Presentation Attack Detection for Smartphone Finger Image Recognition

Christoph Busch

Hochschule Darmstadt - CASED / Gjøvik University College
http://www.christoph-busch.de/

IBPC 2014 conference, Gaithersburg
April 1, 2014

Agenda

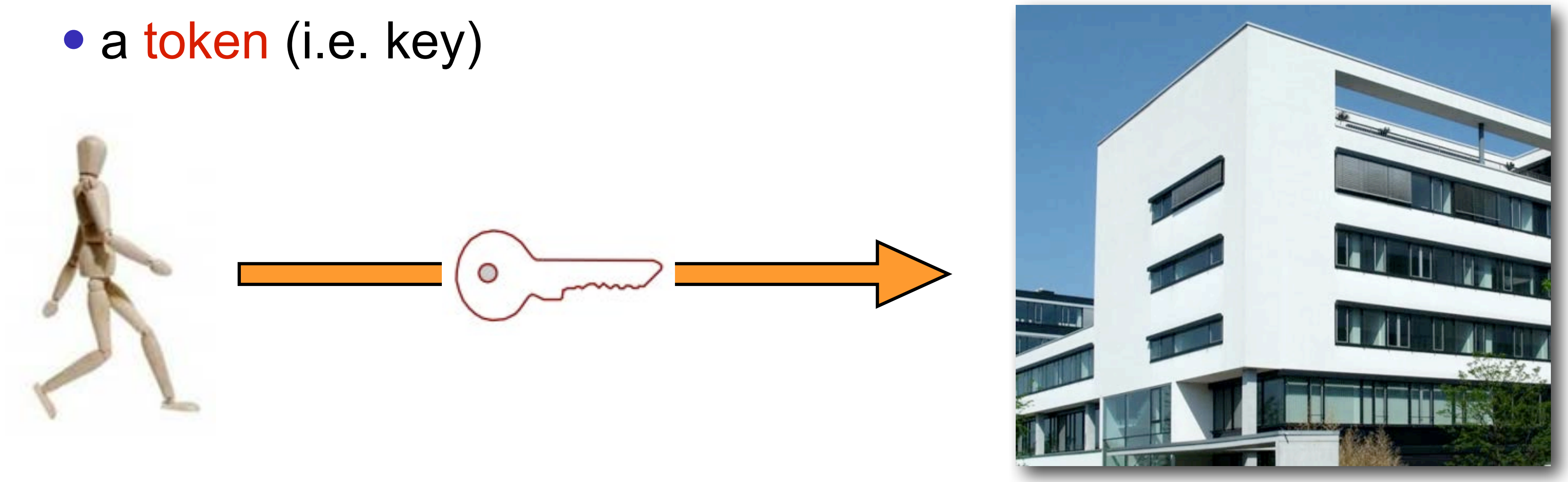
- Access Control
- Biometric authentication on Smartphones
- Presentation Attack Detection
- Are the metrics in 30107-3 applicable?

Access Control

Access Control

Traditionally we place between

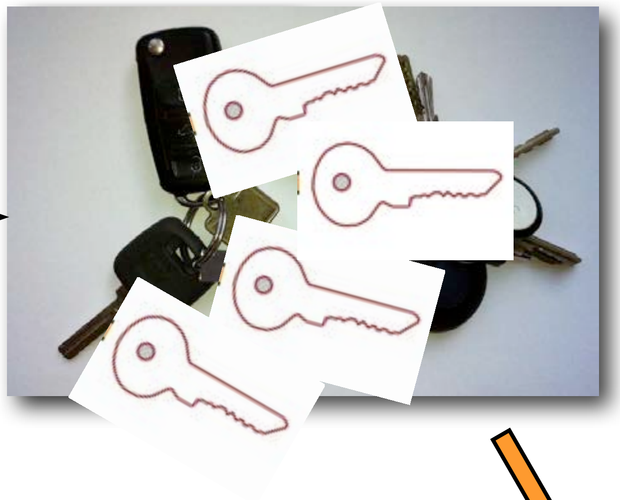
- individuals
- and objects
- a token (i.e. key)



Access Control

But in reality individuals

- do not have just one
- but many keys
- granting access to many doors



Smartphone Based Access Control

It won‘t take long

- that NFC enabled Smartphones will interact with most doors

The Smartphone is a major threat!

