German OWASP Day 2025

Phishing for Passkeys

An Analysis of WebAuthn and CTAP

MICHAEL KUCKUK

Phishing for Passkeys - Regular Phishing

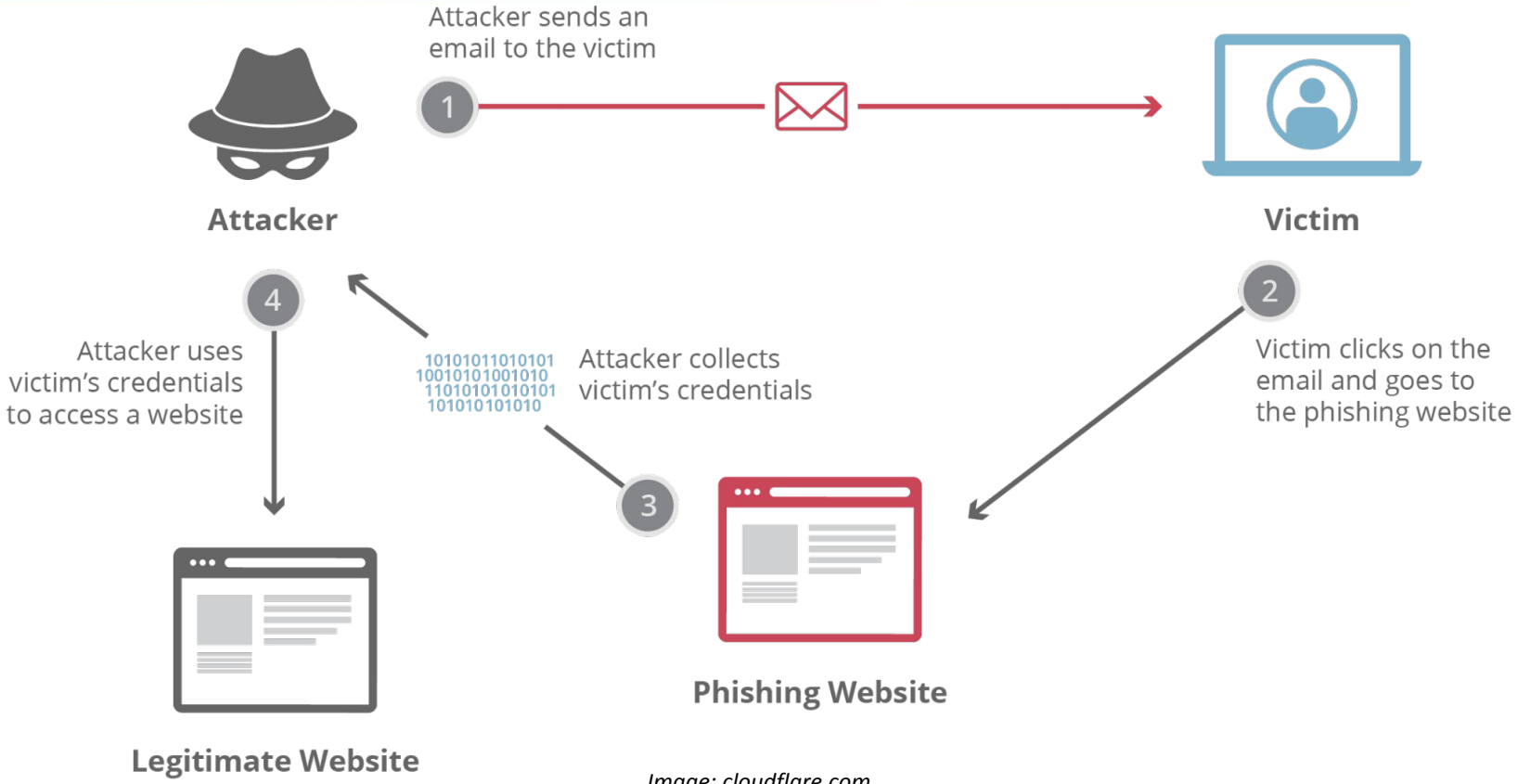


Image: cloudflare.com


Regular Page
Phishing Page
Corporate needs you to find the differences between this picture and this picture.
Humans
They're the same picture.
imgflip.com

Have I Been Pwned: Projektbetreiber Troy Hunt gepwned

Der Betreiber von Have I Been Pwned wurde selbst Opfer eines Phishing-Angriffs. Die E-Mails der Newsletter-Mailingliste wurden gestohlen.

Have I Been Pwned? Yes! (Bild: heise online / dmk)

26.03.2025, 11:06 Uhr Lesezeit: 3 Min. | Security

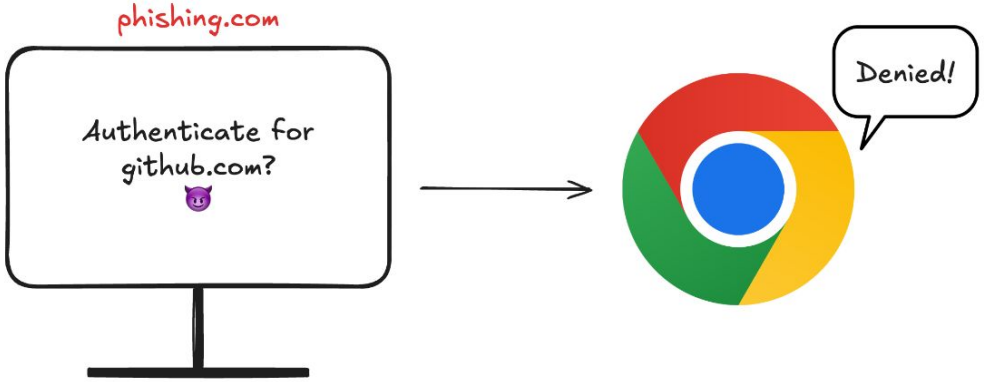
Von Dirk Knop

OWASP.DE

Resistance against phishing

- Server declares its Relying Party ID (RPID, usually the website's domain or superdomain)
- Browser checks if current website may access that RPID
- Authenticator ignores credentials that belong to other RPIDs

