TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion

Liang Cai and Hao Chen

UC Davis
Security Problems on Smartphones

• Old problems
  – Malware
  – Software bugs
  – Information leak
  – ...

• New problems
  – How can attackers exploit sensors?
Sensors on Smartphones

• Privacy-sensitive sensors
  – Microphones
  – Cameras
  – GPS

• Are motion sensors privacy-sensitive?
  – Accelerometers
  – Gyroscopes
Traditional Keyloggers

• Intercepting key events
  – E.g., Trojan programs
• Using out of channels
  – Acoustic frequency signatures of keys
  – Timing between keystrokes
  – Electromagnetic emanations of keystrokes
• Work well on physical keyboards
  – But not on software keyboards
Keylogger for Soft Keyboard

• New out of band channel on smartphones
  – Accelerometers
  – Gyroscopes
• Insight: motion sensor data can infer keystrokes
Threat Model

- Keylogger can read motion sensor
  - Most users do NOT regard motion sensors as sensitive data source
  - W3C’s DeviceOrientation Event Specification allows web applications to read motion sensors via JavaScript
    - supported by both Android 3.0 and iOS 4.2
- User does NOT place phone on fixed surface
Modeling Typing-Induced Motion

• Shift is affected by
  – Striking force of the typing finger
  – Resistance force of the supporting hand

• Rotation is affected by
  – Landing location of the typing finger
  – Location of the supporting hand on the phone

• We observe
  – Shift is more likely user dependent
  – Rotation is more likely user independent
Device Orientation

• Device orientation event consists of
  – $\alpha$: Device rotates along $z$-axis (perpendicular to the screen plane)
  – $\beta$: Device rotates along $x$-axis (parallel to the shorter side of screen)
  – $\gamma$: Device rotates along $y$-axis (parallel to the longer side of screen)
• We use only $\beta$ and $\gamma$
Feature Extraction

[Graph showing the relationship between pitch angle (β) and roll angle (γ) with labeled key points (0-9)].

- Upper Vertex
- Lower Vertex
- Key points (0-9)
Feature Extraction
Evaluation

• HTC Evo 4G smartphone
• Digits 0 ... 9 on number-only soft keyboard
Results

• Collected 3 datasets
  – 2 smaller datasets for training
  – The largest dataset (449 keystrokes) for testing

• Correctly inferred 321 out of 449 (71.5%) keystrokes.
### Detailed Inference Results

<table>
<thead>
<tr>
<th>Actual Key</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>64%</td>
<td>-</td>
<td>6%</td>
<td>10%</td>
<td>-</td>
<td>12%</td>
<td>-</td>
<td>-</td>
<td>8%</td>
<td>-</td>
</tr>
<tr>
<td>1</td>
<td>-</td>
<td>86.3%</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>13.7%</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>2</td>
<td>8.3%</td>
<td>4.2%</td>
<td>68.8%</td>
<td>-</td>
<td>4.2%</td>
<td>-</td>
<td>2.1%</td>
<td>3.1%</td>
<td>4.2%</td>
<td>6.2%</td>
</tr>
<tr>
<td>3</td>
<td>18%</td>
<td>-</td>
<td>-</td>
<td>70%</td>
<td>-</td>
<td>-</td>
<td>6%</td>
<td>-</td>
<td>-</td>
<td>6%</td>
</tr>
<tr>
<td>4</td>
<td>-</td>
<td>10%</td>
<td>8%</td>
<td>-</td>
<td>72%</td>
<td>2%</td>
<td>-</td>
<td>8%</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>5</td>
<td>8%</td>
<td>4%</td>
<td>4%</td>
<td>8%</td>
<td>-</td>
<td>60%</td>
<td>-</td>
<td>-</td>
<td>12%</td>
<td>-</td>
</tr>
<tr>
<td>6</td>
<td>-</td>
<td>-</td>
<td>1.9%</td>
<td>7.5%</td>
<td>-</td>
<td>1.9%</td>
<td>77.4%</td>
<td>-</td>
<td>-</td>
<td>11.3%</td>
</tr>
<tr>
<td>7</td>
<td>2%</td>
<td>-</td>
<td>4%</td>
<td>-</td>
<td>16%</td>
<td>14%</td>
<td>-</td>
<td>56%</td>
<td>8%</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>-</td>
<td>-</td>
<td>10%</td>
<td>-</td>
<td>-</td>
<td>15%</td>
<td>-</td>
<td>-</td>
<td>75%</td>
<td>-</td>
</tr>
<tr>
<td>9</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>3.8%</td>
<td>-</td>
<td>3.8%</td>
<td>11.5%</td>
<td>-</td>
<td>-</td>
<td>80.8%</td>
</tr>
</tbody>
</table>
Training Set Size

![Graph showing the relationship between the size of the training set and the mean of AUB, ALB, AU, and AU/AL for both upper and lower lobe widths.](image)
Conclusion

• Motion sensors on smart phones may reveal keystrokes
• Need to protect motion sensors as diligently as other sensors