

Not All MFAs Are Created Equal

Exploring the Phishing Resistance of Passkeys



1. Passwords and MFA
2. Out-of-band authentication
3. Adversary in the middle
4. Lab 1: AitM and TOTP
5. Passkeys
6. Lab 2: AitM and passkeys



Objectives:

1. Understand why some methods are weak
2. Experience the flow
3. Understand how phishing resistance is achieved in passkeys



Natalia Glina

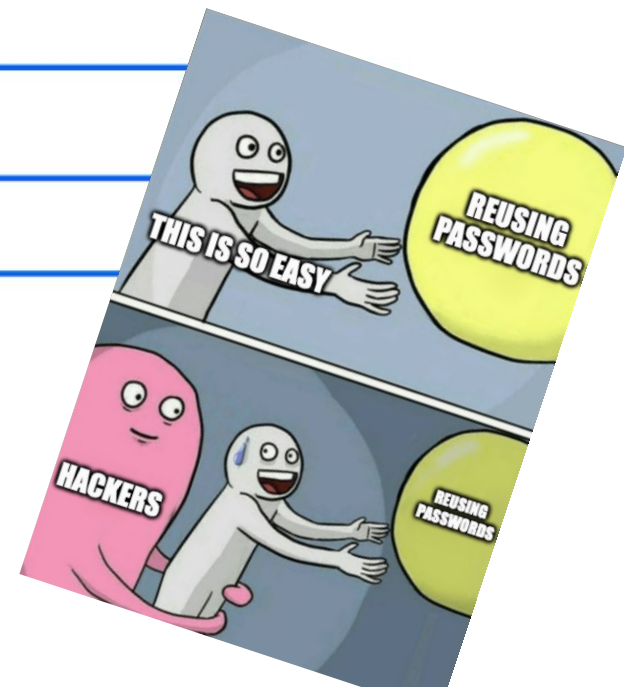
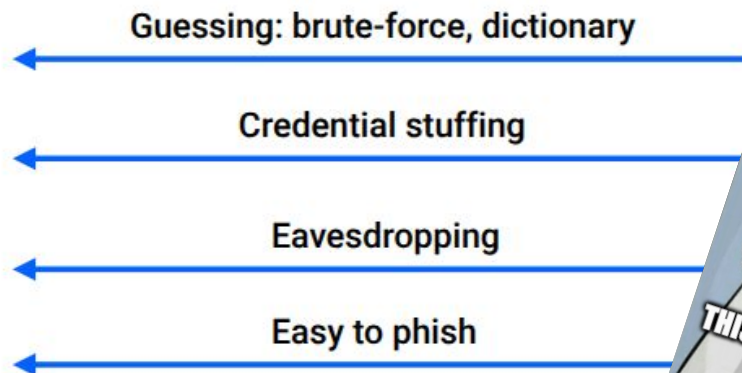
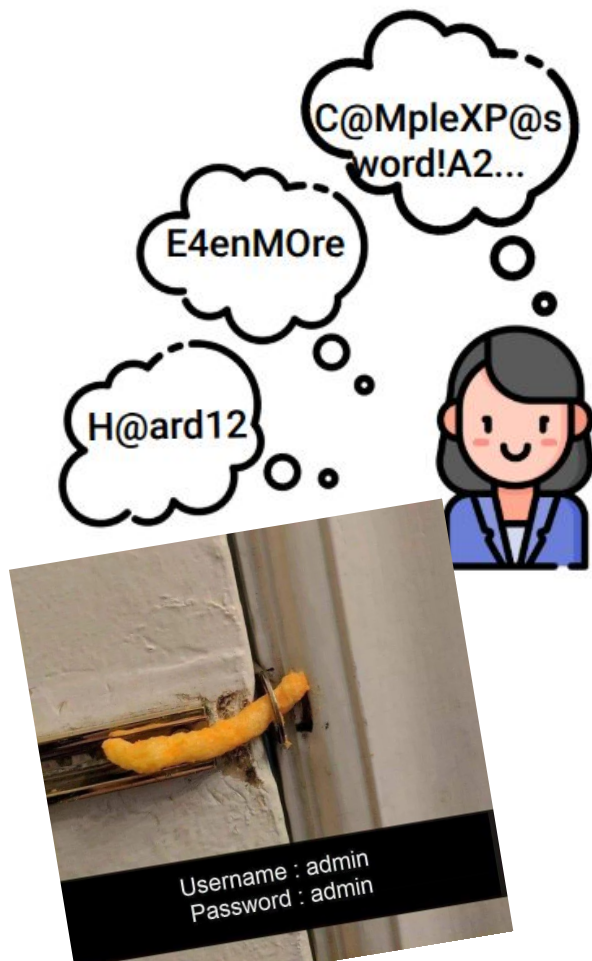
Identity Engineer
Rowe Consulting



