Let The Right One In: Attestation as a Usable CAPTCHA Alternative

Tara Whalen, Thibault Meunier, Mrudula Kodali (Cloudflare Inc.); Alex Davidson (Brave); Marwan Fayed, Armando Faz-Hernández (Cloudflare Inc.); Watson Ladd (Sealance Corp.); Deepak Maram (Cornell Tech); Nick Sullivan, Benedikt Christoph Wolters, Maxime Guerreiro, Andrew Galloni (Cloudflare Inc.)
Problems with CAPTCHAs

- Burdensome: makes users perform extra (frustrating) tasks
- Poor accessibility: often prevents people with disabilities from performing requested procedure
- Cultural knowledge: why would we expect people around the world to recognize an American fire hydrant?
- Poor experience on mobile devices
  - more difficult interaction on small screens
Design goals for better CAPTCHA

- Security
  - task has no solution without a human

- Privacy
  - challenges should reveal minimal information about users
  - should not be substitute identifiers (preclude tracking)

- Usability
  - user should be able to demonstrate “personhood” with minimal burden
Proposal: Cryptographic Attestation of Personhood (CAP)

- Basic idea: person physically interacts with secure hardware to provide reliable signal that they are not a bot
- Requirements:
  - authenticator
    - secure hardware (e.g., USB hardware key, fingerprint reader)
    - test of user presence: authorization (physical) gesture
  - Web Authentication API (WebAuthn) standard
  - attestation
    - cryptographic proof that uses public key signed by trusted manufacturer of secure hardware
Web Authentication: high-level overview

- Web Authentication API (WebAuthn): open standard (W3C, FIDO)
- Commonly used for multi-factor authentication
- Two ceremonies:
  - registration (set up key)
  - authentication (subsequent login)
- CAP does not use login flow
- Registration phase used to obtain attestation only (no user data)
  - modified flow: server requests attestation from client without being prompted by username
Cryptographic attestation in brief

- User is asked to prove they are in control of a public key signed by a trusted manufacturer
- Attestation is generated by device using hardware-embedded secret key
- What is provided:
  - digital signature using private key held on hardware in secure enclave
  - certificate chain that leads to manufacturer
What cryptographic attestation provides

- Security against bots
  - cryptographic attestation can only be generated by physical interaction with trusted hardware
    - cannot be automatically generated through software

- Privacy protections
  - attestation does reveal hard-coded certificate associated with device class
  - but not unique: FIDO standard requires that at least 100000 devices share same attestation certificate
  - info disclosed is limited to the type of device and its batch or model
CAP demo walkthrough
One more step
Please complete the security check to access example.com

Verify with CAP
Learn more

What is happening
One more...
Please complete the verification process.

Verify your identity with cloudflarechallenge.com

Pick an option

- USB security key
- This device

What is happening
Creating a WebAuthn Credential.
One more
Please complete the challenge

Use your security key with cloudflarechallenge.com
Insert your security key and touch it

Choose another option
Cancel

Verify with CAP
Learn more

What is happening
Creating a WebAuthn Credential.
One more
Please complete the

What is happening
Creating a WebAuthn Credential.

cloudflarechallenge.com wants to see the make and model of your security key

Skip  Allow
One more step

Please complete the security check to access example.com

What is happening

Creating a WebAuthn Credential.
Verifying credential.
(this will take around 5 seconds).
Success! You completed the challenge successfully.
Evaluation of CAP usability

- Initial feasibility study (n=17) was promising: quick task completion, low errors, good user satisfaction
- Launched public demos with explanatory blog posts
  - initial launch: May 2021, collected user feedback
  - expanded device support in August 2021, collected more detailed feedback
Logged data: verification attempts on public demo

- 1896 user sessions collected over eight days in August 2021
- sessions included both successful and failed attempts
- collected timing and error data
  - minimal data collection (privacy concerns)

**CAP mean completion time**: 10.6s success; 2.8s failure
- compare: hCaptcha 24.5s
Logged data: verification attempts on public demo

**CAP success rate:** of 1896 sessions, 919 (48.5%) included successful validation
  - majority of these (818, 43%) had no errors

Potential sources of failed validation:
  - real-world interactions subject to error (e.g., incomplete attempts)
  - survey data suggests problems from user environments:
    - WebAuthn attestation requirements not always met
    - secure hardware; combination of hardware and browser/OS
User feedback: survey

After verification attempt, users could elect to complete survey (n=93)

<table>
<thead>
<tr>
<th>Questions, 5-point Likert scale</th>
<th>Agree or Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>I am likely to use this when possible (I have a security key/biometric sensor)</td>
<td>70 (75%)</td>
</tr>
<tr>
<td>Assuming I have what I need, I prefer using this instead of a CAPTCHA</td>
<td>70 (75%)</td>
</tr>
<tr>
<td>It’s frustrating how often I have to prove I’m a human</td>
<td>71 (76%)</td>
</tr>
<tr>
<td>I feel confident that this preserves my privacy</td>
<td>56 (60%)</td>
</tr>
</tbody>
</table>
User feedback: CAP strengths

- Additional feedback provided; option to provide system details

- Most commonly cited strengths:
  - ease of use; speed; improvement over other types of challenges

  “this is much much quicker than selecting all the buses....and trucks. . .” [P15]
  “Passed the challenge with just my fingerprint. Very convenient.” [P43]
User feedback: ability to use CAP

- secure hardware widely available, but not universal
- some combinations of authenticators + browser/OS do not work for CAP

“It didn't work with Brave on macOS using TouchID” [P26]
“support more models, I use a very standard google authentication security key and it didn’t work” [P23]
User feedback: privacy

- Privacy protections are strong, but complex and hard to communicate
- Confusion over what is being transmitted from authenticator
  - example: thinking a unique ID may be transmitted, used to track

  “Will Cloudflare store my 2FA key” [P39]
  “how are you gonna explain that this is not surveillance to ‘the normie folks’?” [P91]
User feedback: communication

- CAP is novel way of verifying personhood: not easy to explain
  - how to easily communicate necessary system requirements?
- CAP design is constrained by how browsers implement WebAuthn
  - user experience may be confusing (e.g., user verification popups do not apply to CAP use case)
  - WebAuthn itself has many usability challenges

“The options that are available on Android can be overwhelming for a non-technical audience. Most people won’t know what a Yubikey is or understand that ‘unlock with screen lock’ means fingerprint sensor.” [P37]
Summary of CAP usability findings

- CAP verification task was completed quickly
- Users with supported hardware and software were able to validate easily
- Majority of survey respondents (75%) indicated they were likely to use CAP if they had necessary hardware
- **Results suggest that CAP is good solution in right circumstances**
- CAP is best positioned as *alternative* challenge method, not sole option
Security considerations

- Tricky to balance security and usability: arms-race
- Need to monitor for how abuse, attacks shift in response to CAP
- Have to consider possibility of facing automated button-pressing systems
- CAP is part of defense in depth
  - one strong signal, can be combined with other signals
Next steps for CAP

● Revising UI/UX: provide clearer communication on challenge page
● Continuing evaluation and analysis
  ○ monitoring security of challenges
  ○ further work in usability (including accessibility)
Thank you!
Feedback and questions welcome

Tara Whalen: twhalen@cloudflare.com
ask-research@cloudflare.com