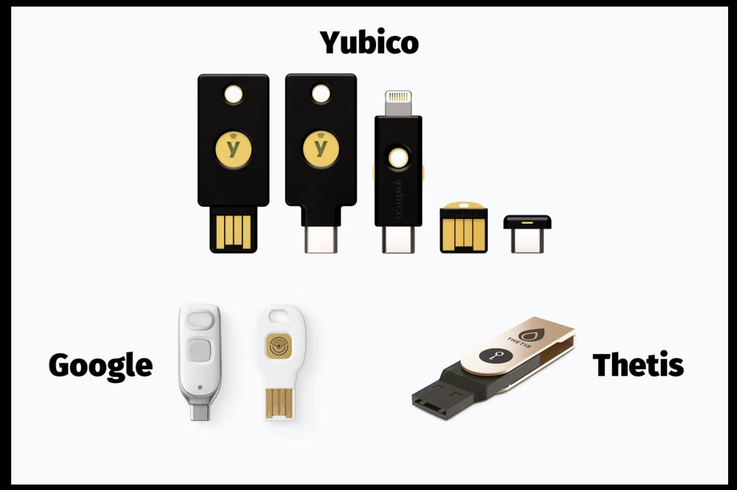
Webauthn in Electron Apps

- Jyotirmay Chauhan

Webauthn Basics

Authenticator

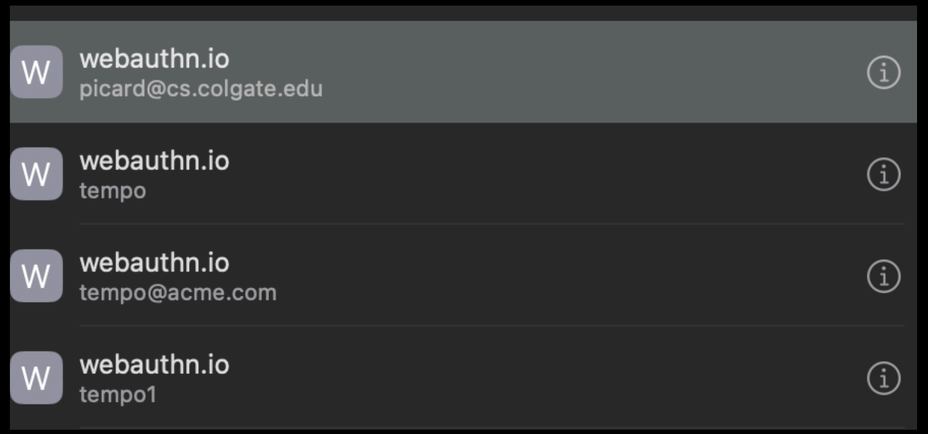
Hardware Keys



On Platform

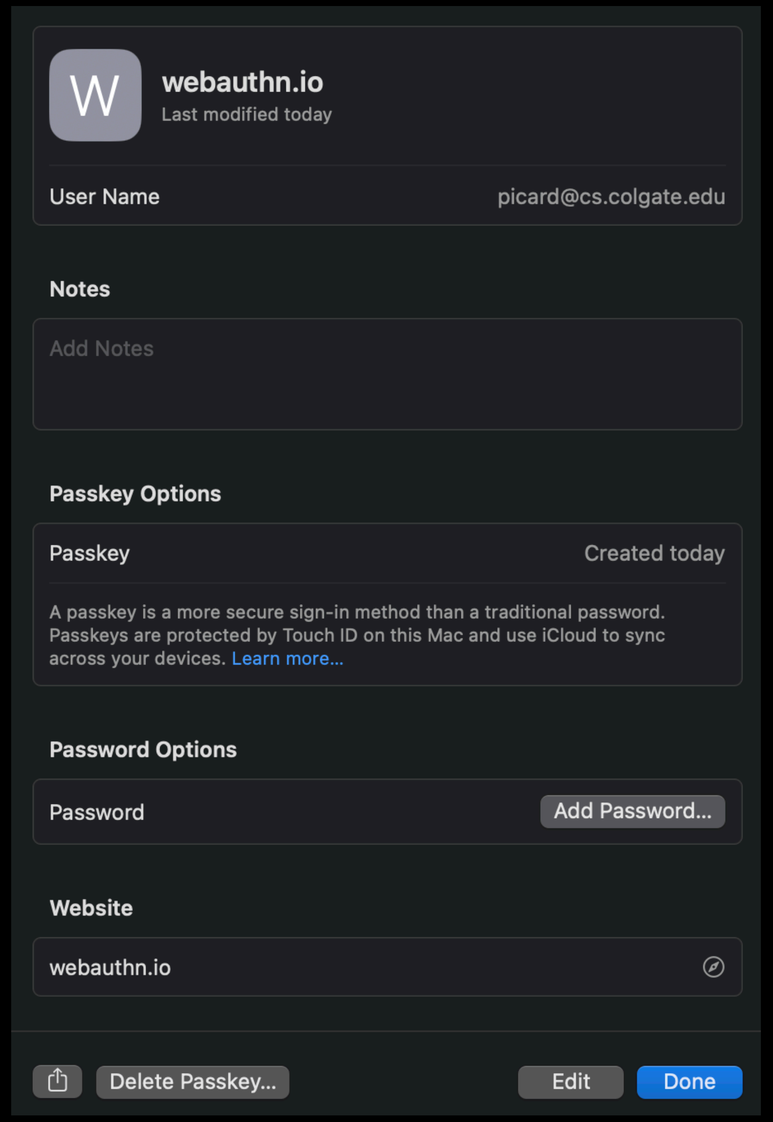
Software Based Authenticator

Key Location



No entries for localhost; Not valid domain

Can’t view the actual passkeys



3 FIDO specifications

U2F

Universal 2nd Factor

FIDO Authenticator as 2nd factor

UAF

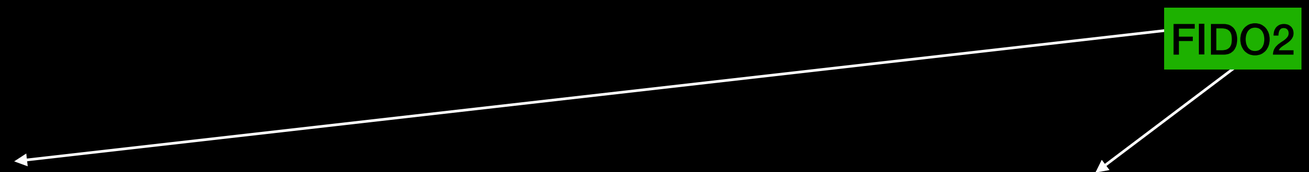
Universal Auth Frameworks

Framework for password-less auth

CTAP

Client To Auth Protocol

OS and Browser Communication
WITH
Authenticators



Webauthn

RP to authenticator
via API

CTAP2

Desktop Applications to authenticator
via API

Certification Standards

L1 L1+

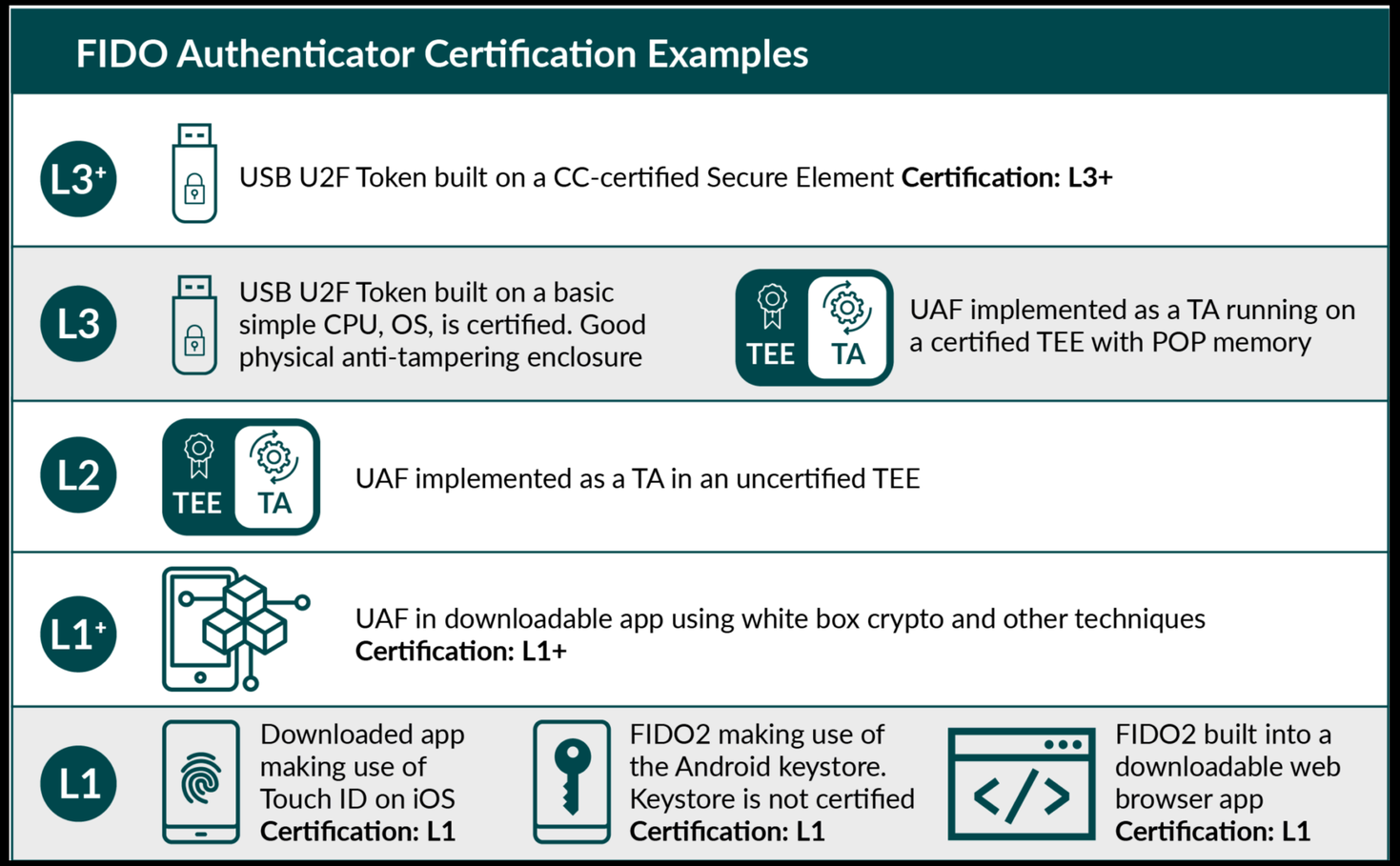
FIDO protocol guarantee
No protection against Malware

