How Privacy Leaks from Bluetooth Mouse?

Xian Pan (University of Massachusetts Lowell)
Zhen Ling (Southeast University)
Aniket Pingley (Intel Inc.)
Wei Yu (Towson University)
Kui Ren (University at Buffalo)
Nan Zhang (George Washington University)
Xinwen Fu (University of Massachusetts Lowell)
No wireless mouse encrypts communication

- Logitech’s white paper on Mar. 2, 2009
  - “Since the displacements of a mouse would not give any useful information to a hacker, the mouse reports are not encrypted”

- No encryption by major brand wireless mouse
  - 27 MHz radio
  - Proprietary 2.4 GHz radio links
  - Bluetooth 2.4 GHz radio
Exposed mouse raw data disclose sensitive information

- Sensitive Information: cursor trajectory on screen
- Example: inferring passwords, passwords clicked on software keyboard and graphical passwords
  - Software keyboard
  - Windows 8 picture password
Issues

1. How to sniff Bluetooth traffic?
   - USRP, FTS4BT and other tools

2. How to transfer sniffed raw mouse data to movement information?
   - Reverse engineering mouse raw data semantics

3. How to reconstruct cursor trajectory?

4. How to infer passwords based on the reconstructed trajectory?
3. How to reconstruct cursor trajectory?

- **Cursor coordinate:** $X = X + A \cdot \Delta x$, $Y = Y + A \cdot \Delta y$

- **Mouse Acceleration Strategies**
  1. **Lightweight Acceleration Strategy**
    
    Algorithm 2 Lightweight Acceleration Algorithm
    
    Require: Raw mouse movement $(\Delta x, \Delta y)$, Threshold $T$; Acceleration Factor $A$
    
    1: if $(|\Delta x| + |\Delta y| \leq T)$ then
    2:     cursor movement = $(\Delta x, \Delta y)$;
    3: else
    4:     cursor movement = $(A \times \Delta x, A \times \Delta y)$;
    5: end if

  2. **Complex Acceleration Strategy**

- **Attacks**
  1. **Prediction Attack:** predict the trajectory based on known acceleration algorithms and captured data
  2. **Replay Attack:** Replay captured data on a similar system to the victim
Evaluation

- Success Rate: number of recognized passwords/totally number of passwords
- Prediction Attack on OpenSUSE 11.1 and Fedora 13

<table>
<thead>
<tr>
<th></th>
<th>Basic Inferring</th>
<th>Smart Inferring</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>small keyboard</td>
<td>large keyboard</td>
</tr>
<tr>
<td>OpenSUSE 11.1</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Fedora 13</td>
<td>99%</td>
<td>98%</td>
</tr>
</tbody>
</table>

- Replay Attack on Fedora 13, Windows 7 and Mac OSX 10.6.5

<table>
<thead>
<tr>
<th></th>
<th>Fedora 13</th>
<th>Windows 7</th>
<th>Mac OSX 10.6.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Inferring</td>
<td>69%</td>
<td>100%</td>
<td>44%</td>
</tr>
<tr>
<td>Smart Inferring</td>
<td>31%</td>
<td>92%</td>
<td>16%</td>
</tr>
</tbody>
</table>
Countermeasures

- Encrypt Bluetooth mouse traffic
  - Numeric comparison mode is recommended

- Adopt randomized software keyboard
  - Implement an input method at application layer
  - Implement a API library
  - Integrate into the OS
Thank you!

Xian Pan