The WorldWideWeb (W3) is a wide-area hypermedia[1] information retrieval
technology. It is a distributed system that operates using a client-server
model, with clients being personal computers and servers being
large mainframe computers or smaller systems.

This is for everyone!
World Wide Web Consortium (W3C)

Voluntary standard-setting. Stewards of the Open Web Platform.

Addressing the collective action challenge of Web security

Modular security

- Component by component (end-to-end)
- Foundations for trust and secure communication

Incentives: keep the platform working jointly, compete on top
Why Web Authentication? @#&!?$%

Passwords annoy users:

- Prompts interrupt the flow of activity (Web purchase, posting, reading, or interaction)
- Entry is even more annoying on mobile
- Passwords are forgettable. Password-generation rules make management harder.
- Some sites block password manager auto-fill.

Passwords are insecure:

- Reuse across sites can mean break-once-break-anywhere
- Vulnerable to interception (phishing) that can compromise accounts
- Trade-off between memorable/enterable and vulnerable to brute-force guessing
Better authentication improves user experience and security

- Faster log-in means faster check-out
- Happier users return more frequently
- Strong authentication leads to greater accountability

Consequences of passwords

- 2013 Yahoo! breach compromised all 3 Billion user accounts (passwords were weakly encrypted)
- 2018 Twitter warned all users to change their passwords because they were stored in plaintext
Web Authentication

Security

- Strong cryptography
- Unphishable
- Resists data-breach and brute force attacks
- Test of user presence
- Attestation

Usability

- Passwordless
- One- or two-factor
- In-device, biometric
Web Authentication

- Member Submission of FIDO2 work to W3C
- Continued work on CTAP (Client to Authenticator Protocol)
- Web API: Enable the browser to mediate between client-side authenticator and web applications
Web Authentication: How it works

WebAuthn enables a cryptographic challenge unique to each website and bound to its origin.

Local authentication such as biometrics never leaves the device.

https://www.w3.org/TR/webauthn/
W3C WebAuthn with FIDO

App calls for FIDO Authn through browser*

W3C Standard: Web Authentication JS API*

OPTION 1: On-device Authenticator*

OPTION 2: External Authenticator

Client To Authenticator Protocol*

* FIDO2 Project
WebAuthn at Candidate Rec.

W3C Working Group Chairs: Tony Nadalin, Microsoft, and John Fontana, Yubico

https://github.com/w3c/webauthn
WebAuthn Implementations

Browser implementations include:

- Chrome 67
- Firefox 60
- Edge development version
- Safari participating in the Working Group

**W3C WG Participants:** Airbnb, Alibaba Group, Apple, Bloomberg, Consensus, Deutsche Telekom, ETRI, Federal Reserve Bank of Minneapolis, Google, HM Government, IBM, Intel, Intuit, Microsoft, Mozilla, NIST, New Zealand Government, Nok Nok Labs, Opera Software AS, Orange, PayGate, PayPal, Qualcomm Innovation Center, SoftBank Corp., Tencent, Thomson Reuters, Trust1Team, Wiley, Yubico
WebAppSec: Encryption Everywhere

Standardizing and Enabling HTTPS for confidentiality, integrity, and authentication

- Secure Contexts
- Upgrade Insecure Requests
- Mixed Content
- Referrer Policy
- Subresource Integrity

HTTPS Work Elsewhere

- Let’s Encrypt
- Certificate Transparency
- HSTS
WebAppSec: Enlisting the User Agent in Cooperative Policy Enforcement

- Content Security Policy
  - Level 2 is Recommendation; Level 3 in development (Editor’s Draft)
- Secure Contexts
- Subresource Integrity (Rec), Mixed Content

Security Related APIs
- Permissions API
- Credential Management
- Clear Site Data

Experiments in the Web Security Model / Same Origin Policy
- Confinement with Origin Web Labels (COWL)
- Suborigin Namespaces
Build a toolbox for trust among users

End-to-End = local self-determination

Modularize

Encrypt everywhere

Build for Open

Enlist and enable the user
Links

Web Authentication: https://www.w3.org/webauthn
WebAuthn spec: https://www.w3.org/TR/webauthn/
WebAppSec: https://www.w3.org/2011/webappsec/
Web Payments: https://www.w3.org/Payments/WG/

Thanks!

Wendy Seltzer
wseltzer@w3.org https://wendy.seltzer.org/
@wseltzer +1.617.715.4883