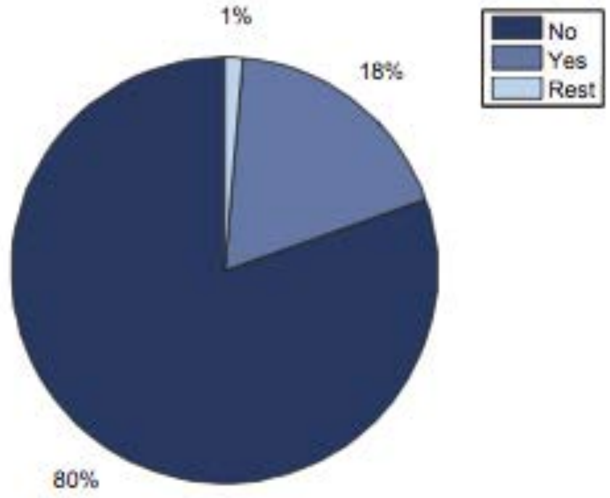
Source: Association of key manufacturers
(as of 2011-12-07)

Do we use Access Control
before we unlock our Smartphone?

End-User Survey

Data in mobile devices is often insufficiently protected

- No PIN-authentication required after stand-by phase
  - Survey-result with 962 users : only 18% use PIN code or visual pattern to unlock
- All data on the phone is freely available
  - Emails, addresses, appointments, photos
  - PINs etc.



Reason for this:

- PIN-authentication is too much effort (30%)
- People are self-responsible for their phones

[Ni12] C. Nickel: „Accelerometer-based Biometric Gait Recognition for Authentication on Smartphones“, PhD-thesis, TUD, 2012

Biometrics on Smartphones

Is the integration of fingerprint sensors in Smartphones a security gain?

- Chaos Computer Club: NO
- cb: YES - it motivated many users to activate access control in the first place

Image Source: Apple 2013

Image Source: Samsung 2013

Preliminary assessment:

- Apples introduction of iPhone 5s offers a convenience solution that satisfies the security requirements for authentication for low volume transaction.
- For the experienced attacker the sensor has shown weaknesses

Smartphone Access Contol

Foreground authentication (user interaction)

- Deliberate decision to capture (wilful act)
- Camera-Sensor
  - Fingerprint recognition
    - Apples iPhone 5S
    - Fingerphoto analysis
  - Face recognition
  - Iris recognition

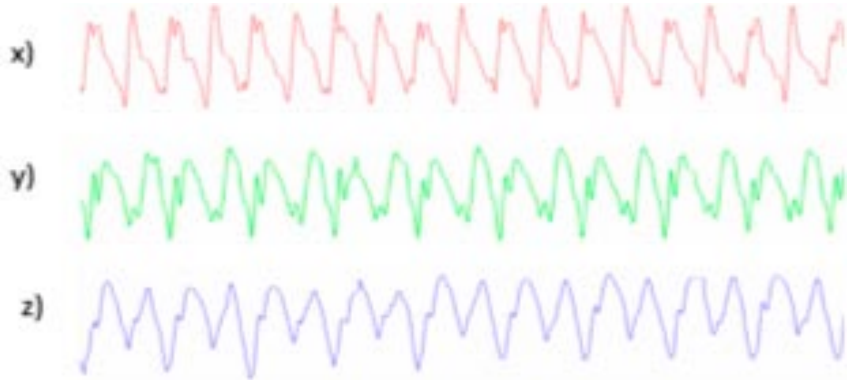
Background authentication (observation of the user)

- Microphone
  - Speaker recogntion
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive

Biometric Gait Recognition

Offer an unobtrusive authentication method

- Use accelerometers - already embedded in mobile devices to record the gait
  - Many phones contain accelerometers
  - No extra hardware is necessary
  - Acceleration measured in 3-directions

