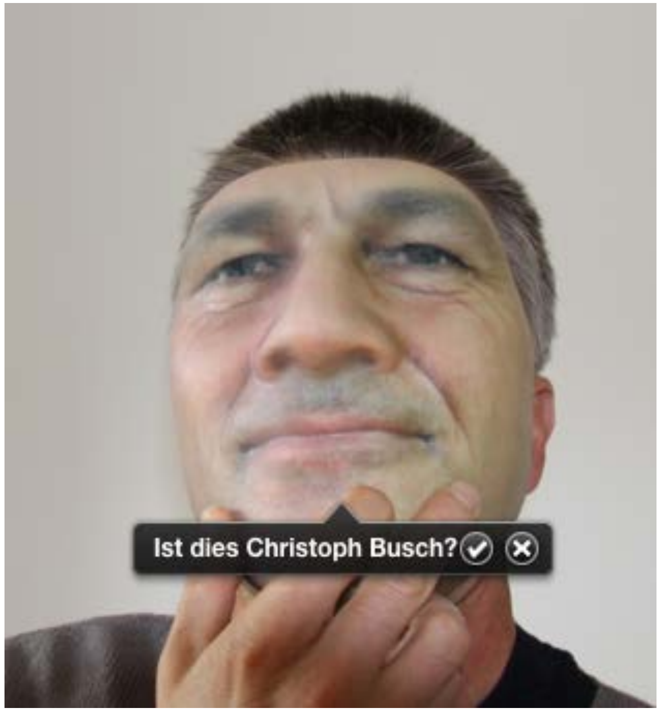


3D Face Mask Production

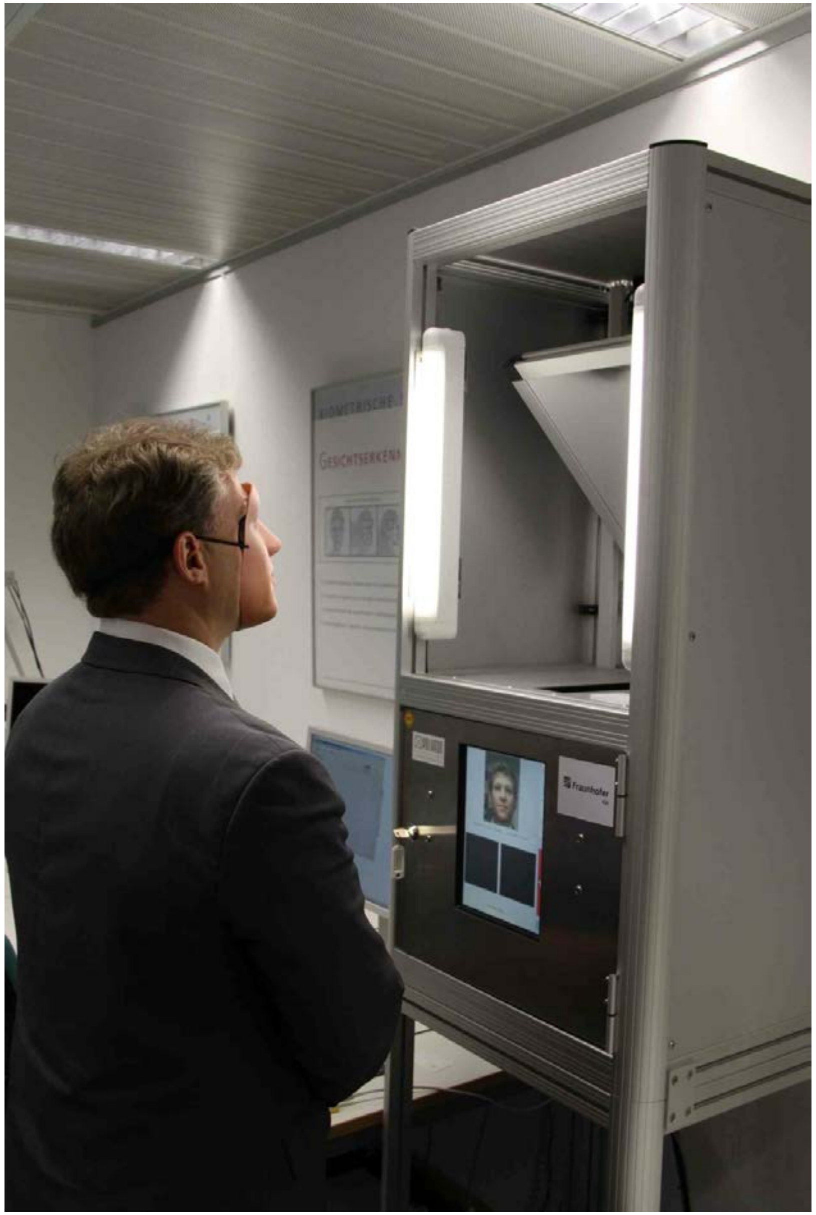
Attack again without support of an enroled individual

