WebAuthn 101

Ståle Pettersen, 11.12.2019
Me

- Dev and security guy for 15+ years
- Head of Product & Application Security in Schibsted (FINN, VG, Prisjakt, Lendo, etc.)
- Poker, Snowboard, Lock-picking, Security stuff
- OWASP Norway Board member
- We are hiring Security Engineers! ([bit.ly/sch-appsec](bit.ly/sch-appsec))
9,139,071,108
pwned accounts
Solution: Password manager
Solution: Password manager
Solution: Password manager
Already have 2FA! SMS/TOTP/HOTP
WebAuthn = Web Authentication API

Standardized JS interface for authenticating users to web-based applications and services using public-key cryptography.

Published by W3C in March 2019
Authenticator types

- Platform authenticator
  - OS backed (stored in TPM, Secure Enclave or similar).
  - Examples: Windows Hello, Android, macOS

- Roaming authenticator
  - Hardware tokens
  - Supported: USB, NFC or BT
  - Examples: Yubico 5, Titan Security Key
WebAuthn support

- Chrome
- Firefox
- Edge
- Safari (macOS and iOS)
- Windows & Windows Hello & AD etc
- Android
- ChromeOS
WebAuthn supports:

- Registration: `authenticatorMakeCredential()`
- Login: `authenticatorGetAssertion()`
WebAuthn privacy:

- No global identifier
WebAuthn Demo
Look! No password
How Security Keys work

Challenge was: 123456
Origin was: google.com

Server

challenge

Alice’s Key

6

https://www.google.com

Google

Alice’s Security Key

4

sign: {challenge, “google.com”}

challenge, “google.com”

USB/NFC/BLE

Who’s calling?

2

Alice Smith
alice@acme.com

Password

Sign in

1

5

{challenge, “google.com”}_signed

https://www.slideshare.net/FIDOAlliance/webauthn-and-security-keys-126400301
Created with open standards

![Diagram of WebAuthn API and CTAP API](https://www.slideshare.net/FIDOAlliance/webauthn-and-security-keys-126400301)
FIDO2 and WebAuthn

FIDO2 = WebAuthn (client API) + CTAP1&2 (authenticator API)
U2F vs FIDO2

U2F = WebAuthn (client API) + “CTAP1” (authenticator API)

U2F: Can only be used as second factor, no passwordless login etc.

Created by Google and Yubico, donated to FIDO Alliance as “FIDO 1”.

WebAuthn history

- FIDO Alliance
- W3C
- FIDO
- WebAuthn
- FIDO2
- U2F
- CTAP1
- CTAP2
- Google
- Yubico
WebAuthn/FIDO2

- Single factor authentication
  
  Credential management API Support Public key crypto

- 2nd Factor Authentication
  
  WebAuthn (supports CTAP1 and CTAP2)

- Multi-Factor: Passwordless + PIN/Bio
  
  CTAP2 Support User Info Verification
Yubikey Bio
YubiKey Bio coming soon!
Second factor

verification

authentication

FIDO2: 2FA auth everywhere

- Web
- Windows Hello
- ChromeOS
- Active Directory
- Even SSH
Recovery

- Register multiple keys on all accounts (minimum 2)
  - But...They both need to be in your possession when registering them, risky state!

U2F/FIDO1 vulnerabilities

Google Titan Security Key - bluetooth pairing issue

Phish Yubikey Neo with Chrome WebUSB weakness

ChromeOS U2F ECDSA vulnerability (64 bits instead of 256 bits)
Questions?

Guide and resources: https://webauthn.guide/
Great Developer guide: https://codelabs.developers.google.com/codelabs/webauthn-reauth/
Yubico WebAuthn Demo: https://demo.yubico.com/webauthn
WebAuthn Demo: https://webauthn.io/