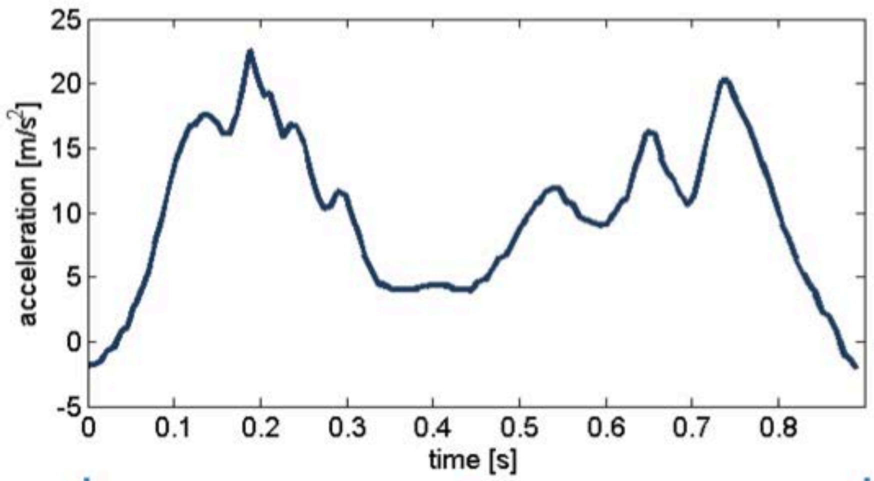


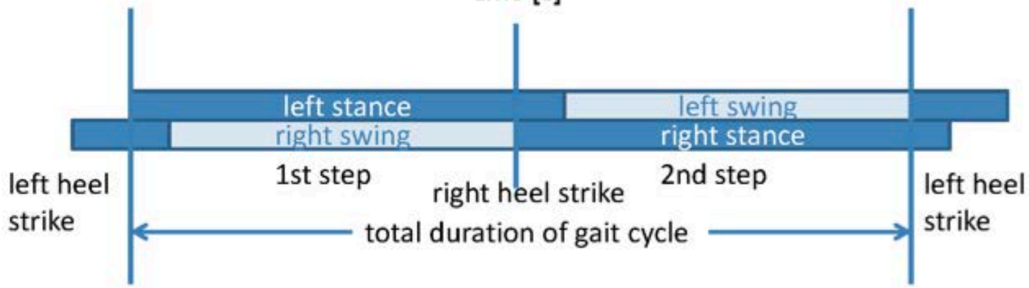
- First paper on this topic:
  [DNBB12] M. Derawi, C. Nickel, P. Bours, C. Busch: „Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition“, Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP 2010)
- EER 20% at that time

Biometric Gait Recognition

Data capture process

- periodical pattern in the recorded signal





Best result

- now at 6.1% EER

The following is prehistoric work

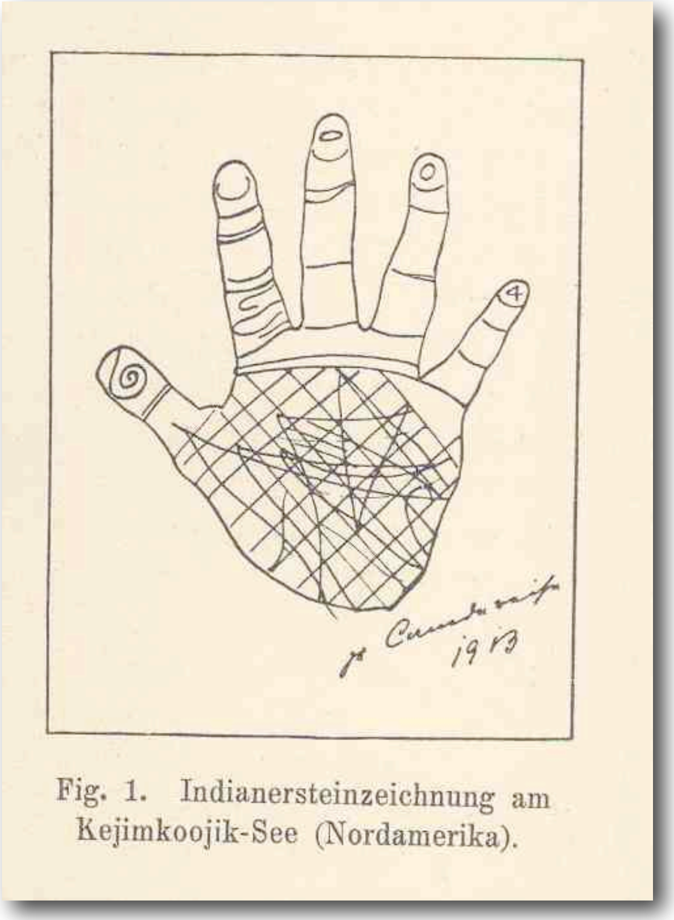


Image Source: Heindl 1927

The following is
prehistoric work (before the Apple iPhone5 arrived)