Michal Kepkowski

Principal Security
Researcher
Oracle

Authentication basics

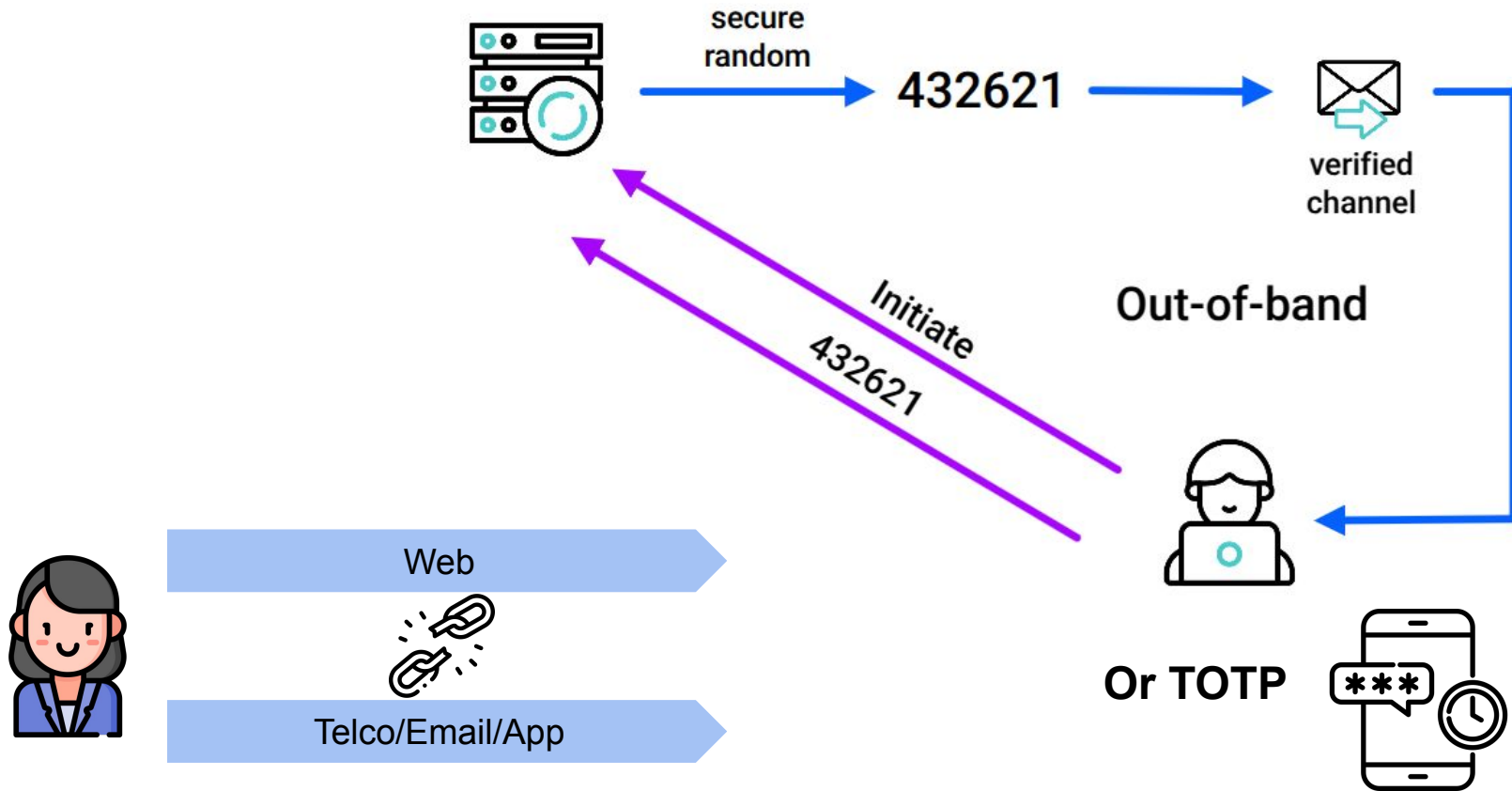