Majority of HSKs

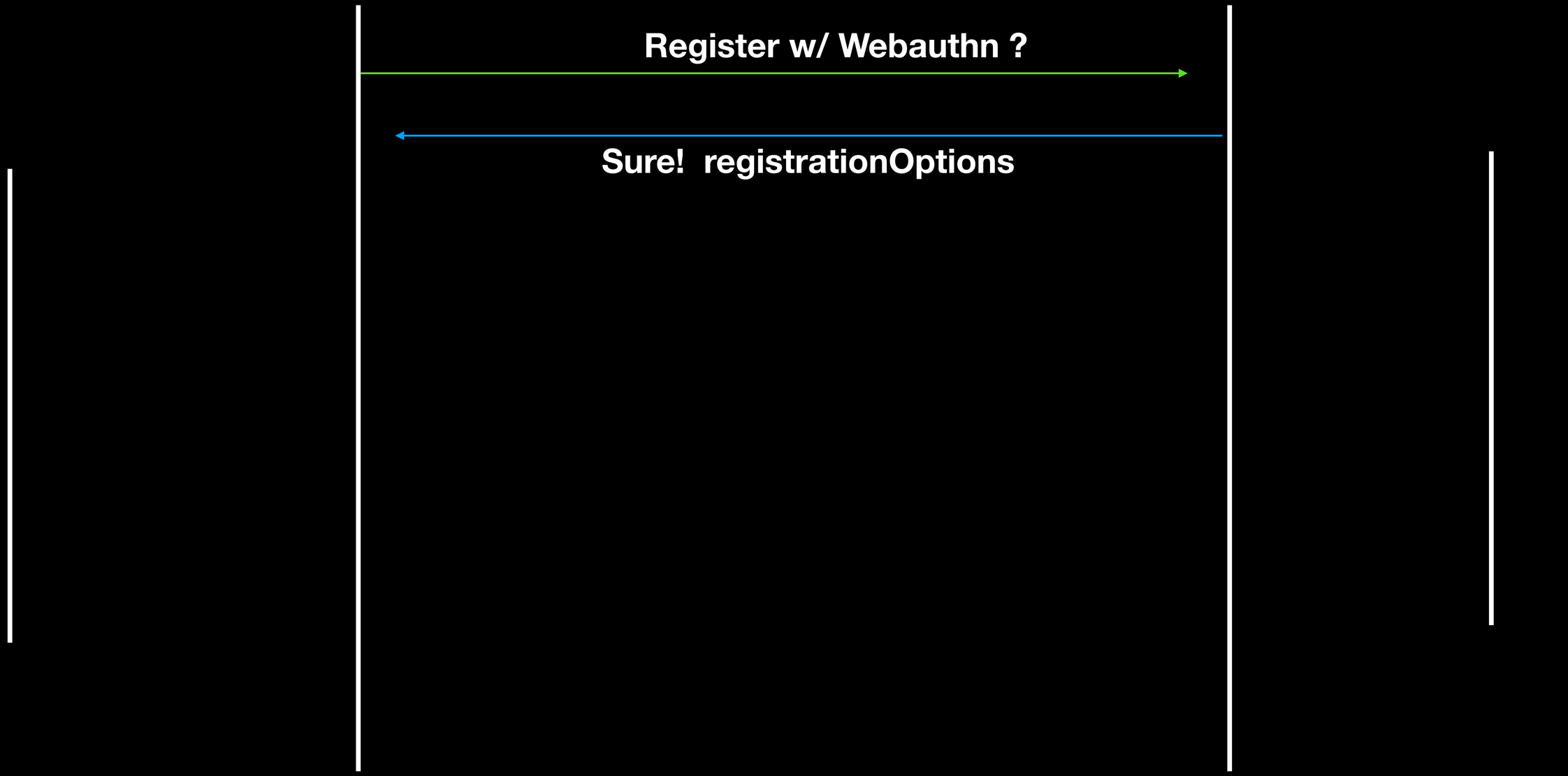
L2

TEE- trusted Execution Environment
FIDO client resides on the hardware itself

L3 L3+



Registration



Registration options

Nonce

RELYING PARTY info

USER
id: might be stored in authenticator

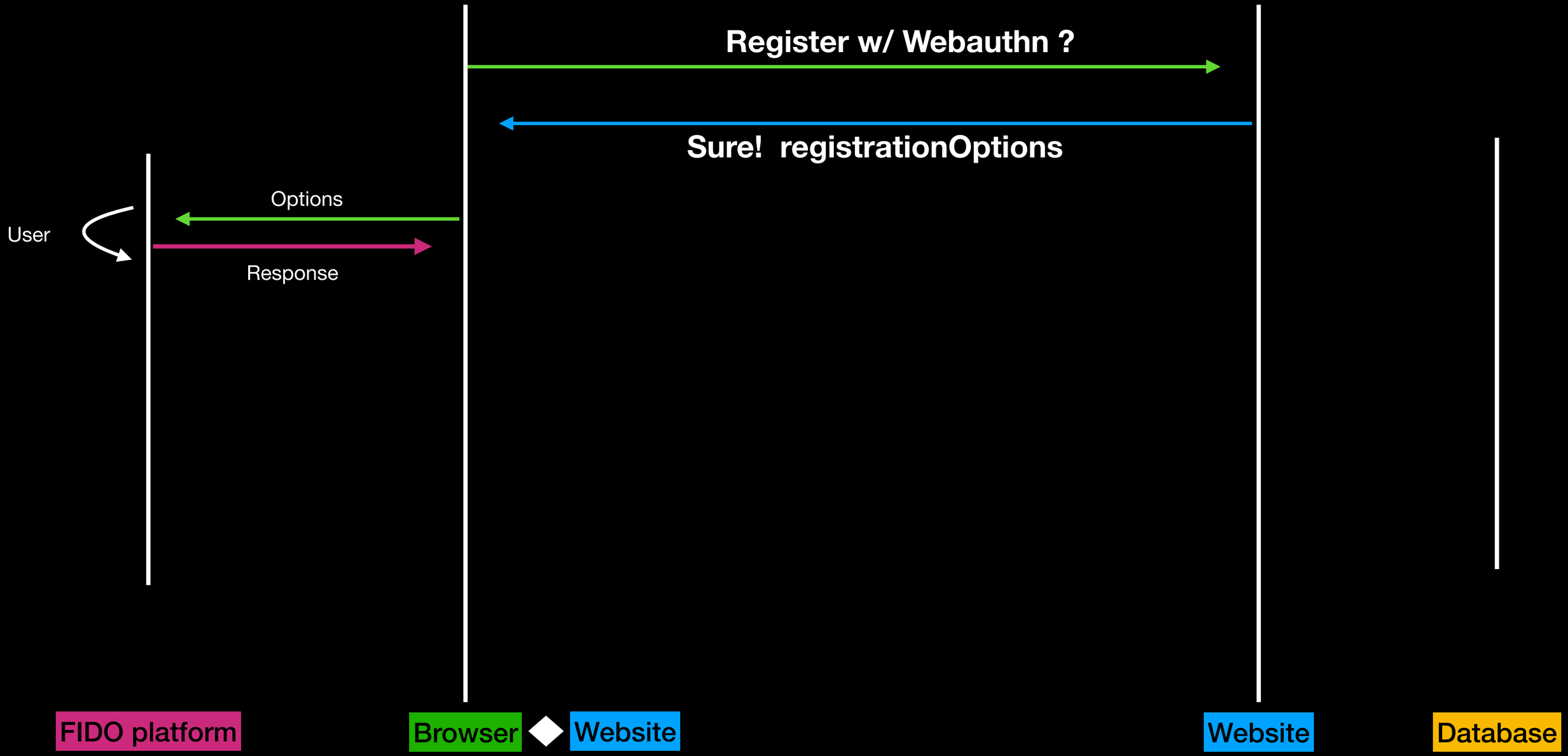
PARAMETERS
hashing algorithm choice + kind of attestation

platform: Touch ID
cross-platform: Yubikey

Kind of Attestation:

