Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn

Leona Lassak, Annika Hildebrandt,
Maximilian Golla, Blase Ur

RUHR UNIVERSITÄT BOCHUM
THE UNIVERSITY OF CHICAGO
Max Planck Institute for Security and Privacy

Appeared at the 30th USENIX Security Symposium, Virtual Conference, August 2021

Study 1 | Identify Misconceptions

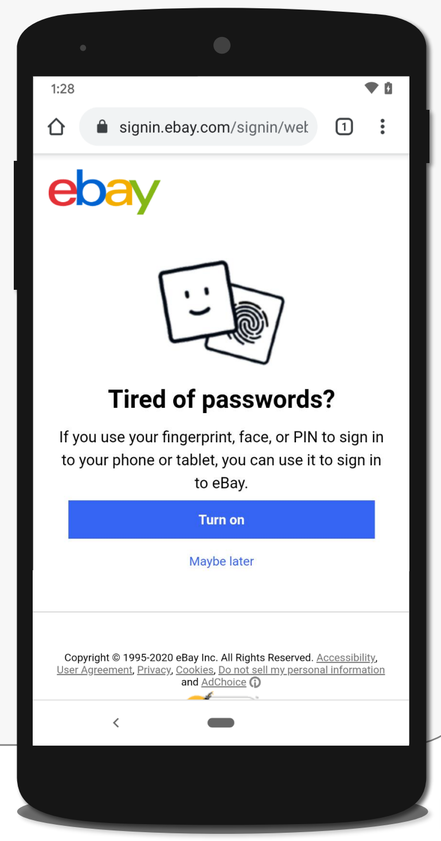
RQ What **misconceptions and understandings** do users hold during first use of **biometric FIDO2**?

METHOD

- Registration & authentication with biometric FIDO2 seeing *Baseline* notification
- Online survey about misconceptions, usability, and security perception
- 42 Prolific crowdworkers on personal smartphones

→ 67% think **biometric** data is **sent to website**
43% think **biometric** data is **not safe** from **attackers**
93% **unaware** of **fallback**

Baseline



[2]

FIDO2

Private key in TPM

Public key on server

Authentication:

1. User unlocks priv. key with biometrics
2. Device signs server challenge
3. Server uses pub. key to verify signature

Who even knows how FIDO2 works?

fido™ [1]

- No password
- Phishing resistant
- Biometrics stored locally

BUT

How should users know that?
How can we communicate FIDO2?
How can we increase adoption?

?

Study 2 | Develop Notifications

RQ What info do notifications need to mitigate misconceptions and communicate advantages best?

METHOD

- Online participatory co-design focus groups with 27 participants

→ **Four Themes:**

1. Convenience
2. Security
3. Comparison to passwords
4. Availability

"No one except you has access"

"Never leaves your phone"

"Only stored on your device"

Study 3 | Evaluate Notifications

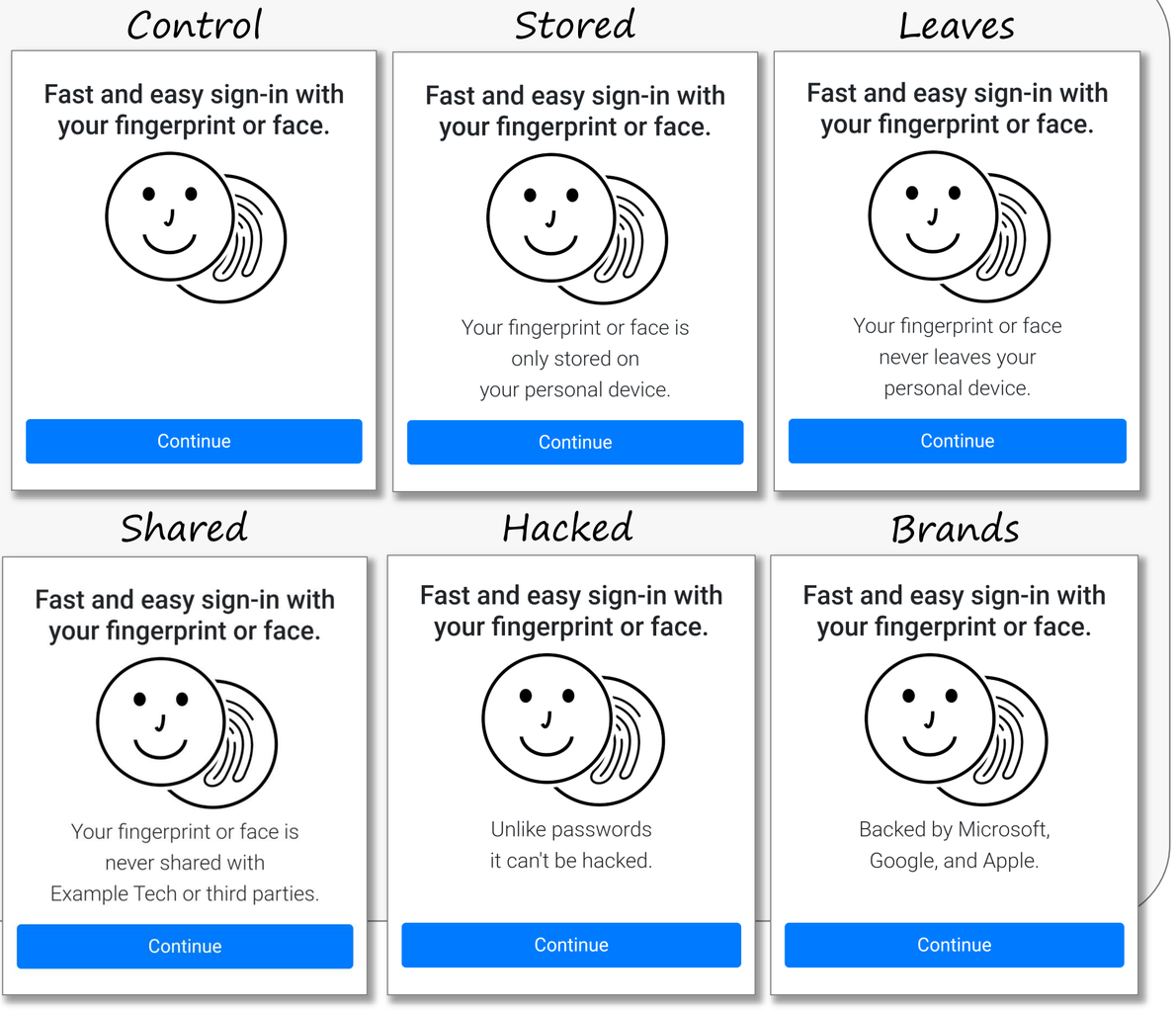
RQ Which notification mitigates the misconceptions best?

METHOD

- Registration & authentication with password, non-biometric FIDO2, or biometric FIDO2 testing 6 notifications
- 345 Prolific crowdworkers

→

- Biometric FIDO2 **perceived more secure** than non-biometric FIDO2 or password
- **Fewer** participants **think biometrics** are **sent to website** (Control 66% vs. Stored 45% & Leaves 50%)



References:
[1] FIDO Alliance Logo. fidoalliance.org/overview/legal/logo-usage/, July '22.
[2] ebay.com FIDO2 Login. signin.ebay.com, Jan. '21.
[3] USENIX Logo. usenix.org, July '22.