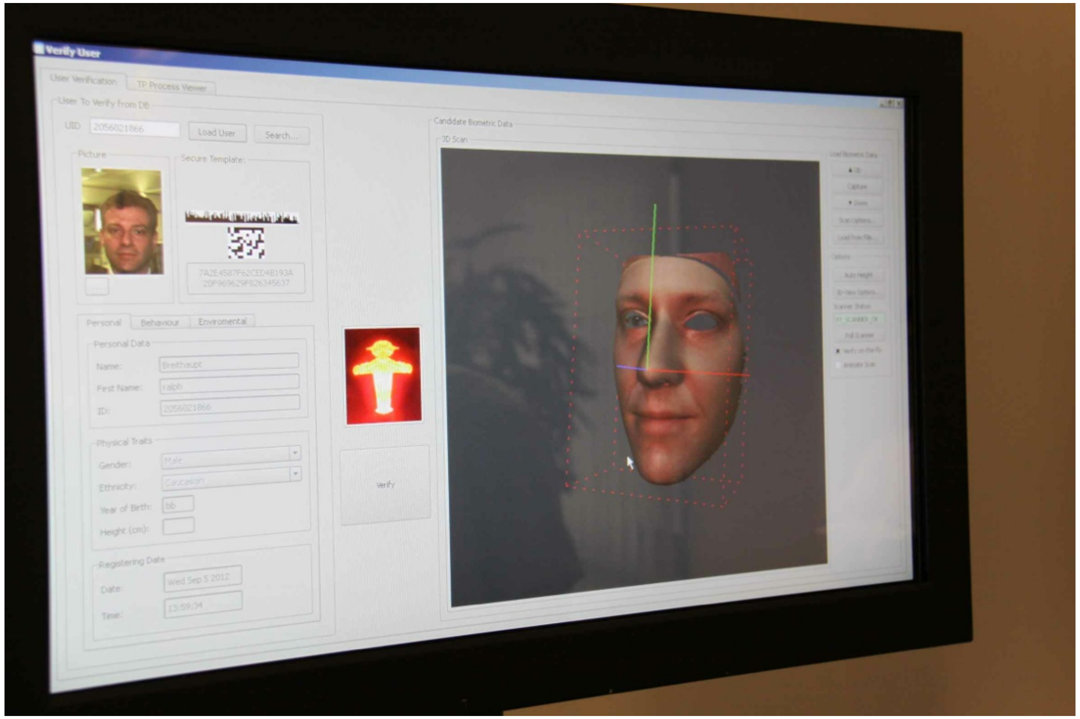
- A static mask is produced and shipped





Face Capture Device Security





Verify User

User Verification | TP Process Viewer

User To Verify from DB

UID: 2056021866

Load User | Search...

Picture

Secure Template:

7A2E4587F62CED4B193A
20F969629F826345637

Personal | Behaviour | Enviromental

Personal Data

Name: Breithaupt

First Name: ralph

ID: 2056021866

Physical Traits

Gender: Male

Ethnicity: Caucasian

Year of Birth: bb

Height (cm):

