Presentation Attack Detection Standards

Christoph Busch
Hochschule Darmstadt - CRISP

TTT Working Group Biometrics
2017-09-20
Presentation Attack Detection

Outline

• International Standardisation on PAD
• ISO/IEC 30107
• ISO/IEC and FIDO
• ISO/IEC 19989
Gummy Finger Production in 2000!

Attack without support of an enroled individual

- Recording of an analog 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
Gummy Finger Production in 2000!

Reported in a publication by the German Federal Police

Established by JTC 1 in June 2002 to ensure

- a high-priority, focused and comprehensive approach worldwide for the rapid development of formal generic biometric standards

**Scope of SC37**

- “Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming *interfaces*; biometric data interchange *formats*; related biometric *profiles*; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects”

- [http://www.jtc1.org](http://www.jtc1.org)

Next meeting: January, 2018
Onion Layers

- **Layer 1: BDIR**
  - Digital representations of biometric characteristics

- **Layer 2: LDS**
  - CBEFF Meta-data

- **Layer 3+4:**
  - System properties
    - Security
    - Performance

- **Layer 5: BioAPI, BIP**
  - System Integration
First Generation Format Standards

G1

19794-1:2006

-2: 2005
-3: 2006
-4: 2005
-5: 2005
-6: 2005
-7: 2007
-8: 2006
-9: 2007
-10: 2007

All parts binary encoding

The 19794-Family: Biometric data interchange formats
ISO/IEC 30107 - Biometric presentation attack detection - Part 1: Framework
ISO/IEC 30107-1:2016 Presentation Attack Detection

- Attacks on Biometric Systems

ISO/IEC 30107

Source: ISO/IEC 30107-1

Presentation Attack Detection

ISO/IEC 30107 - **Scope**

- terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods;
- a common data format for conveying the type of approach used and the assessment of presentation attack in data formats;
- principles and methods for performance assessment of presentation attack detection algorithms or mechanisms; and
- a classification of known attacks types (in an informative annex).

**Outside** the scope are

- standardization of specific PAD detection methods;
- detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors;
- overall system-level security or vulnerability assessment.
Presentation Attack Detection - Framework

ISO/IEC 30107-1

• freely available in the ISO/IEC-Portal
Presentation Attack Detection - Framework


• presentation attack
description 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
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)
  
  Presentation attack instrument

- (Adjectives describing categories)
  
  Artificial
  
  Human
  
  Other Natural

- (Qualifying adjectives)
  
  Complete
  
  Partial
  
  Lifeless
  
  Altered
  
  Non-Conformant
  
  Coerced
  
  Conformant

Source: ISO/IEC 30107-1
## Presentation Attack Detection - Framework

ISO/IEC 30107-1: Examples of Artificial and Human Presentation Attack Instruments

<table>
<thead>
<tr>
<th>Artificial</th>
<th>Complete</th>
<th>gummy finger, video of face</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Partial</td>
<td>glue on finger, sunglasses, artificial/patterned contact lens</td>
</tr>
<tr>
<td>Human</td>
<td>Lifeless</td>
<td>cadaver part, severed finger/hand</td>
</tr>
<tr>
<td></td>
<td>Altered</td>
<td>mutilation, surgical switching of fingerprints between hands and/or toes</td>
</tr>
<tr>
<td></td>
<td>Non-Conformant</td>
<td>facial expression/extreme, tip or side of finger</td>
</tr>
<tr>
<td></td>
<td>Coerced(^1)</td>
<td>unconscious, under duress</td>
</tr>
<tr>
<td></td>
<td>Conformant</td>
<td>zero effort impostor attempt</td>
</tr>
</tbody>
</table>

Source: ISO/IEC 30107-1
Biometric framework with PAD

Source: ISO/IEC 30107-1
ISO/IEC 30107 - Biometric presentation attack detection - Part 2: Data formats
Presentation Attack Detection - Data Formats