but as always:

we can learn from history

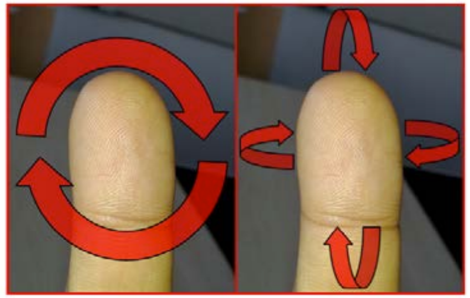
Smartphone Access Contol

Master Thesis Chris Stein 2012: Finger recognition

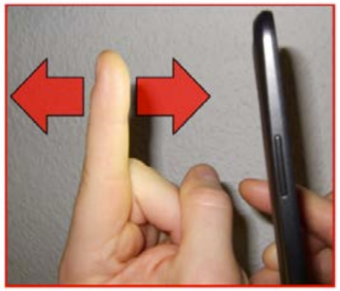
- Smartphone camera as sensor
- Authentication based on photo of the finger

Challenges

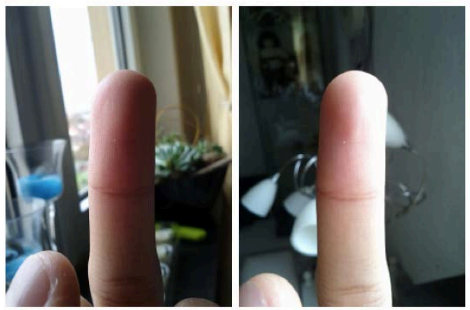
- Translation and rotation



- Distance finger to camera



- uncontrolled background and illumination



Smartphone Access Contol

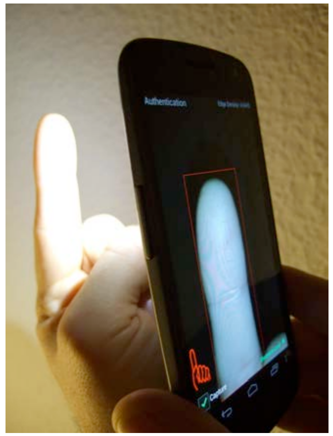
Capture process

- Camera operating in macro modus

Preview image of the camera with LED on (left) and LED off (right)

- LED permanent on

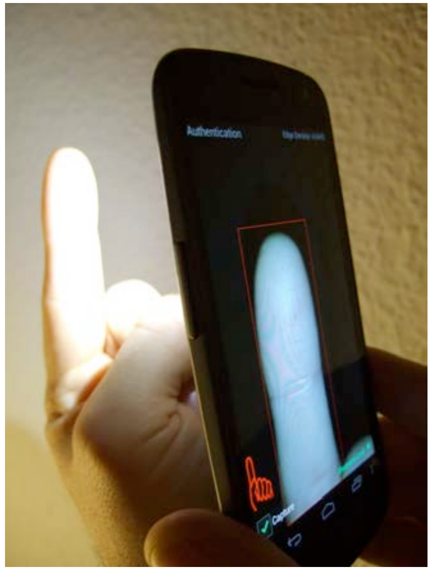
Finger illuminated



[SNB12] C. Stein, C. Nickel, C. Busch, „Fingerphoto Recognition with Smartphone Cameras“, Proceedings 11th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2012)

Smartphone Access Contol

Fingerprint recognition



- Preprocessing, minutiae extraction and comparison are performed on the phone
- Results of 18% EER are based on DigitalPersona FingerJetFX OSE (Open Source Edition) and home-made-minutiae comarator

