Access Control with Fingerprint Recognition

Christoph Busch

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

Finse Winterschool
May 7, 2014

HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

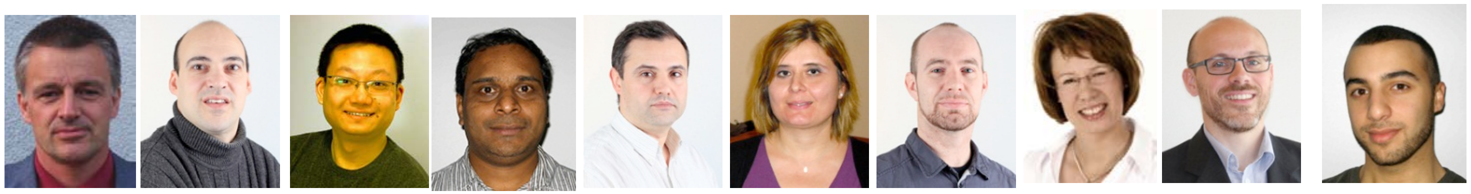
CASED

Norwegian Biometrics Laboratory (NBL)

A very international team

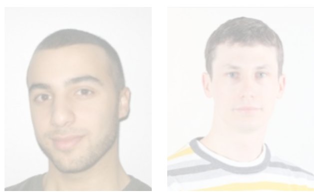
- 19 members from 12 countries

Faculty member



Ph.D. students

Graduated Ph.D.



Norwegian Biometrics Laboratory (NBL)

Biometric research

- covering various physiological and behavioral biometrics including 2D- and 3D-face recognition, iris recognition, fingerprint recognition, fingervein recognition, dental biometrics, ear recognition, signature recognition, gait recognition, keystroke recognition, gesture recognition and mouse dynamics.
- focus on privacy enhancing technologies such as biometric template protection

Projects

- IDEX
- Hitachi
- Fujistu
- Safran Morpho
- U.S. NIST

EU-Projects

- TURBINE
- BEST Network
- FIDELITY
- INGRESS
- PIDaaS
- ORIGINS

Norwegian Biometrics Laboratory (NBL)

NBL at Gjøvik University College

- The focus lab NBL is an integral part of NISlab

Intention

- increase the awareness of biometrics in Norway
  - Norwegian Biometric Forum (NBF) - two meetings per year
- link with European bodies such as
  - the European Association for Biometrics (EAB)
  - the COST Actions IC 1106 and IC 1206
  - the GI Special Interest Group on Biometrics (BIOSIG)
- continously hosting guest researchers
- contribute to the international standardization in the field.
- support international conferences such as
  - IEEE BIOSIG, IEEE ICB, IEEE BTAS, IJCB
  - NIST IBPC

Agenda

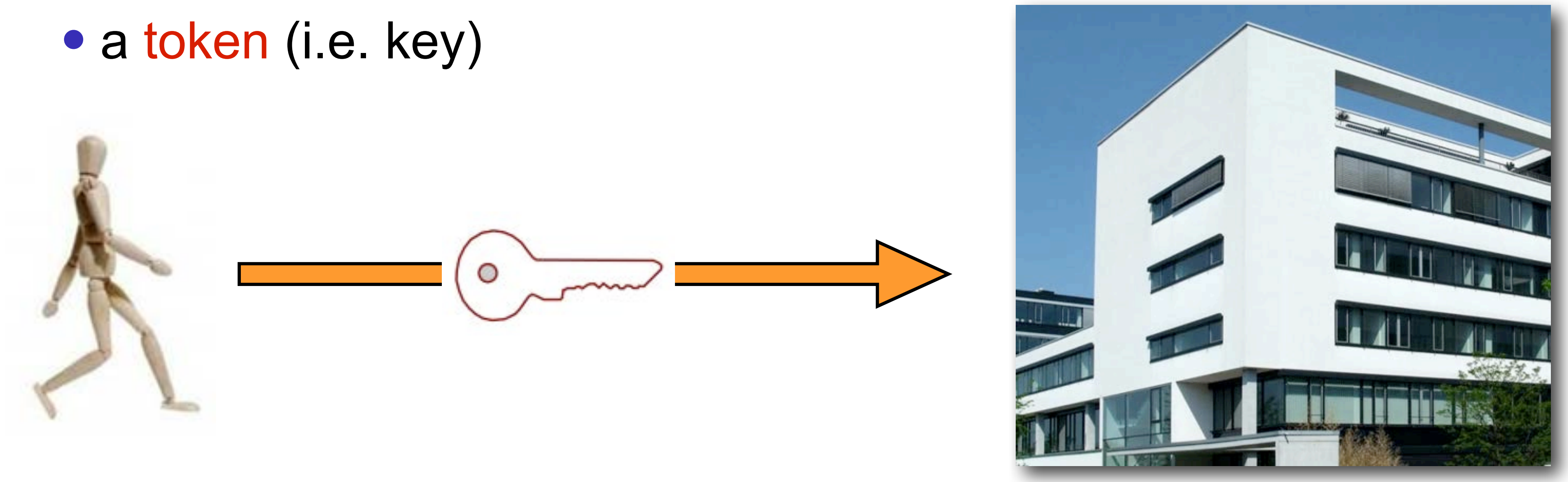
- Access Control - NFC
- Delegation of Authentication Factors
- Fingerprint Recognition on Smartphones
- Trust in Biometrics - Presentation Attack Detection

