Using Graphics and Gestures to Improve Knowledge-based Authentication for Mobile Devices

Emanuel von Zezschwitz
Emanuel.von.zezschwitz@ifi.lmu.de
Motivation

- Pictures, Videos
- Online Banking
- Online Shopping
- E-Mail, Messaging
- Business Data
Authentication on Mobile Devices

- PIN: Usable, Secure
- Password: Usable, Secure
- Pattern: Usable, Secure
- Face: Usable, Secure
- Finger: Usable, Secure

Emanuel von Zeiswitz
(emanuel.von.zeiswitz@ifi.lmu.de)
What about Biometrics?

“It is plain stupid to use something that you can’t change and that you leave everywhere every day as a security token“  
Frank Rieger (CCC)

“Touch ID is designed to minimize the input of your passcode; but your passcode will be needed for additional security validation: After restarting your iPhone 5s [or] when more than 48 hours have elapsed from the last [unlock]“  
Apple Support
Requirements

Passwords have to be
- easy to remember
- hard to guess

Interaction has to be
- hard to observe
- fast & easy

Large practical password space

Emanuel von Zezschwitz
(emanuel.von.zezschwitz@ifi.lmu.de)
Graphical / Gesture-based Passwords

Advantages:
✓ Well suited for touchscreens
✓ Not based on user data
✓ Motor memory
✓ Pictorial superiority effect
✓ More joyful for most users

Emanuel von Zeischwitz
(emanuel.von.zezschwitz@ifi.lmu.de)
Graphical / Gesture-based Passwords

Advantages:
✓ Well suited for touchscreens
✓ Not based on user data
✓ Motor memory
✓ Pictorial superiority effect
✓ More joyful for most users

Drawbacks:
☒ Prone to shoulder surfing
☒ Prone to smudge attacks
☒ Weak passwords? Metrics?

Emanuel von Zeiswitz
(emanuel.von.zeiswitz@ifi.lmu.de)
User-centered Approach

Understand User Behavior & Perception

Emanuel von Zeiswitz
(emanuel.von.zezschwitz@ifi.lmu.de)
User-centered Approach

Understand User Behavior & Perception

Develop Concepts
User-centered Approach

Understand
User Behavior & Perception

Develop
Concepts

Generalize
Results

Emanuel von Zeuschwitz
(emanuel.von.zezschwitz@ifi.lmu.de)
Understanding
Behavior & Perception
User Behavior & Perception

1. [MobileHCI 2013]

2. [SOUPS 2014]

3. [NordiCHI 2014]

Emanuel von Zeischwitz
(emanuel.von.zeischwitz@ifi.lmu.de)
Smartphone (Un)Locking Behavior and Risk Perception

- How, why and in which situations do people use lock screens?
- How often do people access sensitive data?
- Is shoulder surfing and unwanted access an issue?
(Un)lock Frequency

- 83 Activations / Day (sd=43)
- 48 Unlocks / Day (sd=26)
Session Length

Average Session: 70 sec
- Unlocked Device: 104 sec
- Locked Device: 12 sec
Session Length

43 hours smartphone use:
- 2.9 hours on a locked devices
- 1.2 hours unlocking the device

⇒ Overhead: 2.9% (0.6 - 9%)
Shoulder Surfing

- Possible in 17% of all sampled situations
- Likely in 41%, Critical in 19%
- Mostly known persons in private environments
- Considered likely AND critical in 0.3%
Key Results

- Every Additional Second Has an High Impact: Unlock Mechanisms Must be (Perceived) Very Fast
Key Results

- Every Additional Second Has an High Impact: Unlock Mechanisms Must be (Perceived) Very Fast
- Users are Often Dissatisfied with their Current Configuration: The Security Level Should Adapt to the Context
Key Results

- Every Additional Second Has an High Impact: Unlock Mechanisms Must be (Perceived) Very Fast
- Users are Often Dissatisfied with their Current Configuration: The Security Level Should Adapt to the Context
- Sensitive Data is Seldom Accessed: Unlock Mechanisms Should be Content-dependent
Key Results

- Every Additional Second Has an High Impact: Unlock Mechanisms Must be (Perceived) Very Fast
- Users are Often Dissatisfied with their Current Configuration: The Security Level Should Adapt to the Context
- Sensitive Data is Seldom Accessed: Unlock Mechanisms Should be Content-dependent
- Shoulder Surfing Risks are Perceived Low: Shoulder Surfing Resistance Must Not Reduce Performance
Designing Solutions
Design & Evaluate Solutions

1

[IUI 2013]

2

[CHI 2013/2014]

Emanuel von Zeischwitz
(emanuel.von.zezschwitz@ifi.lmu.de)
Smudge Attack Protection

Emanuel von Zezschwitz
Android 90°
Marble

Emanuel von Zezschwitz
Marble
Speed (quantitative)

![Bar chart showing time in seconds for different tasks]