- see video at: http://www.dasec.h-da.de/research/biometrics/mbassy/

Smart Phone Access Contol

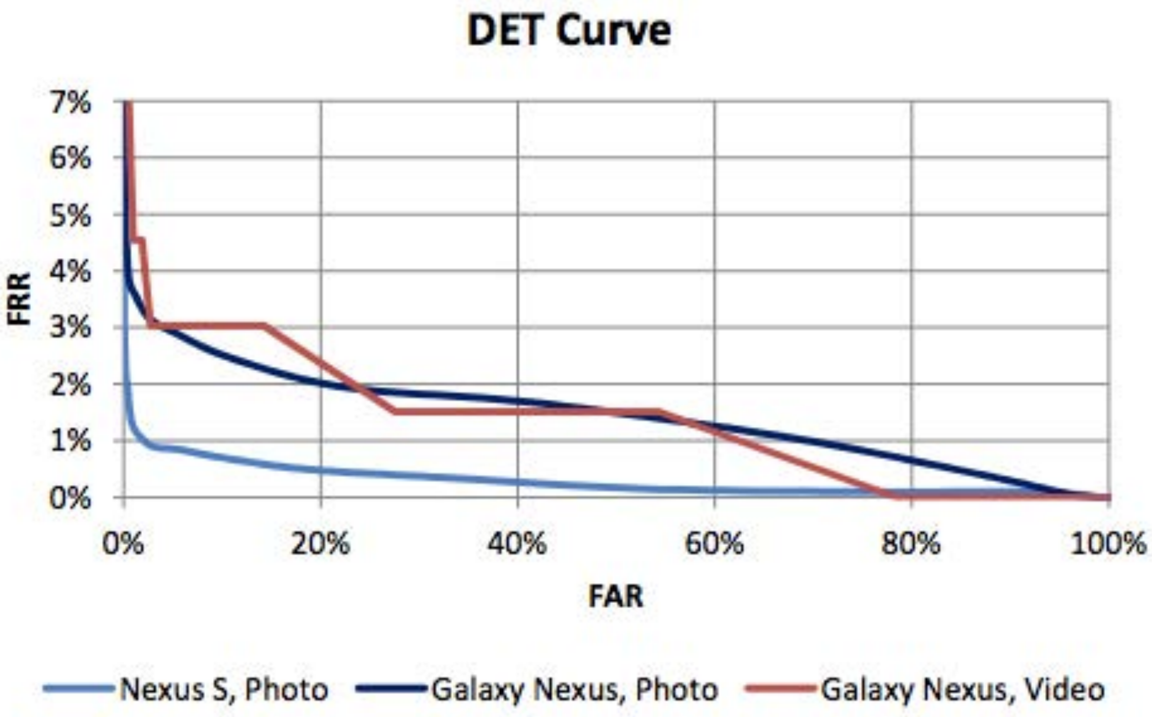
Finger recognition study - 2012/2013

- Objectives:
  - Replace home-made comparator (and the Digital Persona extractor) by COTS standard technology to increase performance
  - Investigate Presentation Attack Detection capabilities with reflection analysis and video recordings

Smart Phone Access Contol

Finger recognition study - 2012/2013

- Results: biometric performance at 1.2% EER



Capture Method and Device	EER from [SC-2012]	EER	FRR (FAR= 0.1%)
Photo, Nexus S	22.3%	1.2%	2.7%
Photo, Galaxy Nexus	19.1%	3.1%	6.7%
Video, Galaxy Nexus	-	3.0%	12.1%

[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)

Smart Phone Access Contol

Finger recognition study - 2012/2013

- Presentation Attacks
  - 1: replay from Smartphone display (simple)
  - 2: self generated print-outs (not critical to detect)
  - 3: Ralph Breithaupt‘s / BSI best artefacts (very challenging)

Replay attack

Simple artefacts

Challenging artefacts

Smart Phone Access Contol

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
  - Angle of the finger to the camera

