Evaluation of Account Recovery Strategies with FIDO2-based Passwordless Authentication

Johannes Kunke, Stephan Wiefling*, Markus Ullmann#, Luigi Lo Iacono

H-BRS University of Applied Sciences
*Ruhr University Bochum
#Bundesamt für Sicherheit in der Informationstechnik
The problem

- Passwords still really relevant in Web
  - Also threats to passwords
    - Phishing \(\rightarrow\) obtaining login credentials with fake emails or websites
    - Credential stuffing \(\rightarrow\) automated injection of breached login credentials to gain access to user accounts
  - Increased due to COVID-19 pandemic and Home-Offices in March 2020
The problem

- FIDO two-factor Authentication
- FIDO2 passwordless Authentication
- Lyastani et al.* mentioned that users are more afraid to lose access rather than get hacked

The problem

- Account recovery very important for user acceptance
- No uniform procedure for account recovery
- FIDO-Whitepaper* recommends to register backup authenticator
  - But: High burden for users
    - Must be done for each web service
    - Must be restored for each web service

* Gomi et al. (2019): Recommended Account Recovery Practices for FIDO Relying Parties
Agenda

- What we did
- What we found
- Results
- Conclusion
What we did

- Heuristic evaluation of 12 account recovery mechanisms
- Criteria orientated on frequently cited heuristics
What we did

- Criteria divided into three categories
  - Usability benefits
  - Deployability benefits
  - Security benefits
What we did

- Set up criteria
- Collection of 12 mechanisms
- Evaluation of mechanisms
- Point out proposals for improvement of passwordless FIDO2 recovery mechanisms
# Mechanisms & criteria

<table>
<thead>
<tr>
<th>Security Questions</th>
<th>OTP</th>
<th>FIDO2 Backup Token</th>
<th>Identity Card</th>
<th>Let’s Authenticate</th>
<th>Key Caps</th>
<th>Online Recovery Storage</th>
<th>Preemptive Syncing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memorywise-Effortless</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Scalable-for-User</td>
<td>✗</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nothing-to-Carry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physically-Effortless</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Easy-to-Learn</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Deployability       |       |                   |               |                    |        |                        |                  |
| Match System-Real World |   |                   |               |                    |        |                        |                  |
| Accessible          |      |                   |               |                    |        |                        |                  |
| Negligible-Cost-per-User |  |                   |               |                    |        |                        |                  |
| Browser-Valid       |      |                   |               |                    |        |                        |                  |
| Non-Proprietary     |      |                   |               |                    |        |                        |                  |
| Implemented         |      |                   |               |                    |        |                        |                  |

| Security            |       |                   |               |                    |        |                        |                  |
| Resilient-Physical-Observation | |                   |               |                    |        |                        |                  |
| Resilient-Targeted-Impersonation |    |                   |               |                    |        |                        |                  |
| Resilient-Internal-Observation |     |                   |               |                    |        |                        |                  |
| Resilient-Leaks-from-Other-Verifiers | |                   |               |                    |        |                        |                  |
| Resilient-Phishing  |      |                   |               |                    |        |                        |                  |
| Resilient-Theft     |      |                   |               |                    |        |                        |                  |
| No-Trusted-Third-Party |      |                   |               |                    |        |                        |                  |
| Requiring-Explicit-Consent |    |                   |               |                    |        |                        |                  |
| Unlinkable          |      |                   |               |                    |        |                        |                  |
| Open                |      |                   |               |                    |        |                        |                  |
| Work-Factor         |      |                   |               |                    |        |                        |                  |
| Complete-Mediation  |      |                   |               |                    |        |                        |                  |

* Criteria fulfilled  ○ Criteria not fulfilled  **Bold:** Deployed in account recovery practice
What we found

- 12 mechanisms
  - Security questions
  - Backup password
  - One-Time Password
  - Pico
  - Delegated Account Recovery
  - FIDO2 Backup Token
What we found

- 12 mechanisms
  - Identity Card
  - Advanced Protection Program
  - Let’s Authenticate
  - Key Copy
  - Online Recovery Storage
  - Pre-emptive Syncing
Results

- Security questions unsuitable as recovery mechanisms
- Backup-Password also unsuitable
- PICO
  - No detailed description of how docking station works with backup
Results

- Delegated Account Recovery Protocol allows traceability
  - Worst overall rating (18/23 failed)

- Google advanced Protection
  - Similar to Facebooks mechanism (17/23 failed)
Results

- Backup-Token achieves best rating (4/23 failed)
  - However not Negligible-Cost-per-User
    - Serious criterion
- nPA/eID meets this criterion
  - However not Easy-to-Learn and Unlinkable
Results

- Let’s Authenticate is ultimately based on passwords again
- Key Copy intuitive
  - Must be kept always up to date
- ORS and Pre-emptive Syncing best compromise (7/23 failed)
  - Just theoretical concepts
  - One-time initialization necessary
Conclusion

- Concepts of pre-emptive syncing should be further investigated
  - To address problem of memory and computational load
- FIDO Alliance take up the proposal to adopt the Transfer Access Protocol in its standards
  - FIDO Alliance could eliminate the problem of inadequate access recovery
Thank you

das.h-brs.de

johannes.kunke@smail.inf.h-brs.de
Pre-emptive syncing 1

Johannes Kunke, Stephan Wiefling, Markus Ullmann, Luigi Lo Iacono

Internet | Open Identity Summit 2021
Pre-emptive syncing 2

Diagram showing the process of syncing a new primary authenticator and the backup authenticator, including steps for generating key pairs and sending keys.

Johannes Kunke, Stephan Wiefling, Markus Ullmann, Luigi Lo Iacono
Internet | Open Identity Summit 2021