W3C Web Authentication and Security

- Web Security Technologies for Payment -

Keiji Takeda
Keio University
W3C / MIT

2015/11/2  W3C Web Payment Seminar in Tokyo
W3C Web Security Area Activities

- Web Payments Working Group
- Web Cryptography Working Group
- Web Authentication Working Group
  - NEW!
- Hardware Security Working Group
  - NEW!
- Web Application Security Working Group
- Privacy Interest Group
Make payments easier and more secure on the Web.

Scope:

- Messages for payment,
- Message flows for payment
- API for payment

Deliverables (FPWD planned March 2016):

- Web Payments Messages Recommendation
- Web Payments APIs Recommendation
- Process and Planning

http://www.w3.org/Payments/
Defines an API that lets developers implement secure application protocols on the level of Web applications, including message confidentiality and authentication services, by exposing trusted cryptographic primitives from the browser.

Deliverables:

Web Cryptography API (Last Call Public Working Draft)

Web Cryptography Use-Cases (Editor’s Draft)

WebCrypto Key Discovery (Editor’s Draft: Key Discovery)

High-Level API (Editor’s Draft)
Defining an API, as well as signature and attestation formats which provide an asymmetric cryptography-based foundation for authentication of users to Web Applications.

Scope:
- entity authentication via a challenge-response protocol
- improved authenticated session management
- attestation formats
- signature message formats

Expected Deliverables:
- Web Authentication API (use FIDO 2.0 as input)
- Data and signature formats (use FIDO 2.0 as input)
  (Test suite, Use Case)

https://w3c.github.io/websec/web-authentication-charter
FIDO Alliance Opens Worldwide Cooperation & Liaison Program – Welcomes Associations to Partner on FIDO Standards for Universal Strong Authentication

October 13, 2015

The World Wide Web Consortium (W3C) looks forward to working with the FIDO Alliance, particularly in areas where web standards for authentication will enhance the Open Web Platform and benefit the entire online ecosystem,” said Dr. Jeff Jaffe, W3C CEO.

https://fidoalliance.org/fido-alliance-opens-worldwide-cooperation-and-liaison-program/
FIDO (Fast IDentity Online) Alliance plans to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services.

Online Crypto Protocol Standardization
The protocol is based on standard public key cryptography — the client registers a public key with the online service at initial setup. Later, when authenticating, the service verifies that the client owns the private key by asking it to sign a challenge. The protocol is designed to ensure user privacy and security in the current day state of the internet.

https://fidoalliance.org/specifications/overview/
Hardware-Based Web Security standard services

Secure services enabled by hardware modules
(Trusted Execution Environment, secure elements, etc.)

Expected Application

Payments – transaction authorization

Identity verification
Hardware Security Working Group (2/2)

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

http://www.w3.org/2015/hasec/2015-hasec-charter.html
W3C Recommendations
  Cross-Origin Resource Sharing
Recommendation-Track Drafts
  Content Security Policy Level 2
  User Interface Security Directives for Content Security Policy
  Subresource Integrity
  Referrer Policy
  Mixed Content
  Privileged Contexts
  Content Security Policy Pinning
  Upgrade Insecure Requests
  The Permissions API
  Credential Management Level 1
  Entry Point Regulation
  Clear Site Data
Confinement with Origin Web Labels (COWL)

http://www.w3.org/2011/webappsec/
Improve the support of privacy in Web standards by monitoring ongoing privacy issues, investigating potential areas for new privacy work, and providing guidelines and advice for addressing privacy in standards development.

Deliverables:
Privacy Considerations for Web Standards, Group Note.

http://www.w3.org/Privacy/
Conclusion

Introduced Web Security Area Activities in W3C

New web authentication standardization with FIDO Alliance

Technical solutions are available to support Web Payment applications
Contact

Keio University / W3C MIT

Keiji Takeda

keiji@sfc.keio.ac.jp / tkeiji@w3.org