→ Users cannot use credentials for unintended (= phishing) website!



Resistance against phishing

- Server declares its Relying Party ID (RPID, usually the website's domain or superdomain)
- Browser checks if current website may access that RPID
- Authenticator ignores credentials that belong to other RPIDs

→ Users cannot use credentials for unintended (= phishing) website!

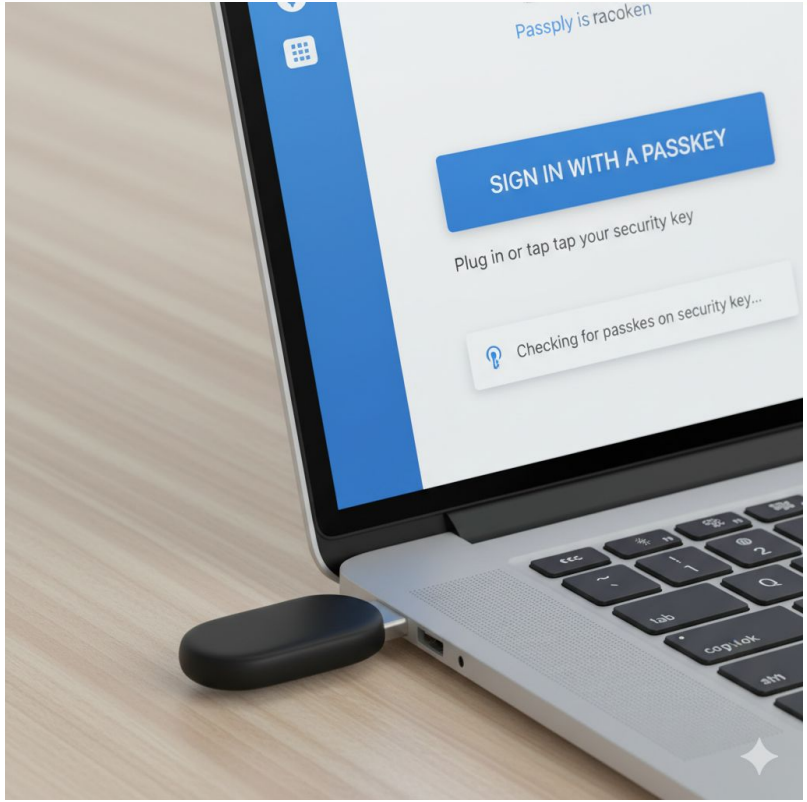


Image is AI generated

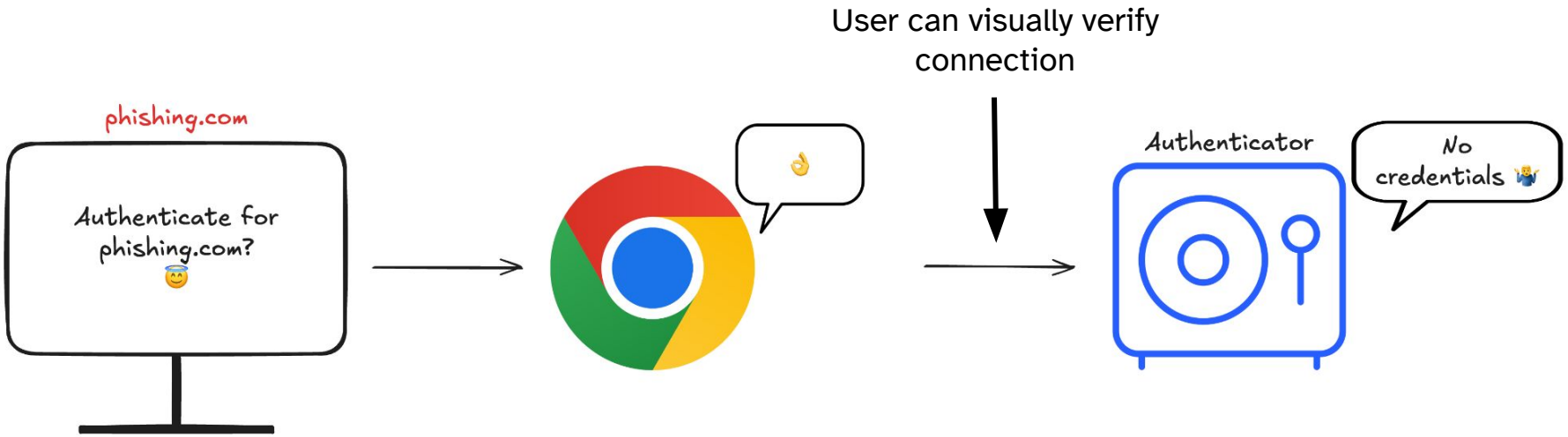
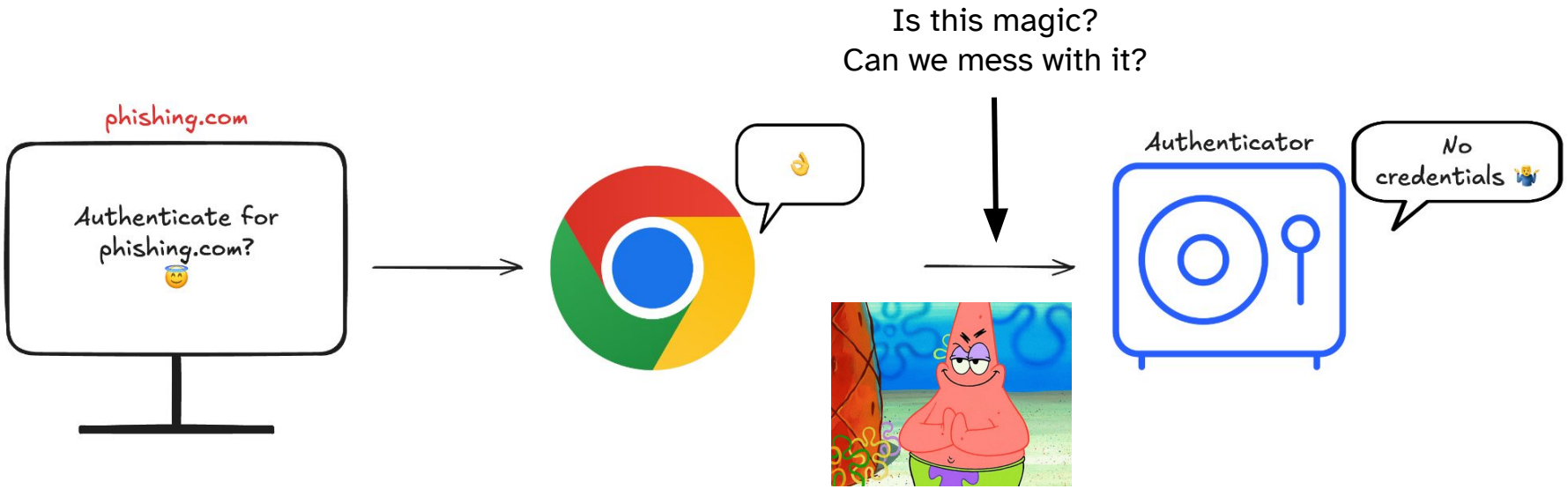

User can visually verify connection
phishing.com
Authenticate for phishing.com?
Authenticator
No credentials

Image is AI generated


Is this magic?
Can we mess with it?
phishing.com
Authenticate for phishing.com?
👌
Authenticator
No credentials

Cross Device Authentication (CDA) & CTAP

- “Platform-attached”: authenticator device = client device 🤔
- “Cross-platform-attached”: authenticator device ≠ client device 👀👀👀👀
- Communication specified in Client To Authenticator Protocol (CTAP)
  - Guarantees physical proximity between client and authenticator
  - Transports*: USB, NFC, Bluetooth Low Energy (BLE)

