MAY THE FORCE BE WITH YOU: FORCE-BASED RELAY ATTACK DETECTION

Iakovos Gurulian\textsuperscript{1}, Gerhard P. Hancke\textsuperscript{2}, Konstantinos Markantonakis\textsuperscript{1}, and Raja Naeem Akram\textsuperscript{1}
iakovos.gurulian.2014@live.rhul.ac.uk, gp.hancke@cityu.edu.hk, \{k.markantonakis, r.n.akram\}@rhul.ac.uk

November 14, 2017

\textsuperscript{1}Information Security Group, Smart Card and IoT Security Centre
Royal Holloway, University of London

\textsuperscript{2}Department of Computer Science
City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, Hong Kong
RELAY ATTACKS
RELAY ATTACKS

Definition

A relay attack is a passive man-in-the-middle attack during which an attacker is extending the communication distance of two legitimate devices by relaying each communication message between them, without the legitimate user’s consent.
Definition

A relay attack is a passive man-in-the-middle attack during which an attacker is extending the communication distance of two legitimate devices by relaying each communication message between them, without the legitimate user’s consent.

Potential attack vectors:

· Unauthorised payments
· Unauthorised access to buildings and facilities
· User impersonation
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
ANATOMY OF A RELAY ATTACK

Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
Use Case: Contactless Payment
(Contactless) Smart Cards

Distance bounding protocols have been proposed.
(Contactless) Smart Cards

Distance bounding protocols have been proposed.

Smartphones

- Distance bounding protocols may not be applicable:
  - Multitude of hardware
  - Multiple processes running
- Sensing the ambient environment has been proposed instead (more on the next slide)
RELAY ATTACK DETECTION USING THE NATURAL AMBIENT ENVIRONMENT
NATURAL AMBIENT ENVIRONMENT-BASED RELAY ATTACK DETECTION
Both devices measure the ambient environment using some sensor(s) for some pre-defined time:
- Temperature
- Accelerometer
- GPS
- ...
Transfer the captured values to one of the devices, or a trusted third party.
Compare the captured values.
Return decision based on the similarity of the captured values.
NATURAL AMBIENT ENVIRONMENT-BASED RELAY ATTACK DETECTION

- Both devices measure the ambient environment using some sensor(s) for some pre-defined time
  - Temperature
  - Accelerometer
  - GPS
  - ...
- Transfer the captured values to one of the devices, or a trusted third party
- Compare the captured values
- Return decision based on the similarity of the captured values
Both devices measure the ambient environment using some sensor(s) for some pre-defined time
- Temperature
- Accelerometer
- GPS
- ...
- Transfer the captured values to one of the devices, or a trusted third party
- Compare the captured values
- Return decision based on the similarity of the captured values
Both devices measure the ambient environment using some sensor(s) for some pre-defined time
- Temperature
- Accelerometer
- GPS
- ...
Transfer the captured values to one of the devices, or a trusted third party
Compare the captured values
Return decision based on the similarity of the captured values
Both devices measure the ambient environment using some sensor(s) for some pre-defined time
- Temperature
- Accelerometer
- GPS
- ...
Transfer the captured values to one of the devices, or a trusted third party
Compare the captured values
Return decision based on the similarity of the captured values
Previously proposed solutions:

- ~9% Equal Error Rate (EER) at best
- Probably not sufficient for tasks like contactless payments
- Timing restrictions in many contactless transactions ≤ 500ms
- Current solutions require more time
Previously proposed solutions:

- \(~9\%\) Equal Error Rate (EER) at best
- Probably not sufficient for tasks like contactless payments
- Timing restrictions in many contactless transactions \(\leq 500\text{ms}\)
- Current solutions require more time