- Android Pattern
- Pattern Rotation
- Marbles
- Marble Gap

- Orientation
- Input
- Given
- Selected

Emanuel von Zezschwitz
Speed (qualitative)

- **Android Pattern**
  - Very Good: 12
  - Good: 8
  - Satisfactory: 4

- **Marble Gap**
  - Very Good: 5
  - Good: 12
  - Satisfactory: 7

- **Marbles**
  - Very Good: 8
  - Good: 10
  - Satisfactory: 5
  - Adequate: 1

- **Pattern Rotation**
  - Very Good: 1
  - Good: 8
  - Satisfactory: 6
  - Adequate: 6
  - Poor: 2
  - Bad: 1

Emanuel von Zezschwitz
Speed (quantitative)

- Android Pattern
- Pattern Rotation
- Marbles
- Marble Gap

<table>
<thead>
<tr>
<th>Time [sec]</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.0</td>
</tr>
<tr>
<td>1.0</td>
</tr>
<tr>
<td>2.0</td>
</tr>
<tr>
<td>3.0</td>
</tr>
<tr>
<td>4.0</td>
</tr>
<tr>
<td>5.0</td>
</tr>
<tr>
<td>6.0</td>
</tr>
<tr>
<td>7.0</td>
</tr>
<tr>
<td>8.0</td>
</tr>
<tr>
<td>9.0</td>
</tr>
</tbody>
</table>

- Orientation
- Input
- Given
- Selected

Emanuel von Zezschwitz
Pattern 90 II: Four Connect

Emanuel von Zezschwitz
Marbles II: Story-based
Field Performance

Erfolgsquote (interpretiert)

- Android Standard
- Connect Four
- Marble Story

Emanuel von Zezschwitz
Field Performance

Gesamtzeit der Eingabe (interpretiert)

Android Standard
Connect Four
Marble Story

Emanuel von Zezschwitz
Key Results

- 83%-100% of the Android patterns were exposed
Key Results

- 83%-100% of the Android patterns were exposed
- Presented concepts are significantly more secure and equally good concerning ease-of-use and perceived speed
Key Results

- 83%-100% of the Android patterns were exposed
- Presented concepts are significantly more secure and equally good concerning ease-of-use and perceived speed
- Orientation time is more critical than input time
Key Results

- 83%-100% of the Android patterns were exposed
- Presented concepts are significantly more secure and equally good concerning ease-of-use and perceived speed
- Orientation time is more critical than input time
- Input complexity influences password composition

Emanuel von Zeischwitz
(emanuel.von.zeischwitz@ifi.lmu.de)
Key Results

- 83%-100% of the Android patterns were exposed
- Presented concepts are significantly more secure and equally good concerning ease-of-use and perceived speed
- Orientation time is more critical than input time
- Input complexity influences password composition
- Authentication methods need to be evaluated in the field
Summary

Current & Future Projects

- The Impact of Pattern Composition on Theoretical and Practical Security
- How to Compute and Increase the Strength of User-selected Grid-based Passwords
Thank You

emanuel.von.zezschwitz@ifi.lmu.de

www.mimuc.de/team/
PIN vs. Pattern

A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices
Speed

PIN: 1.5s  Pattern: 3.1s
Speed

Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices

- **Pattern was fast**
  - Disagree: 3
  - Agree: 10, 16

- **PIN was fast**
  - Disagree: 1, 1
  - Agree: 7, 15

- **Pattern was efficient**
  - Disagree: 3
  - Agree: 10, 16

- **PIN was efficient**
  - Disagree: 1, 3
  - Agree: 9, 11
Speed

Pattern was fast
- Pattern: 3, 10, 16
- PIN: 1, 7, 15

PIN was fast
- Pattern: 3, 10, 16
- PIN: 1, 7, 15

Pattern was efficient
- Pattern: 3, 10, 16
- PIN: 1, 7, 15

PIN was efficient
- Pattern: 3, 10, 16
- PIN: 1, 7, 15

disagree  |  agree
Errors

PIN: 8  Pattern: 99
Errors

Pattern easy to use
- 2% disagree
- 10% agree

PIN easy to use
- 3% disagree
- 10% agree

Pattern easy to recover
- 1% disagree
- 2% agree
- 7% neutral
- 19% agree

PIN easy to recover
- 1% disagree
- 1% agree
- 9% neutral
- 5% agree
Errors

- **Pattern easy to use**
  - Disagree: 2
  - Agree: 10
  - Neutral: 17

- **PIN easy to use**
  - Disagree: 3
  - Agree: 10
  - Neutral: 11

- **Pattern easy to recover**
  - Disagree: 1
  - Agree: 19
  - Neutral: 7

- **PIN easy to recover**
  - Disagree: 1
  - Agree: 8
  - Neutral: 9

Patterns in the Wild: A Field Study of the Usability of Pattern and PIN-based Authentication on Mobile Devices
Key Results

- Patterns are slower and more error prone, but people do not perceive the difference.

- Fast error recovery is more important than error prevention for most users.

- Taxonomy for pattern-based errors.