Access Control

Access Control

Traditionally we place between

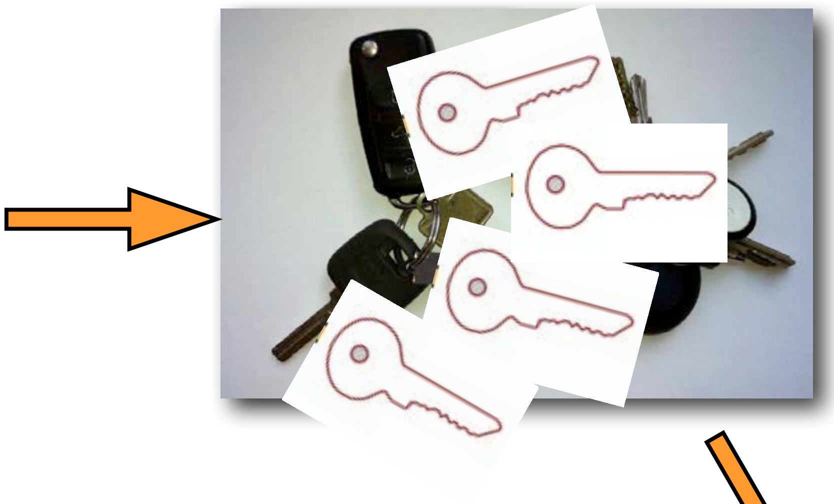
- individuals
- and objects
- a token (i.e. key)