<table>
<thead>
<tr>
<th>Paper</th>
<th>Sensor(s) Used</th>
<th>Sample Duration</th>
<th>Contactless Suitability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ma et al. [2]</td>
<td>GPS</td>
<td>10 seconds</td>
<td>Unlikely</td>
</tr>
<tr>
<td>Halevi et al. [1]</td>
<td>Audio, Light</td>
<td>30 seconds, 2 seconds</td>
<td>Unlikely, More Likely</td>
</tr>
<tr>
<td>Varshavsky et al. [8]</td>
<td>Wi-Fi (Radio Waves), Temperature</td>
<td>1 second, N/A</td>
<td>More Likely, -</td>
</tr>
<tr>
<td>Urien et al. [7]</td>
<td>Wi-Fi, Temperature</td>
<td>1 second, N/A</td>
<td>More Likely, -</td>
</tr>
<tr>
<td>Mehrnezhad et al. [3]</td>
<td>Accelerometer, GPS Raw Data</td>
<td>0.6 to 1.5 Seconds, 120 seconds</td>
<td>More Likely, Unlikely</td>
</tr>
<tr>
<td>Truong et al. [6]</td>
<td>Wi-Fi, Ambient Audio, Bluetooth</td>
<td>30 seconds, 10 seconds, 12 seconds</td>
<td>Unlikely, Unlikely, Unlikely</td>
</tr>
<tr>
<td>Shrestha et al. [5]</td>
<td>Temperature (T), Precision Gas (G), Humidity (H), Altitude (A), HA, HGA, THGA</td>
<td>Few seconds</td>
<td>Unlikely, Unlikely, Unlikely, Unlikely</td>
</tr>
</tbody>
</table>
Previously proposed solutions:

- ~9% Equal Error Rate (EER) at best
  - Probably not sufficient for tasks like contactless payments
- Timing restrictions in many contactless transactions ≤ 500ms
  - Current solutions require more time

Problem
In previous work we questioned the suitability of using the natural ambient environment for proximity detection [4]:

- 17 widely available sensors were tested in 500ms transactions
- Best performance: Pressure sensor
- Still: ~10% False acceptance rate
RELAY ATTACK DETECTION BY GENERATION OF AN ARTIFICIAL AMBIENT ENVIRONMENT
We proposed the generation of an Artificial Ambient Environment (AAE), using peripherals of the transaction devices (terminal and instrument)

- Based on randomly generated streams or sequences
- Easy for the genuine devices to establish proximity assurances
- Hard for an attacker to timely reproduce at a distance location
We proposed the use of the following peripherals:

- **Infrared light**
  - Tested against 6 attack test-beds using off-the-shelf equipment
  - All relay attacks were successfully detected
  - 98% True Accept Rate
  - But:
    - Infrared emitters not available on most modern smartphones
    - Might be vulnerable to more sophisticated attacks

- **Vibration**
  - Tested against 15 attack scenarios
  - \(\sim0\%\) EER (using various popular machine learning classifiers)
  - But might be vulnerable when a more sophisticated attacker is involved
FORCE SENSING-BASED RELAY ATTACK DETECTION
FORCE SENSING-BASED RELAY ATTACK DETECTION

- Different approach (not relying on environmental measurements)
- Part of the transaction (similar to PIN entry)
- Requires user interaction
- Based on the duration of subsequent presses/releases of virtual buttons that appear on the smartphone’s screen
The user is called to position the device on a force-sensitive ‘plate’
- A randomly selected button (out of 6 buttons) is displayed on the device’s display that the user is called to press
- Both devices (payment terminal and payment instrument) record the id of the pressed button, as well as the time of the press (in ms)
- Upon pressing the button, another button is randomly chosen and displayed
- The time between subsequent button presses is also recorded
- Four buttons are displayed in total
- The captured timings and entered PIN from the two devices are compared — if within a certain threshold, we assume that the devices are in proximity (no relay attack)
The Basic Framework Architecture
Transaction Instrument (TI):

- Standard Android libraries

Transaction Terminal (TT):

- Four force sensitive resistors
- Algorithm to detect which of the 6 buttons is being pressed, based on the pressure that the resistors measure
Transaction Instrument (TI):

- Standard Android libraries

Transaction Terminal (TT):