ISO/IEC FDIS 30107-2

- will soon be available in the ISO/IEC Portal

https://www.iso.org/standard/67380.html
ISO/IEC FDIS 30107-2

- Abstract syntax of the PAD information in ASN.1

```asn1
PADDataFormatModule
{iso standard 30107 data-formats(2) modules(0) pad-data(0) version(0)}
DEFINITIONS
IMPLICIT TAGS
BEGIN
PADData ::= [APPLICATION 98] SET {
pADDecision [0] PADDecision OPTIONAL,
pADScoreBlockSequence [1] PADScoreBlockSequence OPTIONAL,
pADExtendedDataSequence [2] PADExtendedDataSequence OPTIONAL,
captureContext [3] CaptureContext OPTIONAL,
supervisionLevel [4] SupervisionLevel OPTIONAL,
riskLevel [5] RiskLevel OPTIONAL,
criteriaCategory [6] CriteriaCategory OPTIONAL,
pADParameter [7] PADParameter OPTIONAL,
pADChallenge [8] PADChallenge OPTIONAL,
pADDataCaptureDateTime [9] GeneralizedTime OPTIONAL,
captureDevice [10] CaptureDevice OPTIONAL,
...}
```

Source: ISO/IEC 30107-2
ISO/IEC FDIS 30107-2

- PAD score

5.2.4 PAD score

Presence: Optional

Abstract values: Integers 0 to 100 and FAILURE_TO_COMPUTE

Contents: If present, this data element shall indicate the PAD result as a score between 0 and 100. Bona-fide presentations shall tend to generate lower scores. Presentation attacks shall tend to generate higher scores. The abstract value FAILURE_TO_COMPUTE shall indicate that the computation of the PAD score has failed.

If the PAD score value is FAILURE_TO_COMPUTE, then, if present, the PAD decision value shall also be FAILURE_TO_COMPUTE.

Source: ISO/IEC 30107-2
ISO/IEC 30107 - Biometric presentation attack detection - Part 3: Testing and reporting
ISO/IEC 30107-3

- available in the ISO/IEC Portal

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:

- 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
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 metrics testing the PAD subsystem response:

  - **Attack presentation non-response rate (APNRR)**
    
    proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem

  - **Bona fide presentation non-response rate (BPNRR)**
    
    proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem

    "NOTE An example of a non-response is a data capture subsystem “time out” if a presentation is not registered within a certain amount of time.”

Source: ISO/IEC 30107-3
Definition of detection capabilities metrics

- Testing the PAD subsystem with security measure and convenience 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

- **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
Definition of PAD metrics elements

- **PAI species**
  class of presentation attack instruments created using a common production method and based on different biometric characteristic

- **Attack potential**
  measure of the capability to attack a TOE given the attacker’s knowledge, proficiency, resources and motivation

- **target of evaluation (TOE)**
  within Common Criteria, the IT product that is the subject of the evaluation

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

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

• \(N_{PAIS}\) 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

Source: ISO/IEC 30107-3
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:

\[
APCER_{AP} = \max_{PAIS \in A_{AP}} (APCER_{PAIS})
\]

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

Source: ISO/IEC 30107-3
Definition of detection capabilities metrics

• Testing the PAD subsystem with convenience measure:

• **Bona fide presentation classification error rate (BPCER)**

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

  - \( N_{BF} \) 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

Source: ISO/IEC 30107-3
Presentation Attack Detection - Testing

Definition of detection capabilities metrics

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

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 $BPCER_{AP} is 5\%$ as $BPCER_{20}$

Source: ISO/IEC 30107-3
ISO/IEC 30107 - Biometric presentation attack detection - Part 4: Testing and reporting
Presentation Attack Detection - Mobile

ISO/IEC WD 30107-4

- Profile for testing and reporting on mobile devices
- Working Draft available in the ISO/IEC livelink
  http://isotc.iso.org/livelink/livelink?func=ll&objId=19121718&objAction=Open&viewType=1
Presentation Attack Detection - Mobile

ISO/IEC WD 30107-4

- **Scope:**
  - This standard provides guidance for testing biometric presentation attack detection mechanisms on mobile devices with local biometric authentication.
  - The standard considers: specification of a minimum PAI species and specification of a minimum number of subjects

