KNOCK KNOCK, WHO’S THERE?

On the Security of LG’s Knock Codes

Raina Samuel**
New Jersey Institute of Technology

Philipp Markert
Ruhr University Bochum

Adam J. Aviv
The George Washington University

Iulian Neamtiu
New Jersey Institute of Technology

USENIX Symposium on Usable Privacy and Security (SOUPS)
August 10th 2020
LG KNOCK CODES: A DIFFERENT WAY TO UNLOCK

- Users select/recall a series of 6 to 10 “knocks” on a 2x2 grid
- Used with the screen off or on
- We estimate 700,000–2,500,000 users in the US alone
How *secure* and *usable* are Knock Codes?
Two online user studies using Amazon Mechanical Turk

Desktop browser study

Mobile only with three treatments:
- control
- blocklist
- larger grid size

1,138 Knock Codes were analyzed

Main Study

Preliminary Study

Security Analysis

Usability Analysis

n=218

n=351

Each participant created two Knock Codes
## SECURITY ANALYSIS: PERFECT KNOWLEDGE ATTACKER

Has complete knowledge of the frequency order Knock Codes, from most to least frequent.

<table>
<thead>
<tr>
<th></th>
<th>3 guesses</th>
<th>10 guesses</th>
<th>30 guesses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>14.2%</td>
<td>28.0%</td>
<td>51.3%</td>
</tr>
<tr>
<td><strong>Blocklist</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.9%</td>
<td>16.0%</td>
<td>35.4%</td>
</tr>
<tr>
<td><strong>Large</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.9%</td>
<td>31.5%</td>
<td>53.4%</td>
</tr>
</tbody>
</table>

### Partial Guessing Entropy (bits)

<table>
<thead>
<tr>
<th></th>
<th>$\alpha=0.1$</th>
<th>$\alpha=0.2$</th>
<th>$\alpha=0.5$</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control</strong></td>
<td>4.20</td>
<td>4.79</td>
<td>5.69</td>
</tr>
<tr>
<td><strong>Blocklist</strong></td>
<td>5.79</td>
<td>6.03</td>
<td>6.72</td>
</tr>
<tr>
<td><strong>Large</strong></td>
<td>4.53</td>
<td>4.70</td>
<td>5.54</td>
</tr>
</tbody>
</table>
Knows a subset of the Knock Codes and constructs a model based on that observed distribution.
**USABILITY ANALYSIS:**

### Entry Time

<table>
<thead>
<tr>
<th>Method</th>
<th>Entry Time (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knock Code (Control)</td>
<td>7.1</td>
</tr>
<tr>
<td>PIN*</td>
<td>4.2</td>
</tr>
<tr>
<td>Android Pattern*</td>
<td>3.0</td>
</tr>
</tbody>
</table>

*Using a blocklist does not affect general entry time*

### Recall Rates

<table>
<thead>
<tr>
<th>Method</th>
<th>Recall Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control</td>
<td>88.8%</td>
</tr>
<tr>
<td>Blocklist</td>
<td>80.6%</td>
</tr>
<tr>
<td>Large</td>
<td>92.9%</td>
</tr>
</tbody>
</table>

*However, other methods such as PINs and patterns have a recall rate of 95%* or higher

---

*Harbach et al. "It's a hard lock life: a field study of smartphone (un)locking behavior and risk perception" SOUPS 2014

*Markert et al. "This PIN can be easily guessed" IEEE Symposium on Security and Privacy 2020*
USABILITY ANALYSIS:
User Responses

“EASY”  “DISCREET”
“HARD TO GUESS”
“DIFFERENT”  “QUICK”

“HARD TO REMEMBER”
“INSECURE”
“NOT AN IMPROVEMENT”
“HARD TO TYPE”
First user study and security analysis of Knock Codes

- Knock Codes offer less security relative to other mobile authentication
- Participants find Knock Codes mostly unusable and insecure
- Using a blocklist with Knock Codes improves security
- Participants are open to new methods of mobile authentication
Thank you! Feel Free to Contact us!

Raina Samuel  
res9@njit.edu

Philipp Markert  
philipp.markert@rub.de

Adam J. Aviv  
aaviv@gwu.edu

Iulian Neamtiu  
ineamtiu@njit.edu