Background

www.eMarketer.com

4 digits PIN
PatternLock
No

Smartphone

Shoulder surfing attack

Photo Audio Video
SMS Call Email
Payment Location
SNS Blog IM
… …
Existing Solutions

**Indirect Entry Mechanism**

- **Human-computable challenge-response**
  - Keypad layout
  - Additional factors
    - Colors
    - Symbols
    - Directions
- **Physical block**
- **Eye tracking**
- **Tactile sensor**
- **Pressure sensor**
- **Vibration sensor**
- **Back-of-Device interface**

**Direct Entry**

- **Visible Channel**
  - **1245**
  - **Bob**
  - **Enter Passcode**
  - **1245**

**Invisible Entry Mechanism**

**Special human-computer Interface**

**Computing burden**

**Memory burden**
SlidePIN Concepts

**Slide-based PIN Entry Mechanism**

**Random Keypad**

Input with random numeric keypad is more secure

**Slide**

**Slide input is faster**

**Slide input is more secure**

PIN: 1245

SlidePIN: *381629458#
Model Design

PIN: 1245

Layout 1
Trajectory 1
Sequence 1
*381629458#

Layout 2
Trajectory 2
Sequence 2
*1472341859#

Slide Map Function

\[ F ( \text{PIN}, \text{Layout} ) \rightarrow \text{Sequence} \]

Attack Function

One-Time
\[ F^{-1}(\text{Sequence 1}) \rightarrow \text{PIN} \]

Multi-Time
\[ F^{-1}(\text{Sequence 1, Sequence 2, \ldots, Sequence n}) \rightarrow \text{PIN} \]
Sequence Length: No limit

Sequence Length Experiment

20*6

Avg Dist Between Keys
Sequence Length Analysis

Unlock Experiment

20*6*4

Group 1,2,3,4

Unlock Time
Error Rate

LCS Analysis

Group 4

20 students

Sequence Length: 9-15

Unlock Time

10*6

Group 1,2,3,4

Attack Experiment

Group Input Keypad

<table>
<thead>
<tr>
<th>Group</th>
<th>Input</th>
<th>Keypad</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click</td>
<td>Traditional</td>
</tr>
<tr>
<td>2</td>
<td>Click</td>
<td>Random</td>
</tr>
<tr>
<td>3</td>
<td>Slide</td>
<td>Traditional</td>
</tr>
<tr>
<td>4</td>
<td>Slide</td>
<td>Random</td>
</tr>
</tbody>
</table>

20 students

20*6
Sequence Length Analysis

**Too long**

*0123456789 0123456789 0123456789 0123456789 #*

**Why**

*3816279450#*

*381629450#*

**Too short**

*31629450#*

**How**

20 students
* 6 times

---

**Estimate of Distance between Keys**

\[
D(A) = (1.03 + 2.24 + 1.11 + 2.08 + 3.03 + 2.25 + 2.84 + 4.00 + 3.33 + 3.83 + 4.88) \approx 2.78
\]
Sequence Length Analysis

(a)  

(b)  

(c)  

\[ D(B) = 2.38 \]
\[ D(C) = 2.25 \]
\[ D(D) = 1.87 \]

\[ D_{avg} = \frac{(D(A) \times 2 + D(B) \times 2) + D(C) \times 4 + D(D) \times 2) \}{10} \approx 2.31 \]

\[ P(Z3) = 1 \]
\[ D(Z3) = 11.55 \]
\[ P(Z2) = 1/6 \]
\[ D(Z2) = 10.82 \]
\[ P(Z1) = 1/200 \]
\[ D(Z1) = 8.08 \]

\[ 8.08 \times 1.87 \approx 15.11 \]

9 - 15
Sequence Length Analysis

- **Estimate of Sequence Length**
  - Mean value of sequence length: 11.55 vs 11.46
  - Lower threshold of sequence length: 9
  - Upper threshold of sequence length: 15
# Security Analysis

- **Shoulder surfing attack**

<table>
<thead>
<tr>
<th>Sequence Length</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
</tr>
</thead>
<tbody>
<tr>
<td>PIN</td>
<td>126</td>
<td>210</td>
<td>330</td>
<td>495</td>
<td>715</td>
<td>1001</td>
<td>1365</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Times</th>
<th>u1</th>
<th>u2</th>
<th>u3</th>
<th>u4</th>
<th>u5</th>
<th>u6</th>
<th>u7</th>
<th>u8</th>
<th>u9</th>
<th>u10</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>6</td>
<td>7</td>
<td>6</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Guessing attack**
  - Brute force attack
  - Dictionary attack

- **Replay attack**
  - Random numeric keypad
Usability Analysis

- **Orientation Time**

<table>
<thead>
<tr>
<th>Groups</th>
<th>Average</th>
<th>Standard Deviation</th>
<th>Threshold Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.687</td>
<td>0.133</td>
<td>0.989</td>
</tr>
<tr>
<td>2</td>
<td>1.064</td>
<td>0.199</td>
<td>1.510</td>
</tr>
<tr>
<td>3</td>
<td>0.798</td>
<td>0.293</td>
<td>1.846</td>
</tr>
<tr>
<td>4</td>
<td>1.186</td>
<td>0.225</td>
<td>1.713</td>
</tr>
</tbody>
</table>
Usability Analysis

- **Unlock time**
  - *Sliding is faster*
  - *Input sequence become longer*
  - *Random number keypad increases unlock time*
Usability Analysis

• Error rate
  ✴ Sequence length limit
  ✴ Start point and end point
  ✴ No familiar enough

<table>
<thead>
<tr>
<th>Groups</th>
<th>Error Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1.67%</td>
</tr>
<tr>
<td>2</td>
<td>3.33%</td>
</tr>
<tr>
<td>3</td>
<td>7.69%</td>
</tr>
<tr>
<td>4</td>
<td>13.04%</td>
</tr>
</tbody>
</table>

• Cost of learning
  ✴ SlidePIN is build based on 4-digits PIN
  ✴ SlidePIN is easy to use
  ✴ SlidePIN is interesting to use
Discussion

1: Fixed start point and end point
2: Same adjacent Digits
3: PIN storage
4: Smudge attack
5: Attack based on Features

Device ID or SIM ID

Key

encrypt

PIN

PIN: 1245

PIN: 2118

*021939168#
SlidePIN performs better than 4-digits PIN against shoulder surfing attack.

At the same time, SlidePIN has acceptable usability.