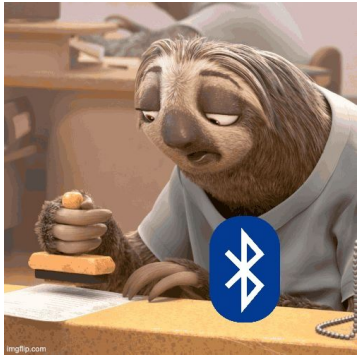
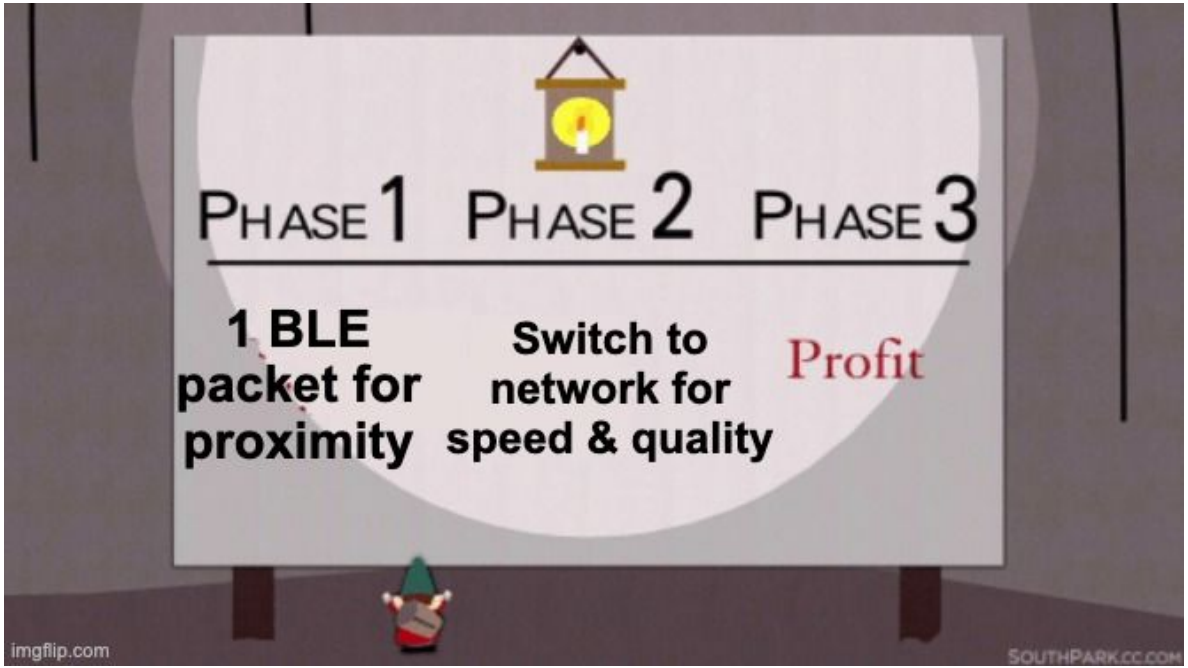
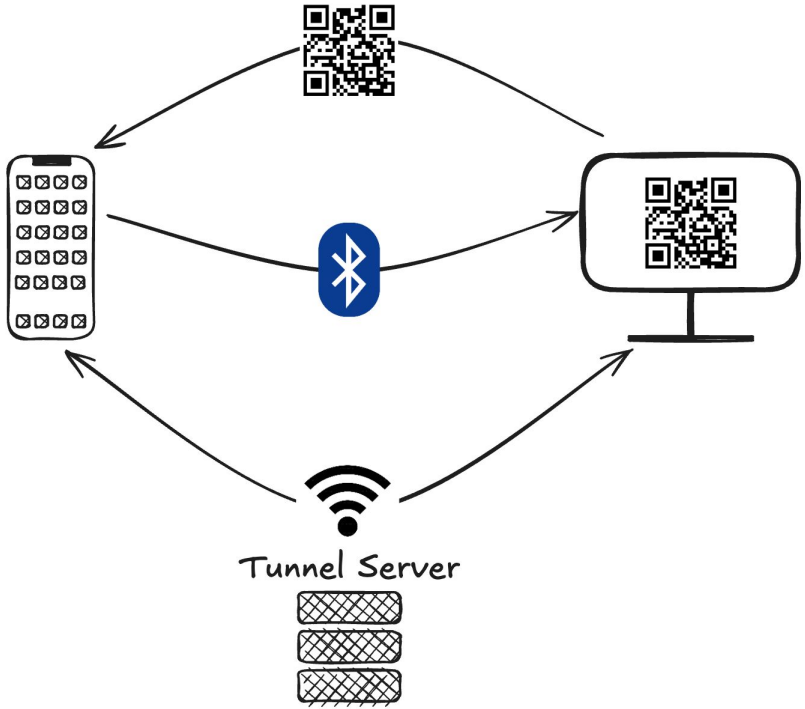


