Status of international standard ISO/IEC 30107

Christoph Busch

- ISO/IEC JTC1/SC37 WG3 Convenor -

EAB European Biometric Symposium

Martigny
2016-01-19
Biometric Standardisation

International Organization for Standardisation

Joint Technical Committee One

International Electrotechnical Commission

International Civil Aviation Organization

TC 68
Banking, Securities
Financial services

SC 17
Cards & Personal Identification

SC 27
IT Security Techniques

SC 37
Biometrics

SC37 to TC68

SC 37 Formal Liaisons
ISO/IEC SC37 Biometrics

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

Next meeting: July, 2016
First Generation Format Standards

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
Liveness Detection

ISO/IEC 30107-1:2016 Presentation Attack Detection

• Attacks on Biometric Systems

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


- **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

- **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 - 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 Attack Detection

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
Presentation Attack Detection

Biometric framework with PAD

Source: ISO/IEC 30107-1
Presentation Attack Detection

ISO/IEC IS 30107-1 Standard

- **now available in the ISO-Portal**
- SC37 has initiated to make this standard freely available
Presentation Attack Detection - Testing


- Security Evaluation
  - for evaluations using the Common Criteria Framework
  - Protection Profile (PP) (e.g. from German BSI)
  - Security Target (ST)
  - Evaluation Assurance Level (EAL)
  - Assessment of the attack potential
    - "if there is at least one artefact that can reproducibly successfully attack the PAD-component - then the PAD failed the test"

- Other approaches
  - for evaluations in academic and technology development
  - tolerating the fact that statistical distribution for small tests is unknown and for sure not normal
    - "a score based metric can tell us, if the method improved"
Definition of PAD metrics in ISO/IEC 30107-3

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

- **Bona Fide presentation classification error rate (BPCER)**
  proportion of *Bona Fide presentations* incorrectly classified as *attack presentations* at the component level in a specific scenario
Presentation Attack Detection

30107 parts

• Part 1 - Framework
  ▸ Elaine Newton
  ▸ status: IS - published

• Part 2 - Data formats
  ▸ Olaf Henniger
  ▸ status: 3rd CD

• Part 3 - Testing and Reporting
  ▸ Michael Thieme
  ▸ status: 2nd CD
What about rubber fingers?

- Protection methods in FIDO
  1. Attacker needs access to the Authenticator and have swipe rubber finger on it. This makes it a non-scalable attack.
  2. Authenticators might implement presentation attack detection methods.

Remember:

Creating hundreds of millions of rubber fingers + stealing the related authenticators is expensive. Stealing hundreds of millions of passwords from a server is not.

Source: R. Lindemann (NokNok) - 2015
References

Web

• Convenors website with latest news and slides
  http://www.christoph-busch.de/standards-sc37wg3.html

• ISO/IEC JTC SC37
  http://isotc.iso.org/livelink/livelink?
  func=ll&objId=2262372&objAction=browse&sort=name

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

Prof. Dr. Christoph Busch
Department IMA

Fraunhoferstrasse 5
64283 Darmstadt, Germany
Phone: +49-6151-155-536
christoph.busch@igd.fraunhofer.de
http://www.christoph-busch.de