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.

DALHOUSIE UNIVERSITY

‘I did a thing so you don’t have to.’

- Me

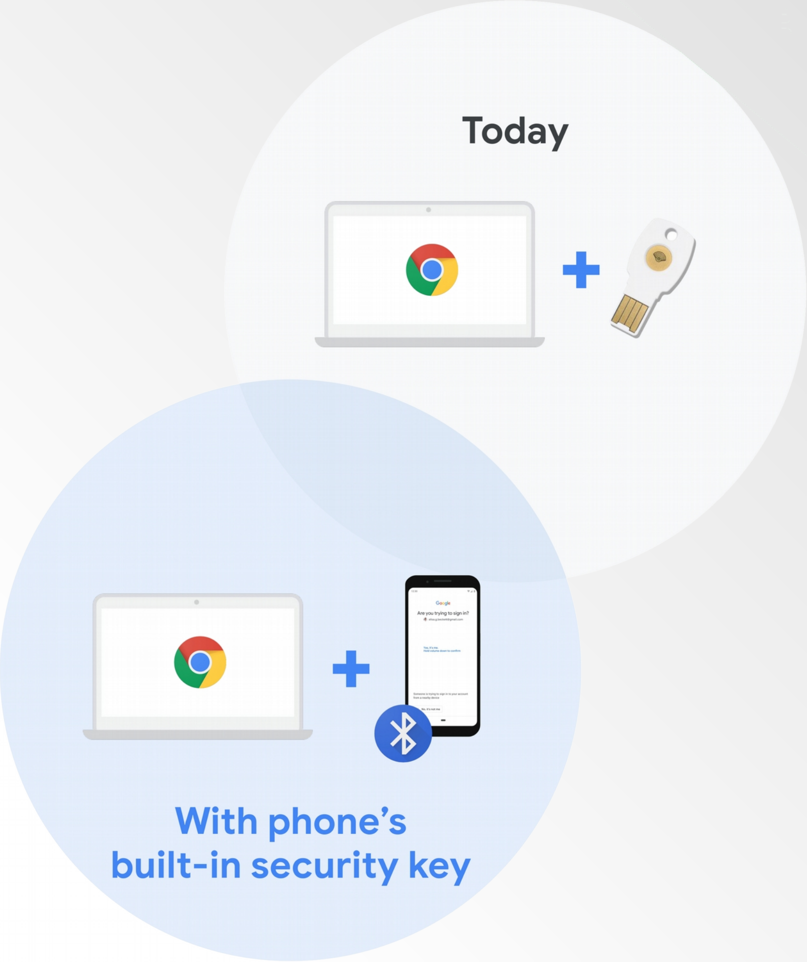
Authentication and Passwords

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?



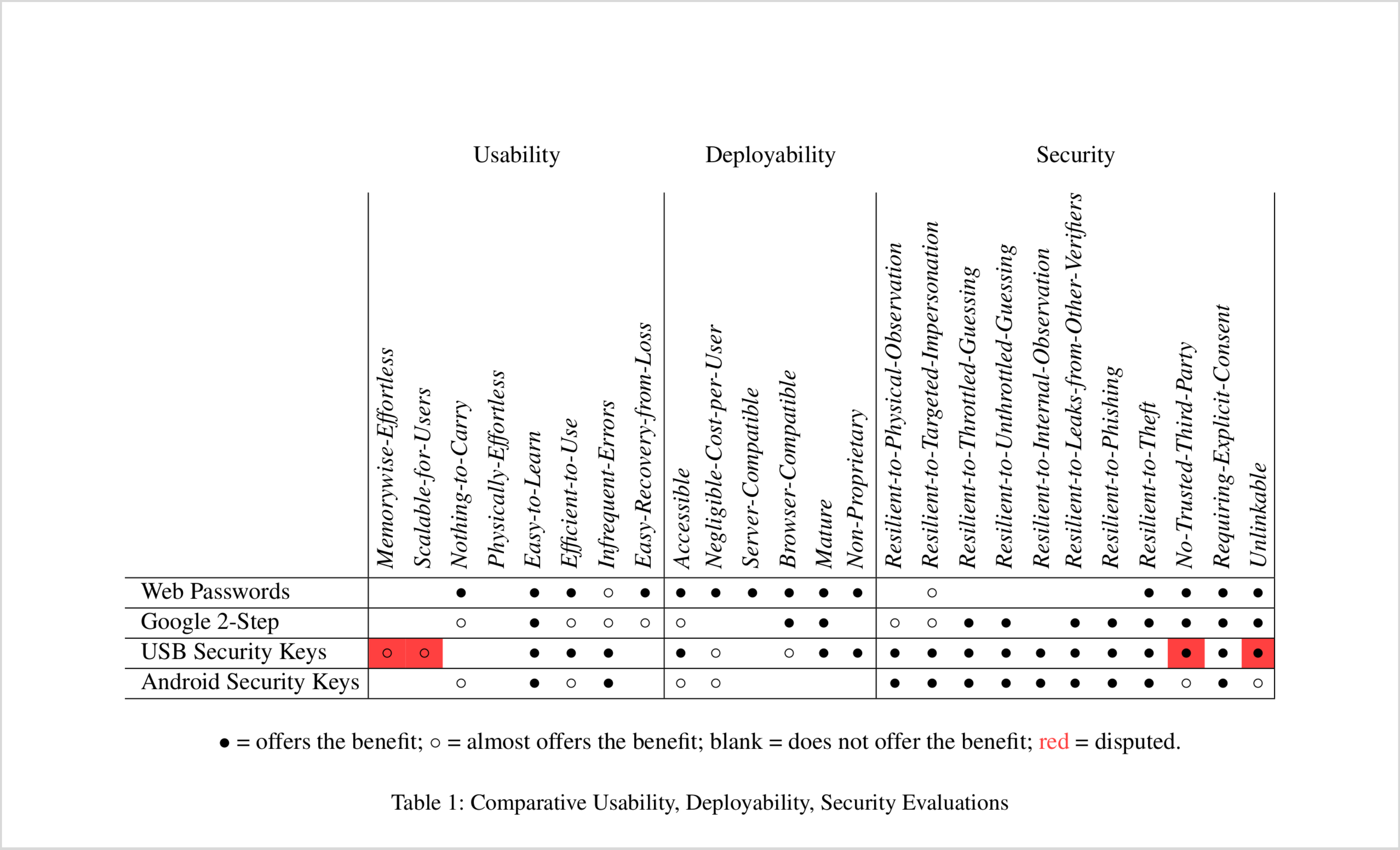
Source: https://cloud.withgoogle.com/next/sf/sessions?session=SEC200

ASKs v. USB Security Keys

- Claim similar security benefits
- More convenient, etc.

Let's prove it… UDS style!

Usability, Deployability, Security



	Usability								Deployability						Security										
	Memorywise-Effortless	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
Web Passwords			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Google 2-Step			○		●	○	○	○	○			●	●		○	○	●	●		●	●	●	●	●	●
USB Security Keys	🟥○	🟥○			●	●	●		●	○		○	●	●	●	●	●	●	●	●	●	●	🟥●	●	🟥●
Android Security Keys			○		●	○	●		○	○					●	●	●	●	●	●	●	●	○	●	○

● = offers the benefit; ○ = 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)