

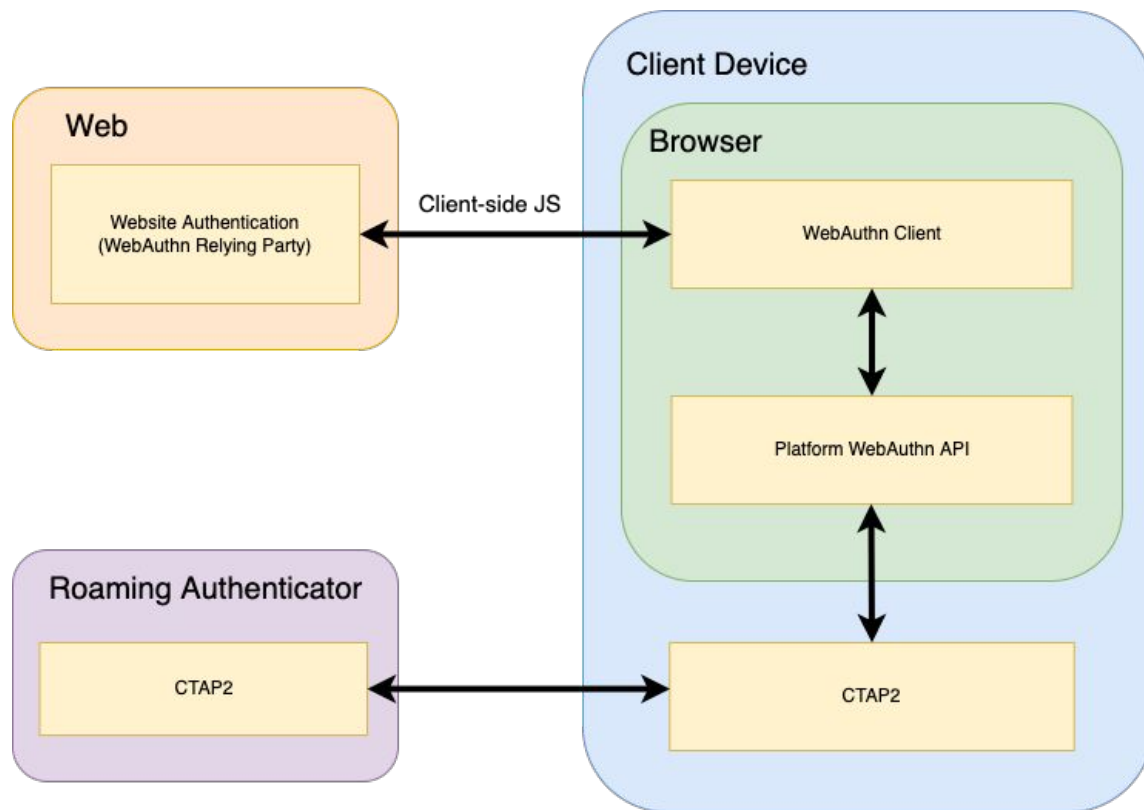
DI Group Meeting:

End of Semester Summary

December 8th

Background

FIDO2 protocol in browsers

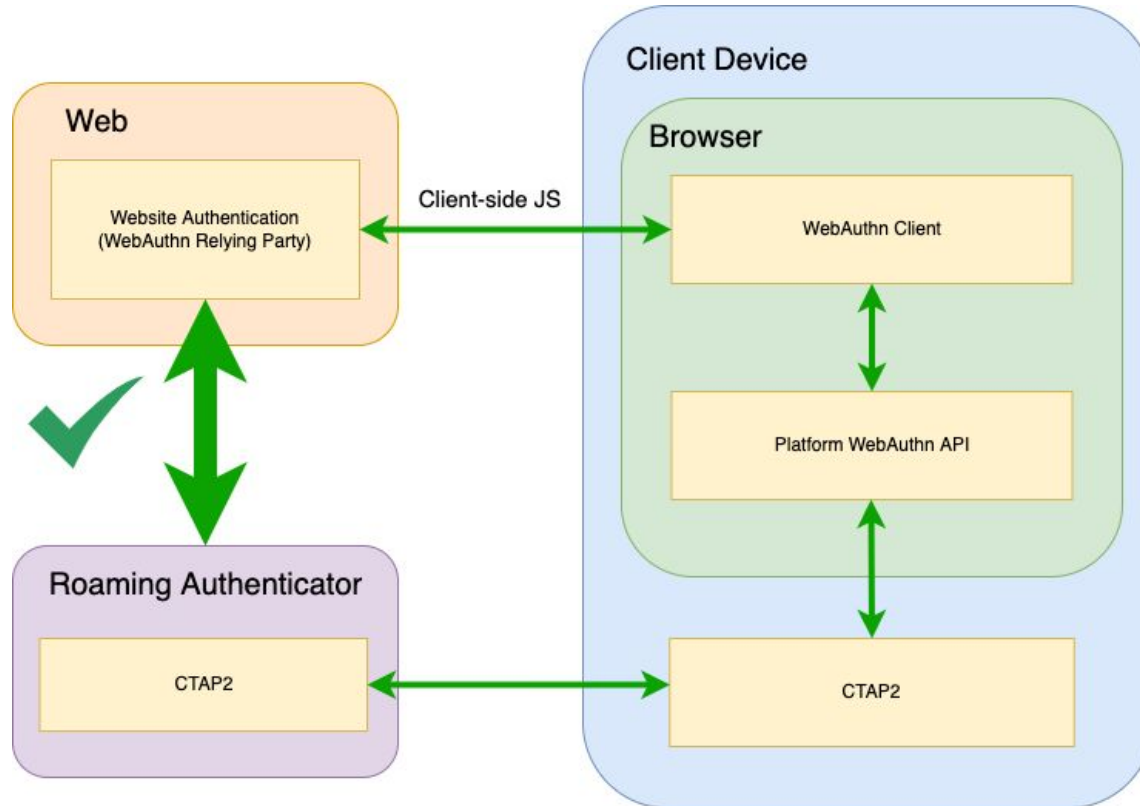


Security Assumption 4

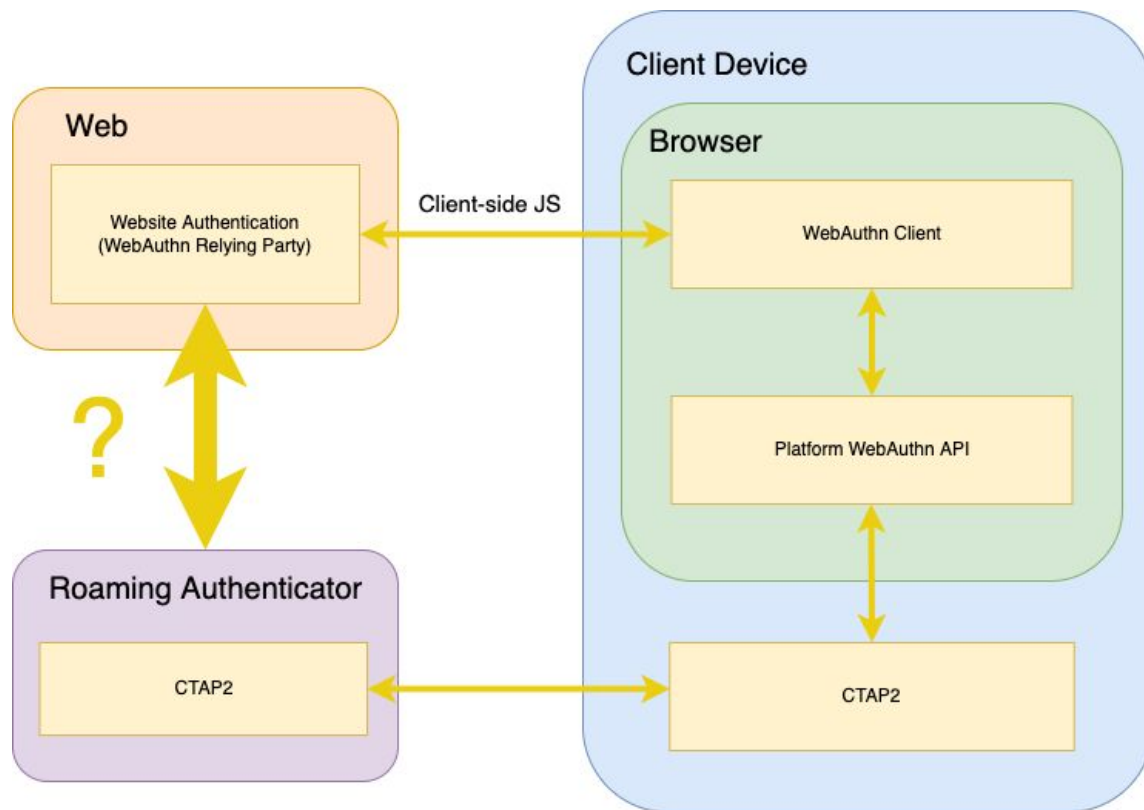
[SA-4]

The computing environment on the FIDO user device and the and applications involved in a FIDO operation act as trustworthy agents of the user.