- Four force sensitive resistors
- Algorithm to detect which of the 6 buttons is being pressed, based on the pressure that the resistors measure
Detection of Presses by the transaction terminal
Algorithm 1: Detection of Pressed Button

**Input**: int sensor1, int sensor2, int sensor3, int sensor4

**Output**: int pressedButtonID

1. leftSide ← sensor1 + sensor2;
2. rightSide ← sensor3 + sensor4;
3. if leftSide > rightSide then
   4. force ← sensor1 / leftSide;
   5. if force ≥ 0 and force < 0.33 then
      6. return 5
   6. else if force ≥ 0.33 and force < 0.66 then
      7. return 3
   7. return 1
4. end
5. force ← sensor3 / rightSide;
6. if force ≥ 0 and force < 0.33 then
   7. return 6
6. else if force ≥ 0.33 and force < 0.66 then
   8. return 4
7. return 2
· Part 1: Set thresholds
· Part 2: Experimental evaluation
PART 1: SET THRESHOLD

<video demonstration>
Captured PIN, Timings, and Difference Between the Captured Timings (in ms) from the Two Devices

<table>
<thead>
<tr>
<th></th>
<th>Terminal (TT)</th>
<th>Genuine User (TI')</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>6315</td>
<td>6315</td>
<td>—</td>
</tr>
<tr>
<td>Press 1</td>
<td>113</td>
<td>129</td>
<td>-16</td>
</tr>
<tr>
<td>Release 1</td>
<td>1120</td>
<td>1081</td>
<td>39</td>
</tr>
<tr>
<td>Press 2</td>
<td>244</td>
<td>262</td>
<td>-18</td>
</tr>
<tr>
<td>Release 2</td>
<td>1168</td>
<td>1136</td>
<td>32</td>
</tr>
<tr>
<td>Press 3</td>
<td>201</td>
<td>214</td>
<td>-13</td>
</tr>
<tr>
<td>Release 3</td>
<td>1263</td>
<td>1232</td>
<td>31</td>
</tr>
<tr>
<td>Press 4</td>
<td>177</td>
<td>190</td>
<td>-13</td>
</tr>
</tbody>
</table>
Based on 100 measurements we set acceptance thresholds for presses and releases.

We repeated the experiment using another 2 devices (heavier and larger), without readjusting the terminal’s setup.

Devices used:
- Samsung Galaxy S5 mini (SGS5 mini) — 4.5” display, 120g
- Samsung Galaxy S4 (SGS 4) — 5” display, 130g
- Nexus 9 tablet — 8.9” display, 425g
Proximity Detection Results – in ms (negative results indicate that TI’s measurement durations were larger than TT’s)

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th></th>
<th>Maximum</th>
<th></th>
<th>Span</th>
<th></th>
<th>Average</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SGS5 mini</td>
<td>-46</td>
<td>11</td>
<td>-11</td>
<td>48</td>
<td>35</td>
<td>37</td>
<td>-29.09</td>
<td>28.71</td>
</tr>
</tbody>
</table>
### Proximity Detection Results – in ms (negative results indicate that TI’s measurement durations were larger than TT’s)

<table>
<thead>
<tr>
<th></th>
<th>Minimum</th>
<th></th>
<th>Maximum</th>
<th></th>
<th>Span</th>
<th></th>
<th>Average</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SGS5 mini</td>
<td>-46</td>
<td>11</td>
<td>-11</td>
<td>48</td>
<td>35</td>
<td>37</td>
<td>-29.09</td>
<td>28.71</td>
</tr>
<tr>
<td>SGS 4</td>
<td>-28</td>
<td>-8</td>
<td>9</td>
<td>30</td>
<td>37</td>
<td>38</td>
<td>-5.32</td>
<td>5.26</td>
</tr>
<tr>
<td>Nexus 9</td>
<td>-18</td>
<td>-8</td>
<td>12</td>
<td>23</td>
<td>30</td>
<td>31</td>
<td>-2.16</td>
<td>2.83</td>
</tr>
<tr>
<td>Total</td>
<td>-46</td>
<td>-8</td>
<td>12</td>
<td>48</td>
<td>58</td>
<td>56</td>
<td>-12.19</td>
<td>12.27</td>
</tr>
</tbody>
</table>
Two phases:

- 10 users were shown 10 videos and tried to attack them by replicating the user’s movement on the device, while the video was playing or afterwards (up to them)
  - The users were familiar with the definition of a relay attack
  - The videos were presented on a 24” computer screen and the users could choose the orientation that suited them best
  - 4 of the users were musicians
- The same users were shown a single video 10 times and called to attack it each time (very powerful attacker)

Two analyses:

- Threshold-based analysis
- Machine learning-based analysis
### Performance of 5 Users

<table>
<thead>
<tr>
<th></th>
<th>Genuine User</th>
<th>Genuine Terminal</th>
<th>Attacker 1</th>
<th>Attacker 2</th>
<th>Attacker 3</th>
<th>Attacker 4</th>
<th>Attacker 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
</tr>
<tr>
<td>Press 1</td>
<td>129</td>
<td>113</td>
<td>91</td>
<td>61</td>
<td>195</td>
<td>102</td>
<td>87</td>
</tr>
<tr>
<td>Release 1</td>
<td>1081</td>
<td>1120</td>
<td>804</td>
<td>847</td>
<td>985</td>
<td>2068</td>
<td>1151</td>
</tr>
<tr>
<td>Press 2</td>
<td>262</td>
<td>244</td>
<td>75</td>
<td>287</td>
<td>86</td>
<td>158</td>
<td>44</td>
</tr>
<tr>
<td>Release 2</td>
<td>1136</td>
<td>1168</td>
<td>1486</td>
<td>1360</td>
<td>1774</td>
<td>930</td>
<td>1454</td>
</tr>
<tr>
<td>Press 3</td>
<td>214</td>
<td>201</td>
<td>262</td>
<td>79</td>
<td>37</td>
<td>105</td>
<td>188</td>
</tr>
<tr>
<td>Release 3</td>
<td>1232</td>
<td>1263</td>
<td>1052</td>
<td>1094</td>
<td>939</td>
<td>1479</td>
<td>1198</td>
</tr>
<tr>
<td>Press 4</td>
<td>190</td>
<td>177</td>
<td>386</td>
<td>197</td>
<td>88</td>
<td>113</td>
<td>173</td>
</tr>
</tbody>
</table>
## Performance of 5 Users

<table>
<thead>
<tr>
<th></th>
<th>Genuine User</th>
<th>Genuine Terminal</th>
<th>Attacker 1</th>
<th>Attacker 2</th>
<th>Attacker 3</th>
<th>Attacker 4</th>
<th>Attacker 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
</tr>
<tr>
<td>Press 1</td>
<td>129</td>
<td>113</td>
<td>91</td>
<td>61</td>
<td>195</td>
<td>102</td>
<td>87</td>
</tr>
<tr>
<td>Release 1</td>
<td>1081</td>
<td>1120</td>
<td>804</td>
<td>847</td>
<td>985</td>
<td>2068</td>
<td>1151</td>
</tr>
<tr>
<td>Press 2</td>
<td>262</td>
<td>244</td>
<td>75</td>
<td>287</td>
<td>86</td>
<td>158</td>
<td>44</td>
</tr>
<tr>
<td>Release 2</td>
<td>1136</td>
<td>1168</td>
<td>1486</td>
<td>1360</td>
<td>1774</td>
<td>930</td>
<td>1454</td>
</tr>
<tr>
<td>Press 3</td>
<td>214</td>
<td>201</td>
<td>262</td>
<td>79</td>
<td>37</td>
<td>105</td>
<td>188</td>
</tr>
<tr>
<td>Release 3</td>
<td>1232</td>
<td>1263</td>
<td>1052</td>
<td>1094</td>
<td>939</td>
<td>1479</td>
<td>1198</td>
</tr>
<tr>
<td>Press 4</td>
<td>190</td>
<td>177</td>
<td>386</td>
<td>197</td>
<td>88</td>
<td>113</td>
<td>173</td>
</tr>
</tbody>
</table>
Performance of 5 Users

