



A Security and Usability Analysis of Local Attacks Against FIDO2

Tarun Kumar Yadav, Kent Seamons
(Brigham Young University)



WHY FIDO2?



Forbes

<https://www.forbes.com> › Innovation › Cybersecurity

Warning As 26 Billion Records Leak: Dropbox, LinkedIn, ...

Jan 23, 2024 — Security researchers have warned that a database containing no less than 26 billion **leaked** data records has been discovered.

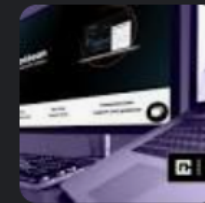


Cybernews

DarkBeam leaks billions of email and password combinations

The leaked logins present cybercriminals with almost limitless attack capabilities. DarkBeam, a digital risk protection firm,...

Nov 15, 2023

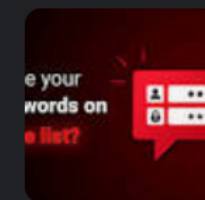


Cybernews

Most Common Passwords 2024 - Is Yours on the List? | CyberNews

We analyzed more than 15 billion passwords to see the most common password phrases, including city, sports team, year, name, and more.

Nov 27, 2023



FIDO2



Hardware Security Key (HSK)



FIDO2 client (browser)



Web server



FIDO2



Hardware Security Key (HSK)



FIDO2 client (browser)



Web server



1. Registration request



FIDO2



Hardware Security Key (HSK)



FIDO2 client (browser)



