Cracking Android Pattern Lock in 5 Attempts

Guixin Ye

Northwest University (China), Lancaster University (UK), Bath University (UK)
Attacking Scenario

- Alice and Bob go to a party (or library etc.)
- Alice leaves her phone unattended for a few minutes, thinking this is okay as she uses pattern lock protection.

Can Bob quickly install malware on Alice’s phone?
How can Bob bypass pattern lock?

Bob only need to observe the fingertip movement!
Evil Bob films how Alice draws the pattern from a distance of 2-3 meters. No need to see the screen content. 😈
Tracking

Bob marks two areas of interest, and runs a vision algorithm to track the fingertip movement.
Tracking Example

The pattern

Tracking algorithm

Resulted fingertip movement trajectory

Bob wants this!
View Transformation

Camera’s perspective

\[ S = TS_1 \]

\[ T = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \]

User’s perspective
Trajectory to Candidate Patterns

Fingertip Trajectory

Candidate Patterns
A large number of possibilities!

Fingertip Trajectory

Possible Patterns (>100)
Use Geometric information

Pattern Lock = Line Length + Line Direction
Example: Identify Candidate Patterns

Rejected patterns

Candidate patterns

Length & Direction

Length & Direction
Test on Alice’s Phone

Correct pattern
Another Example

Pattern Trajectory

Complex Pattern
Evaluation Setup

120 patterns from 215 users
plus
some of the most complex patterns

Other pattern grids

Xiaomi MI4, Meizu2, Huawei Honor7, Samsung Note4
Example Patterns

Simple

Medium

Complex
Complex patterns are less secure

Over 95% of the patterns can be cracked in 5 attempts
Up to 5 candidate patterns generated

For most median and all complex patterns, our system produces just ONE candidate pattern.
Threat distance reaches 2.5m

Over 80% of the patterns can be cracked within a distance of 2.5 meters away from the target device.
More dots helps, but only for simple patterns.
Conclusions

Pattern lock is vulnerable under video based attacks

Complex patterns could be less secure

Data available at:
https://dx.doi.org/10.17635/lancaster/researchdata/113
Related work
Camera Shake
How to identify candidate pattern
How to define the complexity of pattern lock
Video recording devices
Existing Researches on Pattern Lock

Smudge Attack

Wireless-based Attack
Video-based Attacks on PIN- or text-based passwords

Text-based: Directly facing the keyboard or the screen

PIN-based: The dynamics of hand during typing
Pattern Lock v.s. PIN- or text-based password

How to map the fingertip movements to a graphical structure?
Existing attacks methods cannot be used to crack pattern lock

How can the algorithm adapt to the different size of pattern grid

Overlapping lines  Different size of pattern grid
Camera Shake Effect

Unique pattern ➔ Tracking process ➔ Expected trajectory

Actual trajectory
Camera Shake Calibration

Correct pattern

w/ camera shake calibration
Solution: Identify Candidate Patterns

$CP = \{L; D\}
(l_1, l_2, l_3; d_{l_1}, d_{l_2}, d_{l_3})$

- $L$ is the collection of the relative line segments.
- $D$ is collection of the directions corresponding to the line segment.
Example: Extracting Geometric Features

Length Feature

\[ L : (l_{ST_1}, l_{T_1T_2}, l_{T_2E}) \]

\[ D : (5, 11, 5) \]

Direction Feature

All line directions
Pattern Collection and Category

$CS\downarrow P = S\downarrow P \times \log_2 (L\downarrow P + I\downarrow P + O\downarrow P)$

- $S\downarrow P$ is the number of connected dots
- $L\downarrow P$ is the total length of all line segments that form the pattern
- $I\downarrow P$ are the number of intersections
- $O\downarrow P$ are the number of overlapping linear segments

- Simple pattern (40): $S\downarrow P \in [6.34, 19)$
- Median Pattern (40): $S\downarrow P \in [19, 33)$
- Complex pattern (40): $S\downarrow P \in [33, 46.8)$
Video Recording

- **User Participation**
  10 postgraduate: 5 male and 5 female students

- **Test Phones**

<table>
<thead>
<tr>
<th>Size</th>
<th>Brands</th>
<th>Xiaomi MI4</th>
<th>Huawei Honor7</th>
<th>Samsung Note4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Height(cm)×Height(cm)</td>
<td>13.9×6.9</td>
<td>14.3×7.2</td>
<td>15.4×7.9</td>
<td></td>
</tr>
</tbody>
</table>

- **Record Device**
  Apple iPhone4S, Xiaomi MI4 and Meizu2