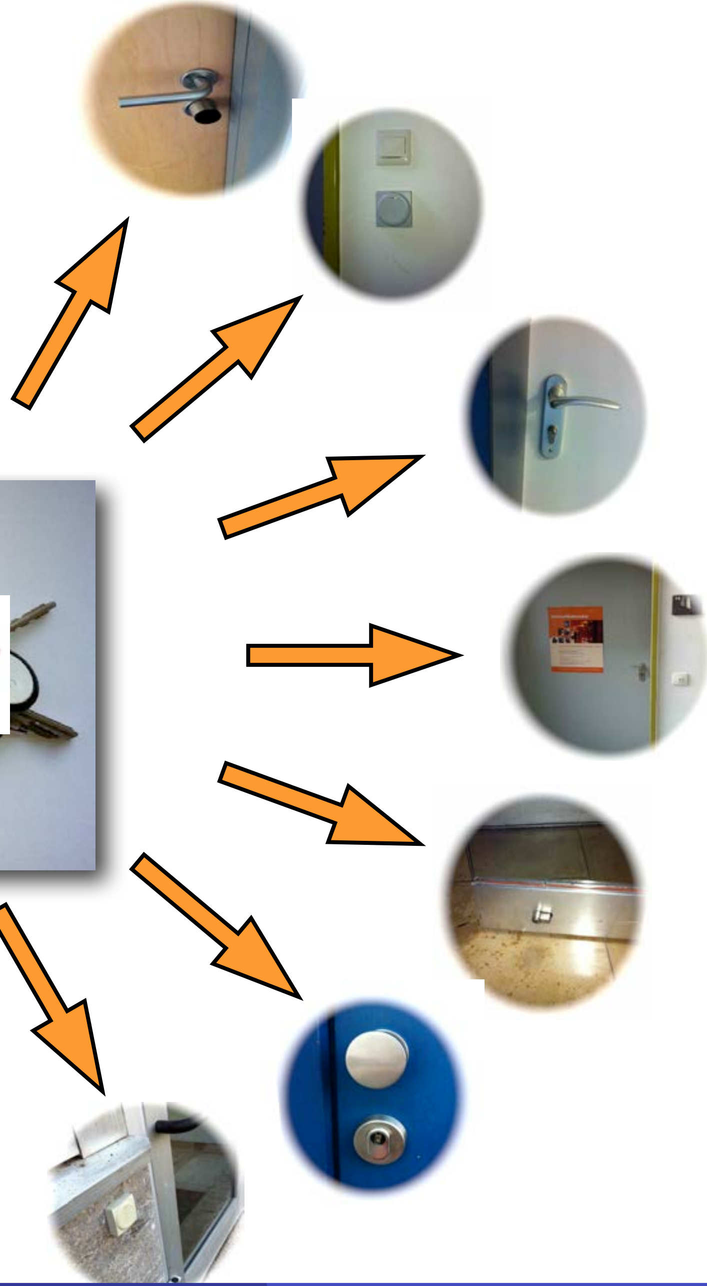


Access Control

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!

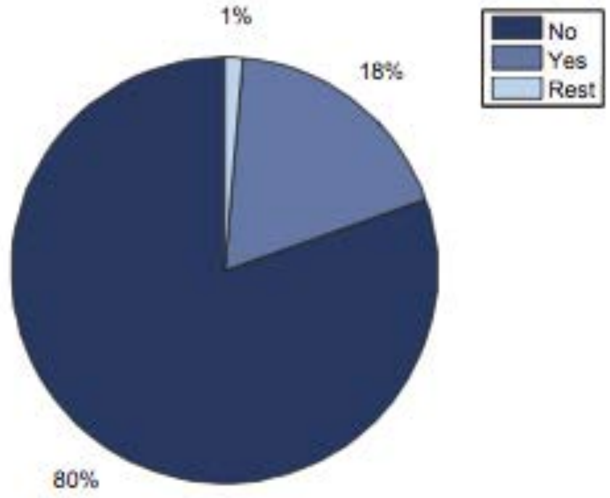
Source: Association of key manufacturers
(as of 2011-12-07)

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 / Samsung Galaxy 5
    - Fingerphoto analysis
  - Face recognition
  - Iris recognition

Background authentication (observation of the user)

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

The following is prehistoric work

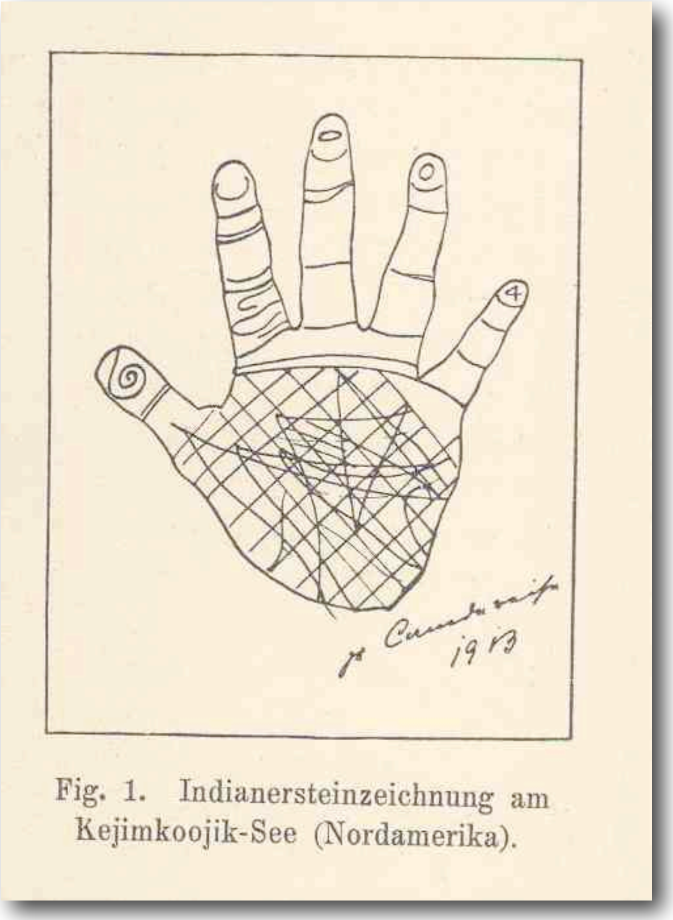


Image Source: Heindl 1927

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

but as always:

we can learn from history

Smartphone Access Contol

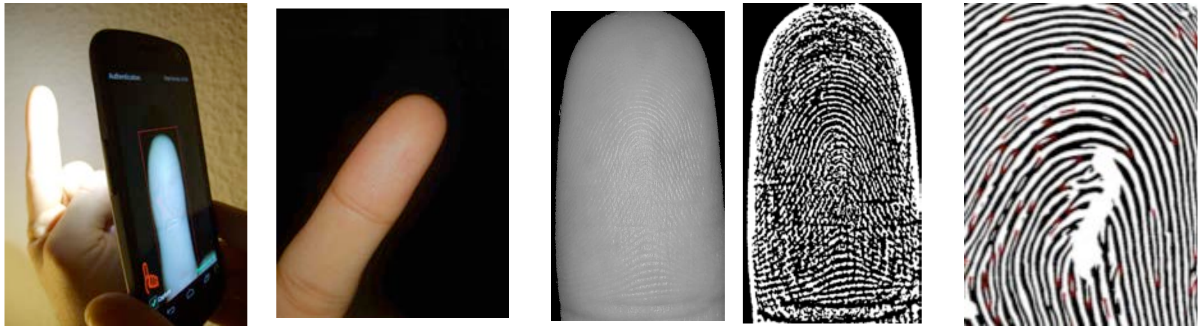
Capture process

- Camera operating in macro modus

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

- LED permanent on

Finger illuminated

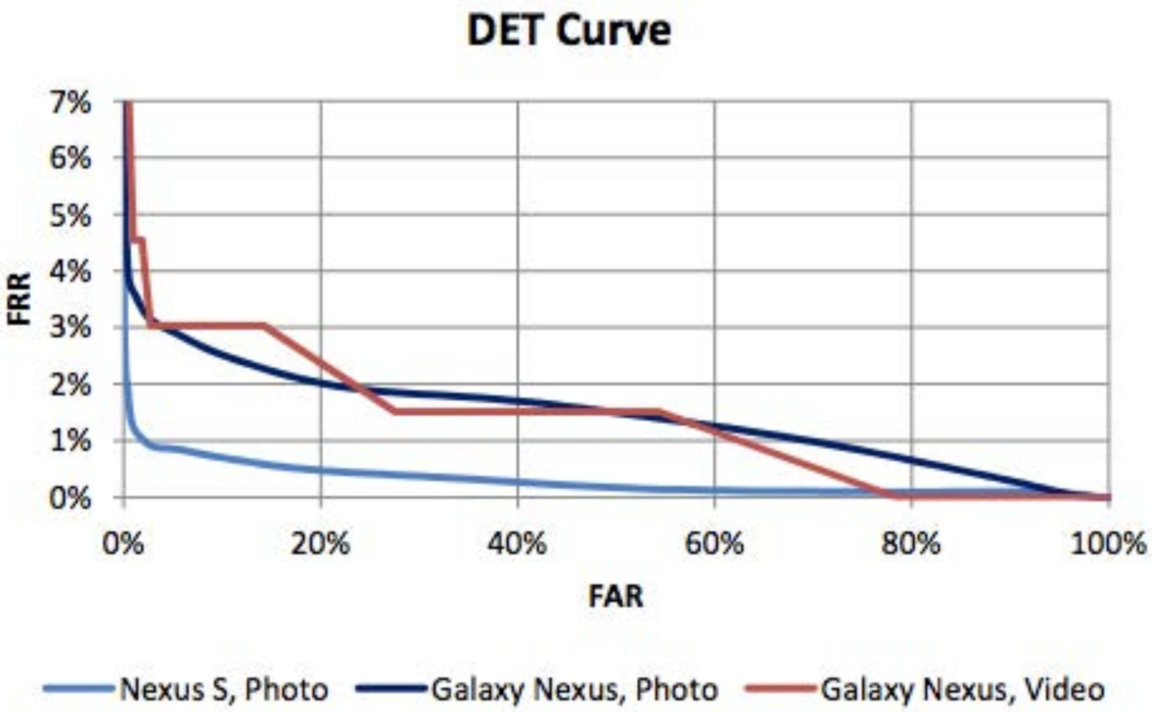


[SNB12] C. Stein, C. Nickel, C. Busch, „Fingerphoto Recognition with