Web server



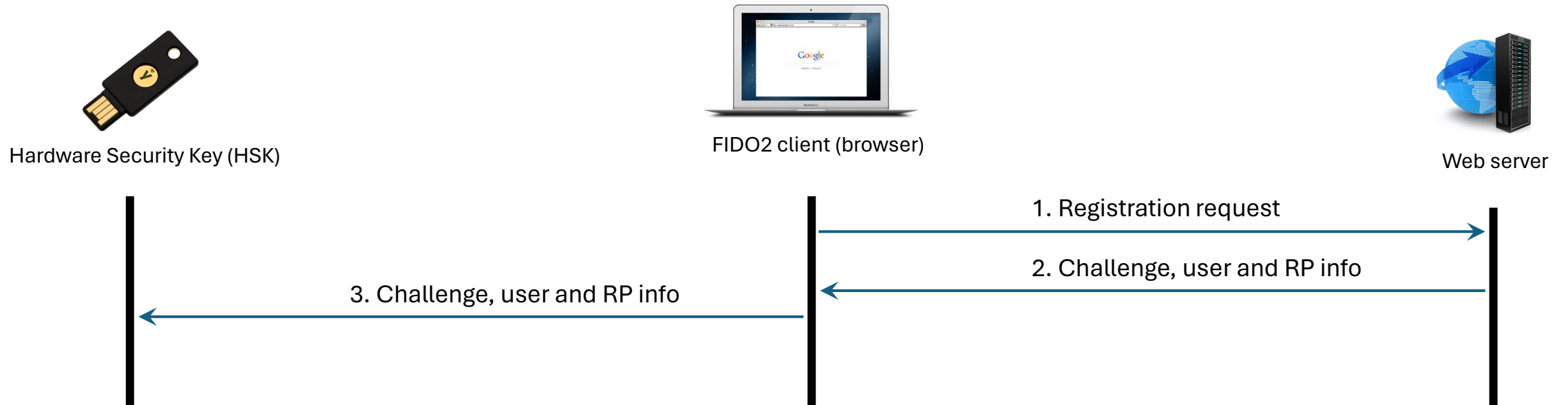
1. Registration request



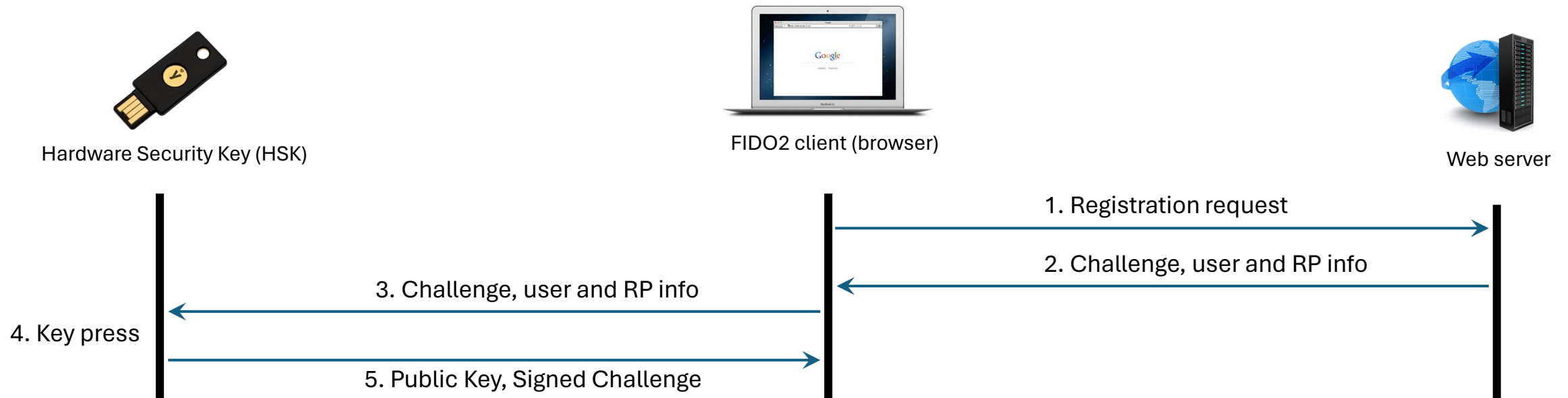
2. Challenge, user and RP info



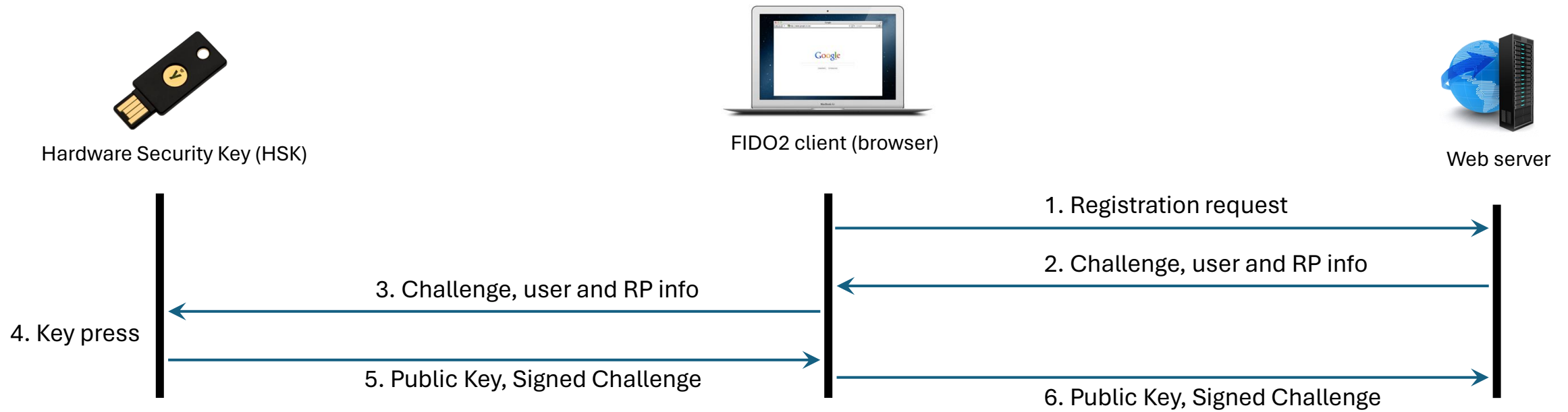
FIDO2



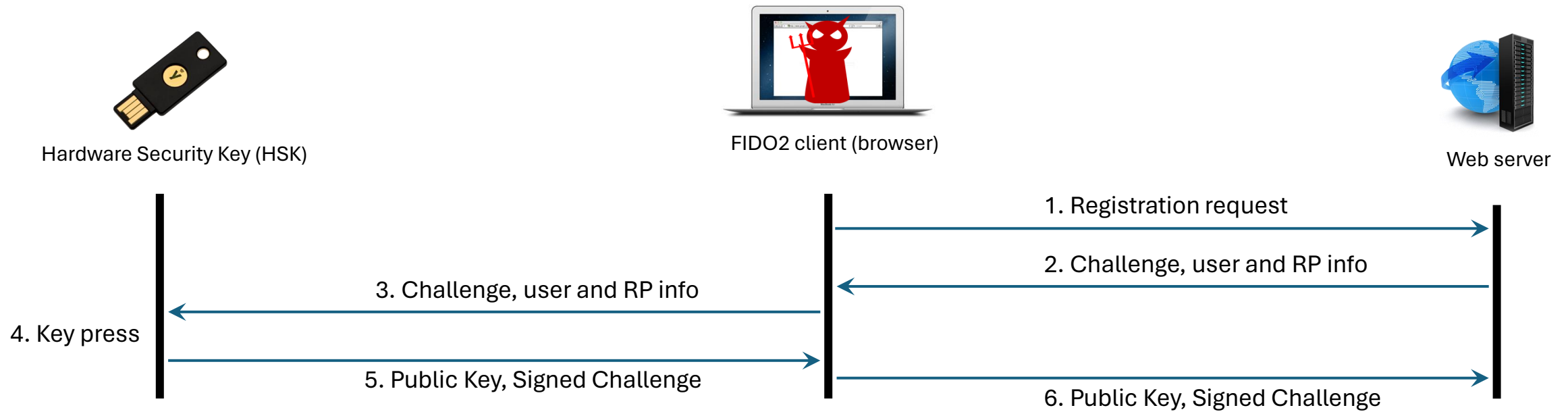
FIDO2



FIDO2