Image is AI generated

Hybrid Transport

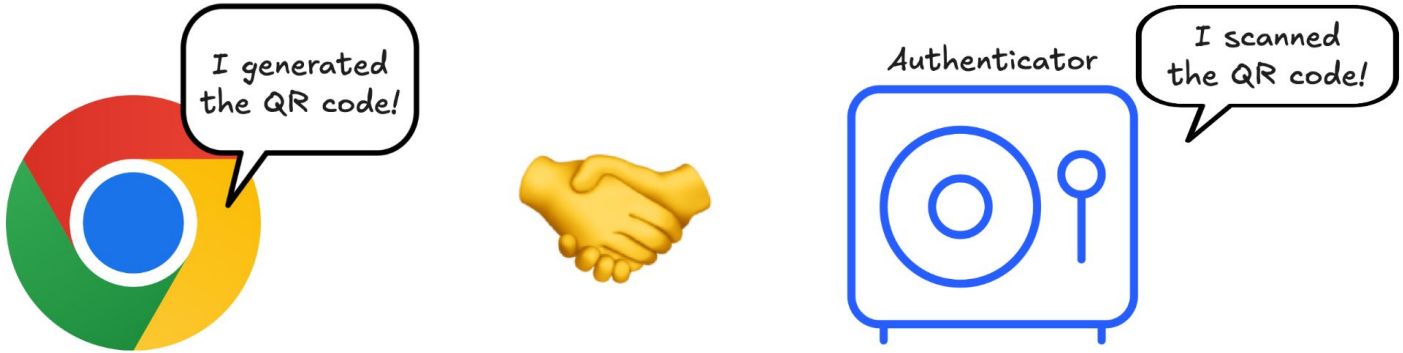


QR-initiated Cross-Device Authentication

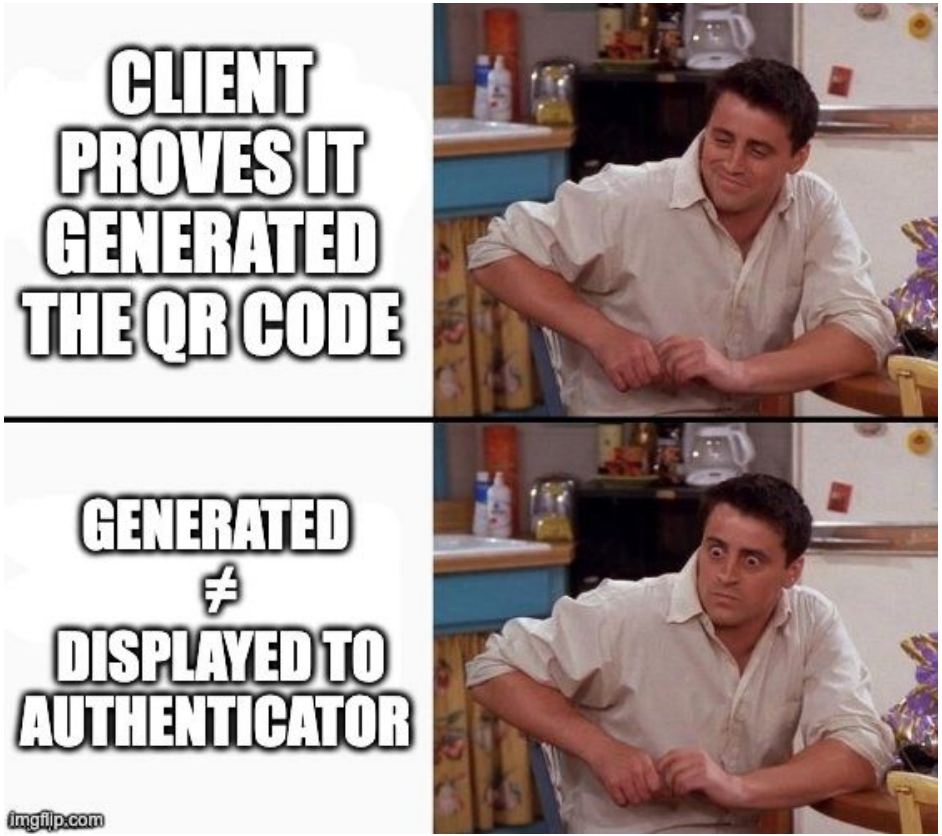


QR-initiated Cross-Device Authentication