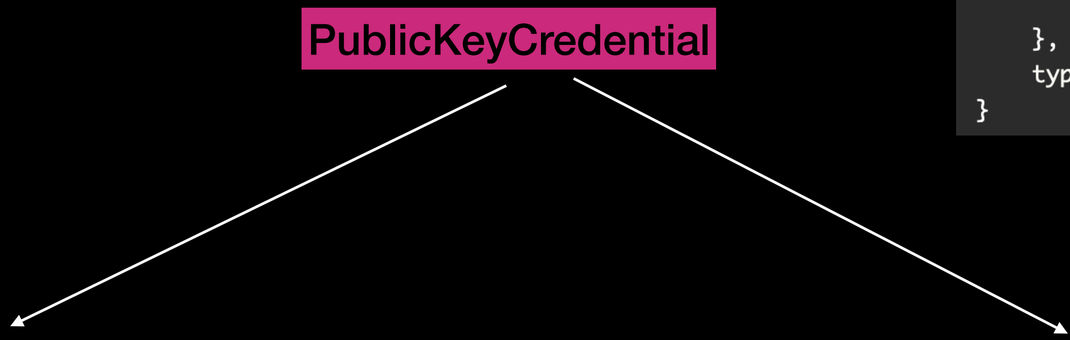
```
const publicKeyCredentialCreationOptions = {
    challenge: Uint8Array.from(
        randomStringFromServer, c => c.charCodeAt(0)),
    rp: {
        name: "Duo Security",
        id: "duosecurity.com",
    },
    user: {
        id: Uint8Array.from(
            "UZSL85T9AFC", c => c.charCodeAt(0)),
        name: "lee@webauthn.guide",
        displayName: "Lee",
    },
    pubKeyCredParams: [{alg: -7, type: "public-key"}],
    authenticatorSelection: {
        authenticatorAttachment: "cross-platform",
    },
    timeout: 60000,
    attestation: "direct"
};

const credential = await navigator.credentials.create({
    publicKey: publicKeyCredentialCreationOptions
});
```

Registration



Response: PublicKeyCredential

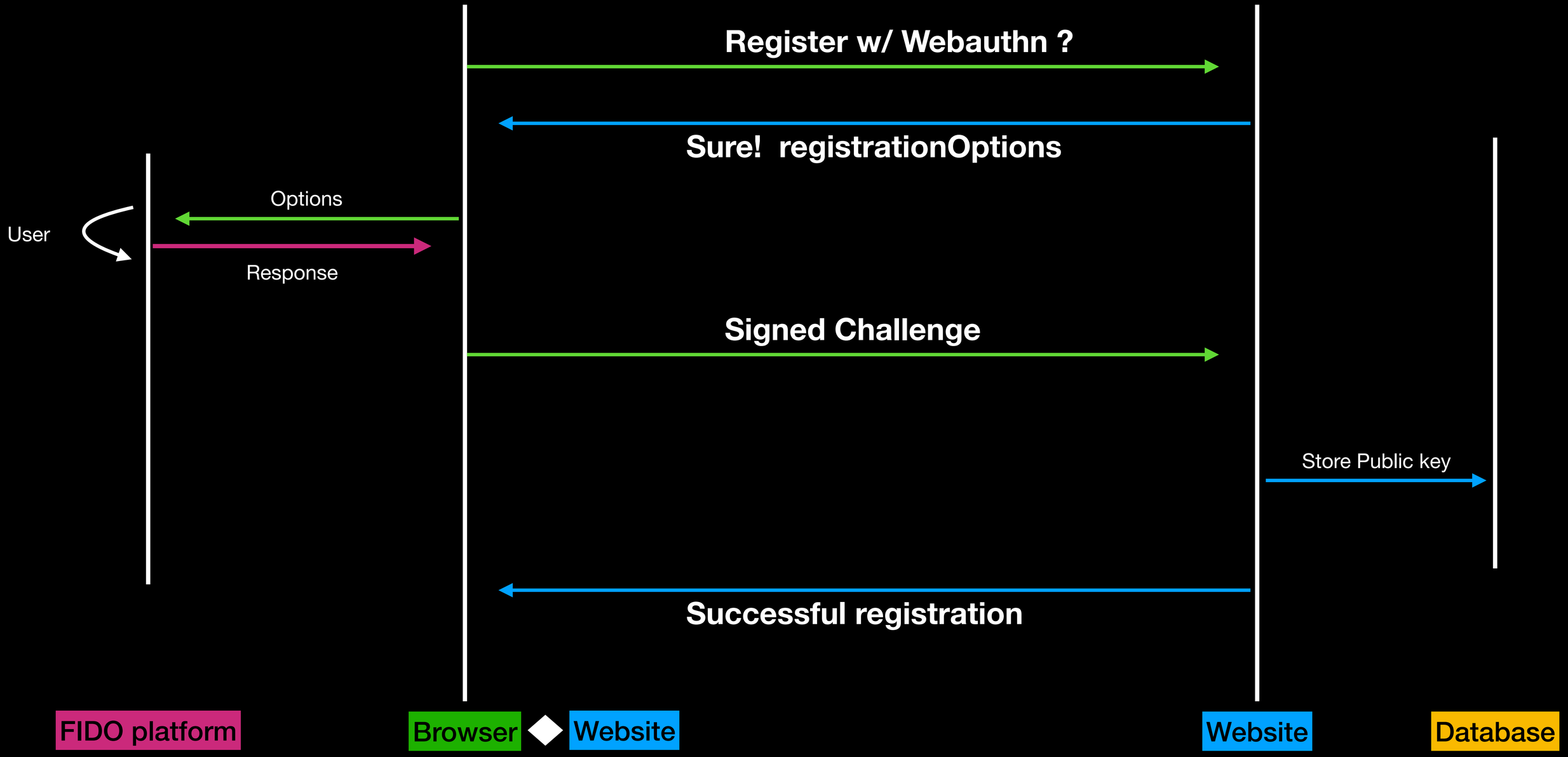
```
PublicKeyCredential {
    id: 'ADSUllKQmbqdGtpu4sjseh4cg2TxSvrbcHDTBsv4NSSX9...',
    rawId: ArrayBuffer(59),
    response: AuthenticatorAttestationResponse {
        clientDataJSON: ArrayBuffer(121),
        attestationObject: ArrayBuffer(306),
    },
    type: 'public-key'
}
```



