Towards Touch-to-Access Device Authentication Using Induced Body Electric Potentials

Zhenyu Yan, Qun Song, Rui Tan, Yang Li, Adams Wai Kin Kong
School of Computer Science and Engineering
Nanyang Technological University, Singapore
Lots of heterogeneous IoT devices to access
Existing access control approaches

<table>
<thead>
<tr>
<th>User authentication</th>
<th>Device authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>password</strong></td>
<td><strong>physiology</strong></td>
</tr>
<tr>
<td>Iris</td>
<td>EMG</td>
</tr>
<tr>
<td>fingerprint</td>
<td>PPG</td>
</tr>
<tr>
<td>Iris</td>
<td><strong>physiology</strong></td>
</tr>
<tr>
<td>Face</td>
<td>Face</td>
</tr>
<tr>
<td>Voice</td>
<td>Voice</td>
</tr>
<tr>
<td>no keypad or touchscreen</td>
<td>dedicated sensors, careful installation</td>
</tr>
<tr>
<td>inconvenient, disturbing</td>
<td>non-trivial design</td>
</tr>
</tbody>
</table>

Easy-to-use device authentication using a wearable token for smart objects?
TouchAuth: device authentication through touching

Recommendation

Preference

Touch to unlock

Image credit: iStockphoto, vectorstock
Induced body electric potential (iBEP)

- Powerline radiation (50Hz or 60Hz)
- Body antenna
- Analog-to-digital converter
- Band pass filter (50/60Hz)

iBEP signal is amplified by human body

[CHI ’12, UbiComp’ 12, IPSN ’17, SenSys ’17]
Source of iBEP

iBEPs are similar at same body, closed locations.

\[ V_{OUT} = V_{IN} - V_{GND} \]

\[ V_{IN} \]: same when on the same person
\[ V_{GND} \]: similar when on closed locations
iBEP on different locations

iBEP signals are:
• Similar at the same body and closed locations
• Different on different bodies or different locations

iBEP signals can be used for same-body detection
System model of TouchAuth

- Token device
- Capture iBEP
- Set up TLS connection
- Clock sync
- Object
- Capture iBEP

Diagram:
- Transmit
- Contact detection & check signal strength
- Compare similarity
- Accept or deny

Image credit: macrovector, rawpixel.com
Evaluation methodology

different users

different attackers

mimicry attacks

locations

meetings room
laboratory
corridor
bedroom
living rm
study rm
kitchen

toaster
electric kettle
hair dryer

ceiling fan
blender
induction cooker

circuit seeker
cellular
wet/dry skin

interferences

0.5m
### Results: Comparison with other device auth. approaches

<table>
<thead>
<tr>
<th>Signal</th>
<th>Sensing time (s)</th>
<th>False Acceptance Rate (%)</th>
<th>True Acceptance Rate (%)</th>
</tr>
</thead>
</table>
| **TouchAuth**  
(simple sensor only) | 1 | 2.0 | 94.2% |
| | 5 | 2.0 | 98.9% |
| **ECG + PPG**  
[IEEE ComMag’06] | ~60 (67 IPIs) | 2.1 | 93.5 |
| | ~30 (34 IPIs) | 4.5 | 90.5 |
| **PPG**  
| **ECG**  
[INFOCOM’13] | ~90 (90 IPIs) | ~0 | ~100 |
**Conclusion**

<table>
<thead>
<tr>
<th>Password</th>
<th>Biometrics</th>
<th>Physiology</th>
<th>Intra-body Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Iris</td>
<td>• EMG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fingerprint</td>
<td>• PPG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Face</td>
<td>• EKG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Voice</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TouchAuth: a novel device authentication approach**

- **iBEP signal**: complex human-ambient coupling
  - Similar at same body and closed locations
- **TouchAuth**
  - Touch-based (intuitive and convenient)
  - Short sensing time