<table>
<thead>
<tr>
<th></th>
<th>Genuine User</th>
<th>Genuine Terminal</th>
<th>Attacker 1</th>
<th>Attacker 2</th>
<th>Attacker 3</th>
<th>Attacker 4</th>
<th>Attacker 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
</tr>
<tr>
<td>Press 1</td>
<td>129</td>
<td>113</td>
<td>91</td>
<td>61</td>
<td>195</td>
<td>102</td>
<td>87</td>
</tr>
<tr>
<td>Release 1</td>
<td>1081</td>
<td>1120</td>
<td>804</td>
<td>847</td>
<td>985</td>
<td>2068</td>
<td>1151</td>
</tr>
<tr>
<td>Press 2</td>
<td>262</td>
<td>244</td>
<td>75</td>
<td>287</td>
<td>86</td>
<td>158</td>
<td>44</td>
</tr>
<tr>
<td>Release 2</td>
<td>1136</td>
<td>1168</td>
<td>1486</td>
<td>1360</td>
<td>1774</td>
<td>930</td>
<td>1454</td>
</tr>
<tr>
<td>Press 3</td>
<td>214</td>
<td>201</td>
<td>262</td>
<td>79</td>
<td>37</td>
<td>105</td>
<td>188</td>
</tr>
<tr>
<td>Release 3</td>
<td>1232</td>
<td>1263</td>
<td>1052</td>
<td>1094</td>
<td>939</td>
<td>1479</td>
<td>1198</td>
</tr>
<tr>
<td>Press 4</td>
<td>190</td>
<td>177</td>
<td>386</td>
<td>197</td>
<td>88</td>
<td>113</td>
<td>173</td>
</tr>
</tbody>
</table>
## Performance of 5 Users

<table>
<thead>
<tr>
<th></th>
<th>Genuine User</th>
<th>Genuine Terminal</th>
<th>Attacker 1</th>
<th>Attacker 2</th>
<th>Attacker 3</th>
<th>Attacker 4</th>
<th>Attacker 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
<td>6315</td>
</tr>
<tr>
<td>Press 1</td>
<td>129</td>
<td>113</td>
<td>91</td>
<td>61</td>
<td>195</td>
<td>102</td>
<td>87</td>
</tr>
<tr>
<td>Release 1</td>
<td>1081</td>
<td>1120</td>
<td>804</td>
<td>847</td>
<td>985</td>
<td>2068</td>
<td>1151</td>
</tr>
<tr>
<td>Press 2</td>
<td>262</td>
<td>244</td>
<td>75</td>
<td>287</td>
<td>86</td>
<td>158</td>
<td>44</td>
</tr>
<tr>
<td>Release 2</td>
<td>1136</td>
<td>1168</td>
<td>1486</td>
<td>1360</td>
<td>1774</td>
<td>930</td>
<td>1454</td>
</tr>
<tr>
<td>Press 3</td>
<td>214</td>
<td>201</td>
<td>262</td>
<td>79</td>
<td>37</td>
<td>105</td>
<td>188</td>
</tr>
<tr>
<td>Release 3</td>
<td>1232</td>
<td>1263</td>
<td>1052</td>
<td>1094</td>
<td>939</td>
<td>1479</td>
<td>1198</td>
</tr>
<tr>
<td>Press 4</td>
<td>190</td>
<td>177</td>
<td>386</td>
<td>197</td>
<td>88</td>
<td>113</td>
<td>173</td>
</tr>
</tbody>
</table>
Threshold-Based Relay Attack Detection Results (out of 100 attempts)