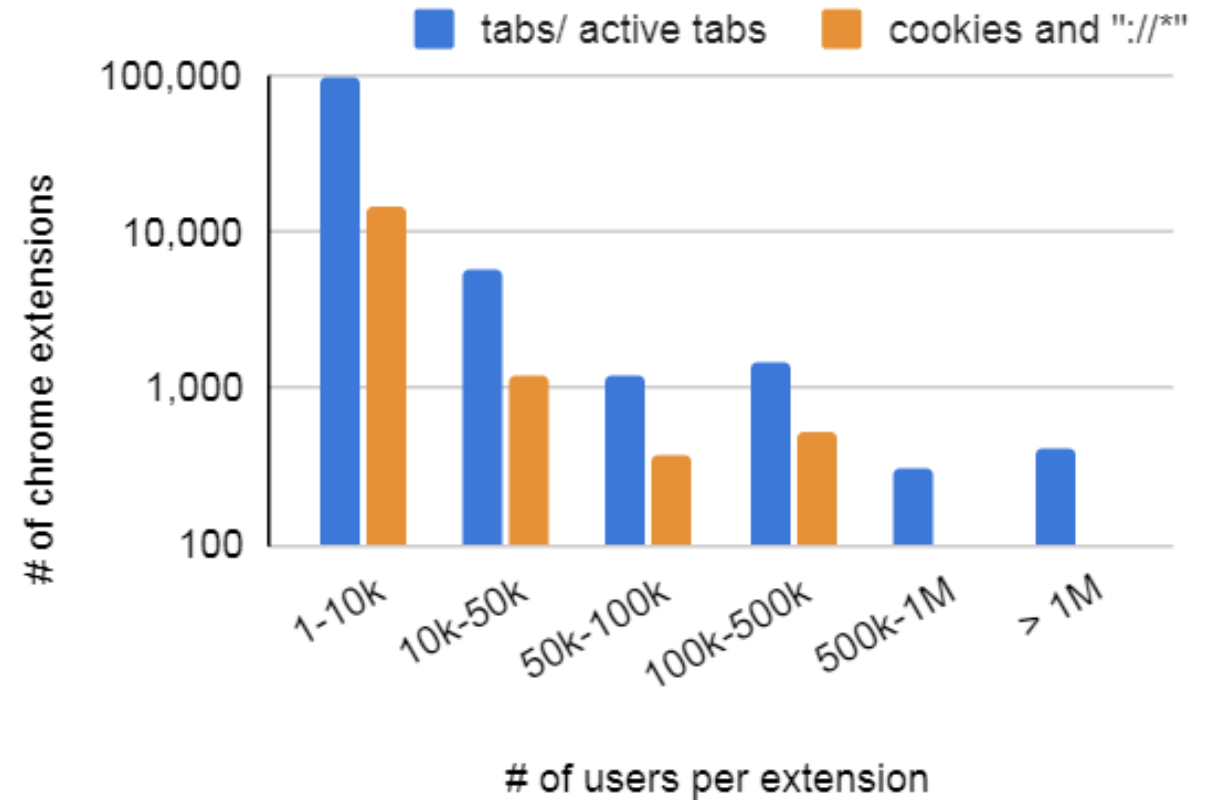


FIDO2



Browser Extensions Analysis

- 105,381 out 211,026 extensions
- 246 extensions has more than 1 million users



FIDO2



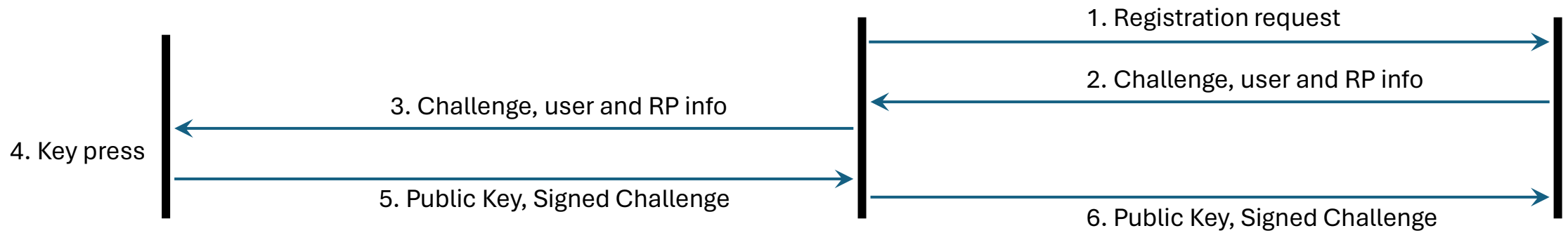
Hardware Security Key (HSK)



FIDO2 client (browser)