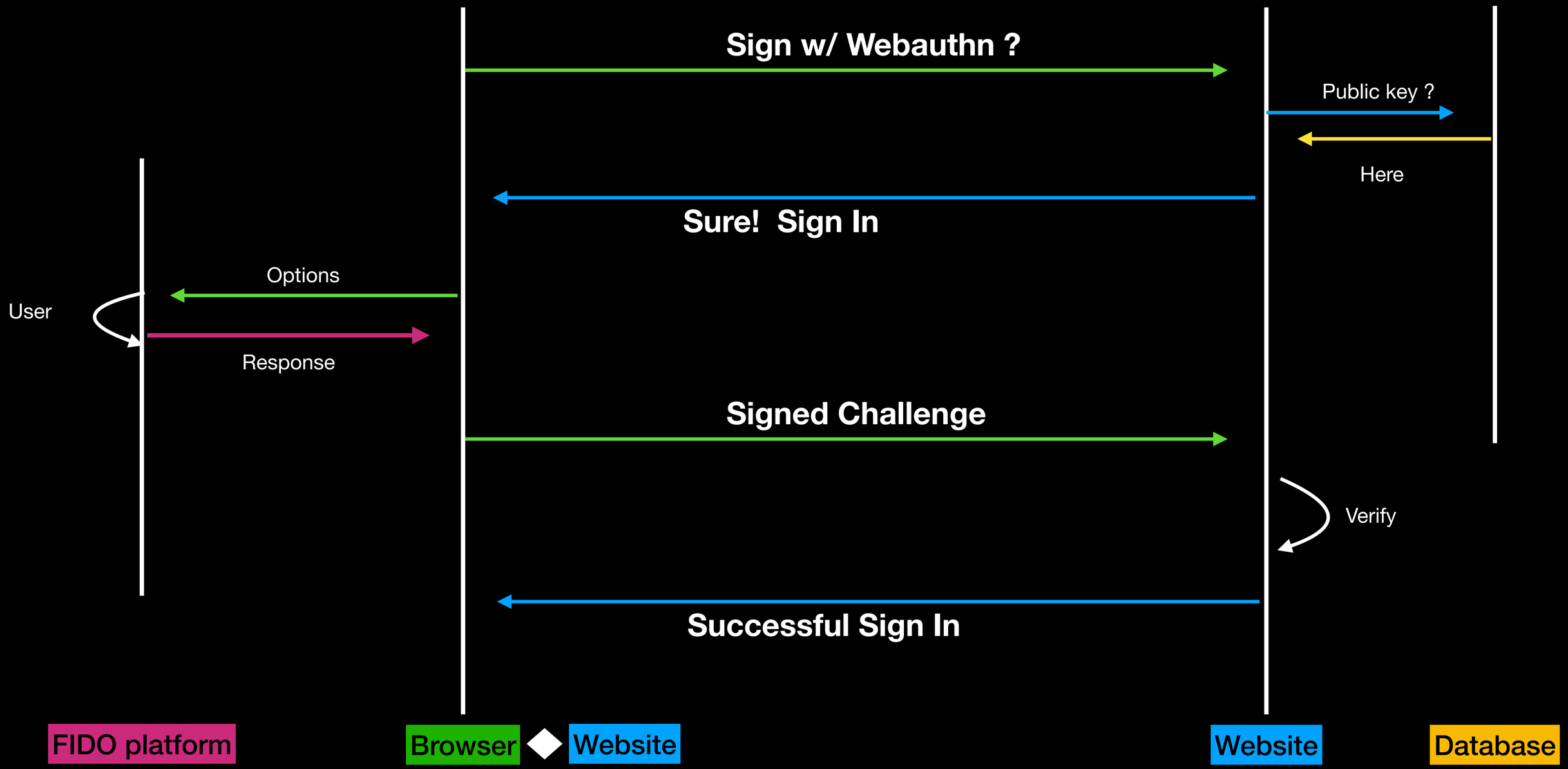

```
challenge: "p5aV2uHXr0AOqUk7HQitvi-Ny1....",
origin: "https://webauthn.guide",
type: "webauthn.create"
```

```
authData: Uint8Array(196),
fmt: "fido-u2f",
attStmt: {
    sig: Uint8Array(70),
    x5c: Array(1),
},
```

