Overview of the ISO/IEC 30107 Project
Anti-Spoofing and Liveness Detection Techniques

Elaine Newton, PhD
NIST
elaine.newton@nist.gov
1-301-975-2532
Remote Authentication in the US Federal Government

• OMB Memo 04-04
  – Describes 4 assurance levels, with qualitative degrees of confidence in the asserted identity’s validity:
    Level 1: Little or no confidence  Level 2: Some confidence
    Level 3: High confidence       Level 4: Very high confidence

• NIST Special Publication 800-63-1
  – Technical requirements for remote authentication over an open network in response to OMB 04-04

• Biometrics not included in authentication protocols in this guidance

• Adopted by other countries and standards orgs.
Biometric Security Issues

Figure by Nalini Ratha, IBM
Authentication Use Case Comparison

For law enforcement, immigration, etc.

• Enrollment and subsequent recognition attempts
  – highly controlled
  – Supervised / Attended

• Successful recognition
  – Answers the question, “Has this person been previously encountered?”
  – Is a unique pattern

For online transactions, e.g. banking, health, etc.

• Enrollment
  – Less controlled
  – Probably not in person

• Subsequent recognition attempts
  – Unattended

• Successful recognition
  – Answers the question, “How confident am I that this is the actual claimant?”
  – Is a tamper-proof rendering of a distinctive pattern
High Confidence in factors available to consumers for authentication (and access) over open networks.

QPL, Validation, or Certification Program

Data / Data Formats (for Metrics)

Countermeasures

Measurement/ Evaluation

Threats/ Attacks
Types of Biometric “Spoofing”*

From the 3rd Working Draft of IS Project 30107
## Types of Detection

<table>
<thead>
<tr>
<th>Through a biometric system</th>
<th>Artefact Detection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Liveness Detection</td>
</tr>
<tr>
<td></td>
<td>Challenge-Response</td>
</tr>
<tr>
<td></td>
<td>Alteration Detection</td>
</tr>
<tr>
<td></td>
<td>Non-conformance Detection</td>
</tr>
<tr>
<td></td>
<td>Coercion Detection</td>
</tr>
<tr>
<td></td>
<td>Obscuration Detection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Through system security policies</th>
<th>Failed attempt detection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Geographic</td>
</tr>
<tr>
<td></td>
<td>Temporal</td>
</tr>
</tbody>
</table>

From the 3rd Working Draft of IS Project 30107
Examples of Data Fields for Detecting Suspicious Presentations*

• Is there a local check for SPD (yes/no)?
• The local SPD decision (pass/fail)
• A score between 0 and 100 provided by the spoof detection mechanism, with lower scores being indicative of spoofed samples
• technique specific data and their units;
• level of supervision / surveillance during capture (qualitative categories)

(In addition to: vendor ID, algorithm ID, and sensor ID.)

*From the 3rd Working Draft of IS Project 30107
How to Participate in the Development of 30107

• In the US, interested parties participate through INCITS M1
  – http://standards.incits.org/a/public/group/m1

• In other countries, interested parties participate in their country’s Technical Advisory Group (TAG) to ISO/IEC JTC1 SC37
If you liked this…

Join us Friday for Satellite Workshop II: Artefact, Liveness, & Suspicious Presentation Detection

Where we will discuss testing, error rates, and terms and concepts.

• Location: Portrait Room, NIST
• Time: 09:00 - 12:00, Friday March 9, 2012
If you hated this…

Join us Friday for Satellite Workshop II: Artefact, Liveness, & Suspicious Presentation Detection

Where we will discuss testing, error rates, and terms and concepts.

• Location: Portrait Room, NIST
• Time: 09:00 - 12:00, Friday March 9, 2012
Thank you

Questions?

Elaine Newton
elaine.newton@nist.gov
1-301-975-2532
### Examples of Artificial and Human Subversive Presentation Characteristic Types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Artificial</td>
<td></td>
</tr>
<tr>
<td>Complete</td>
<td>gummy finger, latex finger, photo of face, photo of iris, recording of voice, video of face, artificial hand, custom contact lens, artificial/patterned contact lens, facial mask (ski, theatrical, Halloween), opaque or theatrical contact lenses</td>
</tr>
<tr>
<td>Partial</td>
<td>glue on finger, false facial hair, cosmetics, removable implants, sunglasses</td>
</tr>
<tr>
<td>Human</td>
<td></td>
</tr>
<tr>
<td>Lifeless</td>
<td>cadaver part, severed finger/hand</td>
</tr>
<tr>
<td>Altered</td>
<td>nose job, face lift, amputation, mutilation, surgical switching of fingerprints between hands and/or toes</td>
</tr>
<tr>
<td>Non-Conformant</td>
<td>voice mimicry, hand shape control, forged signature, facial expression/extreme, tip or side of finger, falsetto voice</td>
</tr>
<tr>
<td>Conformant</td>
<td>zero effort imposter attempt</td>
</tr>
<tr>
<td>Coerced</td>
<td>unconscious, under duress, drugged</td>
</tr>
</tbody>
</table>