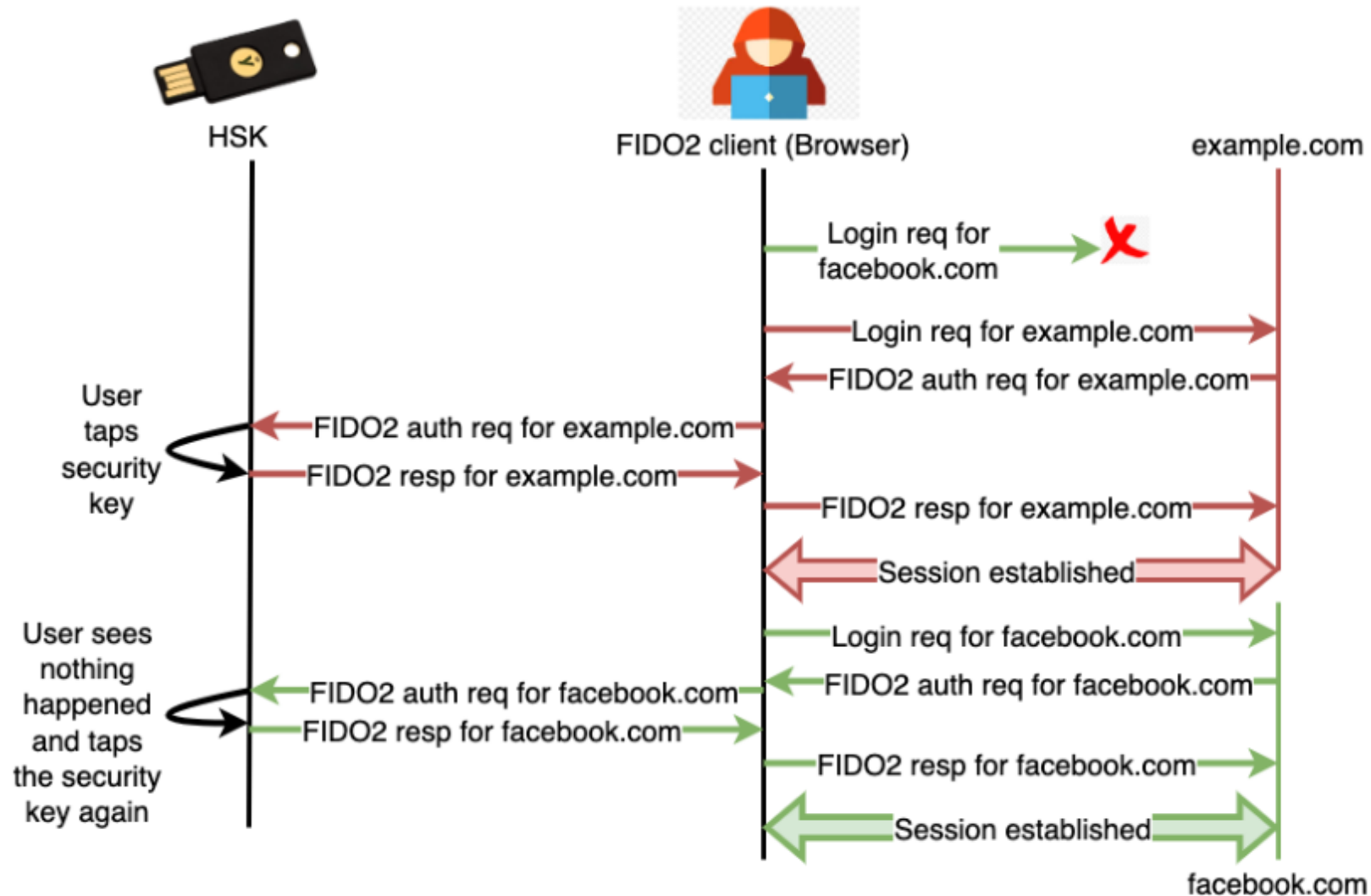


Web server

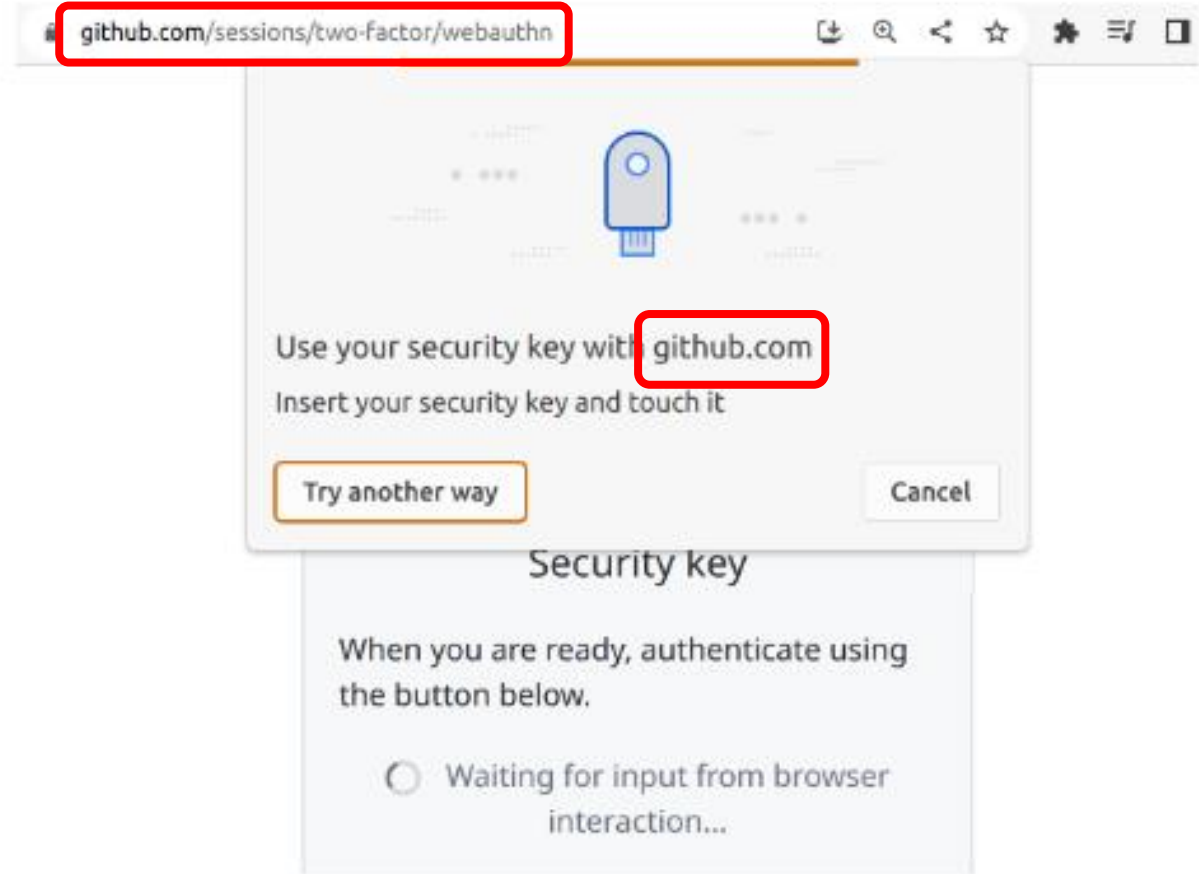
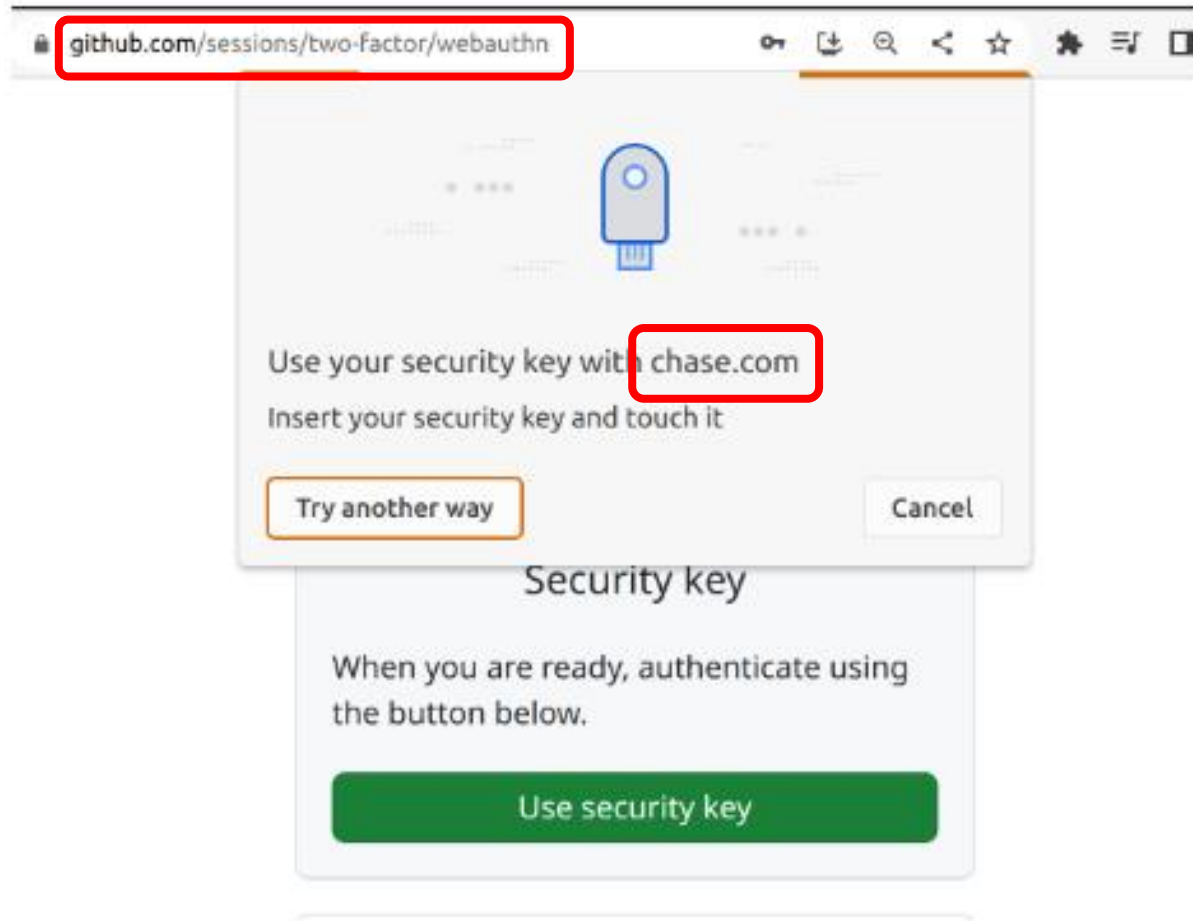


Attacks and Their Feasibility – User Study

Attack 1 – Synchronized Login



Attack 1 – Synchronized Login



Synchronized login to `chase.com` while user logs into `github.com`

User study RQs

RQ1 Synchronized login–

- a) How do users interpret pressing the HSK button twice before logging in?
- b) Do they detect the attack by observing the browser's popup displaying the website name?