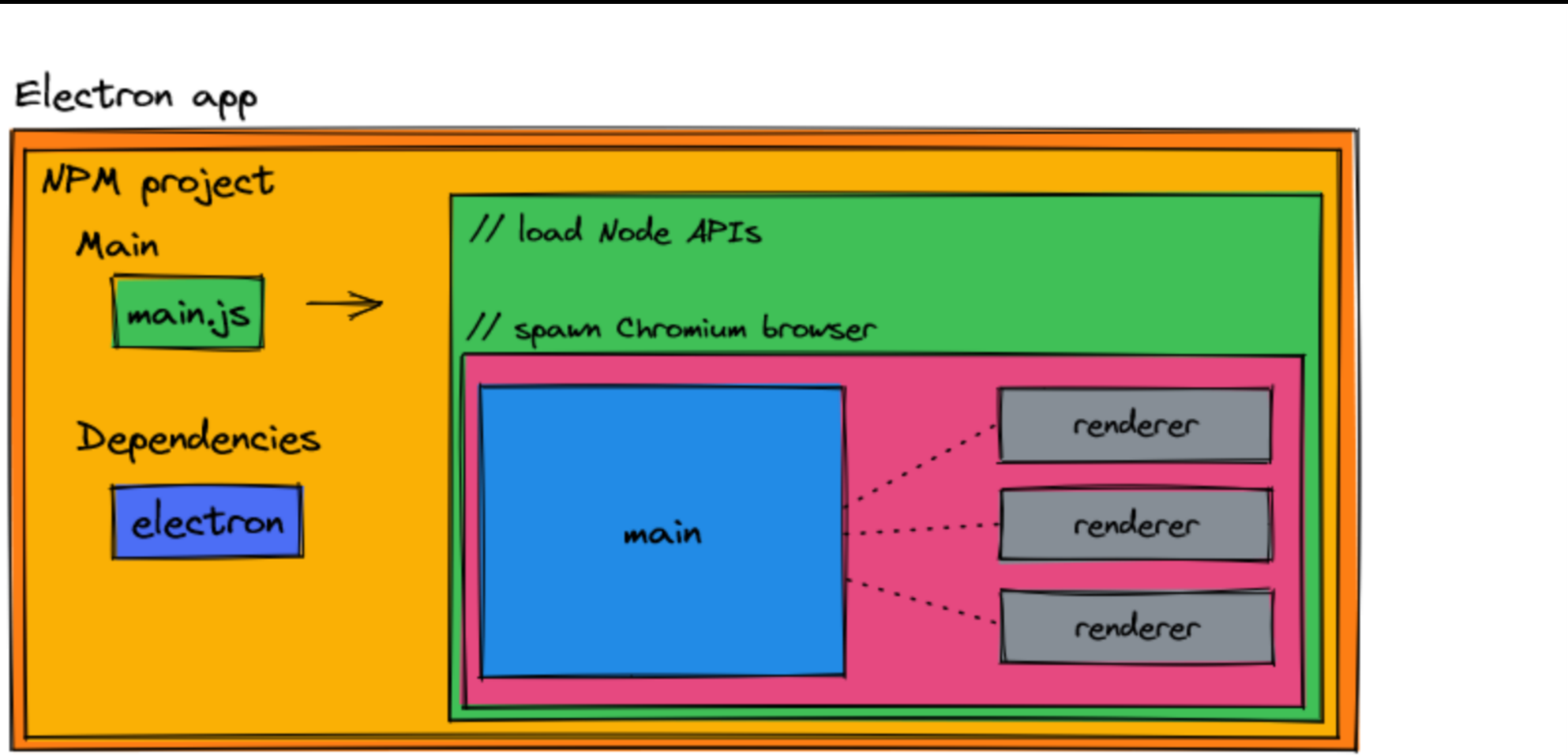
Registration



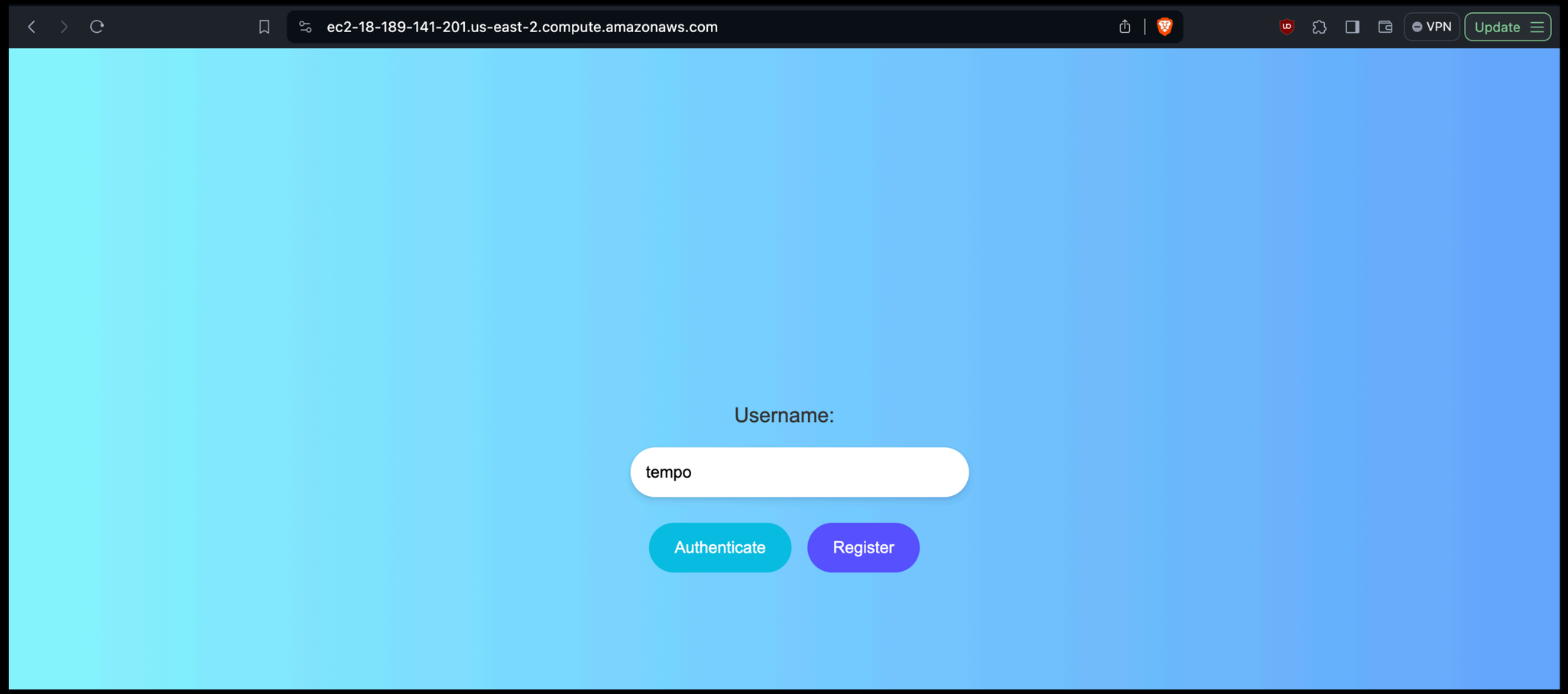
Sign In

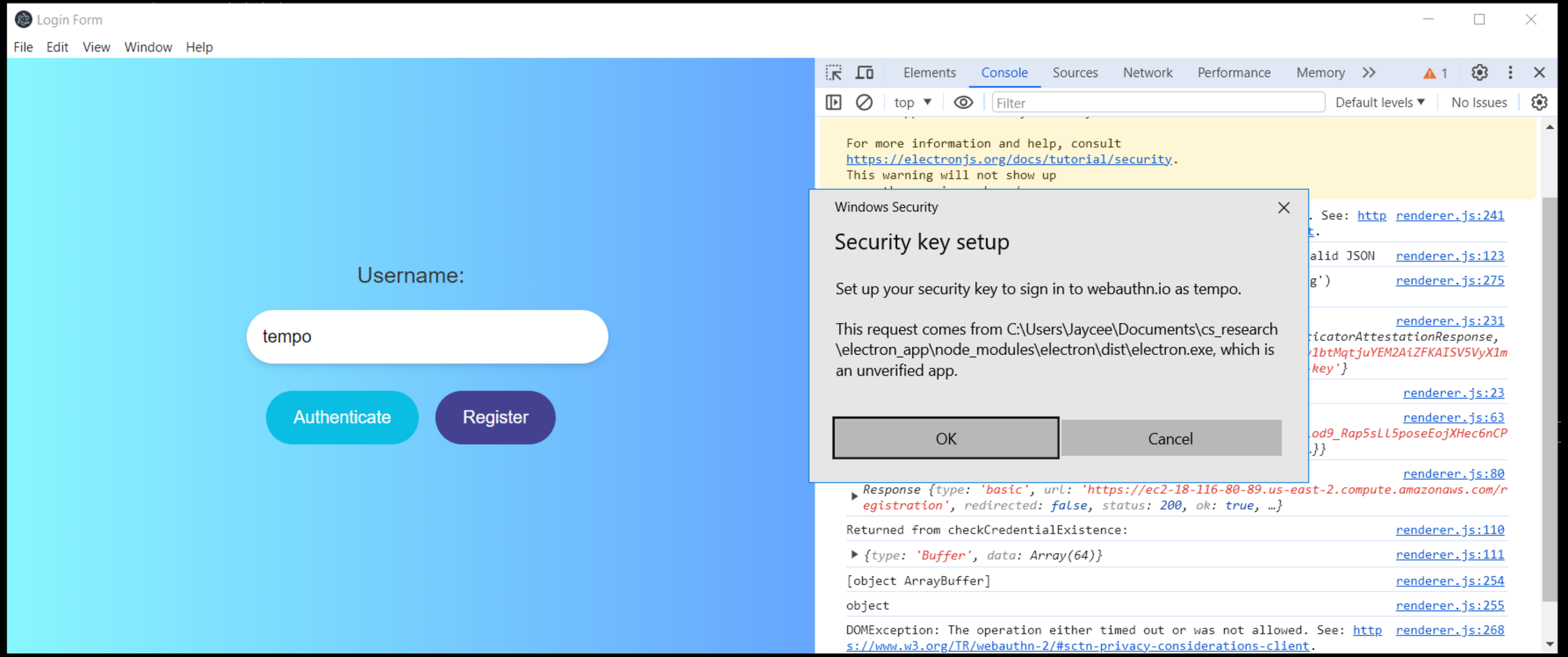

Sign w/ Webauthn ?
Public key ?
Here
Sure! Sign In
Options
User
Response
Signed Challenge
Verify
Successful Sign In
FIDO platform
Browser
Website
Website
Database

Electron


Electron app
NPM project
Main
main.js
Dependencies
electron
// load Node APIs
// spawn Chromium browser
main
renderer
renderer
renderer

Deployed on AWS EC2



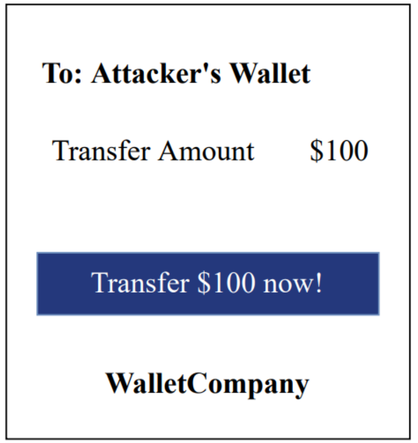

Login Form
File Edit View Window Help
Username:
tempo
Authenticate
Register
Elements Console Sources Network Performance Memory
top
Filter
Default levels
No Issues
For more information and help, consult
https://electronjs.org/docs/tutorial/security.
This warning will not show up
Windows Security
Security key setup
Set up your security key to sign in to webauthn.io as tempo.
This request comes from C:\Users\Jaycee\Documents\cs_research\electron_app\node_modules\electron\dist\electron.exe, which is an unverified app.
OK
Cancel
renderer.js:241
renderer.js:123
renderer.js:275
renderer.js:231
renderer.js:23
renderer.js:63
renderer.js:80
Response {type: 'basic', url: 'https://ec2-18-116-80-89.us-east-2.compute.amazonaws.com/registration', redirected: false, status: 200, ok: true, …}
Returned from checkCredentialExistence:
renderer.js:110
{type: 'Buffer', data: Array(64)}
renderer.js:111
[object ArrayBuffer]
renderer.js:254
object
renderer.js:255
DOMException: The operation either timed out or was not allowed. See: https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client.
renderer.js:268

Prior Work

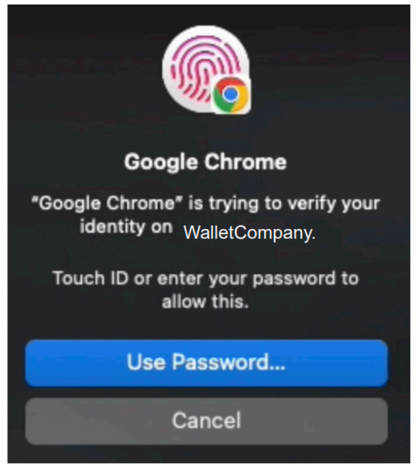
Social Engineering Attack

(a) User downloads and installs a malicious browser extension [61].

(b) With an active session on WalletCo., user attempts to make a transaction on another merchant site, say MerchantCo.



(c) Extension detects the transaction and attempts attacker-initiated action (e.g., transferring funds to the attacker's wallet) in a background tab. This triggers a FIDO2 authentication prompt.



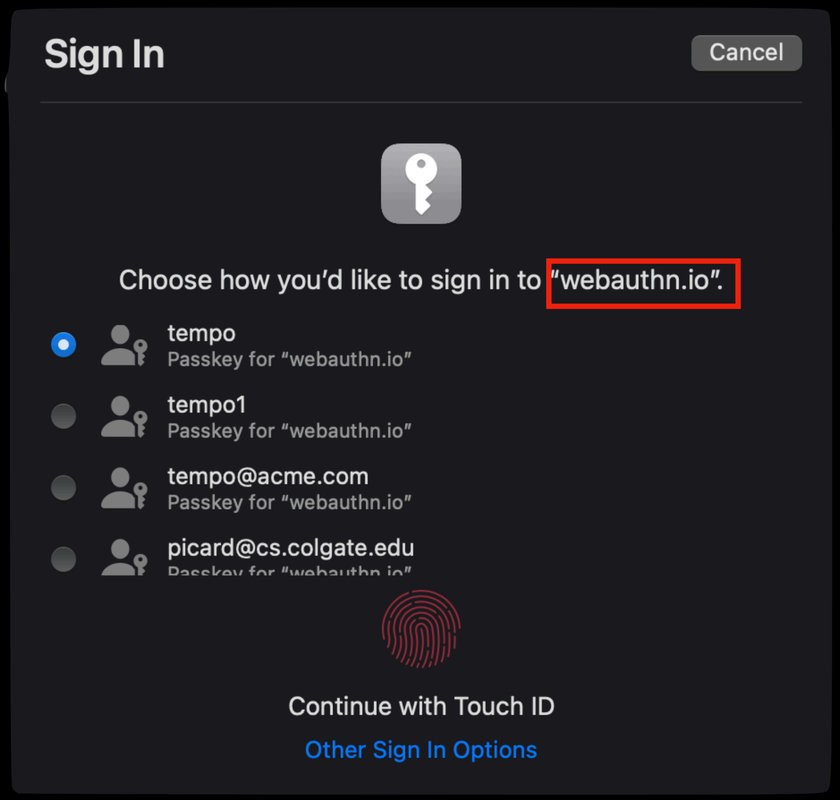
(d) User is tricked into authenticating the attacker's transaction, mistaking it as authenticating their own transaction (which did not actually require authentication).