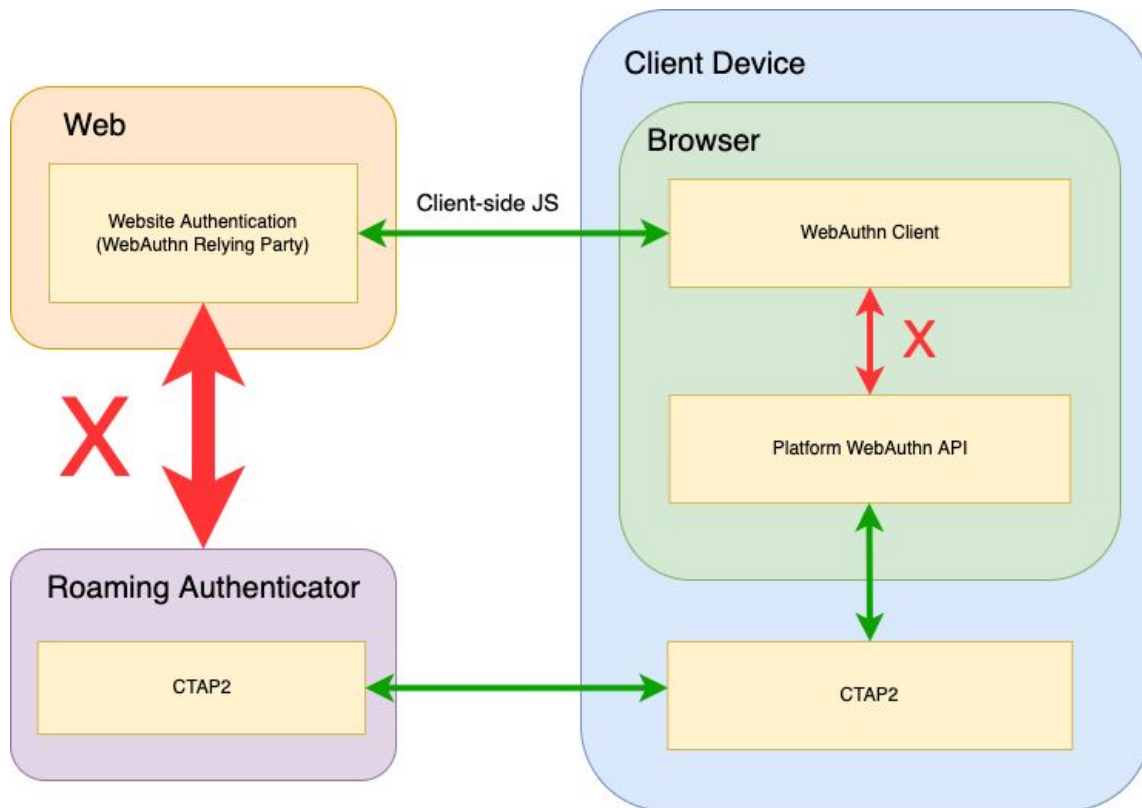
Security Assumption 4



Reality



Reality

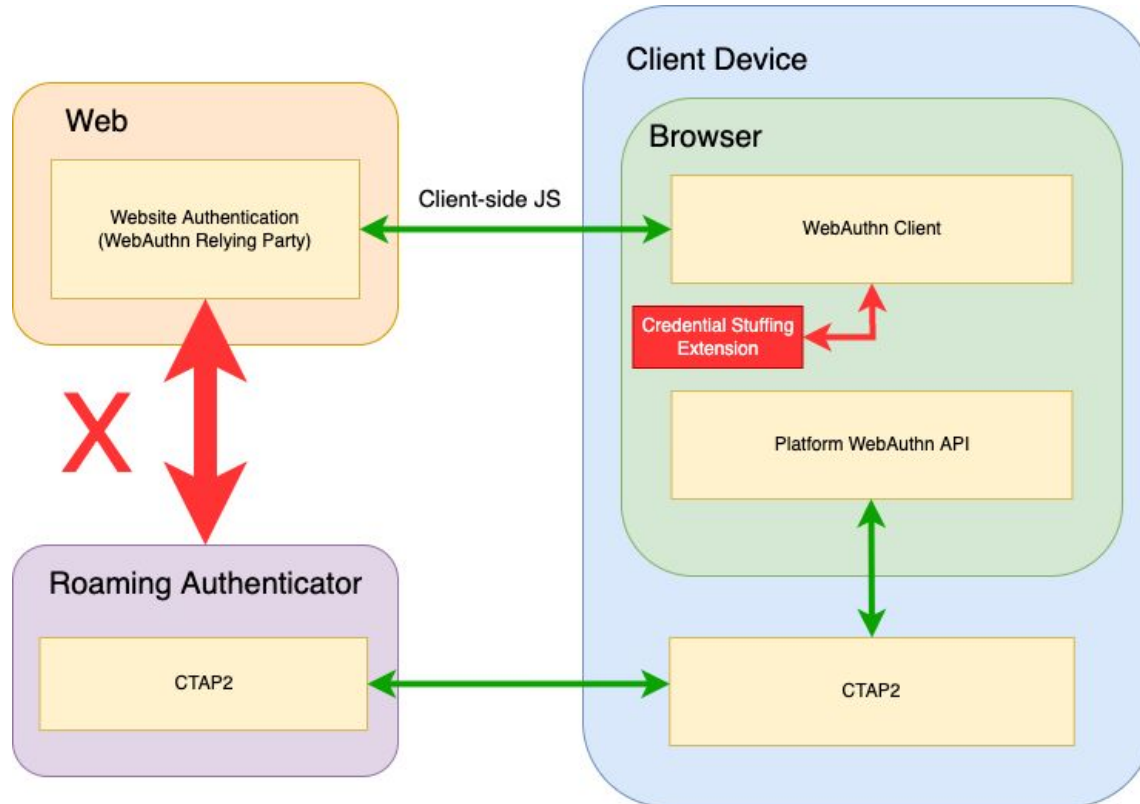


Even if one of the exchange points is insecure, the authentication succeeds

PoC

The main goal of the PoC was to show the architectural weakness of the FIDO2 protocol

Attack Vector



Steps

1. Recognize Registration Websites
 - a. URL targeting
 - b. Brute-force all websites
2. Create Virtual Authentication Token
3. Catch and Intercept WebAuthn call
4. Stuff Credentials and send credentials to controlled server

