WebAuthn

A new standard in securing ourselves online

by Anthony Grimes
whoami

• Software Engineer at JPMC

• Security Advocate

• Maker of stuff
Passwords, passwords...

- In most systems a password is king, it’s what guards your valuable data.
- Less than a third of users are using 2FA\(^1\)
- As many as 81% of hacking-related breaches are from compromised passwords\(^2\)
A passwordless future

- FIDO2
  - CTAP
  - WebAuthn
Registration/Authentication Flow

- USER
- USER AGENT
- AUTHENTICATOR
- HTTP POST
- RELYING PARTY

1. Get challenge
2. Challenge and new credentials
3. New credentials, signed challenge (sc)
4. Authenticated ->
5. New credentials, sc
6. Registered
Behind the scenes

```javascript
{
  challenge: Uint8Array.from(
    randomStringFromServer, c => c.charCodeAt(0)),
  rp: {
    name: "RP Name",
    id: "example.com",
  },
  user: {
    id: Uint8Array.from(
      "UZSL85T9AFC", c => c.charCodeAt(0)),
    name: "contact@anthonygrimes.co.uk",
    displayName: "Anthony",
  },
  pubKeyCredParams: [{alg: -7, type: "public-key"}],
  authenticatorSelection: {
    authenticatorAttachment: "cross-platform",
  },
  timeout: 60000,
  attestation: "direct"
}
```

PublicKeyCredential {
  id: 'ADSUI1KQmbqGtpu4sjseh4cg2TsvrbcHDTBsv4NSSX9...',
  rawId: ArrayBuffer(59),
  response: AuthenticatorAttestationResponse {
    clientDataJSON: ArrayBuffer(121),
    attestationObject: ArrayBuffer(306),
  },
  type: 'public-key'
}
What are the benefits?

• Virtually unphishable
• No biometrics or private keys are ever transmitted during registration/authentication
• Unique keys per service, aids removing tracking
• Unified API via WebAuthn and more...
Where is this adopted?

- Chrome, Firefox, Edge, Safari (limited support)
- Android
- Windows 10, macOS (limited support)
Demonstration
References