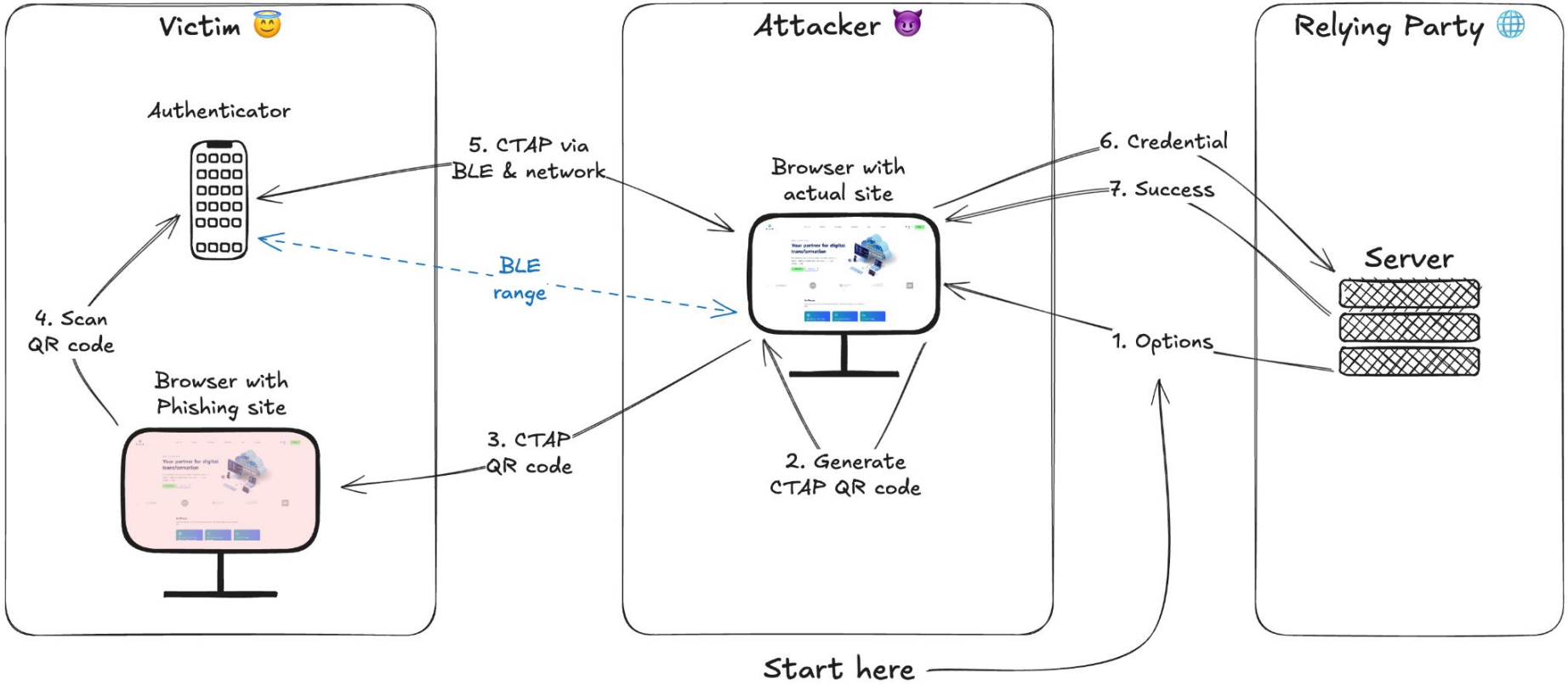
- Hybrid: Use BLE advertisement for proximity, then switch to network
- Network connection through a tunnel server
- QR code ensures connections are made correctly