User study RQs

RQ1 Synchronized login–

- a) How do users interpret pressing the HSK button twice before logging in?
 - No one considered it malicious
- b) Do they detect the attack by observing the browser's popup displaying the website name?
 - 1/ 20 participants detected

Attack 2 – Clone Detection Bypass

Counter = 230



Counter = 230

Attack 2 – Clone Detection Bypass

Before Counter = 230

After Counter = 231



Increments counter after signing an auth request



Before Counter = 230

After Counter = 231

Increments counter on every successful authentication

Attack 2 – Clone Detection Bypass

Counter = 231

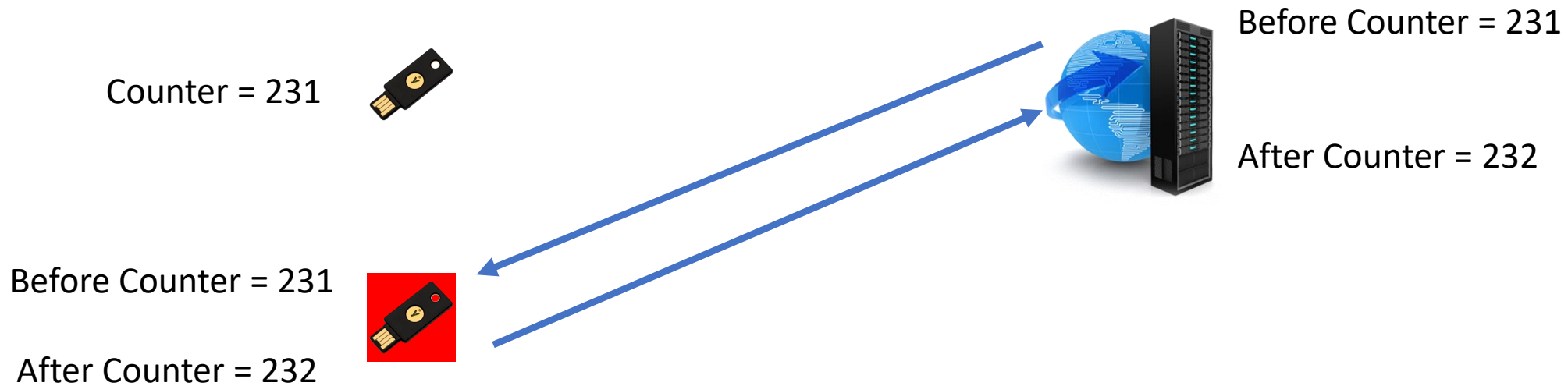


Counter = 231

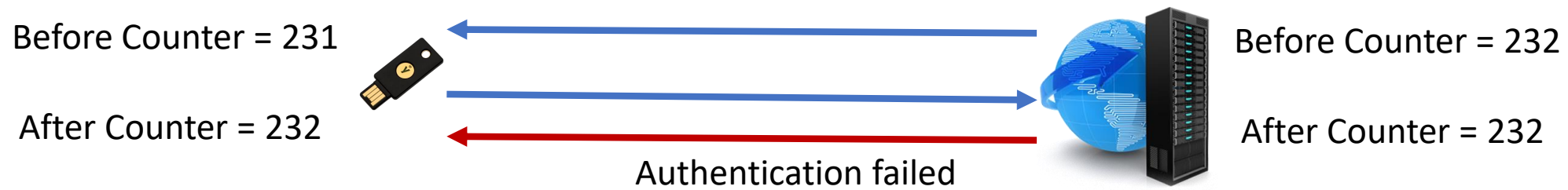