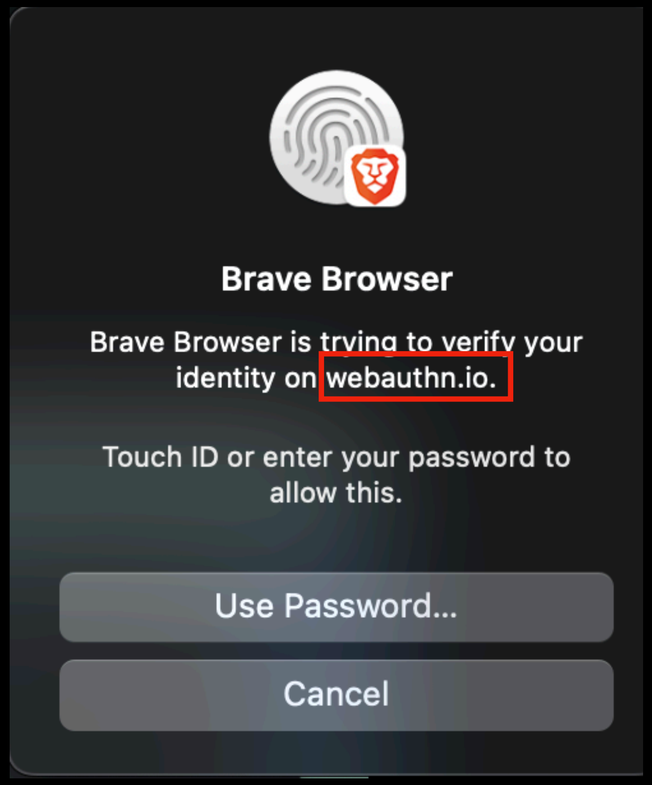
Via browser Extensions
permission: tabs, scripting, host extension

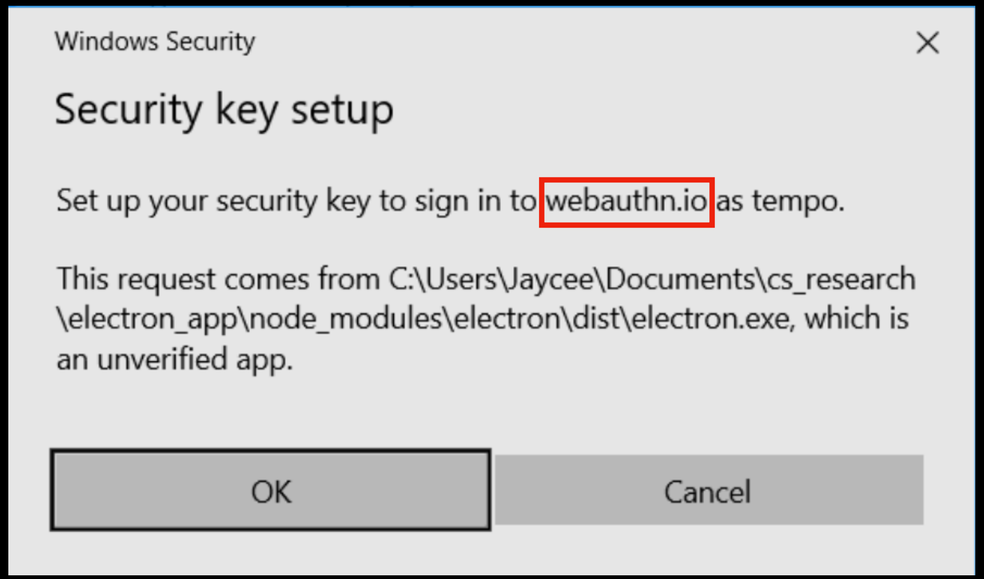
The Popup

How does it look like?

Any common component ?