- **Example:**

<table>
<thead>
<tr>
<th>30107-3 Clause</th>
<th>Requirement</th>
<th>Approach in PAD Tests for Mobile Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.1</td>
<td>Evaluations of PAD mechanisms shall report the following:</td>
<td>Evaluator provides the basis and narrative. Notional values provided in the rows below:</td>
</tr>
<tr>
<td></td>
<td>— number of presentation attack instruments used in the evaluation</td>
<td>Evaluator documents this figure based on number of IUTs, subjects, species, and series</td>
</tr>
<tr>
<td></td>
<td>— number of PAI species used in the evaluation</td>
<td>Minimum of 3</td>
</tr>
<tr>
<td></td>
<td>— number of PAI series used in the evaluation</td>
<td>Minimum of 3 per species</td>
</tr>
<tr>
<td></td>
<td>— number of test subjects involved in the testing, including those unable to utilize artefacts or present non-conformant characteristics</td>
<td>Minimum of 50</td>
</tr>
<tr>
<td></td>
<td>— number of artefacts created per test subject for each material tested</td>
<td>Minimum of 3</td>
</tr>
<tr>
<td></td>
<td>— number of sources from which artefact characteristics were derived</td>
<td>Evaluator provides basis and narrative</td>
</tr>
</tbody>
</table>
Presentation Attack Detection

ISO/IEC 19989
Common Criteria

Common („joint“) criteria

- for evaluation and assessment of IT-security technology
Presentation Attack Detection - Security

ISO/IEC 19989 - Criteria and methodology for security evaluation of biometric systems

- Part 1: Framework
  https://www.iso.org/standard/72402.html
- Part 2: Biometric recognition performance
  https://www.iso.org/standard/72403.html
- Part 3: Presentation attack detection
  https://www.iso.org/standard/73721.html

- Scope:
  For security evaluation of biometric recognition performance and presentation attack detection for biometric systems, this International Standard specifies:
  
  - Extended security functional components to SFR Classes in ISO/IEC 15408-2,
ISO/IEC 2nd WD 19989-1

• Calculating attack potential (in Annex A.3.3)
  ‣ Overall rating for elapse time
  ‣ Overall rating for expertise
  ‣ Overall rating for knowledge of TOE
  ‣ Overall rating for window of opportunity
  ‣ Overall rating for equipment

• Example

<table>
<thead>
<tr>
<th>Factor</th>
<th>Identification</th>
<th>Exploitation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed Time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;= one day</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>&lt;= one week</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>&lt;= two weeks</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>&lt;= one month</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>&gt; one month</td>
<td>8</td>
<td>16</td>
</tr>
<tr>
<td>Expertise</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layman</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Proficient</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Expert</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>Multiple experts</td>
<td>8</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

Source: ISO/IEC 2nd WD 19989-1
ISO/IEC 2nd WD 19989-1

- Example calculating attack potential

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>0</td>
<td>Not applicable</td>
<td>Standard 0</td>
</tr>
<tr>
<td>Restricted</td>
<td>2</td>
<td>Not applicable</td>
<td>Specialised 2</td>
</tr>
<tr>
<td>Sensitive</td>
<td>4</td>
<td>Not applicable</td>
<td>Bespoke 4</td>
</tr>
<tr>
<td>Critical</td>
<td>8</td>
<td>Not applicable</td>
<td></td>
</tr>
<tr>
<td>Window of Opportunity</td>
<td>(Access to TOE)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Easy</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Difficult</td>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Immediate</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Window of Opportunity</td>
<td>(Access to Biometric Characteristics)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Easy</td>
<td>Not applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Not applicable</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Difficult</td>
<td>Not applicable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: ISO/IEC 2nd WD 19989-1
ISO/IEC 2nd WD 19989-3

- Relation among error rates, presentation type, and attack classification for PAD subsystem

<table>
<thead>
<tr>
<th>Presentation Type (Input)</th>
<th>PAD Result (Output)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Attack</td>
</tr>
<tr>
<td>Attack</td>
<td>---</td>
</tr>
<tr>
<td>Bona Fide</td>
<td>BPCER</td>
</tr>
</tbody>
</table>

Source: ISO/IEC 2nd WD 19989-3
References

Standards

- ISO/IEC Standards
  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on


  https://www.iso.org/standard/72402.html

  https://www.iso.org/standard/73721.html

Contact

Prof. Dr. Christoph Busch
Principal Investigator

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

Telefon +49-6151-16-30090;
www.dasec.h-da.de
www.crisp-da.de