Counter = 231



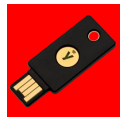
Attack 2 – Clone Detection Bypass



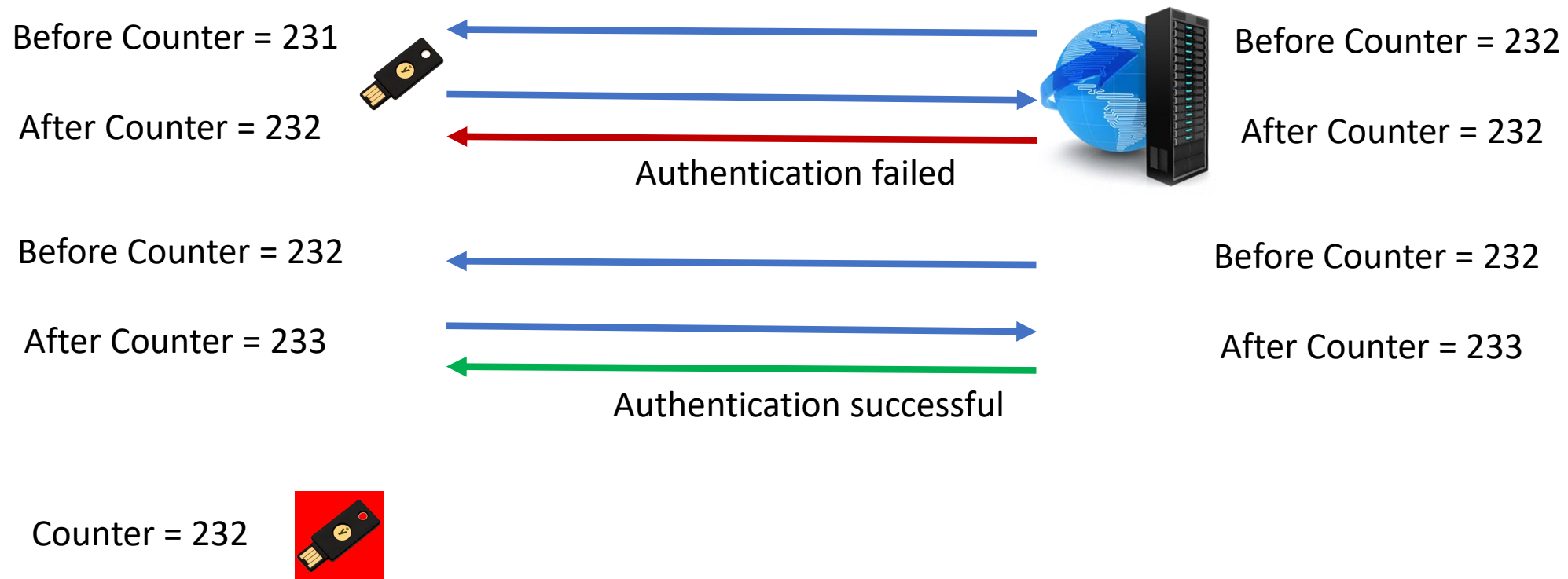
Attack 2 – Clone Detection Bypass



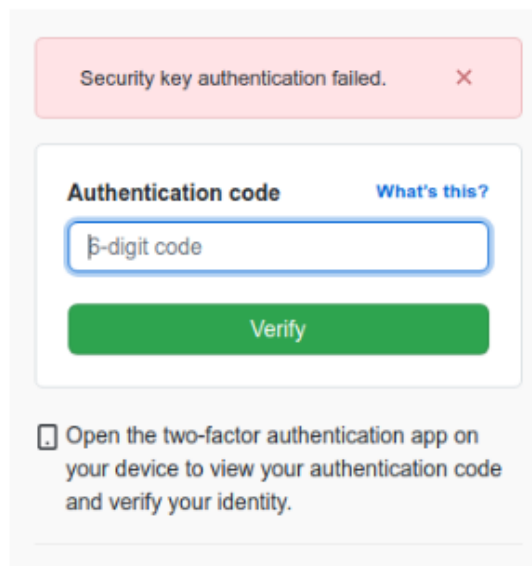
Counter = 232



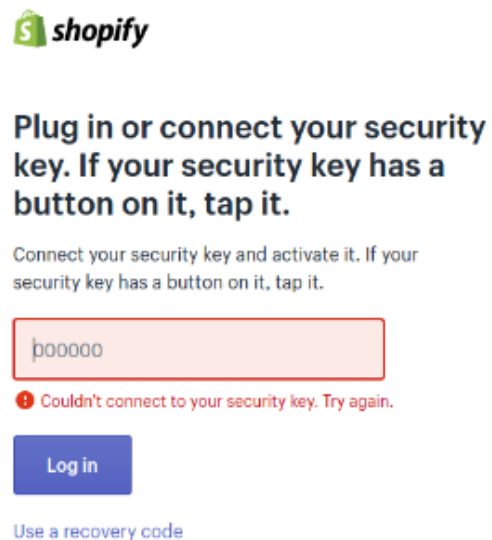
Attack 2 – Clone Detection Bypass



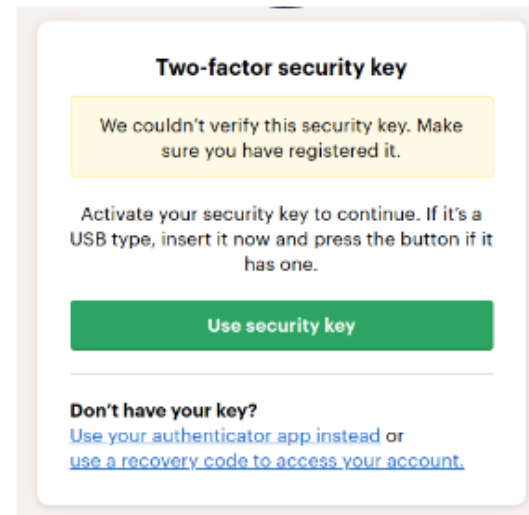
Attack 2 – Clone Detection Bypass



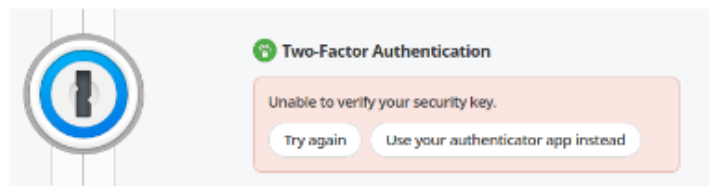
(a) GitHub



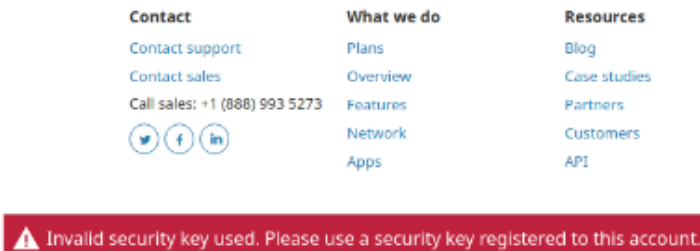
(b) Shopify



(c) Basecamp



(d) 1Password



(e) Cloudflare

User study RQs

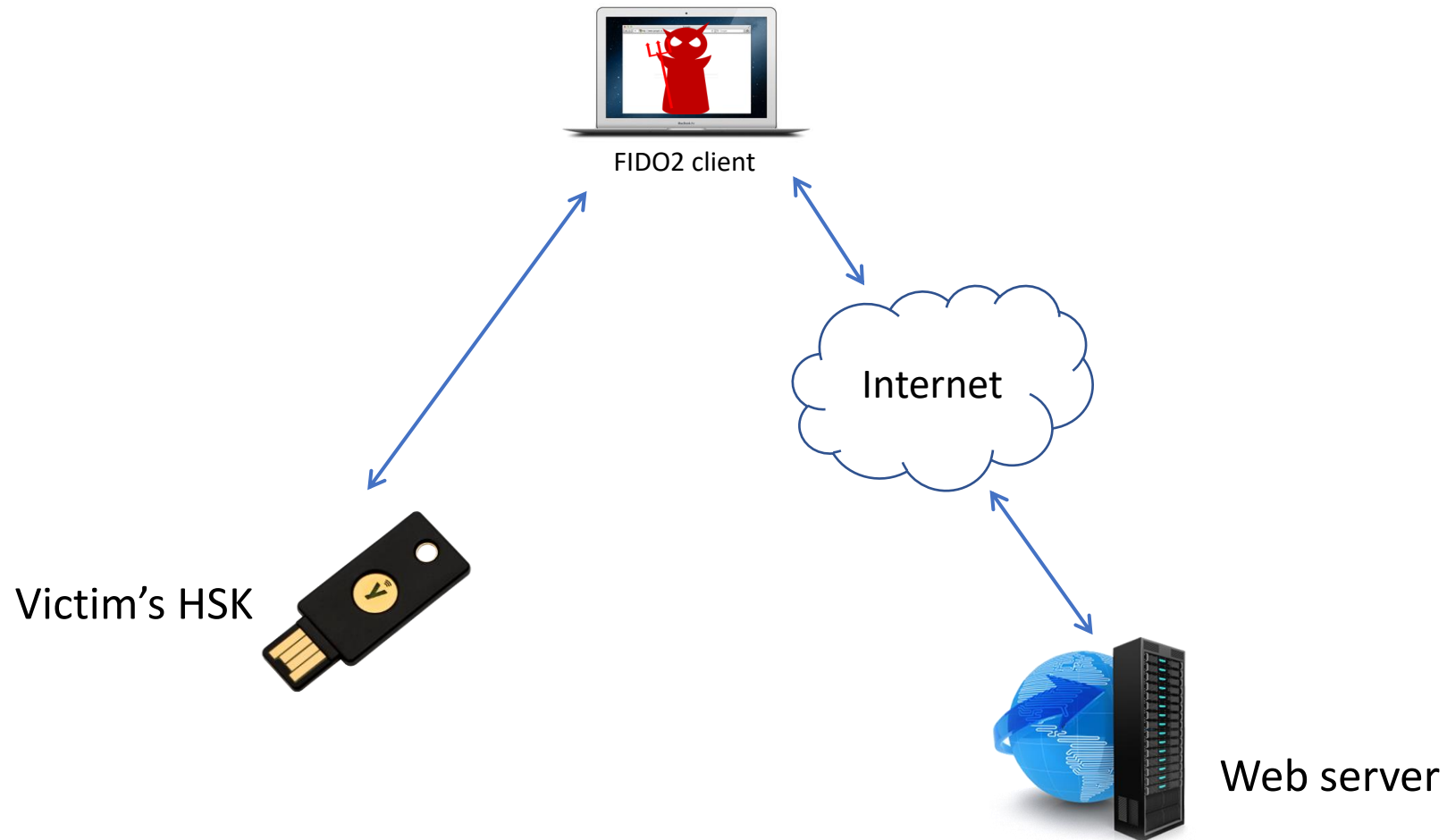
RQ2 Clone detection–

How do users interpret clone detection error messages they encounter during the login process?