Phishing for Passkeys - Attack sketch


CLIENT PROVES IT GENERATED THE QR CODE
GENERATED ≠ DISPLAYED TO AUTHENTICATOR
imgflip.com

Phishing for Passkeys - Attack sketch

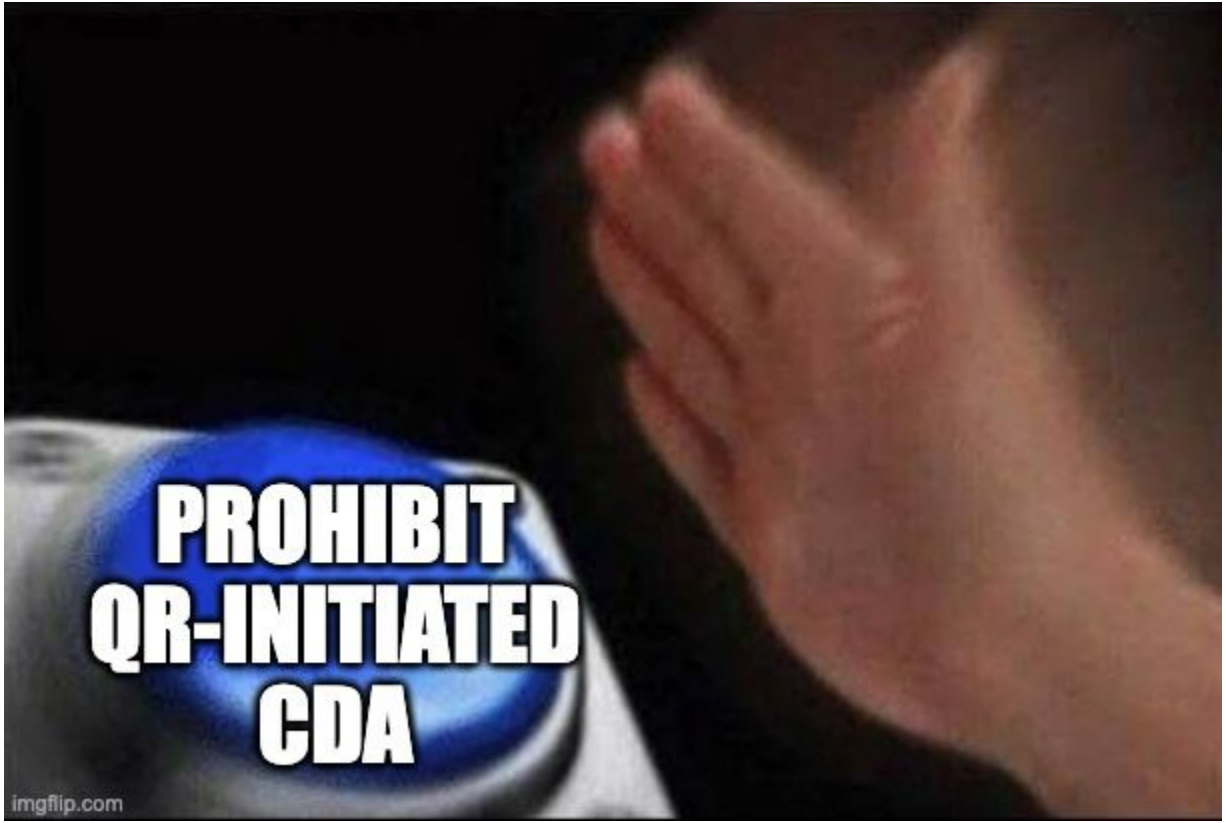


Threat Model

- Victims must be tricked into not notice
  - Spear phishing attack with fake website
  - Fake authentication UI (usually rendered by browser, not website!)
  - Forced QR-initiated CDA
- Attack requires user interaction (open phishing page, scan QR code, complete authentication)
- Attacker must have device within BLE range of victim **while the victim's trying to authenticate**
- Successful attack → attacker can spoof their victim

You should care if you...

- ... support passkeys for authentication
- ... expect highly motivated and technically skilled attackers
- ... expect attackers that can get within BLE range (up to ~100m) of users (e.g. parked in front of office, travelling on the same train)


PROHIBIT
QR-INITIATED
CDA
imgflip.com

Can RPs prohibit QR-initiated CDA?

Based on CTAP

- Relying party is not involved at all

→ ❌

Based on WebAuthn

- Relying Party can ask client to not allow certain transports (e.g. BLE)
- Client specifies authenticator attachment in response (e.g. cross-platform)

→ 👀👉👈

Live Demo 🤞

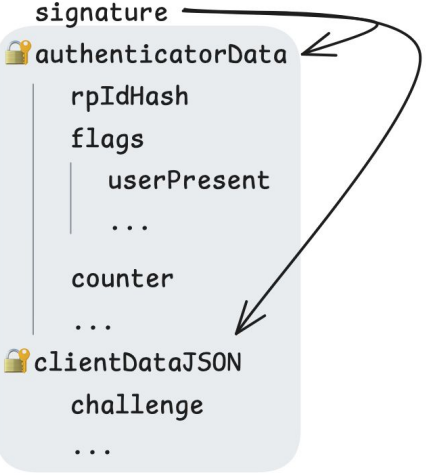

Passkeys & Security Keys
Definitely the target website

PublicKeyCredential RequestOptions

- challenge
- timeout
- allowCredentials
  - id
  - type
  - transports
- userVerification
- extensions

PublicKeyCredential

- id
- authenticatorAttachment
- type
- response
  - userHandle
  - signature
  - authenticatorData
    - rpIdHash
    - flags
      - userPresent
      - ...
    - counter
    - ...
  - clientDataJSON
    - challenge
    - ...



