Mobile Token-Based Authentication

On a Budget

Hristo Bojinov    Dan Boneh
Stanford Computer Security Lab
Talk overview

General theme: Unlocking smartphones

Part 1: About this work
- Compass as a receiver
- Microphone as a receiver
- Cost and power

Part 2: On-going and future work
Compass
Permanent magnets
Poor resolution: distance to magnets is too great!
Magkey prototype
Magkey circuit

[Diagram of Magkey circuit with components labeled, including ICs, resistors, capacitors, and diodes.

Saturday, April 16, 2011]
MagLock app

up to ~5 baud (NI)
about 1 inch range
MagLock app

Saturday, April 16, 2011
Microphone
Mickey prototype
Mickey circuit

Magkey, minus the coil, plus:
MicLock app

up to ~100 baud (NI) about 1 foot range
MicLock app

Record

01001 11.69029219268588

01001 19.977471429378834

01001 19.977471429378834

Scale 1:100

Scale 1:100

Scale 1:10
Cost and Power
<table>
<thead>
<tr>
<th>Component</th>
<th>Unit cost</th>
<th>Magkey</th>
<th>Mickey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer IC</td>
<td>$0.20</td>
<td>$0.20</td>
<td>$0.40</td>
</tr>
<tr>
<td>Shift Register IC</td>
<td>$0.25</td>
<td>$0.50</td>
<td>$0.50</td>
</tr>
<tr>
<td>Discrete</td>
<td>varies</td>
<td>$0.37</td>
<td>$0.38</td>
</tr>
<tr>
<td>Total (Prototype)</td>
<td></td>
<td>$1.07</td>
<td>$1.28</td>
</tr>
<tr>
<td>PIC IC</td>
<td>$0.38</td>
<td>$0.38</td>
<td>$0.38</td>
</tr>
<tr>
<td>Total (PIC)</td>
<td></td>
<td>$0.75</td>
<td>$0.76</td>
</tr>
</tbody>
</table>
## Current and Longevity

<table>
<thead>
<tr>
<th>Current</th>
<th>Mode</th>
<th>Magkey</th>
<th>Mickey</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average</td>
<td></td>
<td>6.91 mA</td>
<td>0.23 mA</td>
</tr>
<tr>
<td>Peak</td>
<td></td>
<td>16.00 mA</td>
<td>0.25 mA</td>
</tr>
<tr>
<td>Continuous</td>
<td></td>
<td>210 hrs</td>
<td>6500 hrs</td>
</tr>
<tr>
<td>On-demand</td>
<td></td>
<td>&gt;5 yrs</td>
<td>&gt;10 yrs</td>
</tr>
</tbody>
</table>
What’s Next?
Low-power wireless

Contactless cards (e.g. NFC)
- No batteries required in token
- Off-the-shelf tokens: today
- Short practical range

Bluetooth 4.0 (Low-energy)
- Might be more pervasive than NFC: laptops, PCs
- Designed for long-term, synchronous operation
- A decent alternative we might consider
So, what is next?

Prove token authentication viability (mobile devices)

- Analyze more [proprietary] technologies
- Influence NFC security agenda

Develop end-to-end token authentication theme

- Authentication on the web, multi-tenant tokens
- PC authentication... keychains, PAM, Windows?
Massive opportunity to redo user authentication:

- Phones are the most versatile computers to date
  - Rapid, on-going evolution, diverse inputs
- Momentum to standardize light-weight wireless
- Threats are more abundant than ever before

Address local, mobile app, and web authentication.

Drive the security agenda into standards efforts.
Time for Q&A.

http://seclab.stanford.edu