Authentication - adding more

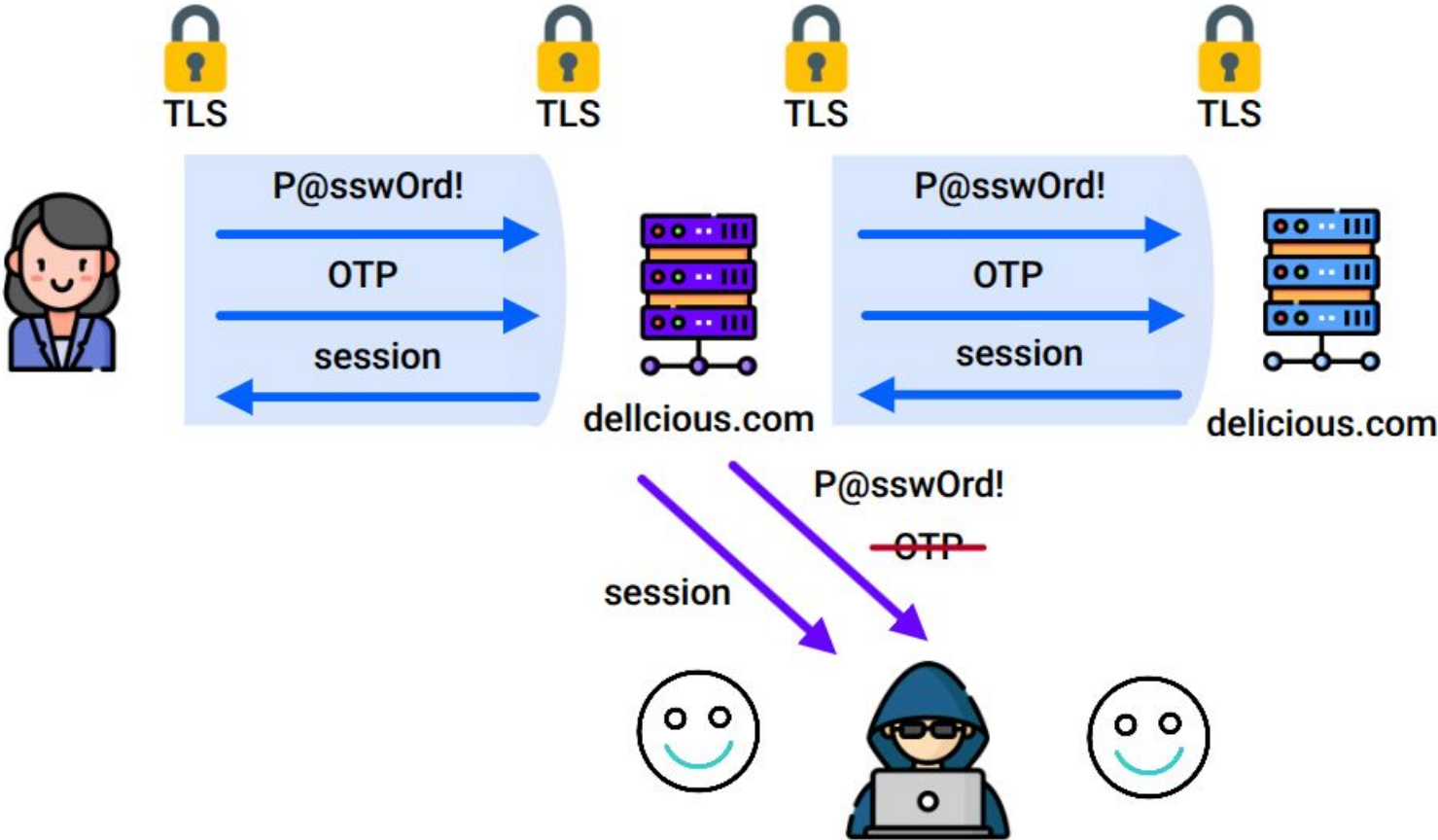
Something you know	Something you have	Something you are
		