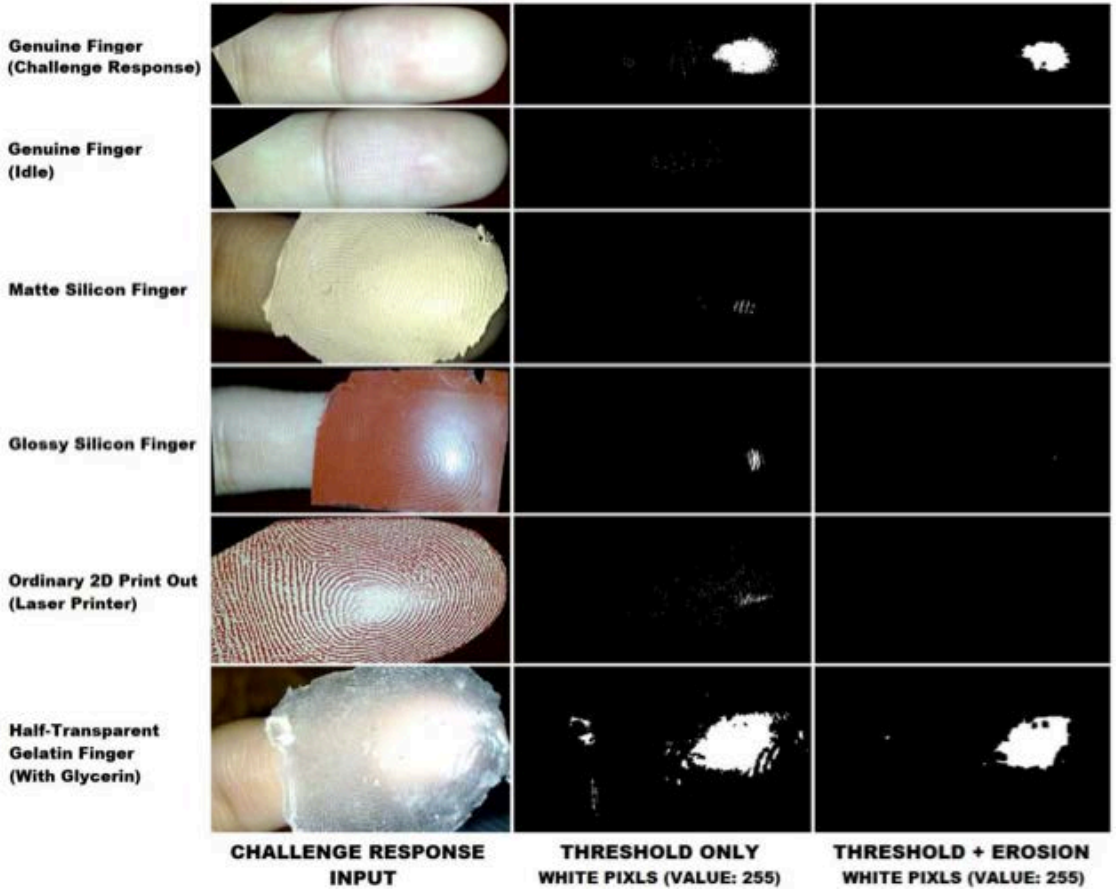
- Attack detection, as light reflection differs from artefacts to genuine fingers

- [SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

Smart Phone Access Contol

Finger recognition study - 2012/2013

- Results: Presentation Attack Detection



- Conclusion:
  better Presentation Attack Detection than capacitive sensors

Reporting about the PAD using ISO/IEC WD 30107

PAD-Standard

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

- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns.
- **artefact species**
  artefacts based on sources whose biometric characteristics differ but which are otherwise identical (e.g. based on a common medium and production method but with different biometric characteristic sources)
- **attack potential** *(this defenition is from CC terminology)*
  attribute of a biometric presentation attack expressing the effort expended in the preparation and execution of the attack in terms of elapsed time, expertise, knowledge about the capture device being attacked, window of opportunity and equipment, graded as “no rating“, “minimal”, “basic”, "enhanced-basic,” “moderate” or “high.

PAD-Standard

Metrics in ISO/IEC 30107 PAD - Part 3: Testing and reporting and classification of attacks

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations incorrectly classified as normal presentations in at the component level a specific scenario
- **Normal presentation classification error rate (NPCER)**
  proportion of normal presentations incorrectly classified as attack presentations at the component level in a specific scenario

Applying ISO/IEC 30107-3 Metrics

Do the metrics currently in ISO/IEC 30107 PAD - Part 3: serve to provide a meaningful report?

