We have evaluated face recognition software to be used with hand held devices (smartphones). We contrast the robustness against presentation attacks with the systems usability during regular use, and highlight where currently state of the art systems (CoFS) stand in that regard. We will look at the results specifically under the tradeoff between acceptance, linked with usability, and security, which usually negatively impacts usability.

**ABSTRACT**

**Basic information**
- We were tasked by a company with evaluating the usability and security of face recognition systems.
- System is used to unlock a smartphone via self-based face recognition.
- Liveness detection on client side.
- Matching is done server side.

**Constraints, shortcomings**
- Testing time limited, due to licensing issues.
- Limited number of users/attempts.
- Should be shown as a showcase for obvious problems which happen outside a "lab setup".

What do we want to know?
- How secure are these systems?
- That is, how hard is it for an adversary to unlock the phone.
- How usable are these systems?
- That is, how easy is it for a legitimate user to unlock the phone.

What are we doing?
- We will look at the security of the two systems under test PassiveSys and ActiveSys, with the goal of unlocking the device with minimal fuss on the part of the user.

**Liveness detection modes of the different tools**
- PassiveSys:
  - video: seems to take a video.
  - lessvid: stringent version of video.
  - image: simply takes a picture
- ActiveSys:
  - Blink: user has to keep still and blink on cue.
  - Arrow: requires turning the head to steer an arrow along a line to a target, when the arrow and target align the user has to blink.

**Introduction**

Results are split between liveness detection test (LD) and veriﬁcation results (Match). The presence of glasses in the probe (Pr) and gallery (Gal.) images is given as well.

**Usability and Baseline Outdoors**

- **Baseline for PassiveSys for modes: video, lessvid, image.**
- **Baseline for ActiveSys for modes: blink and arrow.**

<table>
<thead>
<tr>
<th>Pr. Gal.</th>
<th>LD Match</th>
<th>Pr. Gal.</th>
<th>LD Match</th>
</tr>
</thead>
<tbody>
<tr>
<td>yes</td>
<td>0/20</td>
<td>yes</td>
<td>20/20</td>
</tr>
<tr>
<td>no</td>
<td>0/20</td>
<td>no</td>
<td>12/20</td>
</tr>
<tr>
<td>yes</td>
<td>0/20</td>
<td>yes</td>
<td>20/20</td>
</tr>
<tr>
<td>yes</td>
<td>20/20</td>
<td>no</td>
<td>12/20</td>
</tr>
<tr>
<td>yes</td>
<td>0/20</td>
<td>yes</td>
<td>20/20</td>
</tr>
<tr>
<td>yes</td>
<td>0/20</td>
<td>yes</td>
<td>20/20</td>
</tr>
</tbody>
</table>

**Usability and Baseline Outdoors**

- **Suspicion:** Failure for images with glasses was due to reflection on the glasses.
- **We performed another test in natural sunlight, during a bright day. Facing was either towards the sun or away from it.**

**Presentation Attack: Replay Attacks**

- **Record an image or video and present that to the device instead**
- **video mode will no longer be used (not practical given the light test).**
- **20 trios per attack were performed**

**System Mode:**
- **PassiveSys**
  - Image Level A 5%
  - Image Level B 10%
  - Image Level C 15%
  - Video Level A 5%
  - Video Level B 10%
  - Video Level C 15%
- **ActiveSys**
  - Mask Level A 5%
  - Mask Level B 10%

**Erase of Attack**

- **Only for PassiveSys/image combination with the screen attack**
- **How degraded an image can still unlock the device?**
- **The number of successful attacks out of 10 attempts is given.**

**Ease of Attack**

- **Type**
  - Low med strong
  - **Resolution**
    - 10 10 10
    - 10 10 60

**Presentation Attack: Masks**

- **We used two attack types based on wearable masks:**
  - Latex based and handcrafted
  - 3D printed resin composite

**Usability versus Security**

- **Compare threat level, presentation attack success rate and usability per mode and system.**

**Threat Level A**
- PassiveSys level 5% Level B 10% Level C 15%
- ActiveSys level 5%

**Threat Level B**
- PassiveSys level 10% Level B 20% Level C 30%
- ActiveSys level 10%

**Threat Level C**
- PassiveSys level 15% Level B 30% Level C 45%
- ActiveSys level 15%