		
Passwords Knowledge-based questions PINs	Push notifications OTPs Hardware authenticators	Fingerprint Palm scan Face scan



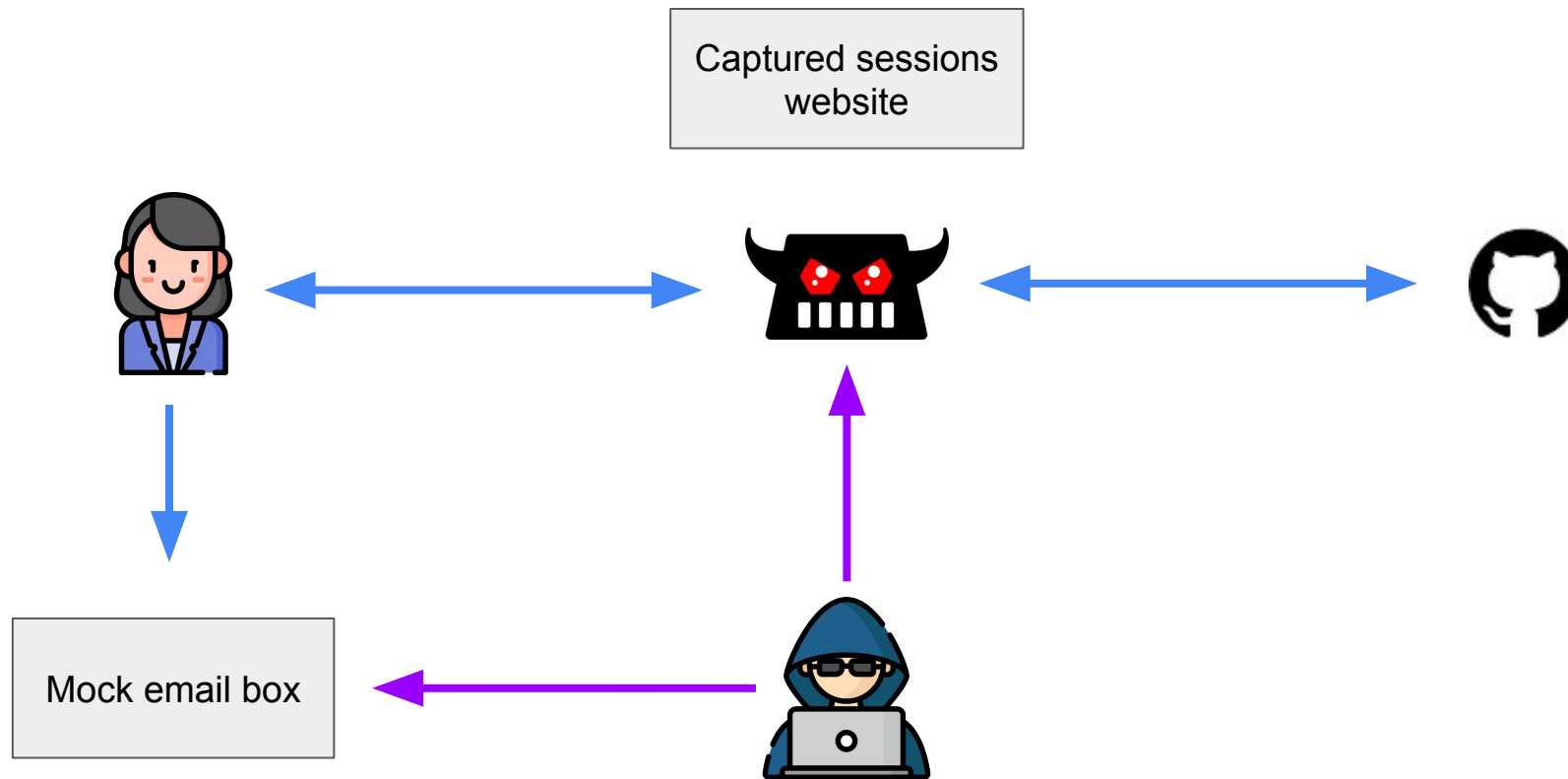
Authentication - out-of-band



Authentication - AitM