Smartphone Cameras“, Proceedings 11th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2012)

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

- Presentation Attacks

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

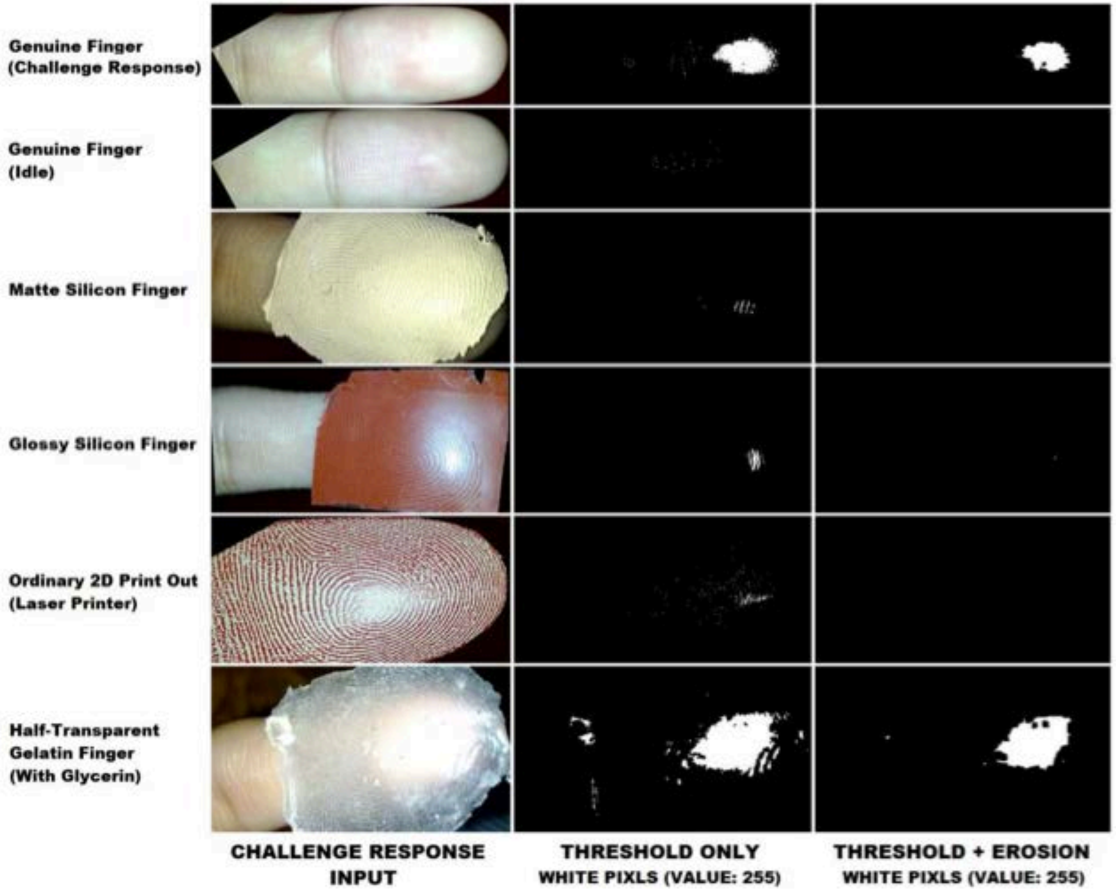
- Attack detection, as light reflection differs from artefacts to genuine fingers