Registering Date

Date: Wed Sep 5 2012

Time: 13:59:34

Verify

Candidate Biometric Data

3D Scan

Impostor Presentation Attack

3D silicon mask

- Targeted attack with 3D silicon custom mask
- Cost more than 3000 USD

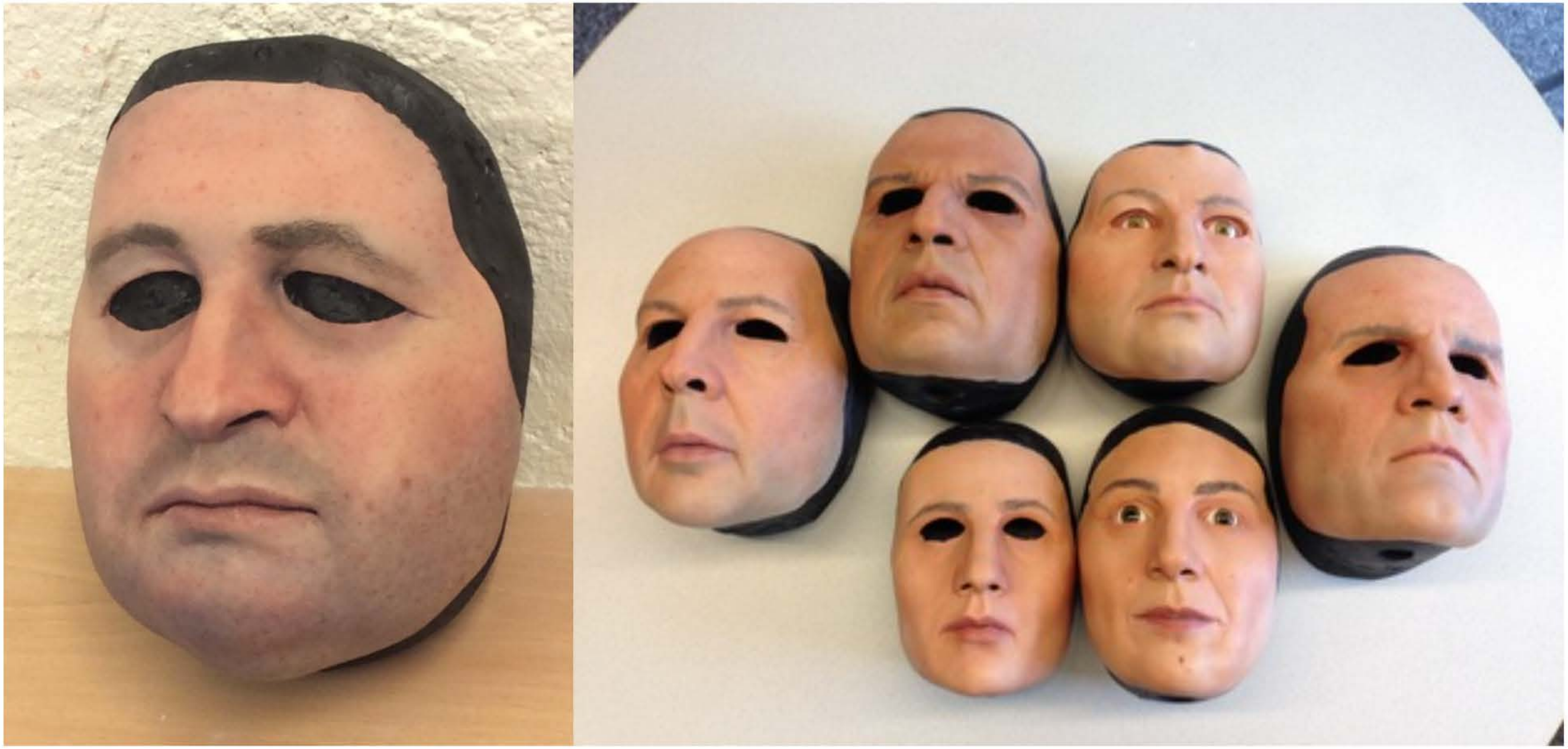
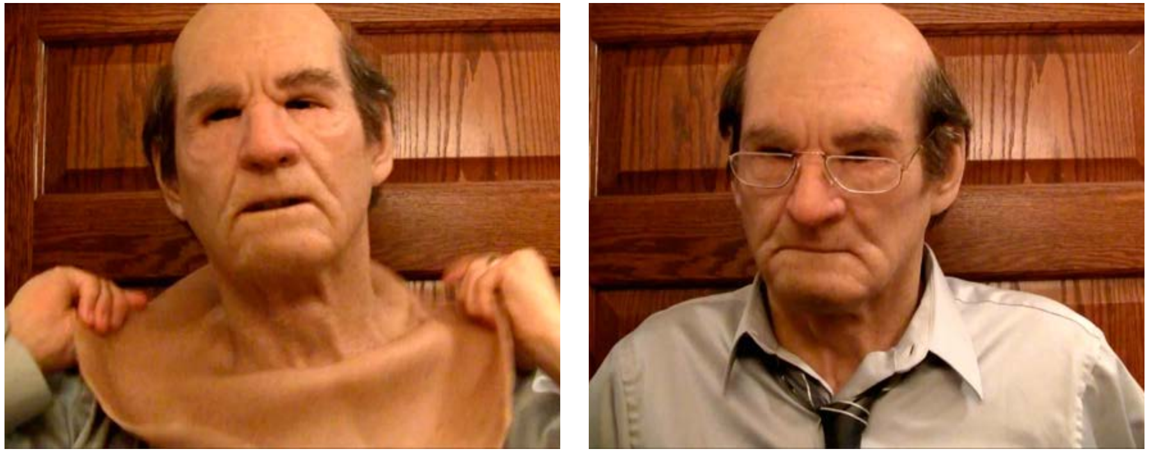


Image Source: Sebastien Marcel (Idiap)