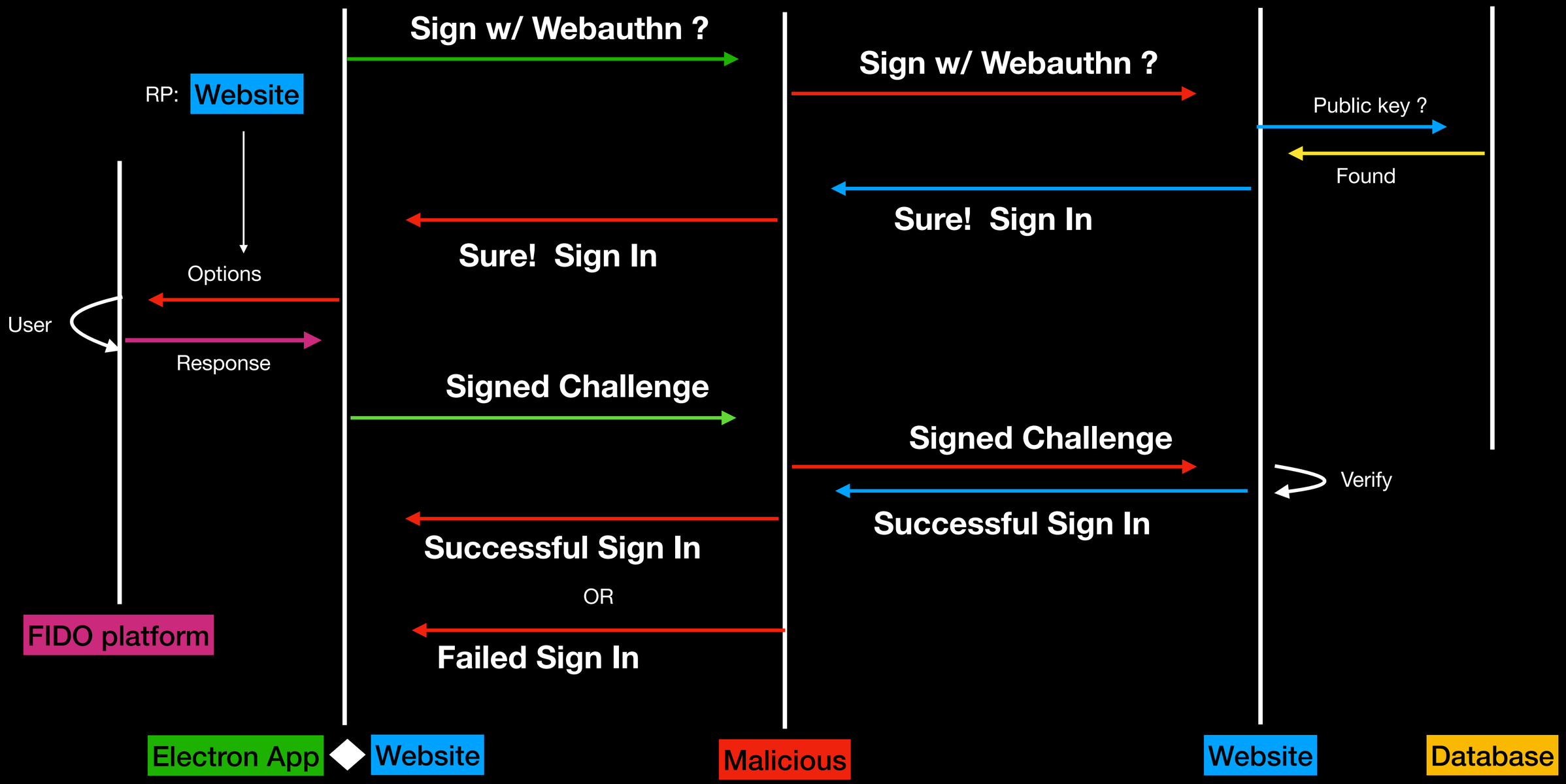


Attacker Model: Origin Spoofing

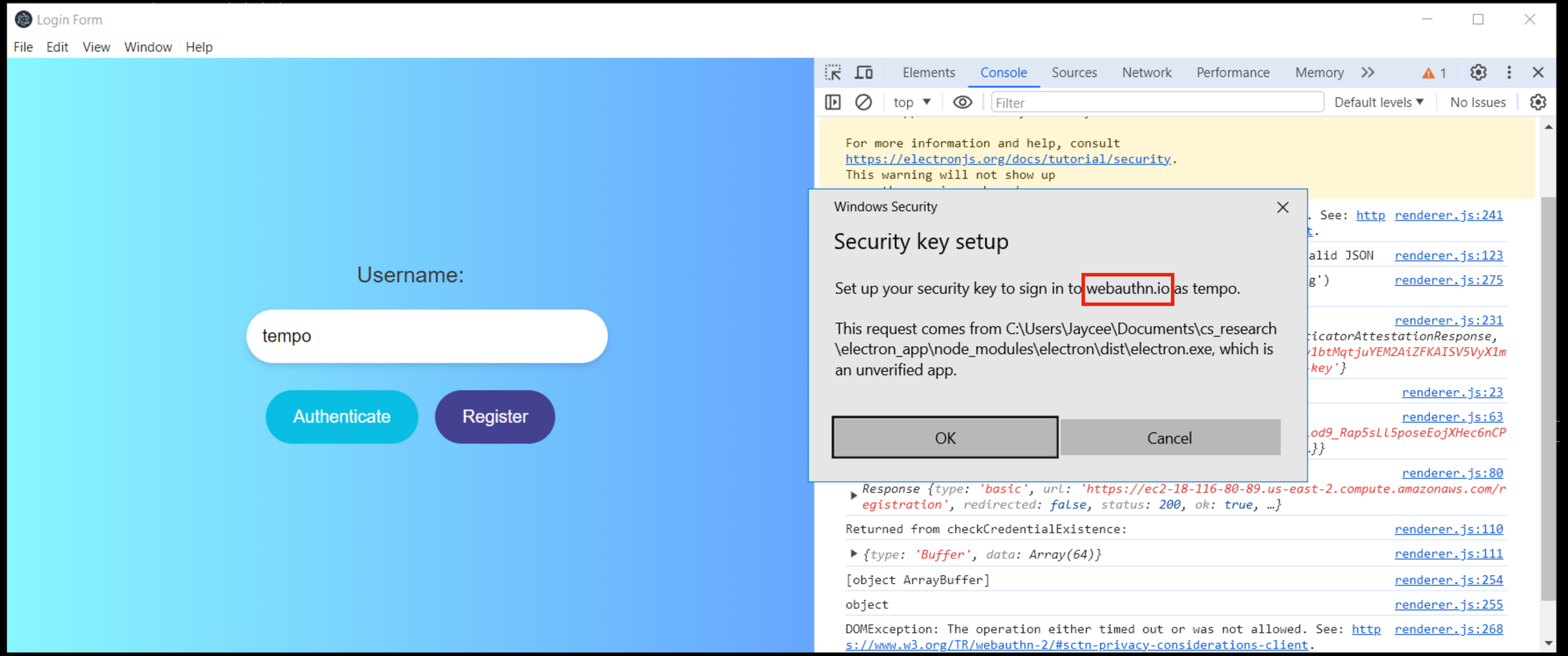
Main Idea

- If I can spoof the ORIGIN

- Load a phishing page and steal credentials.
  - But passive credential stealing won’t work


Sign w/ Webauthn ?
Sign w/ Webauthn ?
RP:
Website
Public key ?
Found
Sure! Sign In
Sure! Sign In
Options
User
Response
Signed Challenge
Signed Challenge
Verify
Successful Sign In
Successful Sign In
OR
Failed Sign In
FIDO platform
Electron App
Website
Malicious
Website
Database

Proof of Concept


Login Form
File Edit View Window Help
Username:
tempo
Authenticate
Register
Elements Console Sources Network Performance Memory
top
Filter
Default levels
No Issues
For more information and help, consult
https://electronjs.org/docs/tutorial/security.
This warning will not show up
Windows Security
Security key setup
Set up your security key to sign in to webauthn.io as tempo.
This request comes from C:\Users\Jaycee\Documents\cs_research\electron_app\node_modules\electron\dist\electron.exe, which is an unverified app.
OK
Cancel
renderer.js:241
renderer.js:123
renderer.js:275
renderer.js:231
renderer.js:23
renderer.js:63
renderer.js:80
Response {type: 'basic', url: 'https://ec2-18-116-80-89.us-east-2.compute.amazonaws.com/registration', redirected: false, status: 200, ok: true, …}
Returned from checkCredentialExistence:
renderer.js:110
{type: 'Buffer', data: Array(64)}
renderer.js:111
[object ArrayBuffer]
renderer.js:254
object
renderer.js:255
DOMException: The operation either timed out or was not allowed. See: https://www.w3.org/TR/webauthn-2/#sctn-privacy-considerations-client.
renderer.js:268

webauthn.io

WebAuthn.io

A demo of the WebAuthn specification

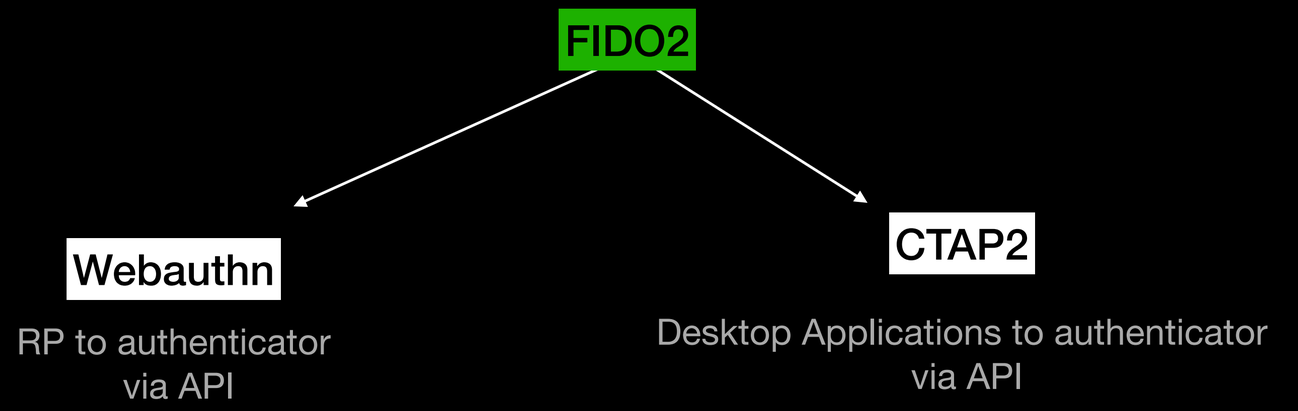
example_username

Register | Authenticate

Advanced Settings

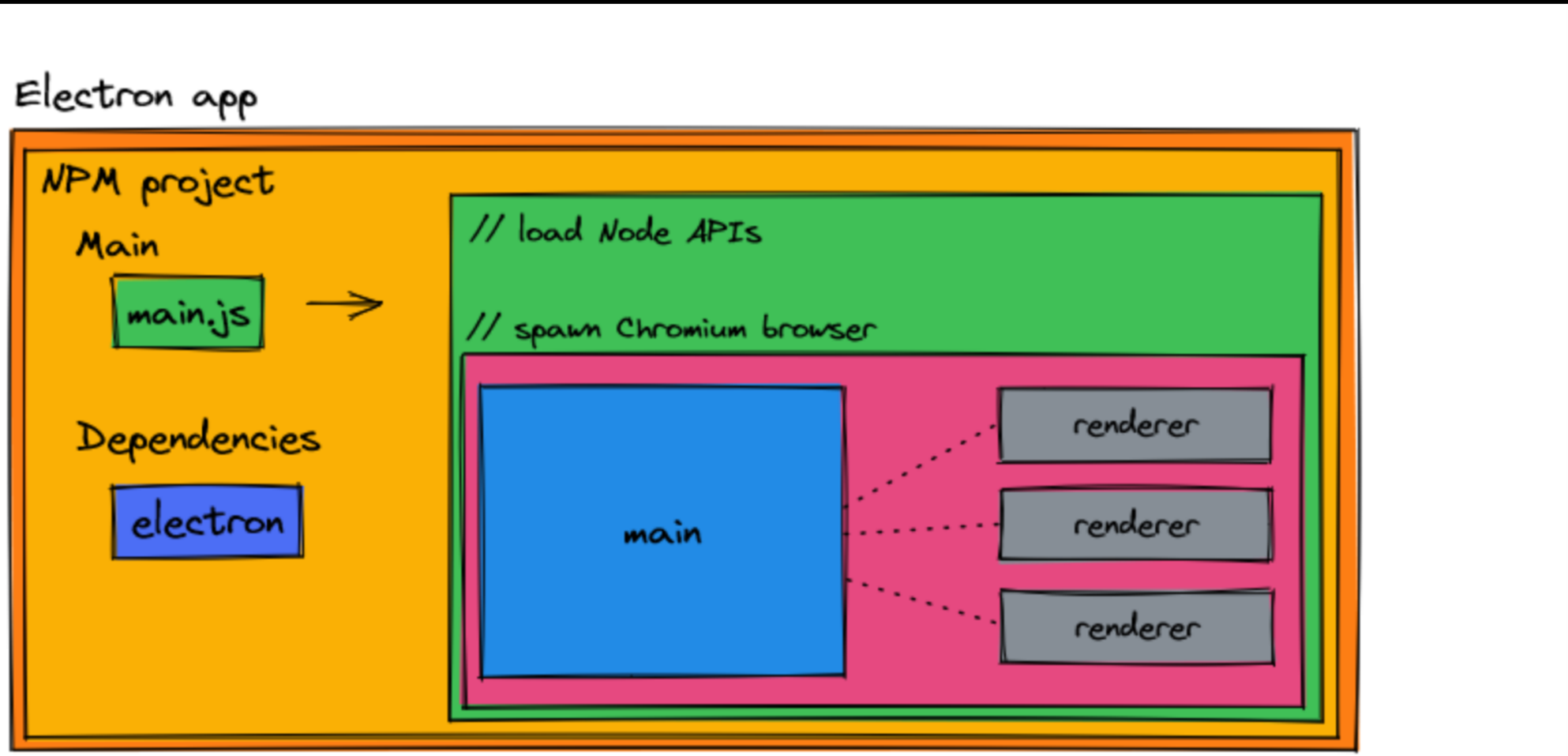
Vulnerability

App or Website?