- [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

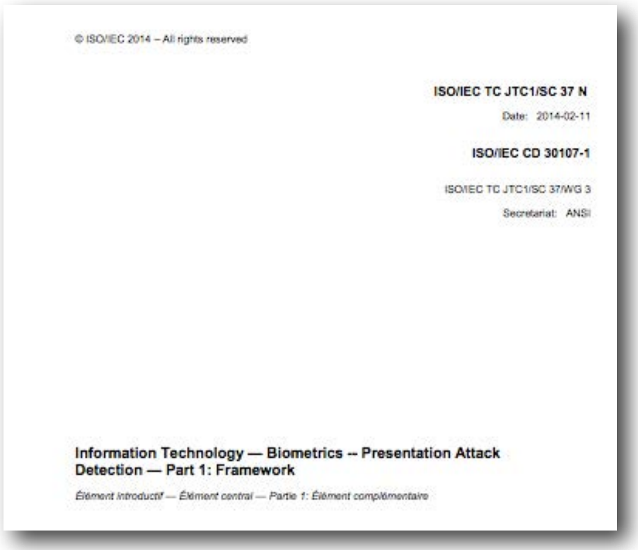
Finger recognition study - 2012/2013

- Results: Presentation Attack Detection (PAD)



- Conclusion:
  better Presentation Attack Detection than capacitive sensors

Reporting about the PAD using ISO/IEC 30107



© ISO/IEC 2014 – All rights reserved

ISO/IEC TC JTC1/SC 37 N

Date: 2014-02-11

ISO/IEC CD 30107-1

ISO/IEC TC JTC1/SC 37/WG 3

Secretariat: ANSI

Information Technology — Biometrics -- Presentation Attack Detection — Part 1: Framework

Élément introductif — Élément central — Partie 1: Élément complémentaire

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)

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

Applying ISO/IEC 30107-3 Metrics

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

- [SBB13] - Publication:
  The reported number of attack presentations incorrectly classified as normal presentations was one out of four artefacts
- Thus the APCER to be reported is

$$APCER = \frac{1}{4} = 0.25$$

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

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

Thoughts for improving

ISO/IEC WD 30107

Refining ISO/IEC 30107-3 Metrics

Trust in a biometric sensor relates to risk

Apply classical risk assessment ?

- *Risk = Impact of Risk event x Probability of Occurrence*
- we do not know the impact!

Modified assessment

- *Vulnerability = Attack Potential x Probability of Occurrence*

Refining ISO/IEC 30107-3 Metrics

Needed Change

- The size of the corpus with the artefact species is essential
- 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 and might be an approximation for the probability of occurrence

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 attack instrument 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)

Refining ISO/IEC 30107-3 Metrics

Suggested refined metrics for ISO/IEC 30107-3

- **Normal presentation classification error rate (NPCER)**: *proportion of normal presentations incorrectly classified as attack presentations at the component level in a specific scenario*
- The NPCER could thus be expressed as

$$NPCER = \frac{\sum_{i=1}^{N_{GPA}} RES_i}{N_{GPA}}$$

- N_{GPA} number of normal presentations from a genuine subject
- RES_i result of presentation detection component for the i^{th} attempt {0 for no detected attack, 1 for false alarm}

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 Apple iPhone5 and Samsung Galaxy S5 has changed this
- Biometric sensors are available in Smartphones at zero cost
  - even though they were built-in for other purposes
- Currently defined metrics in ISO/IEC 30107-3 deserves refinement

Visit us on Campus in 2015

Norwegian Biometrics Laboratory Workshop 2015

- Presentation Attack Detection in Biometrics: Solved and Unsolved Challenges
- Chair: Dr. Raghavendra Ramachandra
- Friday, Feburary 27, 2015
- please follow us at: http://nislab.no/biometrics_lab

ISO/IEC JTC1 SC37 Conference

- Working Group Meetings
- June 22 to 26, 2015 in GUC
- Standards Norge
- We are seeking Sponsors for the ISO - conference

Contact


HØGSKOLEN I GJØVIK
GJØVIK UNIVERSITY COLLEGE
FACULTY OF COMPUTER SCIENCE AND MEDIA TECHNOLOGY
Christoph Busch, Dr.-Ing.
Professor
P.O. Box 191, N-2802 Gjøvik, Norway
Phone: +47 61 13 51 94
Fax: +47 61 13 52 40
E-mail: christoph.busch@hig.no
www.hig.no | www.nislab.no