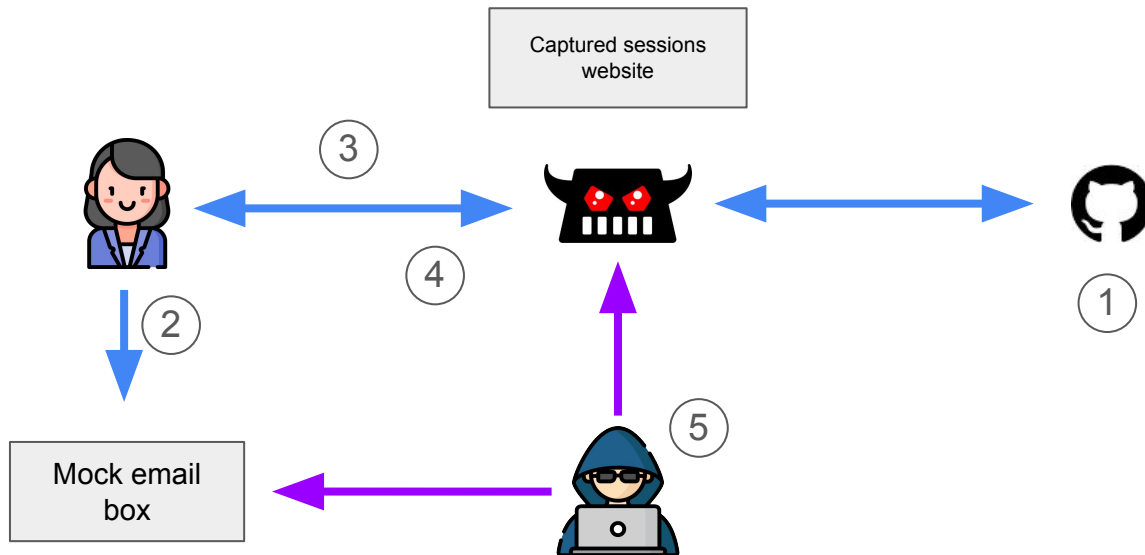
Lab - Setup



1. User has account in github with password and TOTP
2. User opens phishing email
3. User clicks on lure URL
4. User completes authentication
5. Attacker captures session