- Webauthn - Origin
- CTAP - Relying Party ID of Application

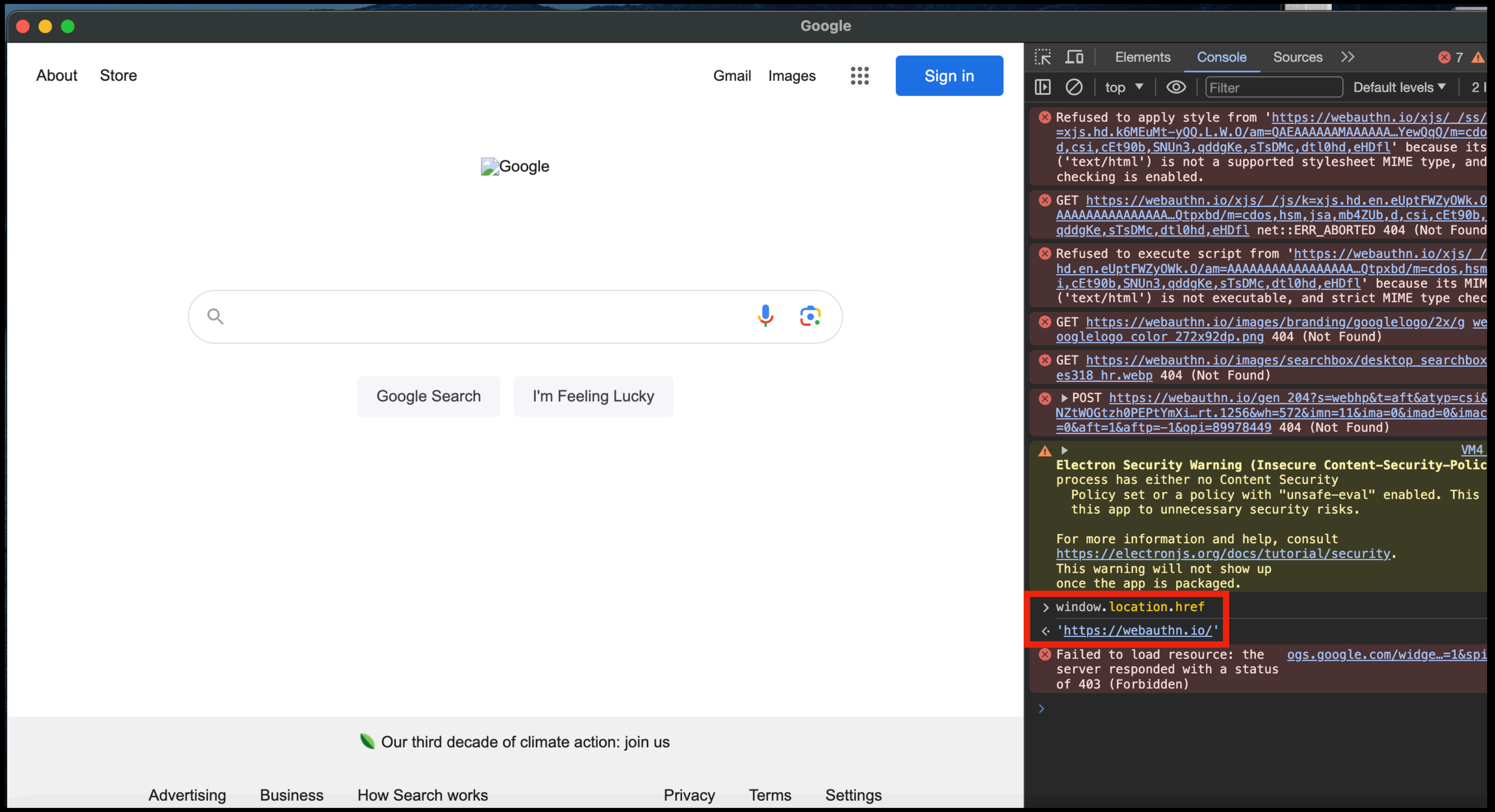
- Which one to use on electron?


Electron app
NPM project
Main
main.js
Dependencies
electron
// load Node APIs
// spawn Chromium browser
main
renderer
renderer
renderer

```
protocol.handle('https', (req) => {
  const { host, pathname } = new URL(req.url);
  if (host === 'webauthn.io' && (pathname === '/' || pathname === '/renderer.js' )) {
    const url = new URL('.' + (pathname === '/' ? '/index.html' : pathname), pathToFileURL(__filename));
    return net.fetch("https://google.com");
  }
  return net.fetch(req, { bypassCustomProtocolHandlers: true });
});
```

Malicious URL

old library perhaps.
ANY URL endpoint on the Internet


Google
About
Store
Gmail
Images
Sign in
Google
Google Search
I'm Feeling Lucky
Our third decade of climate action: join us
Advertising
Business
How Search works
Privacy
Terms
Settings
Elements
Console
Sources
top
Filter
Default levels
Refused to apply style from 'https://webauthn.io/xjs/_/ss/=xjs.hd.k6MEuMt-yQQ.L.W.O/am=QAEAAAAAAMAAAAAA…YewQqQ/m=cdod,csi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl' because its ('text/html') is not a supported stylesheet MIME type, and checking is enabled.
GET https://webauthn.io/xjs/_/js/k=xjs.hd.en.eUptFWZyOWk.O AAAAAAAAAAAAAAA…Qtpxbd/m=cdos,hsm,jsa,mb4ZUb,d,csi,cEt90b,qddgKe,sTsDMc,dtl0hd,eHDfl net::ERR_ABORTED 404 (Not Found
Refused to execute script from 'https://webauthn.io/xjs/_/hd.en.eUptFWZyOWk.O/am=AAAAAAAAAAAAAAAA…Qtpxbd/m=cdos,hsmi,cEt90b,SNUn3,qddgKe,sTsDMc,dtl0hd,eHDfl' because its MIM ('text/html') is not executable, and strict MIME type chec
GET https://webauthn.io/images/branding/googlelogo/2x/g ooglelogo_color_272x92dp.png 404 (Not Found)
GET https://webauthn.io/images/searchbox/desktop_searchbox es318_hr.webp 404 (Not Found)
POST https://webauthn.io/gen_204?s=webhp&t=aft&atyp=csi&NZtWOGtzh0PEPtYmXi…rt.1256&wh=572&imn=11&ima=0&imad=0&imac=0&aft=1&aftp=-1&opi=89978449 404 (Not Found)
VM4
Electron Security Warning (Insecure Content-Security-Polic
process has either no Content Security
Policy set or a policy with "unsafe-eval" enabled. This
this app to unnecessary security risks.
For more information and help, consult
https://electronjs.org/docs/tutorial/security.
This warning will not show up
once the app is packaged.
window.location.href
'https://webauthn.io/'
Failed to load resource: the server responded with a status of 403 (Forbidden)
ogs.google.com/widge…=1&spi

Future Work

- Looking at Webauthn in electron apps

- Github:
  - Doesn’t do webauthn in app
  - Custom schemes:
  - GOAL: Hijack callback url w/ custom schema

```
<key>CFBundleURLTypes</key>
<array>
  <dict>
    <key>CFBundleURLName</key>
    <string>com.github.GitHubClient</string>
    <key>CFBundleURLSchemes</key>
    <array>
      <string>x-github-desktop-auth</string>
      <string>x-github-client</string>
      <string>github-mac</string>
    </array>
  </dict>
</array>
```

Future Work

- Lots of possibilities beyond webauthn
- Possible exploits:
  - Phishing Attack
  - Malware distribution
  - Session hijack

JUDGEMENT &. QnA

- What do you guys think ?