PassApp
My App is My Password!

Huiping Sun, Ke Wang, Xu Li, Nan Qin, Zhong Chen

Peking University
**Backgrounds**

- **Graphical Password**
  - more applicable on mobile devices than text passwords
  - vulnerable to shoulder surfing attacks
  - most existing graphical password schemes require users to actively memorize passwords

- Authentication based on existing memory
  - weak passwords
  - security questions
  - dynamic security questions
  - autobiographical authentication
PassApp Concept

PassApp is a novel recognition-based graphical password which utilizes users’ installed apps on their mobile devices as passwords.
PassApp Mechanisms

**Key App Selection Mechanism**

- **Decoy App Library**: Add decoy apps to the decoy app library.
- **Key App Library**: Add the key app to the key app library.

**Challenge Panel Generation Mechanism**

- **Authentication Mechanism**: Authenticate the user.

**Mobile Device**

- **App Update Mechanism**: Update apps.
- **Decoy App Selection Mechanism**: Select decoy apps.
- **Key App Selection Mechanism**: Select key apps.

**User**

- **Authenticate**: Rule out apps preinstalled by device and OS manufactures.

**App Market**

- **Install a new app**: Add this app to the key app library, add 3 decoy apps to the decoy app library.

- **Uninstall an app**: Delete this app from the key app library, move it into a blacklist, remove corresponding decoy apps from the decoy app library.

**Key : decoy = 1:3, same category, similar rankings, etc**
User Study

Day 1

User Study 1: How well can users correctly recognize the apps they have installed?

Day 2

User Study 2: How well can PassApp perform on usability?

42 participants

unlock 10 times 42 * 10

Login Time Success Rate
Memory about Installed Apps

Max: 79, Min: 11, SD: 16.79

\[ F_{\text{measure}} = \frac{P \times R}{P + R} \times 2 \]

\[ P(\text{precision}) = \frac{\sum \text{picked installed apps}}{\sum \text{all apps picked}} \]

\[ R(\text{recall}) = \frac{\sum \text{picked installed apps}}{\sum \text{all installed apps}} \]
Login Time and Success Rate

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Time</td>
<td>7s (5s-10s)</td>
<td>90-180s</td>
<td>72s</td>
<td>32-36s</td>
<td>14-88s</td>
</tr>
<tr>
<td>Success Rate</td>
<td>&gt;95%</td>
<td>90%</td>
<td>90-100%</td>
<td>72-100%</td>
<td>89-100%</td>
</tr>
</tbody>
</table>

Average login time: 7.27s

Average confirmation time: 0.76s
**Security Analysis**

**Brutal-force Attacks**

\[
1 / \binom{16}{4} = 1 / 1820, \\
\text{0.055%}
\]

**One-time shoulder Surfing Attacks**

\[
E = \sum_{i=0}^{4} \left( \frac{\binom{4}{i} \times \binom{s-4}{4-i}}{\binom{s}{4}} \right) \times i
\]

\[s = 31, E = 0.52\]

**Multi-time shoulder Surfing Attacks**

Monte Carlo Method

\[y = (-6.86) + 1.27x\]

\[R^2 = 0.9955\]
Session 1: Guessing Attacks
know nothing about the victims

Session 2: Acquaintance Attacks #1
Observe: 10 seconds/screen; break: 3 minutes; 5 login attempts

Session 3: Acquaintance Attacks #2
Observe: 10 seconds/screen; break: 3 minutes; 5 login attempts

Session 4: Acquaintance Attacks #3
Observe: 10 seconds/screen; break: 3 minutes; 5 login attempts

8 victims X 10 attackers X 5 login attempts = 400 attempts (each session)

<table>
<thead>
<tr>
<th>Session</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Successful Logins</td>
<td>3</td>
<td>68</td>
<td>127</td>
<td>186</td>
</tr>
<tr>
<td>Percentage</td>
<td>0.75%</td>
<td>17.00%</td>
<td>31.75%</td>
<td>46.50%</td>
</tr>
</tbody>
</table>

0.055% (theoretical)
Limitations of PassApp

- Key app selection
  - popular apps, communication apps

- Decoy app selection
  - app market, device manufacture, OS, language, etc

- Login time (challenge)
Conclusion

- **PassApp** is the first graphical password that utilizes user’s existing memory about installed apps as passwords
  - without a password registration stage
  - no extra memory burden
- **PassApp** performs better on login time and success rate than most graphical passwords
  - reasonable login time: 7.27s (6.51s when OK button is removed)
  - high success rate: >95%
- **PassApp** has sufficient security against common attacks
  - brute-force attacks (0.055%) and dictionary attacks (0.75%)
  - shoulder surfing attacks: average 30 times
  - acquaintance attacks: to some extent, it can withstand such attacks
Download PassApp for Android: sunhp.org/passapp/passapp.apk
or scan the QR Code and Download

Web: sunhp.org/passapp
Email: pass_app@yahoo.com

Information Security Lab of Peking University