Can RPs prohibit QR-initiated CDA?

Based on CTAP

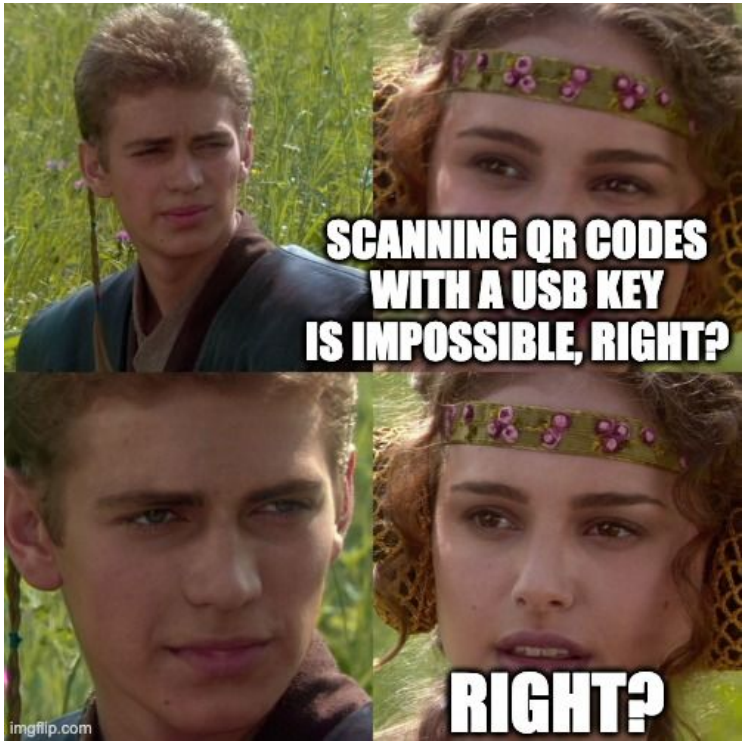
- Relying party is not involved at all

→ ❌

Based on WebAuthn

- Relying Party can ask client to not allow certain transports (e.g. BLE)
- Client specifies authenticator attachment in response (e.g. cross-platform)

→ ❌🤷



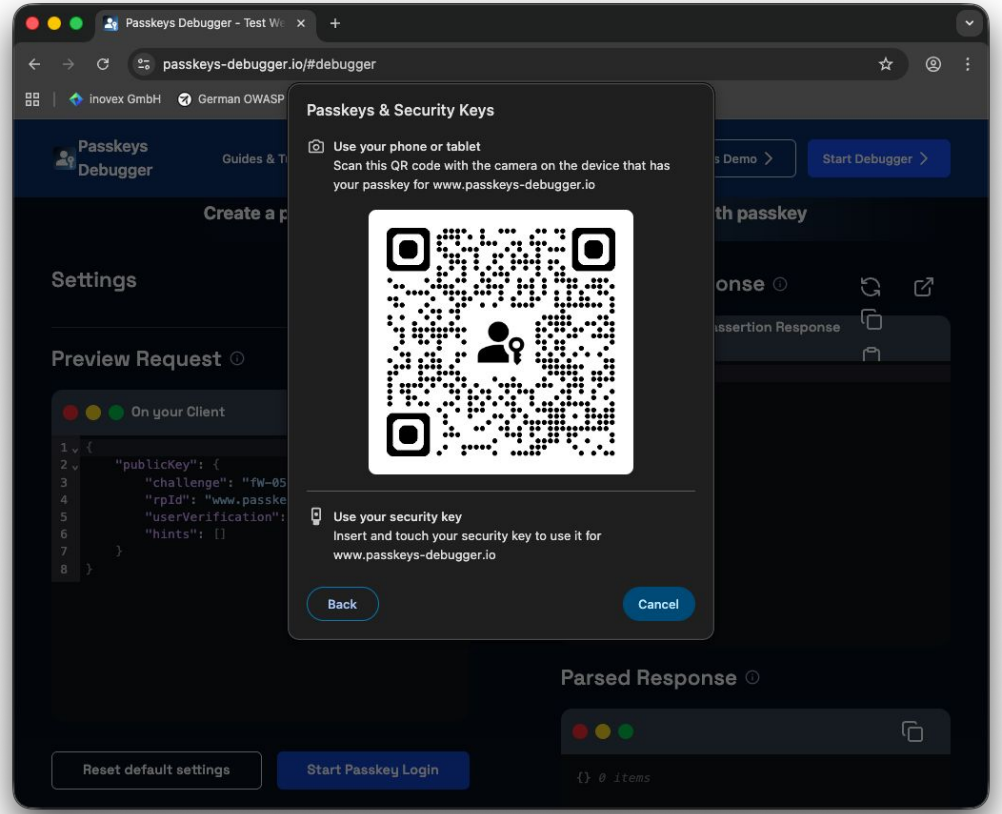
https://denniskniep.github.io/posts/14-fido-cross-device-phishing/