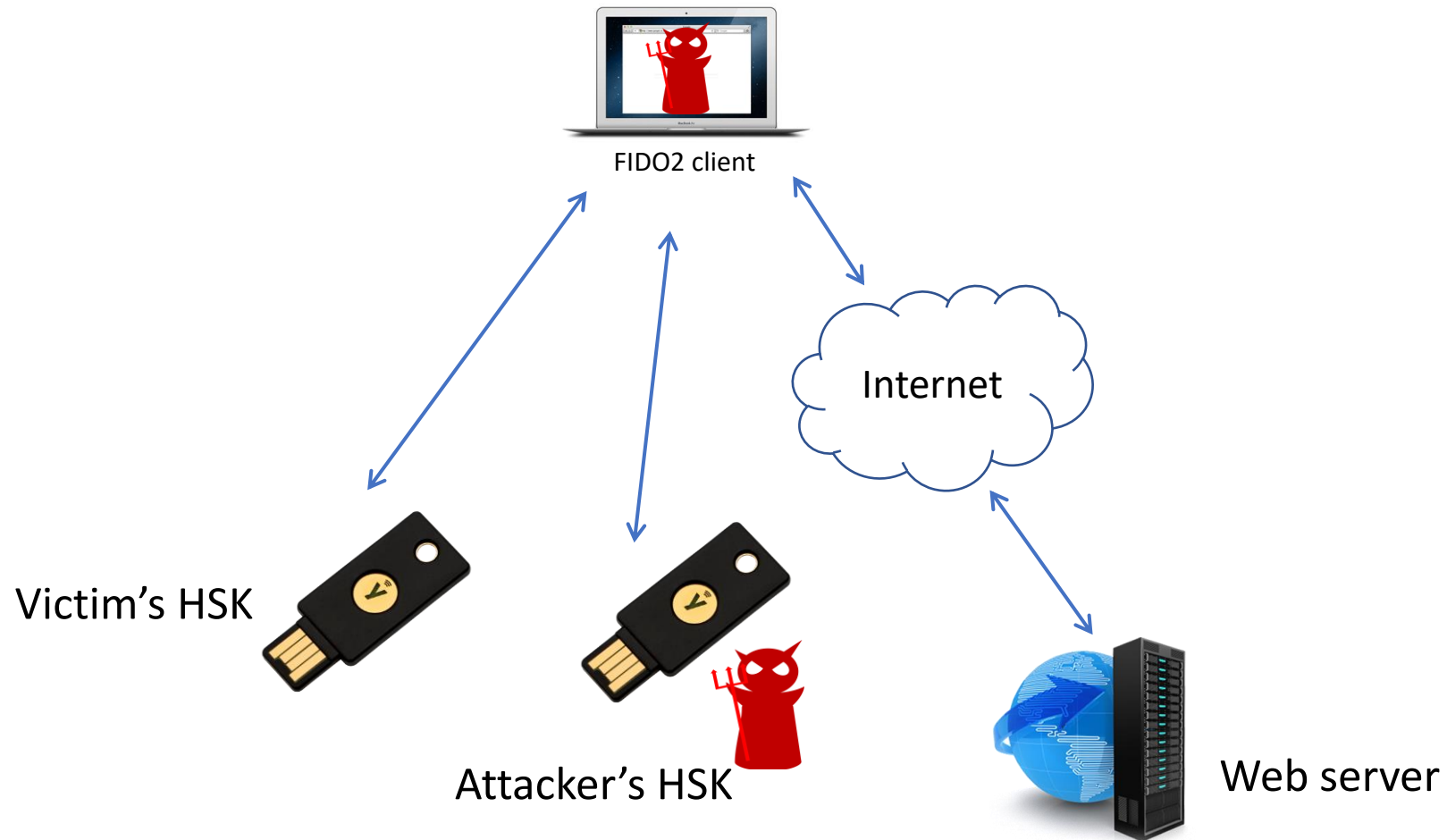
No participant considered it a malicious behavior

P2: *“It worked the second time so it might have just been an error in when I inserted the key.”*

Attack 3 – Double binding



Attack 3 – Double binding



User study RQs

RQ3 Double-binding–

- a) How do users interpret when they receive two registration emails after a HSK registration?
- b) How do users interpret the addition of a rogue HSK they encounter on the settings page?

Attack 3: Double binding – Email Notifications

You just added a security key to your account.

Please take a moment to download your recovery codes and set a fallback SMS phone number at:

<https://github.com/settings/auth/recovery-codes>

Recovery codes are the only way to access your account again. By saving your recovery codes, you'll be able to regain access if you lose your security key and phone.

GitHub Support will not be able to restore access to your account.

To disable two-factor authentication or remove your security

Hi 

This is to confirm that you've successfully updated the two-factor authentication settings on your account.

A security key used for two-factor authentication was added to your account.

To disable two-factor authentication or remove your security key, visit [Launchpad](#).

If you didn't make this change, someone else could have access to your account. Please reply to this email or contact our [support team](#) right away.

You've enabled Security key authentication for your Shopify account. From now on, you'll be asked for Security key authentication.

If you lose your device, you can log in using the recovery codes given to you when you enabled two-step authentication. Remember to keep these codes in a safe place.

If you didn't make this change, please [contact Shopify Support](#).



© Shopify | 150 Elgin Street, Ottawa ON, K2P 1L4

Have questions? Need help? [Contact our support team](#) and we'll get back to you in just a few minutes – promise.

Attack 3: Double binding – Email Notifications

P11: *“It doesn’t seem like there was any suspicious activity. There were only 3 emails and 2 of them talked about 2-step authentication processes.”*

You just added a security key to your account.