**If something goes wrong
you will be rickrolled!**



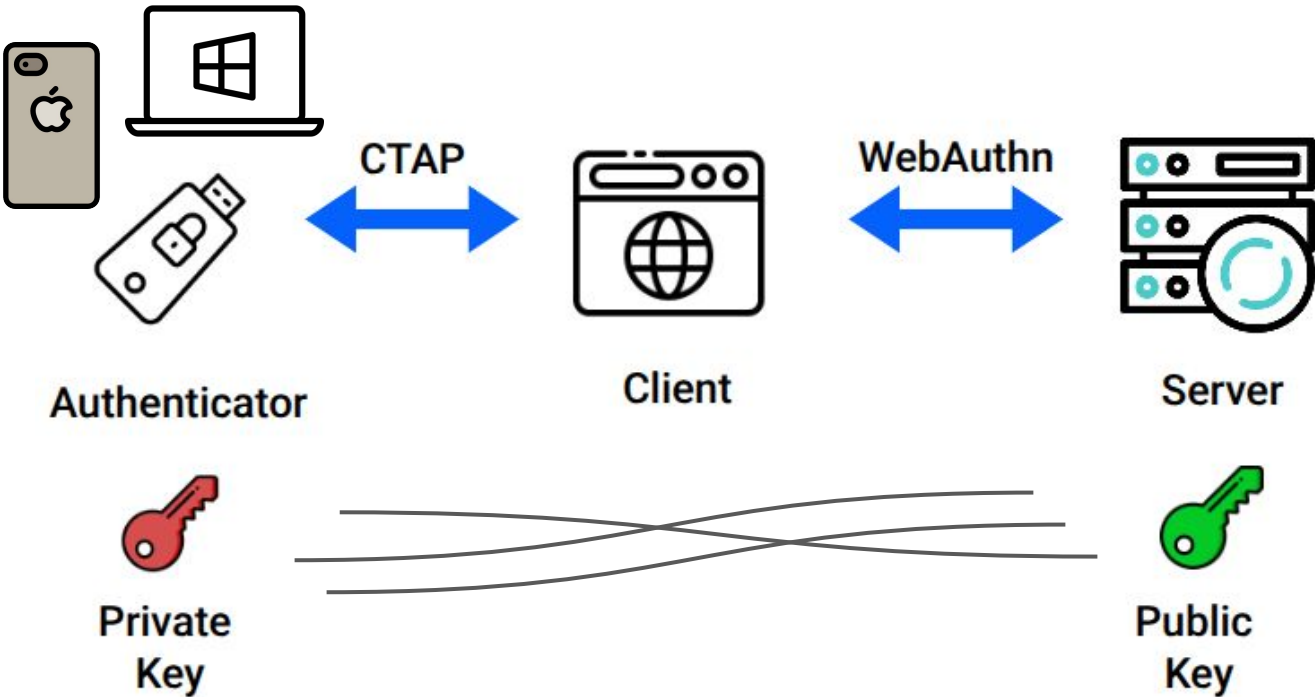
PDF: <https://mailbox.cybersoup.org/lab1.pdf>

1. Create test github account (**don't use your personal/work one**)
 - a. Create temporary email - e.g., <https://temp-mail.org> or <https://emailondeck.com>
 - b. Register in github.com
2. Register TOTP (use any app you like)
 - a. In Github: click on your profile (top right) -> Settings -> Password and Authentication -> Enable two-factor Authentication
3. Sign out
4. Go to demo email box - <https://mailbox.cybersoup.org>
5. Open phishing email
6. Click on **Regenerate your token** button
7. Authenticate using TOTP
8. Check captured session - <https://web.cybersoup.org/sessions>

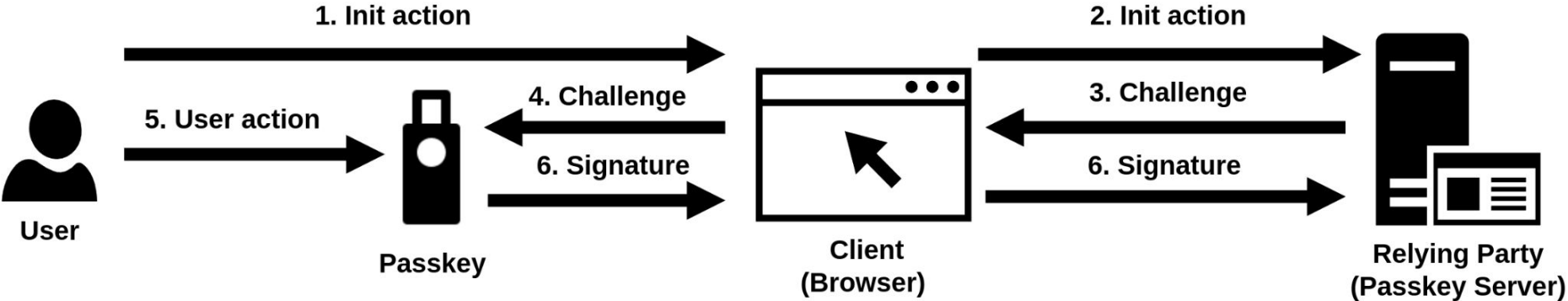
Bonus: use session in Chrome using cookie-editor plugin

