RFIDs and Secret Handshakes: Defending Against Ghost-and-Leech Attacks and Unauthorized Reads with Context-Aware Communications

By: Bo Qin
RFID

- Radio-frequency identification provides contactless communication between **tags** and **readers** using radio waves.

**Tags:**

**Readers:**
Problem

- Ghost-Leech attack (Relay attack):
  - Tags are always ready to be read
Problem

• Tracking (privacy issue):
Problem

- **Goals:**
  - Backward Compatibility
  - Consistent Usage

- **Possible solutions:**
  - Sleeve – BC: Yes, CU: No
  - Button – BC: Yes, CU: No
  - Timing constraint – BC: No, CU: Yes
The tags should only be read when the user is using it near a card reader
Survey:

- Where is your card?

<table>
<thead>
<tr>
<th>Location of Card by Card Type</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>On lanyard, below clothes</td>
<td>2.6%</td>
</tr>
<tr>
<td>On lanyard, above clothes</td>
<td>11.0%</td>
</tr>
<tr>
<td>In Wallet (male or female)</td>
<td>64.4%</td>
</tr>
<tr>
<td>Directly in purse</td>
<td>5.2%</td>
</tr>
<tr>
<td>Directly in pocket</td>
<td>16.8%</td>
</tr>
<tr>
<td>On lanyard, below clothes</td>
<td>0.9%</td>
</tr>
<tr>
<td>On lanyard, above clothes</td>
<td>3.0%</td>
</tr>
<tr>
<td>In Wallet (male or female)</td>
<td>68.5%</td>
</tr>
<tr>
<td>Directly in purse</td>
<td>2.6%</td>
</tr>
<tr>
<td>Directly in pocket</td>
<td>25.0%</td>
</tr>
</tbody>
</table>

Number of Participants
Survey:

- How do you use your card?

```
<table>
<thead>
<tr>
<th>Authentication Action</th>
<th>Number of Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>Touch purse to reader, leave card in purse</td>
<td>2.1%</td>
</tr>
<tr>
<td>Touch badge to reader without removing lanyard</td>
<td>12.0%</td>
</tr>
<tr>
<td>Remove lanyard, touch badge to reader</td>
<td>1.0%</td>
</tr>
<tr>
<td>Press card to reader (card not in wallet, pocket, purse, or backpack)</td>
<td>24.6%</td>
</tr>
<tr>
<td>Other</td>
<td>8.4%</td>
</tr>
<tr>
<td>Leave card in wallet, press wallet to reader</td>
<td>31.9%</td>
</tr>
<tr>
<td>Leave card in wallet in purse/backpack, Press purse/backpack to reader</td>
<td>4.2%</td>
</tr>
<tr>
<td>Hip twist, leave card in pocket</td>
<td>2.1%</td>
</tr>
<tr>
<td>Hip twist, card in wallet, wallet in pocket</td>
<td>13.6%</td>
</tr>
</tbody>
</table>
```
“We” have the solution

- Secret Handshake
  - User performs a gesture with the card to **activate** the card to communicate with the reader
Gestures

- Alpha
- Circle/Double circle
- Triangle
- Key Twist
- 1.5 Wave
- Hip Twist
Implementation

- Goals:
  - Cost Effective
  - Passive (no battery!)

- Hardware
  - Intel’s WISP (Wireless Identification and Sensing Platform)
    - Only passive RFID device that’s programmable
    - MSP430 Accelerometer
Hardware Limitations

- Memory
  - Only 144 bytes of RAM for accelerometer data

- Power
  - Turning on accelerometer consumes most power
    - Sampling rate: 40Hz

- Gestures < 1 sec
Experiment

- Gather data for effectiveness of gestures
  - 8 gestures
  - 3 participants
  - Collected accelerometer data during daily activities
    - Sit, Walk, Stand, Bike, Fidget, Play Ping Pong, etc.
Gesture comparison

- False Negative (FN): Card failed to activate
- False Positive (FP): Card activated when not

- Threshold (simplified): values for calculating what is a gesture from accelerometer data

- Best gestures:
  - 1.5 wave and double circle
    - Largest range of threshold values with 0 FN and 0 FP

- Worst gesture:
  - Hip twist
Extension

- Different gestures for different cards
  - Bob’s bus card (in wallet) with one gesture prevents driver, Eve, from reading Bob’s credit card
Thank You

- Alexei and Yoshi for the slides