Is Real-time Phishing Eliminated with FIDO?
Social Engineering Downgrade Attacks against FIDO Protocols

Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun
Phishing Trend: attackers adapt continuously

Passwords: weak, reuse, leakage, keyloggers, phishing,…

‘00: Collect credentials, exploit later.

Cheap & Scalable

‘10: Real-time phishing to bypass 2FA.

Cheap* & Scalable

‘20: Real-time phishing against FIDO?

Cheap & Scalable?

* Automated tools similar to Evilginx reduce manual efforts to mount real-time phishing.
FIDO: Motivation

Goals:

- Secure Authentication
  - Privacy preserving.
- Easy to use
- Scalable

FIDO2 reflects the industry’s answer to the global password problem and addresses all of the issues of traditional authentication:

FIDO2 cryptographic login credentials are unique across every website, never leave the user’s device and are never stored on a server. This security model eliminates the risks of phishing, all forms of password theft and replay attacks.

https://fidoalliance.org/fido2
FIDO Overview

Trusted:
- FIDO servers.
- Client software (host).
  - WebAuthn & CTAP
- Authenticators (security keys).

FIDO Enrollment

Authenticator {master key} → Browser (JS)

User click → [Data, appID]

[Data, appID]_signed → Server

enrollment req.

Data: username, nonce, opts

[Data, appID]_signed → [Data, pK]

Images from https://fidoalliance.org
Weakness 1: No (secure) feedback to the user

The lack of secure feedback allows an attacker to render the usual success message for FIDO step, thus potentially giving a false sense of security to the victim!
Weakness 2: Recovery and fallbacks

- FIDO: [security and usability] vs availability.
- Secure recovery at scale is difficult.
- Common practice: weaker 2FA
  - SMS / e-mails
  - OTP
  - Prompts
  - ...

Vulnerable to phishing
Intuition: FIDO & other 2FAs

Alexa Top-100:

<table>
<thead>
<tr>
<th></th>
<th>Support FIDO allow alternatives</th>
<th>Do not support FIDO</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIDO partner</td>
<td>14</td>
<td>15</td>
<td>29</td>
</tr>
<tr>
<td>Others</td>
<td>9</td>
<td>62</td>
<td>71</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>23</strong></td>
<td><strong>77</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

- Does FIDO eliminate phishing?
- Is FIDO enough to secure a user account?
- What is the security of FIDO + other 2FAs?
Browser: FIDO prompt & OTP

Images from https://google.com
Attack Overview: user feedback + alternatives

False sense of security

Downgrade

Typical Phishing

Easy to Scale
Mimicry: FIDO prompt & OTP
Evaluation: User Study

- Study design: Role playing experiment + semi structured interview (~1 hour).
- Scenario: New employee in a tech company.
- 15 email: 4 phishing
- 51 participants
  - 25 in Zurich, 26 in Ottawa
  - Age: 18-64, mean: 29.9, median: 27

“If we told you that 50% of our participants access fake websites during their study sessions, do you think you are one of them? Why/Why not?”
### Evaluation: Results

Regardless if they:
- hesitated
- OR
gave examples of non-phishing emails
- OR
named only some phishing emails and asserted there were no others

<table>
<thead>
<tr>
<th>Case</th>
<th>aware-of-phishing-attempts</th>
<th>submitted credentials</th>
<th>Susceptible</th>
<th>Results #</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unaware</td>
<td>Yes</td>
<td>Yes</td>
<td>28</td>
<td>55</td>
</tr>
<tr>
<td>2</td>
<td>Unaware</td>
<td>No</td>
<td>Potentially</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>Aware</td>
<td>Yes</td>
<td>Potentially</td>
<td>17</td>
<td>33</td>
</tr>
<tr>
<td>4</td>
<td>Aware</td>
<td>No</td>
<td>No</td>
<td>5</td>
<td>10</td>
</tr>
</tbody>
</table>
User’s perceptions

Security of FIDO + OTP:

“I had to put in the information [OTP] as well and I felt secure: the company even took me to verify everything [using OTP + FIDO] to make sure that it was secured”

FIDO vs OTP security:

“If you have to use the authentication app on the phone, with the changing number always, it is really difficult for someone to hack your system to find this kind of information.”

Indicators:

“[...] if the website looks fine, I mean the front page, I am not suspicious”, “It’s the same because it looks the same up here [refers to logo section], and I would be trusting it’s fine”
Possible Countermeasures

- **Disable Weaker Alternatives**
  - Cons: Degradation on usability & availability. Scalable & Secure Recovery?

- **Risk Based Authentication**
  - Cons: Mimicry of user’s attributes/behaviour.

- **Browser Hints**
  - Cons: User habituation; User are vulnerable to social engineering; FIDO’ added value?

- **Secure Login and Recovery Alternatives**
  - Challenge: Scalability & availability.

- **User Education**
  - Plausible (yet somewhat ineffective) countermeasure.
Concluding Remarks

- Even with FIDO, users remain potentially vulnerable to real-time phishing that downgrades FIDO to weaker alternatives.
- Despite understanding how to use FIDO, users do not understand how FIDO protects them.
- Enabling only FIDO alternatives to FIDO is an effective countermeasure.
- Fallbacks & recovery schemes should prioritize security over usability.
Thank you

Danke
Merci
Faleminderit
Hvala