Evaluating the Android Security Key Scheme: An Early Usability, Deployability, Security Evaluation with Comparative Analysis

Robbie MacGregor

5th Who Are You?! Adventures in Authentication (WAY), Santa Clara, CA, USA, 2019.
‘I did a thing so you don’t have to.’
- Me
Authentication and Passwords

Want to talk about passwords, password managers, password reuse, MFA, etc.?
• Convince your advisor/readers/audience that PASSWORDS AREN’T GOING ANYWHERE
• Address the ‘new hotness’
Android Security Keys

• Very new
• Very hot
• Is that even what they’re called?

Source: https://cloud.withgoogle.com/next/sf/sessions?session=SEC200
ASKs v. USB Security Keys

• Claim similar security benefits
• More convenient, etc.

Let’s prove it… UDS style!
## Usability, Deployability, Security

<table>
<thead>
<tr>
<th></th>
<th>Usability</th>
<th>Deployability</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Passwords</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Google 2-Step</td>
<td>o</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>USB Security Keys</td>
<td>o</td>
<td>o</td>
<td>•</td>
</tr>
<tr>
<td>Android Security Keys</td>
<td>o</td>
<td>o</td>
<td>o</td>
</tr>
</tbody>
</table>

- • = offers the benefit; o = almost offers the benefit; blank = does not offer the benefit; red = disputed.

Table 1: Comparative Usability, Deployability, Security Evaluations
Subjectively Similar

• Usability
  - convenience of quasi-nothing-to-carry
  - less efficient login task

• Deployability
  - differ or defer?

• Security
  - time for a closer look
A Closer Look

• No physical connection (I/O)
• No pairing
  - caBLE
Up Next

• Formal verifications
  - caBLE
  - unlinkability
  - POP
• Availability
• Interoperability
QUESTION TIME!

(Robbie MacGregor | macg@dal.ca)