<https://chromewebstore.google.com/detail/cookie-editor/hlkenndednhfkekhgcdcicdfddnkalmdm>

Passkeys - passwordless authentication

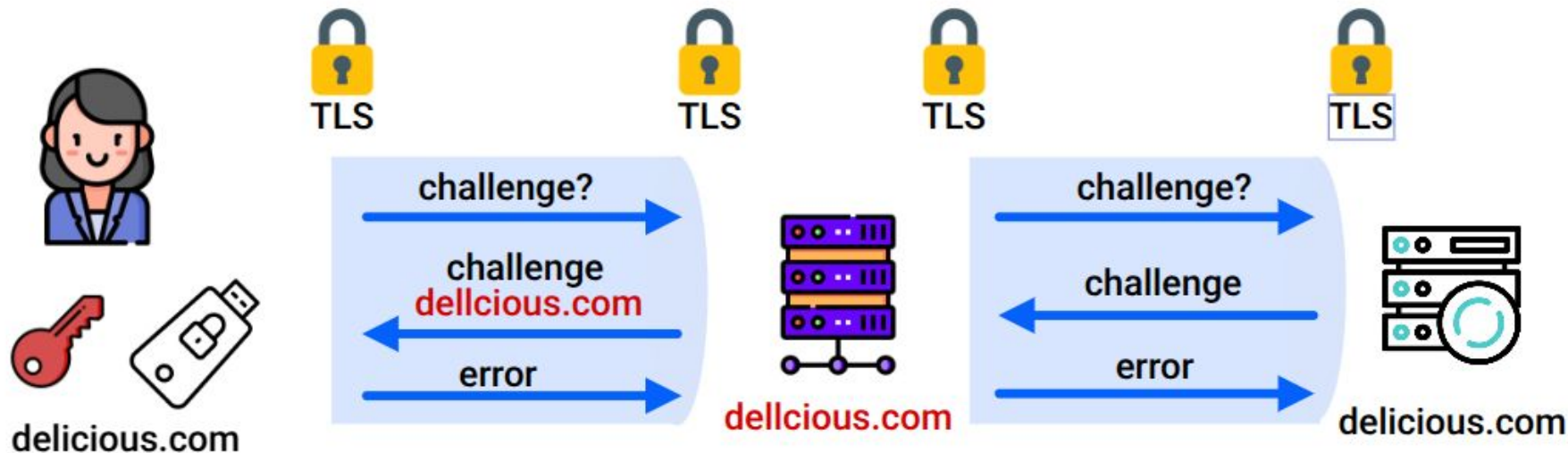


Passkeys - passwordless authentication



Passkeys - phishing resistance

Will you receive a phishing email?	Yes
Can you click on the phishing link?	Yes
Can you authenticate?	No



delicious.com $\neq$ dellcious.com

PDF: <https://mailbox.cybersoup.org/lab2.pdf>

1. Register passkey in your Github account (use github.com)
 - a. In Github: click on your profile (top right) -> Settings -> Password and Authentication -> Passkeys
2. Sign out
3. Go to demo mailbox - <https://mailbox.cybersoup.org>
4. Open phishing email
5. Click on **Regenerate your token** button
6. Try to authenticate using passkey

github.com ≠ github.cybersoup.org

- ✓ Passkeys remove the need for human validation
- ✓ Cryptography-based authentication is the way to go!
- ✓ It's technically impossible to authenticate on the phished domain
- ✓ Usability gain = happier users and developers 😊

**Questions? Comments?
Suggestions?**



Introduction to passkeys
micro-course

<https://www.cybersoup.org>