

Passkeys

"The future of Passwordless Authentication"...maybe?

Mattis Turin-Zelenko, chax.at

Outline

- What is a Passkey?
 - Problems with Passwords?
 - How does it work?
 - What does it solve?
- Demo
- Developer Integration
- Future & Issues

History

- Authenticate with username + password
- Different password for each website
 - must be long + complex
- Never enter your password anywhere else
 - but always remember it

Passkeys - the idea

- "Device" stores a private key
- Website stores user's public key
- Browser->OS sends challenge to passkey "device", including URL
 - via Webauthn
 - Phishing website on different URL cannot access passkey
- "Device" returns signed response - if valid, login successful
 - "Device" protected by PIN / biometrics
 - Private key never leaves the "device"

Passkeys - "Device"

- What *is* a passkey "device"?
- FIDO2 security key (e.g. Yubikey)
 - secured by fingerprint or PIN
- Smartphone
 - cross-device syncing (Google Password Manager, iCloud Keychain)
 - Cross Device possible: scan QR code on PC
- TPM (e.g. Windows Hello)
- Password Manager

Passkeys - Demo

Developer Integration

- `SimpleWebAuthn` TS package is actually simple!
 - packages for browser + server
- Just tell the browser to create/authenticate a passkey
 - some configuration: e.g. do we require PIN/biometrics?
- OS will handle everything else...
 - ...in a super confusing way
- How can we get users to *actually* use and understand passkeys?
 - Do we even want to?

Issues

- Webauthn spec is still "new": Early Adopter problems
 - lacking browser support
 - lacking OS support (no passkey management UI in Windows 10)
 - still adding/removing functionality (e.g. privacy concerns)
- Device syncing works great in your ecosystem
 - Syncing between Google <-> Apple is not possible
 - "it's a feature" - private key never leaves your device!
 - perfect vendor lock-in
- How to recover when losing "device" / forgetting PIN?

Adoption Tips

- Suggest passkeys after login (after "annoying experience")
 - Webauthn allows silently creating passkeys on the device as well - maybe even more confusing for user?
- Conditional UI: Some browser allow "auto-completion" for passkeys
- Ask for username/e-mail first, prompt for passkey first instead of password
- Check out passkey flow from Google, Amazon, ...
- It's hard: we don't know what the browser/OS will do exactly

Resources

- <https://webauthn.io/>
- <https://simplewebauthn.dev/>
- <https://www.corbado.com/blog/passkey-login-best-practices>