- [SBB12] - Publication:
  The reported number of attack presentations incorrectly classified as normal presentations was one out of five artefacts
- Thus the APCER to be reported is

$$APCER = \frac{1}{5} = 0.2$$

- but there were in fact 27 artefact species, that were used in the background but not reported as they are not challenging

$$APCER = \frac{1}{27} = 0.04$$

Refining ISO/IEC 30107-3 Metrics

Findings

- The size of the corpus with the artefact species is essential
- The APCER should be based on presentation attack instrument (PAI) and not only on artefacts, which includes both artefacts and lifeless biometric characteristics (i.e. stemming from dead bodies)
  - 30107-1: **PAI** - *biometric trait or object used in a presentation attack.*
- The CC-related attack potential should be included in the definition
  - 30107-1: **attack potential** - *attribute of a biometric presentation attack expressing the effort expended in the preparation and execution of the attack in terms of elapsed time, expertise, knowledge about the capture device being attacked, window of opportunity and equipment, graded as “no rating“, “minimal”, “basic”, "enhanced-basic,” “moderate” or “high.*
- The known success rate of an artefact species is relevant

Refining ISO/IEC 30107-3 Metrics

Suggested augmented metric for ISO/IEC 30107-3

- **Attack presentation classification error rate (APCER)** *proportion of attack presentations incorrectly classified as normal presentations at the component level a specific scenario* - taking the attack potential and the known artefact species success rate into account.
- **Attack potential (AP)** = {0.2 for “minimal”, 0.4 for “basic”, 0.6 for "enhanced-basic,” 0.8 for “moderate” . 1.0 for “high.}
- **Presentation attack instrument success rate (PAISR)** Proportion of evaluated capture devices that could be spoofed by the specific PAI (i.e. artefact).
  - would start with a value of 1 for a new discovered artefact species and could be reduced over time (as more sensors become robust)

Refining ISO/IEC 30107-3 Metrics

Suggested refined metrics for ISO/IEC 30107-3

- The APCER could thus be expressed as

$$APCER = \frac{\sum_{i=1}^{N_{AS}} RES_i * AP_i * PAISR_i)}{N_{AS}}$$

N_{AS}	number of presentation attack instruments (PAI) (i.e. artefact species) in the corpus
RES_i	result of attack with i^{th} PAI {0 for detected attack, 1 for successful attack}
AP_i	attack potential of the i^{th} PAI (close to zero, if artefact is easy to produce)
$PAISR_i$	presentation attack instrument success rate (close to zero, if all sensor can detect this artefact)

Open Question

To be clarified

- Should there be a fixed-size of the corpus,
  such that all labs use a minimum number of artefact species
- Can one expect that a testing lab has access to
  non-artefact PAI (from dead bodies)?
- What happens with the new sensor?
  The success rates starts with 1 and is decrease as
  robust sensor do appear
- How can evaluation labs have an equivalent set of PAI
  with all the same attack potential?

Conclusion

- Smartphones without biometric access control are a risk today and will be a critical factor tomorrow
  - once they will open doors via NFC
- The iPhone5 has changed this
- Biometric sensors are available in Smartphones at zero cost
  - even though they were built-in for other purposes
- Gait recognition shows reasonable biometric performance
- Currently defined metrics in ISO/IEC 30107-3 deserves refinement

Credits

Thanks to all that supported this work

This talk is based:

- on the work of my group members
  - Claudia Nickel (survey on Phone security) and
  - Chris Stein (Presentation Attack Detection)
- on Ralph Breithaupt - providing the artefacts / presesentation attack instruments used in this study
- Morpho (Safran Group) - funding the study
- Elaine Newton. Olaf Henniger and Michael Thieme serving as editor for ISO/IEC 30107
- all ISO/IEC JTC1 SC37 WG3 members providing the energy and patience to generate a good PAD-multipart standard

Contact

CASED

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

CASED
Mornewegstr. 32
64293 Darmstadt/Germany
christoph.busch@cased.de

Telefon +49 6151/16 9444
Fax
www.cased.de