Security Roadmap

Wendy Seltzer
wseltzer@w3.org

Roadmap: https://github.com/w3c/websec/blob/master/security-roadmap.md

Web User Security

- Crypto API in CR
- Authentication: 2 new charters in draft
- HTTPS for confidentiality, integrity, authenticity; Secure Contexts

Web Application Security

- CSP, Referrer Policy, SRI, Credential Management, Permissions, EPR, COWL
- HTTPS support: Mixed Content, Upgrade Insecure Requests

Web Platform Security

- Security & Privacy Considerations (reviews)
- Liaisons: IETF, ICANN, FIDO, Automotive

Security: Draft WG Charters

Web Authentication

https://w3c.github.io/websec/web-authentication-charter

Initial drafts from FIDO 2.0: Web API, Attestation Format & Signature Format

Hardware-Based Security

https://w3c.github.io/websec/hwsec-charter

Seeking initial draft(s)

Web Authentication

Goals: The Web Authentication Working Group will develop recommendation track specifications defining an API, as well as signature and attestation formats which provide an asymmetric cryptography-based foundation for authentication of users to Web Applications. https://w3c.github.io/websec/web-authentication-charter

Deliverables:

- Web API
- Attestation Format
- Signature Format

Hardware Security

Goals: To define a set of Hardware-Based Web Security standard services providing Web Applications usage of secure services enabled by hardware modules (TEE, secure elements, and other secure enablers). https://w3c.github.io/websec/hwsec-charter

Deliverables in-scope:

- Secure Hardware Discovery & Attestation
- Secure Hardware Crypto Key Discovery
- Secure Hardware Crypto Key Management
- Secure Hardware Crypto API
- Secure Hardware Storage API
- Secure Hardware IO
- Secure Worker
- Binding mechanism
- Identity semantics
- Web payments access