This PIN Can Be Easily Guessed
Analyzing the Security of Smartphone Unlock PINs

Philipp Markert, Daniel V. Bailey, Maximilian Golla, Markus Dürmuth, and Adam J. Aviv
Overview

Why study PINs?

User Study

Results

Agenda

Practice

Priming

Creation
Why PINs?

- Fingerprint
- Face
- Iris

PHOTO: Dan Seifert | The Verge (Vox Media)
Who uses PINs?

1220 participants

210 use a PIN
461 do not use a biometric

759 use a biometric
595 use a PIN

Overall 805 (66%) use a PIN

595 use a PIN
210 use a PIN
461 do not use a biometric
759 use a biometric
What we know about PINs

- User chosen 4-digit PINs are predictable [1]
- User chosen 6-digit PINs aren’t any better [2]
- Blacklisting popular PINs can increase security [1]

What we don’t know

- How secure are 4- or 6-digit PINs in the smartphone unlock setting?
- What are the effects of different blacklists on the security of PINs?
- How to balance security and usability when composing a blacklist?

This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs

Treatments

No Blacklist

4-digit

1. Control

2. Placebo

3. iOS

4. DD Small

5. DD Large

Blacklist

6-digit

6. Control

7. Placebo

8. iOS

Placebo

“Test general effect of warning”

Blacklist:

- “1st choice” blocked
- Any other PIN allowed

iOS

“Test effect of iOS blacklists”

Blacklist:

- 274 PINs (4-digit)
- 2910 PINs (6-digit)

Data-Driven (DD)

“Test effect of different blacklist sizes”

Blacklist:

- Top 27 PINs of Amitay (small)
- Top 2740 PINs of Amitay (large)
This PIN Can Be Easily Guessed: Analyzing the Security of Smartphone Unlock PINs
User Study

Consent → Priming → PIN Creation

Create a 4-digit PIN
A PIN protects your data and is used to unlock your smartphone.

This PIN Can Be Easily Guessed
Your PIN will be used to unlock your smartphone and to protect access to your data.
Attacker Model

- No information about the victim
Attacker Model

- No information about the victim
- Guesses PINs in decreasing probability order

<table>
<thead>
<tr>
<th>Rank</th>
<th>4-digit PINs</th>
<th>6-digit PINs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1234</td>
<td>123456</td>
</tr>
<tr>
<td>2</td>
<td>0000</td>
<td>123123</td>
</tr>
<tr>
<td>3</td>
<td>2580</td>
<td>111111</td>
</tr>
</tbody>
</table>
Attacker Model

- No information about the victim
- Guesses PINs in decreasing probability order
- Slowed down by rate-limiting

<table>
<thead>
<tr>
<th></th>
<th>Android</th>
<th>iOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Guesses</td>
<td>30s</td>
<td>1h 36m 0s</td>
</tr>
<tr>
<td>100 Guesses</td>
<td>10h 45min 30s</td>
<td>—</td>
</tr>
</tbody>
</table>
### Attacker Model

- **No information about the victim**

- **Guesses PINs in decreasing probability order**

- **Slowed down by rate-limiting**

- **Knows the blacklist and skips impossible choices**

<table>
<thead>
<tr>
<th>Rank</th>
<th>4-digit PINs</th>
<th>6-digit PINs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1234</td>
<td>123456</td>
</tr>
<tr>
<td>2</td>
<td>0000</td>
<td>not allowed</td>
</tr>
<tr>
<td>3</td>
<td>2580</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td></td>
</tr>
</tbody>
</table>

#### This PIN Can Be Easily Guessed

Your PIN will be used to unlock your smartphone and to protect access to your data.

[Change PIN]
Research Questions

RQ1: How secure are 4- and 6-digit PINs in the smartphone unlock setting?

RQ2: What are the effects of different blacklists on the security of PINs?

RQ3: How to balance security and usability when composing a blacklist?
RQ1: 4- vs. 6-digit PINs

Observations:

- Overall comparable security of 4- and 6-digit PINs in the defined attacker model
- Differences depending on the number of guesses
RQ2: Different Blacklist Sizes

Observations:

- **iOS and Data-Driven Small** offer comparable security.
- **Data-Driven Large** drastically increases the security.
- **Blacklist Hitrate:**
  - DD Small 5%
  - iOS 15%
  - DD Large 70%
RQ3: Balancing Security and Usability

Observations:

- Different extrema throughout the curve
- Maxima: users choose popular PINs
- Minima: users choose unpopular PINs
- Blacklisting ~10% is ideal
**Takeaways**

**Why study PINs?**

- **No biometric**
  - Most of the participants in our study (66%) use a PIN

- **Biometric**

**User Study**

- **Agenda**
- **Priming**
- **Practice**
- **Creation**

**Results**

- **4 ≈ 6** Security of 4- and 6-digit PINs is comparable
- **XXL** Blacklists need to be large to have an effect
- **Blacklisting ~10% is ideal**

---

**User Study**

- **No biometric**
  - Most of the participants in our study (66%) use a PIN

**Results**

- **4 ≈ 6** Security of 4- and 6-digit PINs is comparable
- **XXL** Blacklists need to be large to have an effect
- **Blacklisting ~10% is ideal**

---

**Contact:**

- philipp.markert@rub.de
- @philipp_markert
- https://this-pin-can-be-easily-guessed.github.io