Impostor Presentation Attack

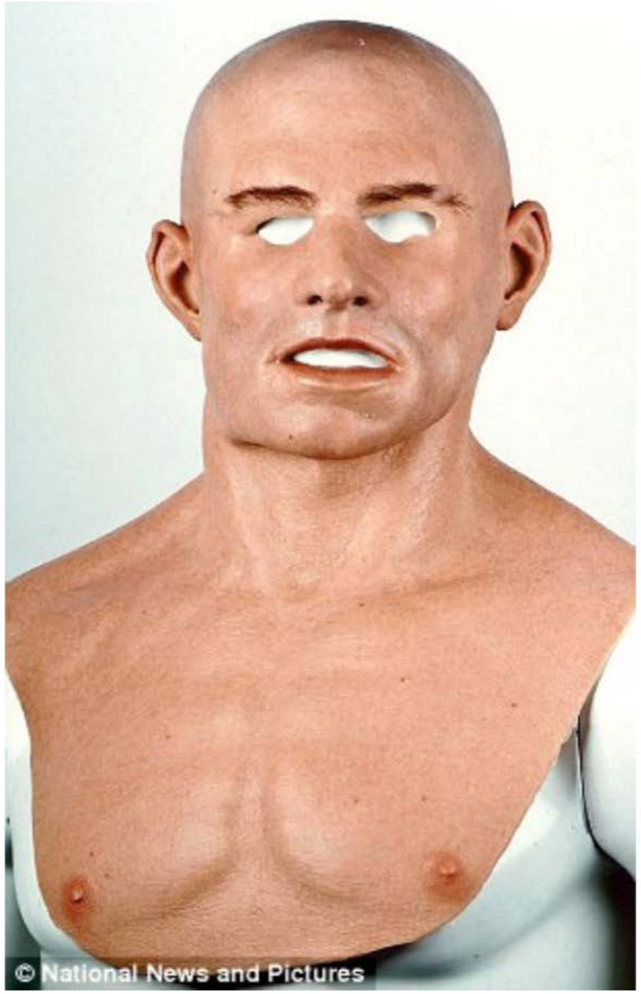


Source: BSI

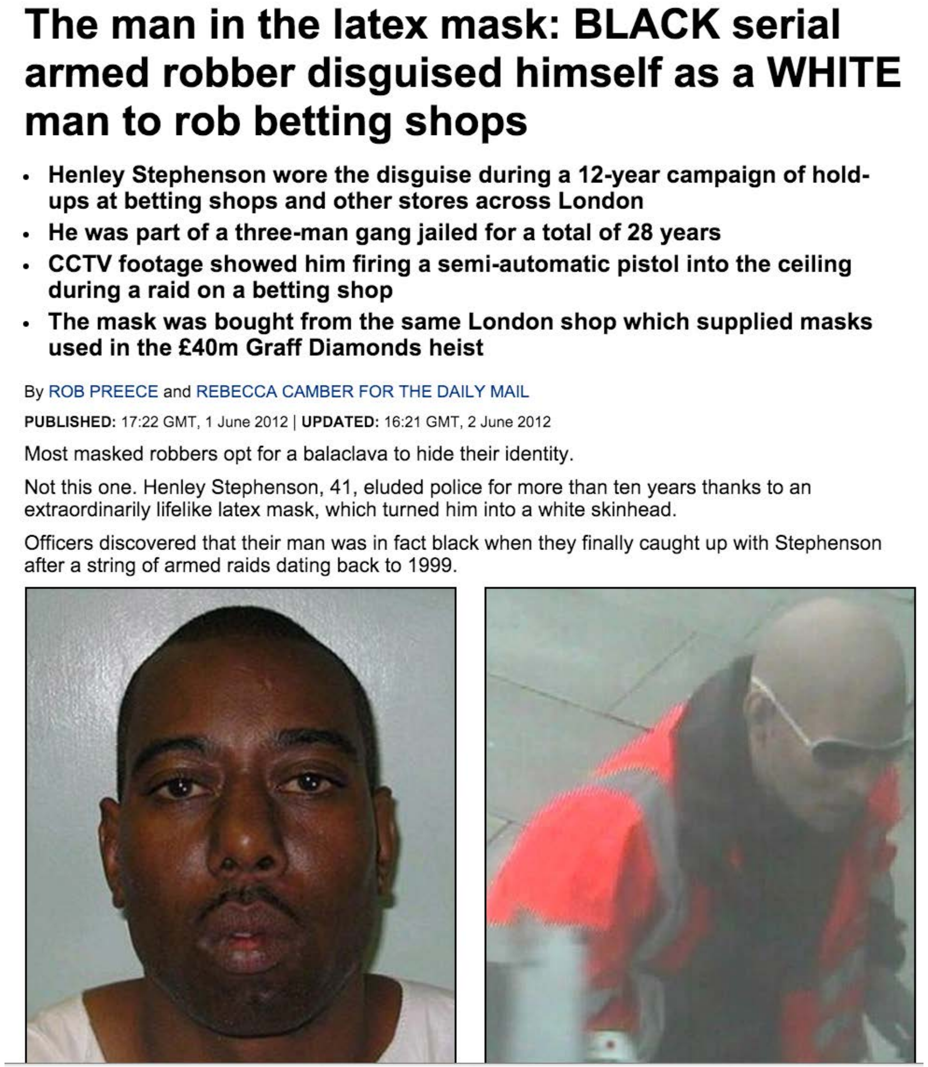
Face Capture Device Security

Face disguise for organized crime (June 2012)