https://github.com/w3c/webauthn/issues/2349

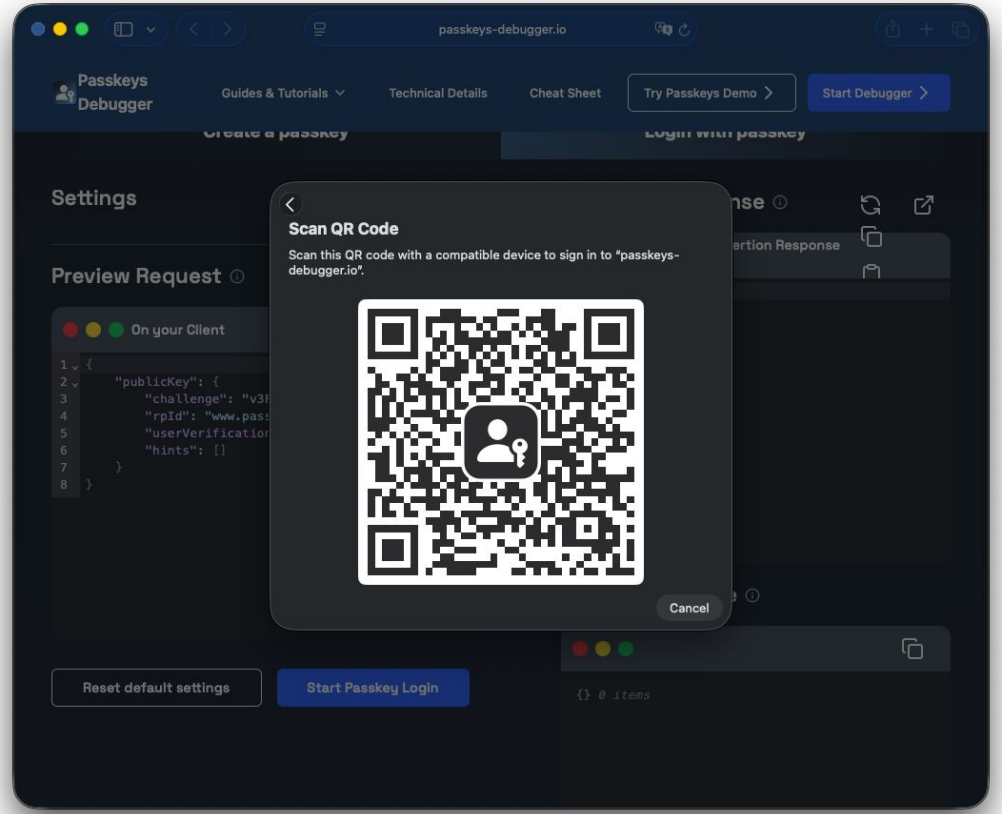
Other prevention methods

- More layers of authentication (e.g. identity managed devices)
- Improve WebAuthn & CTAP
  - Cryptographically protect properties regarding authenticator attachment & transport
  - Not possible short-term
- Educate users
  - Attackers need to force QR-initiated CDA
  - Browsers can render UI in positions unavailable to websites (outside of the website’s rectangle)
  - Relying on user vigilance has proven ineffective (see phishing in general)

Phishing for Passkeys - Other prevention methods



Phishing for Passkeys - Other prevention methods



Other prevention methods

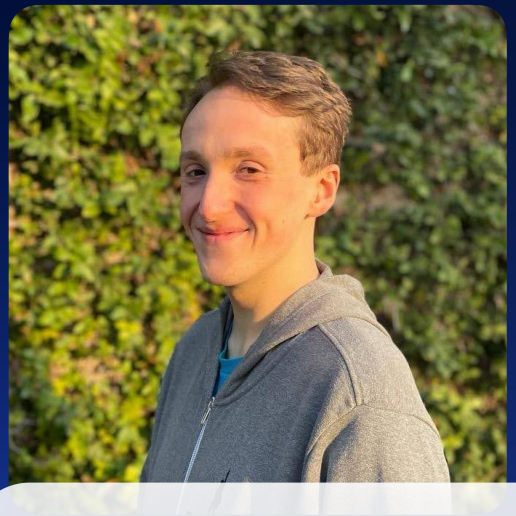
- More layers of authentication (e.g. identity managed devices)
- Improve WebAuthn & CTAP
  - Cryptographically protect properties regarding authenticator attachment & transport
  - Not possible short-term
- Educate users
  - Attackers need to force QR-initiated CDA
  - Browsers can render UI in positions unavailable to websites (outside of the website’s rectangle)
  - Relying on user vigilance has proven ineffective (see phishing in general)

Conclusion

- Passkeys are still resistant to regular phishing
- Depending on threat model, passkeys may be vulnerable to spear phishing attacks
- QR-initiated CDA cannot be prohibited directly by relying parties
- Protection measures are more involved (e.g. adding more authentication layers)

Thanks for listening!

Got any questions?



Read the full blog post for more details!

inovex

Data & AI
Application Development
Skalierbare IT-Infrastrukturen
Training & Coaching

Michael Kuckuk

Fullstack Developer & Student

@michael-david-kuckuk-6a698425b

@LBBO@mastodontech.de

@LBBO.de