<table>
<thead>
<tr>
<th></th>
<th>Press 1</th>
<th>Release 1</th>
<th>Press 2</th>
<th>Release 2</th>
<th>Press 3</th>
<th>Release 3</th>
<th>Press 4</th>
<th>False Accept</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General Threshold – Phase 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detected</td>
<td>73</td>
<td>24</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Correct</td>
<td>27</td>
<td>10</td>
<td>37</td>
<td>10</td>
<td>24</td>
<td>5</td>
<td>31</td>
<td>—</td>
</tr>
<tr>
<td><strong>Device Specific Threshold – Phase 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detected</td>
<td>84</td>
<td>16</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Correct</td>
<td>16</td>
<td>7</td>
<td>25</td>
<td>9</td>
<td>9</td>
<td>4</td>
<td>23</td>
<td>—</td>
</tr>
<tr>
<td><strong>General Threshold – Phase 2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detected</td>
<td>57</td>
<td>37</td>
<td>5</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Correct</td>
<td>43</td>
<td>11</td>
<td>29</td>
<td>24</td>
<td>26</td>
<td>9</td>
<td>20</td>
<td>—</td>
</tr>
<tr>
<td><strong>Device Specific Threshold – Phase 2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detected</td>
<td>65</td>
<td>33</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Correct</td>
<td>35</td>
<td>6</td>
<td>21</td>
<td>22</td>
<td>20</td>
<td>6</td>
<td>9</td>
<td>—</td>
</tr>
</tbody>
</table>
Graphical Representation of the Best Attack Attempt (TT – TI) Versus the Corresponding Genuine Transaction (TT – TI')
Graphical Representation of the Best Attack Attempt (TT – TI) Versus the Corresponding Genuine Transaction (TT – TI’) using device specific threshold
Graphical Representation of a Typical Attack Attempt (TT – TI) Versus the Corresponding Genuine Transaction (TT – TI’)

USER STUDY — DATA ANALYSIS: THRESHOLD-BASED
• The same video was presented 10 times to each participant
• The participant was asked to attack it after each time
Performance Variation of Each of the 10 Attempts in the Second Phase

Presses Linear Regression ($r = 0.11$)
Releases Linear Regression ($r = 0.72$)
MULTIPLE ATTACKS AGAINST THE SAME VIDEO

- Result: Minor performance improvement over time
- This scenario is not likely to occur
Machine Learning Classification Results Obtained by Repeating 10-Fold Cross-Validation 10 Times

<table>
<thead>
<tr>
<th></th>
<th>Random Forest</th>
<th>Naïve Bayes</th>
<th>Logistic Regression</th>
<th>Decision Tree</th>
<th>Support Vector Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accuracy (%)</strong></td>
<td>99.62</td>
<td>99.80</td>
<td>86.58</td>
<td>98.78</td>
<td>100.00</td>
</tr>
<tr>
<td><strong>AUC</strong></td>
<td>0.9999</td>
<td>0.9996</td>
<td>0.8163</td>
<td>0.9873</td>
<td>1.0</td>
</tr>
<tr>
<td><strong>F1-score</strong></td>
<td>0.9969</td>
<td>0.9984</td>
<td>0.90</td>
<td>0.9901</td>
<td>1.0</td>
</tr>
<tr>
<td><strong>EER</strong></td>
<td>0.0022</td>
<td>0.0047</td>
<td>0.1993</td>
<td>0.104</td>
<td>0.0</td>
</tr>
</tbody>
</table>
· Both threshold-based and machine learning-based approaches could detect all relay attack attempts
· Even when the device was not position perfectly the accuracy of the terminal was very high
· Tried with 8 buttons instead of 6 with good results (not as good)
· (Musicians did not perform better than the rest of the users)

Potential concerns:
· A robotic arm might be more accurate — but will easily be spotted by the terminal’s operator
· Not very user friendly (compared to just tapping the devices)
· Requires extra HW
· Phone cases might obstruct
· Extend user study
· Find new approaches to more accurately measure the force (e.g. in case the placement is not good)
· Add more features, like the amount of pressure (most smartphones do not support this or the accuracy is very low)
CONCLUSION

- Proposed a novel approach to relay attack detection on smartphones
- Experimental evaluation of the approach showed promising results
- 100% relay attack detection rate was achieved, using threshold- and machine learning-based analyses
REFERENCES


THANK YOU!

ANY QUESTIONS OR SUGGESTIONS?