- http://www.dailymail.co.uk/news/article-2153346/Black-armed-robber-disguised-white-man-using-latex-mask.html



© National News and Pictures



The man in the latex mask: BLACK serial armed robber disguised himself as a WHITE man to rob betting shops

- **Henley Stephenson wore the disguise during a 12-year campaign of hold-ups at betting shops and other stores across London**
- **He was part of a three-man gang jailed for a total of 28 years**
- **CCTV footage showed him firing a semi-automatic pistol into the ceiling during a raid on a betting shop**
- **The mask was bought from the same London shop which supplied masks used in the £40m Graff Diamonds heist**

By ROB PREECE and REBECCA CAMBER FOR THE DAILY MAIL

PUBLISHED: 17:22 GMT, 1 June 2012 | **UPDATED:** 16:21 GMT, 2 June 2012

Most masked robbers opt for a balaclava to hide their identity.

Not this one. Henley Stephenson, 41, eluded police for more than ten years thanks to an extraordinarily lifelike latex mask, which turned him into a white skinhead.

Officers discovered that their man was in fact black when they finally caught up with Stephenson after a string of armed raids dating back to 1999.

We are close to the end of this talk!

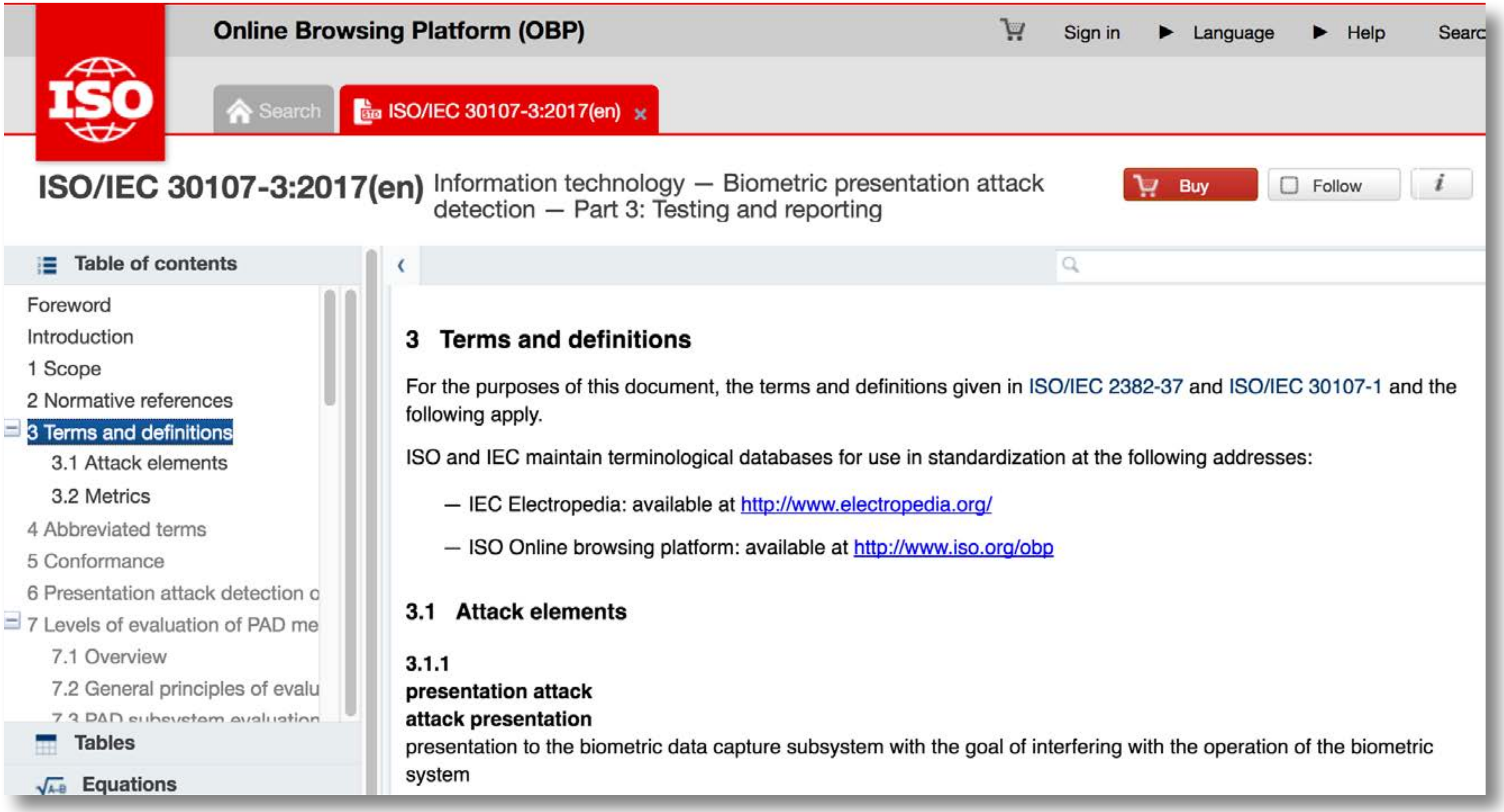
Now - the bonus material in this talk:

More on
Standardized Metrics

Presentation Attack Detection - Testing

ISO/IEC 30107-3

- available in the ISO/IEC Portal
  https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en



ISO/IEC 30107-3:2017(en) Information technology — Biometric presentation attack detection — Part 3: Testing and reporting

Foreword
Introduction
1 Scope
2 Normative references
3 Terms and definitions
3.1 Attack elements
3.2 Metrics
4 Abbreviated terms
5 Conformance
6 Presentation attack detection o
7 Levels of evaluation of PAD me
7.1 Overview
7.2 General principles of evalu
7.3 PAD subsystem evaluation

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and ISO/IEC 30107-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1 Attack elements

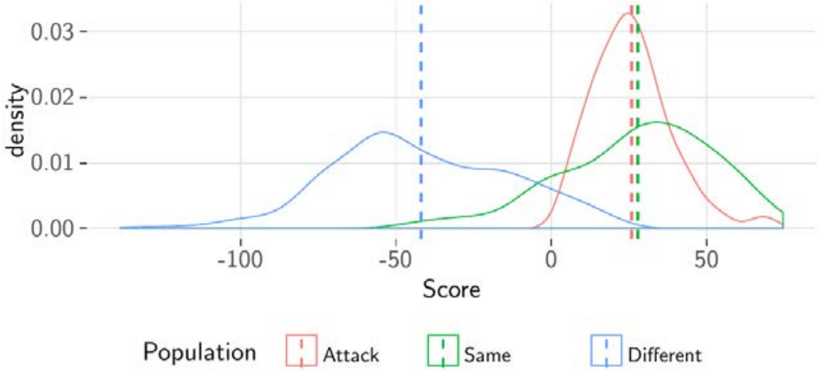
3.1.1
presentation attack
attack presentation
presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Presentation Attack Detection - Testing

Definition of full system vulnerability metric w.r.t attacks

- **Impostor attack presentation match rate (IAPMR)**
  <in a full-system evaluation of a verification system> the proportion of impostor attack presentation using the same PAI species in which the target reference is matched

Source: ISO/IEC 30107-3



- **Concealer attack presentation non-match rate (CAPNMR)**
  in a full-system evaluation of a verification system, the proportion of concealer attack presentation using the same PAI species in which the target reference is not matched.

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with security measure:

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations using the same PAI species incorrectly classified as bona fide presentations in a specific scenario

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}}\right)\sum_{i=1}^{N_{PAIS}} Res_i$$

Source: ISO/IEC 30107-3

- *N_{PAIS} is the number of attack presentations for the given PAI species*
- *Res_i takes value 1 if the i^{th} presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with security measure:

- **Attack presentation classification error rate (APCER)**
  the highest APCER (i.e. that of the most successful PAI species) should be reported as follows:

$$APCER_{AP} = \max_{PAIS \in \mathcal{A}_{AP}} (APCER_{PAIS})$$

Source: ISO/IEC 30107-3

where A_{AP} is a subset of PAI species with attack potential at or below AP.