Extension requirements

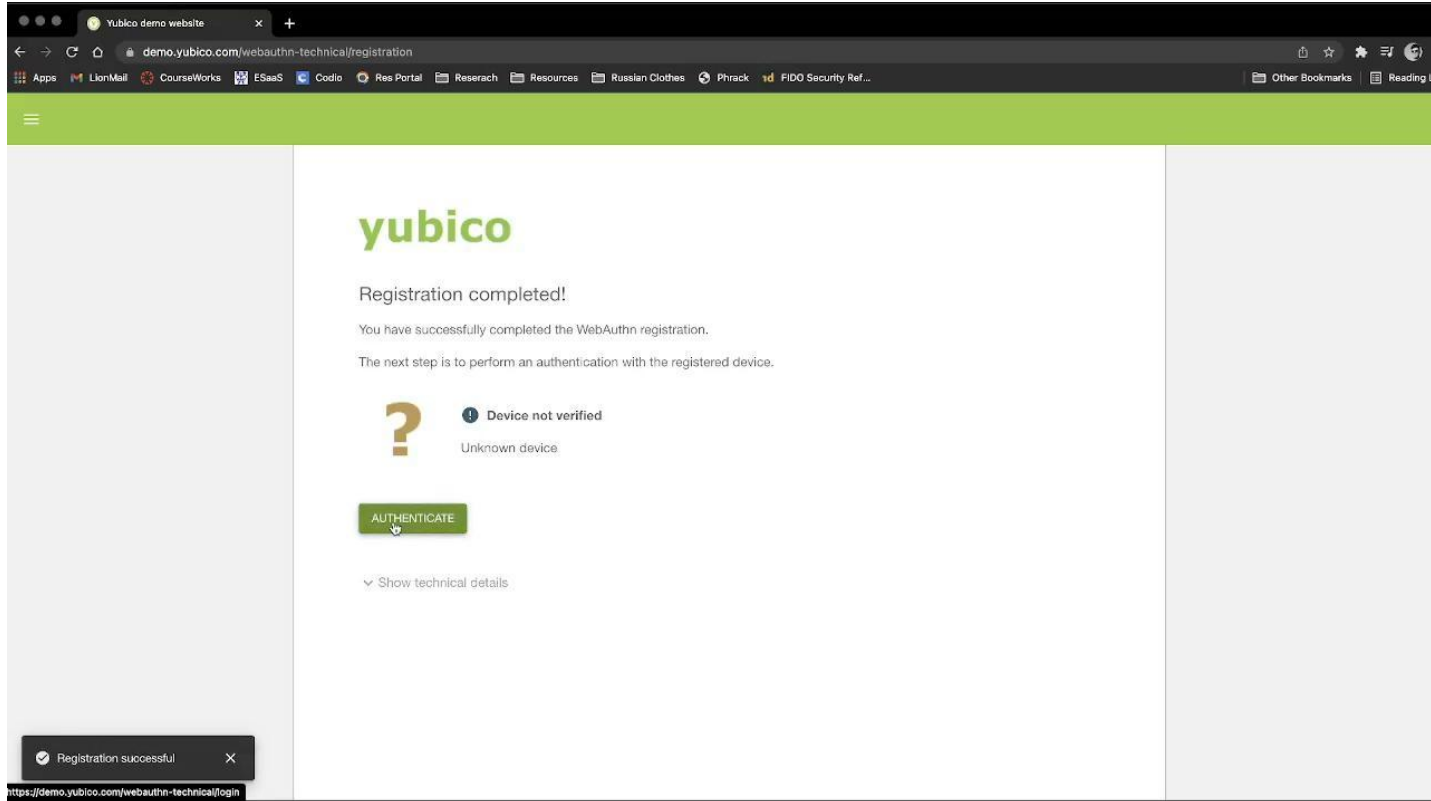
- Interact with tab and it's status
 - Allowed with “tabs” permission
- Extension must be able to intercept WebAuthn calls
 - Only allowed with attached debugger
 - “debugger” permission
- Send commands to tab
 - Only allowed with attached debugger
 - “debugger” permission
- Send stuffed credentials to controlled server
 - Only allowed with Cross Origin permissions to specific website

* permissions are enforced by the browser

Developed MVP

- Upon opening any website, automatic stuffing is attempted
- If succeeded, credential is automatically sent to server through Cross-Origin Resource Sharing (CORS)

Regular Registration-Login Procedure




The screenshot shows a web browser window with the address bar displaying `demo.yubico.com/webauthn-technical/registration`. The page content includes the Yubico logo, a confirmation message, and an authentication prompt.

Registration completed!

You have successfully completed the WebAuthn registration.

The next step is to perform an authentication with the registered device.