Please take a moment to download your recovery codes and set a fallback SMS phone number at:

<https://github.com/settings/auth/recovery-codes>

Recovery codes are the only way to access your account again. By saving your recovery codes, you’ll be able to regain access if you lose your security key and phone.

GitHub Support will not be able to restore access to your account.

To disable two-factor authentication or remove your security

Hi 

This is to confirm that you’ve successfully updated the two-factor authentication settings on your account.

A security key used for two-factor authentication was added to your account.

To disable two-factor authentication or remove your security key, visit [Launchpad](#).

If you didn’t make this change, someone else could have access to your account. Please reply to this email or contact our [support team](#) right away.

You’ve enabled Security key authentication for your Shopify account. From now on, you’ll be asked for Security key authentication.

If you lose your device, you can log in using the recovery codes given to you when you enabled two-step authentication. Remember to keep these codes in a safe place.

If you didn’t make this change, please [contact Shopify Support](#).



© Shopify | 150 Elgin Street, Ottawa ON, K2P 1L4

Have questions? Need help? [Contact our support team](#) and we’ll get back to you in just a few minutes – promise.

Attack 3: Double Binding – Settings Page

Organizations

Moderation

Code, planning, and automation

Repositories

Codespaces

Packages

Copilot

Pages

← Saved replies

Security

Code security and analysis

Integrations

Applications

Scheduled reminders

Archives

Security log

Sponsorship log

Two-factor authentication Enabled





Two-factor authentication adds an additional layer of security to your account by requiring more than just a password to sign in. [Learn more about two-factor authentication.](#)

Preferred 2FA method

Set your preferred method to use for two-factor authentication when signing into GitHub.

Security keys

Two-factor methods

 Authenticator app	Add
<p>Use an authentication app or browser extension to generate one-time codes.</p>	
 SMS/Text message Configured	Edit
<p>You will receive authentication code to this phone number: +1 9189316040</p>	
 Security keys Configured 2 keys	Edit
<p>Security keys are hardware devices that can be used as your second factor of authentication.</p>	
 GitHub Mobile	Add
<p>GitHub Mobile can be used for two-factor authentication by installing the GitHub Mobile app and signing in to your account.</p>	

Attack 3: Double Binding – Settings Page

- Pages
- Saved replies

- Security
 - Code security and analysis

- Integrations
 - Applications
 - Scheduled reminders

- Archives
 - Security log
 - Sponsorship log

- Developer settings

Two-factor methods

- Authenticator app** Add
Use an authentication app or browser extension to generate one-time codes.

- SMS/Text message** Configured Edit
You will receive authentication code to this phone number: +1 9189316040

- Security keys** Configured 2 keys Hide
Security keys are hardware devices that can be used as your second factor of authentication.
 - admin — registered on Jun 20, 2023 🗑️
 - myKey — registered on Jun 20, 2023 🗑️

Register new security key

User study RQs

RQ3 Double-binding–

- a) How do users interpret when they receive two registration emails after a HSK registration?
 - No participant considered it malicious
- b) How do users interpret the addition of a rogue HSK they encounter on the settings page?
 - 1/20 participants observed it



Recommendations

- Include and highlight *Nicknames, Make & Model* in email notifications
- Require HSK authentication before adding a second HSK
- Provide more specific context in Error messages

Improved Clone Detection Algorithm

Before Counter = Hash(*Challenge*₅)



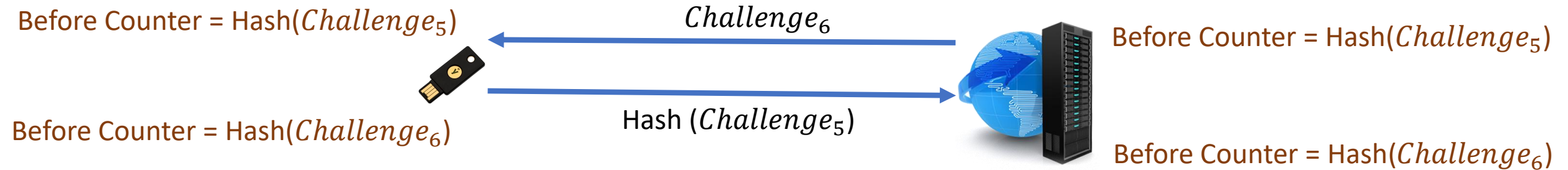
*Challenge*₆



Before Counter = Hash(*Challenge*₅)

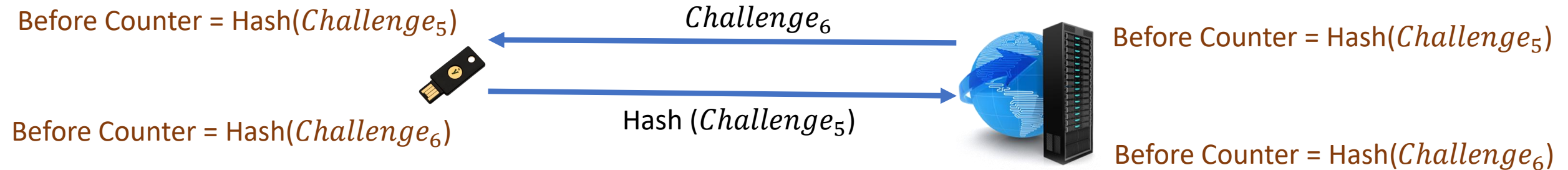
1. HSK and server saves the hash of the request's challenge

Improved Clone Detection Algorithm



1. HSK and server saves the hash of the request's challenge
2. HSK returns $Hash(previous\ challenge)$ on next authentication to RP

Improved Clone Detection Algorithm



1. HSK and server saves the hash of the request's challenge
2. HSK returns $Hash(previous\ challenge)$ on next authentication to RP
3. RP verifies if it matches with previous challenge's hash

Improved Clone Detection Algorithm

Authenticator	Cloned device	Relying party
$x = \text{hash}(\text{challenge}_0)$	x	x
Attacker authenticates with challenge1		

Improved Clone Detection Algorithm

Authenticator	Cloned device	Relying party
$x = \text{hash}(\text{challenge}_0)$	x	x
Attacker authenticates with challenge1		
x	$z = \text{hash}(\text{challenge}_1)$	$z = \text{hash}(\text{challenge}_1)$
Victim gets clone detection error message		

Summary

- Demonstrated the feasibility of seven local the attacks
 - Prototyped a malicious browser extension
 - 105,381 out of 211,026 chrome extensions have sufficient permissions
 - No evidence of these attacks in the wild
 - Two user studies (n=80, n=20) shows the ineffectiveness of current error messages, email notifications, and change in the UX due to attacks
- Improved clone detection algorithm and recommendations

Thanks!



QUESTIONS?