“It’s Stored, Hopefully, on an Encrypted Server”:

Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

Leona Lassak, Annika Hildebrandt, Maximilian Golla, and Blase Ur

August 11, 2021 | 30th USENIX Security Symposium
Tired of passwords?

If you use your fingerprint, face, or PIN to sign in to your phone or tablet, you can use it to sign in to eBay.

Turn on

Maybe later
"It’s Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn
"It’s Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn
Authentication | FIDO2 Protocol

Sign In

Challenge

Signed Challenge

Authorization

Private

Public

"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn
Advantages | WebAuthn

- Fast
- Nothing to remember
- Phishing resistant
Tired of passwords?

If you use your fingerprint, face, or PIN to sign in to your phone or tablet, you can use it to sign in to eBay.

Turn on

Maybe later
"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn

**STUDY 1**
- **Identify Misconceptions**
  - Task / Survey
  - 42 Participants

**STUDY 2**
- **Design Notifications**
  - 7 Focus Groups
  - 29 Participants

**STUDY 3**
- **Compare Notifications**
  - Experiment
  - 345 Participants
"It’s Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

**STUDY 1**

**Identify Misconceptions**
- Task / Survey
- 42 Participants

**STUDY 2**

**Design Notifications**
- 7 Focus Groups
- 29 Participants

**STUDY 3**

**Compare Notifications**
- Experiment
- 345 Participants
Methodology | Study 1

"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

Notification

Depending on your device, you can sign in with your fingerprint, face, or iris.

Continue
Methodology | Study 1

"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn
Methodology | Study 1

Notification → Registration → Survey
Methodology | Study 1

- Notification
- Survey
- Registration

1 Week

- Survey
- Login
- Authentication
Misconceptions | Study 1

67% think biometric sent to website
Misconceptions | Study 1

67% think biometric sent to website

43% biometric not safe from attacker
Misconceptions | Study 1

67% think biometrics sent to website
43% believe biometric not safe from attacker
93% unaware of fallback
"It’s Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

**STUDY 1**
Identify Misconceptions
- Task / Survey
- 42 Participants

**STUDY 2**
Design Notifications
- 7 Focus Groups
- 29 Participants

**STUDY 3**
Compare Notifications
- Experiment
- 345 Participants
Focus Groups | Study 2
Methodology | Study 2

Welcome
Methodology | Study 2

Welcome

Video
Methodology | Study 2

Welcome  Video  Impressions
Methodology | Study 2

"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn
Methodology | Study 2

Welcome → Impressions → Design

Video → Reading

"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn
Methodology | Study 2

Welcome, Impressions, Design, Discussion
Results | Study 2

<table>
<thead>
<tr>
<th>Convenience</th>
<th>Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords</td>
<td>Availability</td>
</tr>
</tbody>
</table>

"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn
Results | Study 2

Convenience

Security

Passwords

Availability

."It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn
## Results | Study 2

### Convenience

- No one except you has access

### Security

- Never leaves your phone

### Availability

- Only stored on your device

<table>
<thead>
<tr>
<th>Study 2</th>
<th>Convenience</th>
<th>Security</th>
<th>Availability</th>
<th>Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>

"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users' Misconceptions About FIDO2 Biometric WebAuthn
Results | Study 2

- Convenience
- Security
- Passwords
- Availability
Results | Study 2

Convenience

Security

Passwords

Availability
“It’s Stored, Hopefully, on an Encrypted Server”: Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

STUDY 1
Identify Misconceptions
Task / Survey
42 Participants

STUDY 2
Design Notifications
7 Focus Groups
29 Participants

STUDY 3
Compare Notifications
Experiment
345 Participants
"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn
Notifications | Study 3

Fast and easy sign-in with your device's PIN, pattern, or password.

Registration
- Your Prolific ID: FAKE Prolific ID 1234567
- What is your gender?
  - Please select...
- How old are you?
- Password
  - Enter password
  - Confirm password
  - Must be at least 8 characters long.

Continue
Register

Non-biometric
Password
"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

Perception of Security | Study 3

<table>
<thead>
<tr>
<th>Strongly agree</th>
<th>Somewhat agree</th>
<th>Neither agree nor disagree</th>
<th>Somewhat disagree</th>
<th>Strongly disagree</th>
</tr>
</thead>
<tbody>
<tr>
<td>80%</td>
<td>15%</td>
<td>5%</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>70%</td>
<td>20%</td>
<td>15%</td>
<td>5%</td>
<td>0%</td>
</tr>
<tr>
<td>60%</td>
<td>30%</td>
<td>25%</td>
<td>10%</td>
<td>5%</td>
</tr>
<tr>
<td>50%</td>
<td>40%</td>
<td>30%</td>
<td>20%</td>
<td>10%</td>
</tr>
<tr>
<td>40%</td>
<td>50%</td>
<td>40%</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>30%</td>
<td>60%</td>
<td>50%</td>
<td>40%</td>
<td>30%</td>
</tr>
<tr>
<td>20%</td>
<td>70%</td>
<td>60%</td>
<td>50%</td>
<td>40%</td>
</tr>
<tr>
<td>10%</td>
<td>80%</td>
<td>70%</td>
<td>60%</td>
<td>50%</td>
</tr>
<tr>
<td>0%</td>
<td>90%</td>
<td>80%</td>
<td>70%</td>
<td>60%</td>
</tr>
</tbody>
</table>
Notifications | Study 3

Fast and easy sign-in with your fingerprint or face.

Your fingerprint or face is only stored on your personal device.

Continue

Fast and easy sign-in with your fingerprint or face.

Your fingerprint or face never leaves your personal device.

Continue
Misconceptions | Study 3

66% in Control think biometrics sent to website

45% stored

50% leaves
"It's Stored, Hopefully, on an Encrypted Server": Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

Takeaways

Perceptions

- Misconceptions about where biometrics are stored
- Biometric WebAuthn perceived very positively

Notifications

- Stored and Leaves notifications most effective
- Emphasize speed and ease, not comparison to passwords
“It’s Stored, Hopefully, on an Encrypted Server”: Mitigating Users’ Misconceptions About FIDO2 Biometric WebAuthn

Leona Lassak
leona.lassak@rub.de

Annika Hildebrandt
ahildebrandt@uchicago.edu

Maximilian Golla
maximilian.golla@rub.de

Blase Ur
blase@uchicago.edu

Takeaways

Biometric WebAuthn perceived positively

Stored and Leaves notifications effective

Emphasize speed / ease

Extended Version