 **Device not verified**
Unknown device

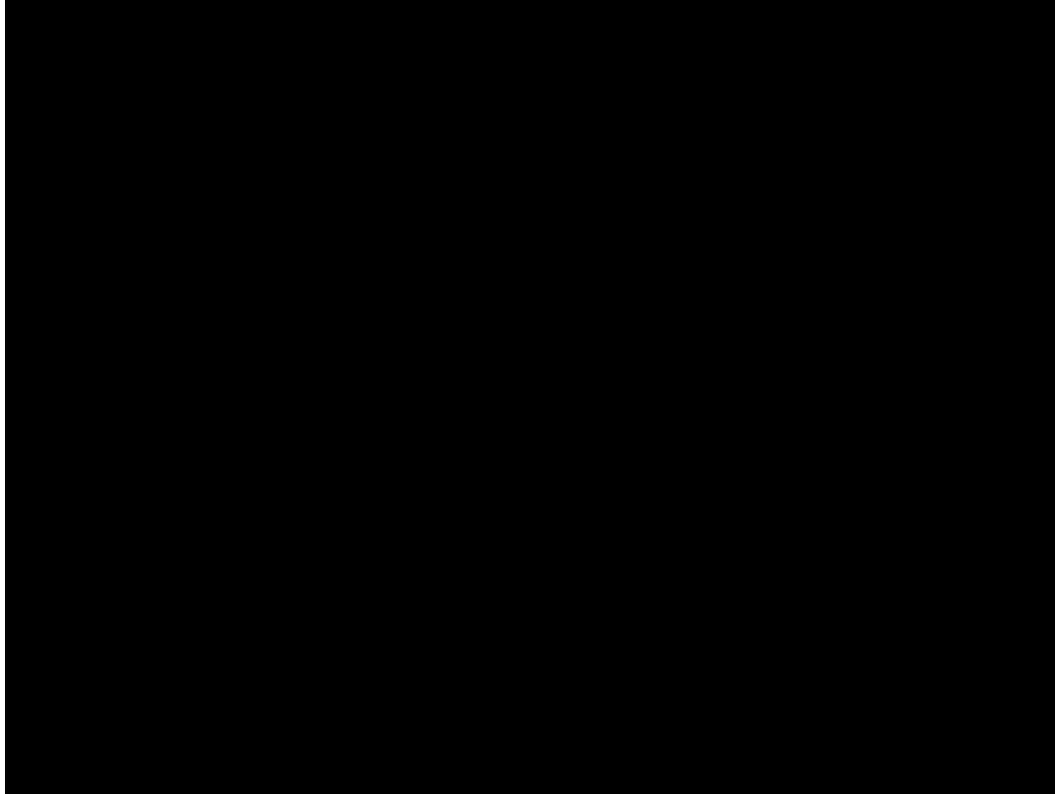
AUTHENTICATE

[Show technical details](#)

Registration successful

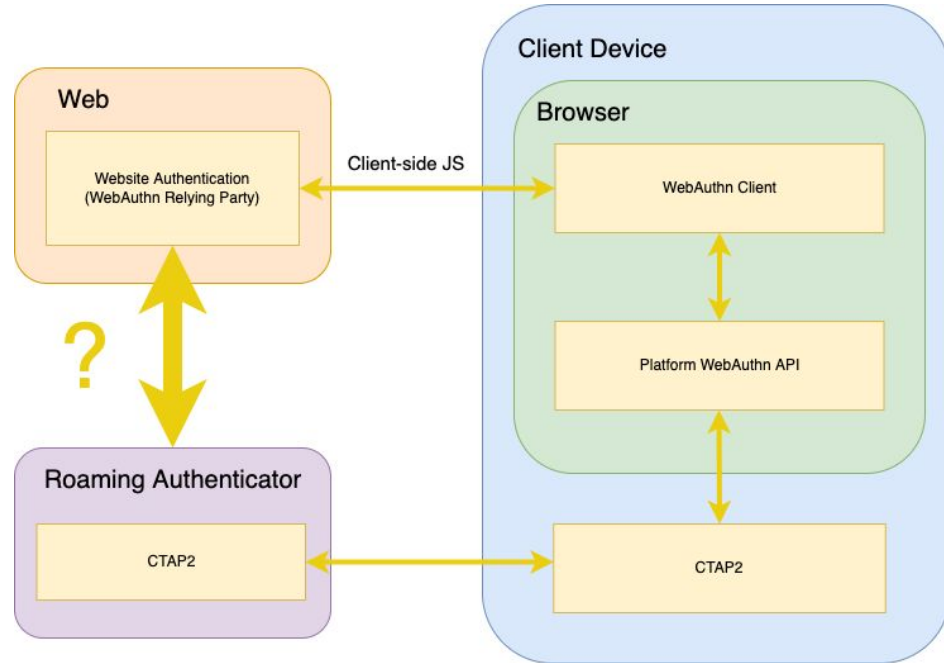
`https://demo.yubico.com/webauthn-technical/login`

PoC Registration-Login Procedure



Thoughts and Discussion

- Attack Vector is feasible, although it's scope is narrow
- Displays the weakness in the FIDO2 protocol architecture
 - If there is a RCE bug in Chrome, sophisticated attacker is able to exploit FIDO2 protocol
- Enterprise mode is secure (for now) if unique identifier is correctly checked



Future Work:

What can be added or re-used in the FIDO2 protocol to make it secure against this attack vector?

How do we make the registration secure in an insecure environment?

Appendix

Chrome bug

- Virtual WebAuthn token requests are automatically accepted without prompt
- Stuffing is done automatically without letting user choose

Issue 1259690: WebAuthn requests from extension background contexts aren't immediately rejected.

Reported by agl@google.com on Wed, Oct 13, 2021, 1:58 PM

EDT

Project Member



Code

[◀ Prev](#) 8 of 126 [Next ▶](#)

[Back to list](#)

A WebAuthn request made from an extension's background context is processed, but cannot display any Chrome UI. It should be rejected immediately instead. Extensions can make requests from pages they `_host_`, but those pages need to be in a tab.