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with convenience measure:

- **Bona fide presentation classification error rate (BPCER)**
  BPCER shall be calculated as follows:

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} RES_i}{N_{BF}}$$

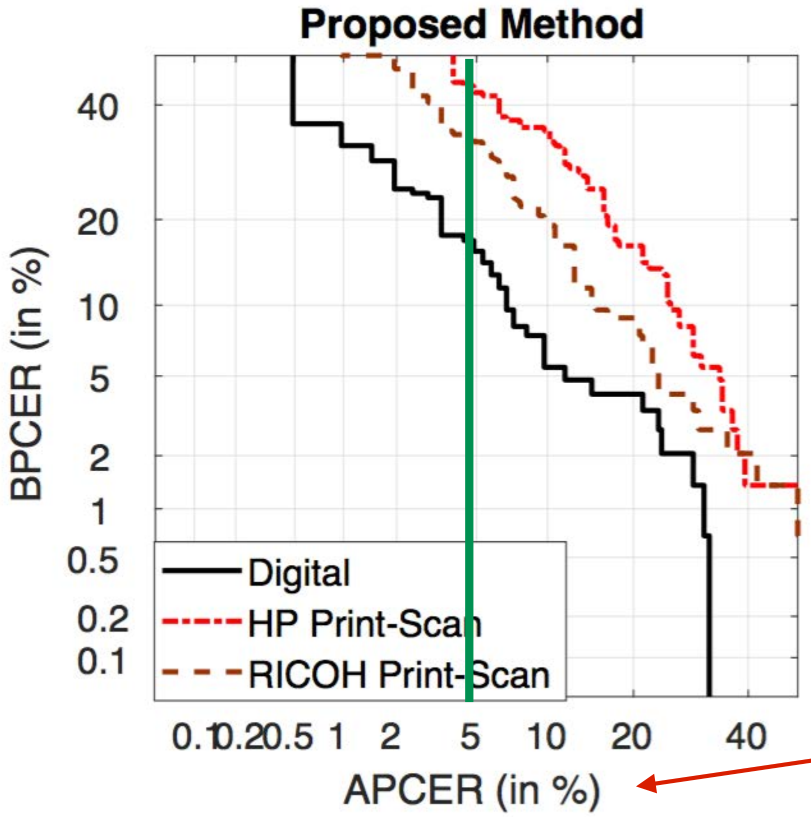
Source: ISO/IEC 30107-3

- *N_{BF} is the number of bona fide presentations*
- *Res_i takes value 1 if the i^{th} presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- DET curve analyzing operating points for various security measures and convenience measures
- Example:



convenience measure

security measure (strength of function)

Source: IR. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), Honolulu, Hawaii, July 21-26, (2017)

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing a specific security level:

  PAD mechanism may be reported in a single figure

- *BPCER at a fixed APCER:*

  One may report BPCER when APCER$_{AP}$is 5% as BPCER20

Source: ISO/IEC 30107-3

References

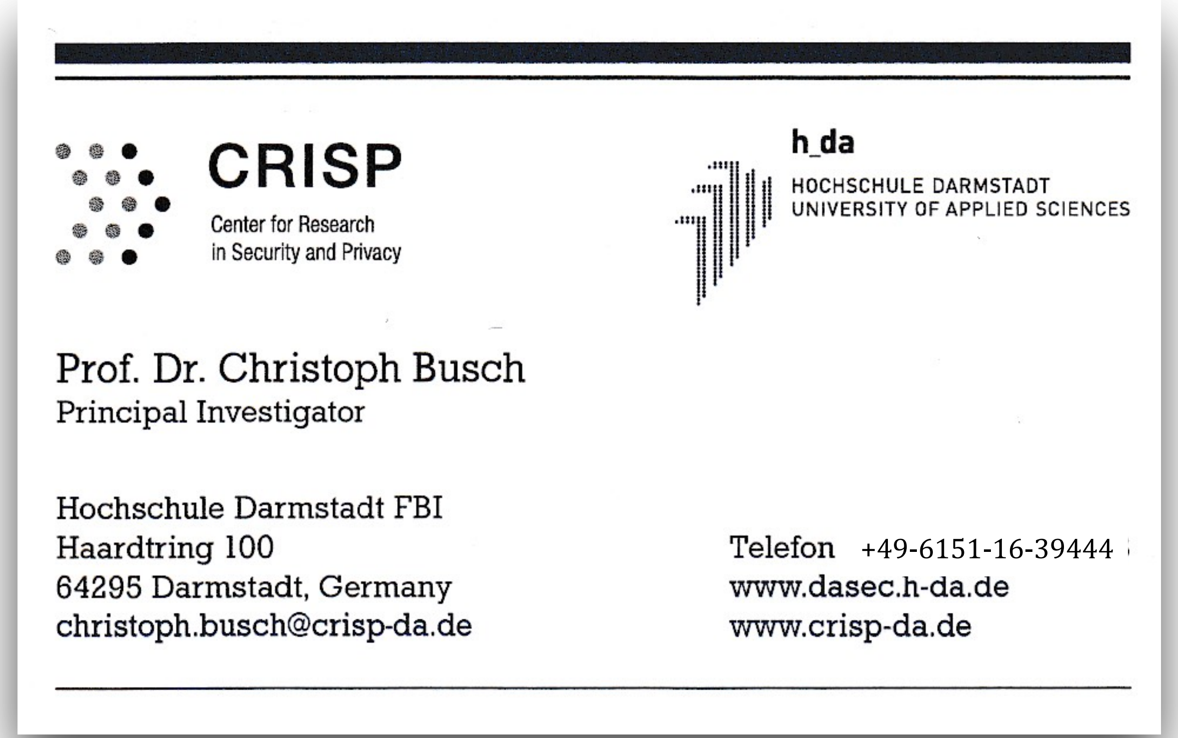
Standards

- ISO/IEC Standards
  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on
- ISO/IEC 30107-1, “Biometric presentation attack detection - Part 1: Framework”, 2016
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip
- ISO/IEC 30107-3, “Biometric presentation attack detection - Part 3: Framework”, 2017
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67381
- ISO/IEC 2nd WD 19989-1, “Criteria and methodology for security evaluation of biometric systems - Part 1: Framework”
  https://www.iso.org/standard/72402.html
- ISO/IEC 2nd WD 19989-3, “Criteria and methodology for security evaluation of biometric systems - Part 3: Presentation attack detection
  https://www.iso.org/standard/73721.html

Contact

If you have a student interested in an internship

- then please contact:



CRISP
Center for Research
in Security and Privacy

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

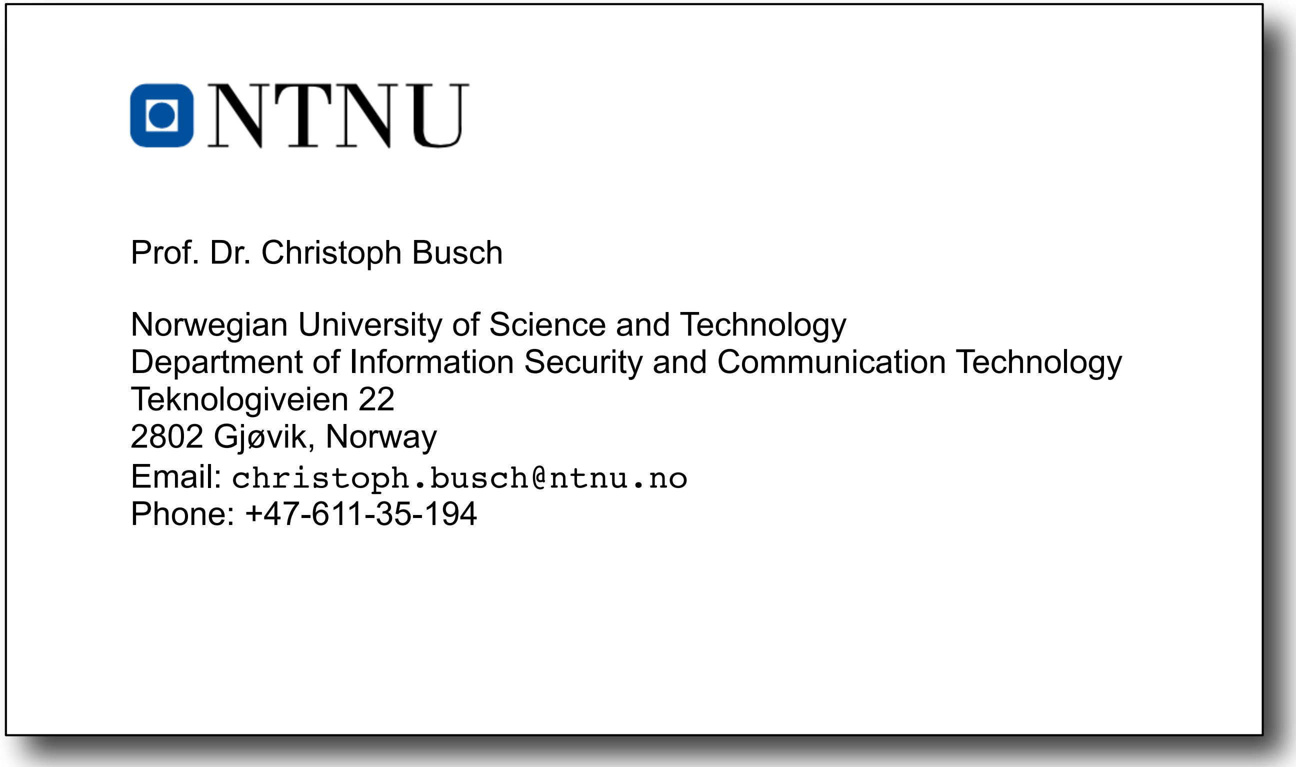
Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@crisp-da.de

Telefon +49-6151-16-39444
www.dasec.h-da.de
www.crisp-da.de

Contact

Contact:



NTNU

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: `christoph.busch@ntnu.no`
Phone: +47-611-35-194