HEY AUTHN

Emma Guo
Sehyun Chung
Vivek Bhupatiraju

02/03/22

Background

heyauthn + WebAuthn + ZK apps

What is heyauthn?

- Post anonymous Q&A during these presentations to Discord!
- Set up identity with **WebAuthn**, a modern API designed to improve the security of the login experience
  - First use (as far as we know) of this tech being used in ZK messaging applications!
- Join the group with the **IYK disc** being passed around! If you tap it with the top of your phone, it generates a unique invitation link that can’t be shared

What is WebAuthn? (1)

- New standard for authentication from W3C and FIDO, to remove passwords and related security risks
  - phishing, password breaches, LastPass hacks lol
- Generates a website specific public/private key pair, the website stores your public key
- Log in by signing a challenge with private key, which is only generated by device after FaceID/TouchID

What is WebAuthn? (2)

- Signing API for *website.com* is only available in a **secure context** (HTTPS connection or localhost), which means signatures cannot be phished by an alternate website like *webs1te.com*

- Can log onto other devices by scanning a QR code and sending a valid signature over

- Rare example of a better user experience with more privacy! No more passwords, just FaceID/TouchID

WebAuthn for ZK apps?

- We have a super clean flow to generate ECDSA P-256 signatures on arbitrary messages with TouchID / FaceID

- Built into all devices and slowly becoming more adopted

- Seems like a convenient and easy-to-use identity management system, and its cryptographic setup makes it more amenable to ZK identity setups!

Constructions

How do we use this in practice?

Construction 1: Using ECDSA P-256 directly

- We can sign arbitrary messages with our P-256 public key
- CloudFlare implemented a bespoke ring membership scheme for P-256 keys: https://github.com/cloudflare/zkp-ecdsa
- Can only be “forged” if hacker has access to your device; can’t extract WebAuthn private key from device (afaik)
- No nullifiers; can’t assign reputation which is necessary for non-toxic anonymity

Construction 2: Combining with Semaphore

- In addition to key pair, authenticator creates a unique credential ID that no one else knows (unless sent to a server)

- Can use this as our **Semaphore private key** to get a WebAuthn-based Semaphore identity!

- Essentially using WebAuthn as a Semaphore wallet; avoid storing keys in localStorage and

Backend / posting messages

- Post questions to Discord instead of a fully anonymous message board

- Can interact with the messages using your “real” identity if you feel comfortable!

Full setup

1. Generate unique sign up link using IYK tap device (ensures you were in person and didn’t just get sent a link from a friend)

2. Generate a key pair for heyauthn.xyz, along with a unique and private credential ID

3. Use this credential ID as your Semaphore private key for questions + upvotes!

Demo

Let’s ask some questions!

Extras for later

- Tracking reputation across anonymous identities
  - +1 reputation if you ask questions
  - +2 reputation if others upvote / had the same question
  - +3 reputation if you answer

- Attaching more identity to your new WebAuthn semaphore identity, can use your full reputation when asking and answering questions or sharing feedback
  - ZK IAP Staff member
  - Took 6.875 before
  - Is a PhD student

Total Contributions

- Built an easy-to-use and secure Semaphore wallet across devices using WebAuthn

- Used IYK’s physical devices to make for a very smooth in-person sign up experience

- Built out anonymous Q&A message board that people can continue to use after the course ends!

Thank you!

https://github.com/vb7401/heyauthn