W3C Web Crypto APIs

Status of current specifications and future plans

Virginie GALINDO – chair of Web Crypto WG

Web Crypto APIs use cases

- Web Crypto APIs allow web apps to build their own security model, by managing cryptographic primitives, independently from HTTPS operations

- Usual use cases are
  - Secure communication
  - Secure back-up
  - Document signature
  - Protected content

Web Crypto APIs documents

- The W3C Web Crypto WG handles two specifications, expected to become recommendations
  - Web Crypto API : to manage key creation and operations
  - Web Crypto Key Discovery : to retrieve previously created keys, via their name

Web Crypto API - overview

- Editor's draft https://dvcs.w3.org/hg/webcrypto-api/raw-file/tip/spec/Overview.html
- Editors
  - Ryan Sleevi (Google)
  - Mark Watson (Netflix)
- Implementers
  - Google
  - Microsoft
  - Apple
- Experiments
  - BBN, Netflix plug-in, INRIA (to be confirmed)

Web Crypto API - overview

- Issue review
  - No more issue
- Bug review
  - 46 bugs as of today, 15 related to technical aspects
  - https://www.w3.org/Bugs/Public/buglist.cgi?component=Web%20Cryptography%20API%20Document&product=Web%20Cryptography&resolution=---
- Reviewers
  - W3C PING review : done
  - W3C TAG review : on going right now ;)
  - Few feedbacks from outside W3C
    - Except Dan Boneh

Web Crypto API - overview

- Timeline
  - Next draft version will trigger Last Call
  - Expected to be released in January 2014
    - #crossingfingers

Web Crypto API in few lines

- With the API one can
  - Generate a random
  - Generate a key
  - Derive key (or bits)
  - Import or expert a key
  - Encrypt, decrypt, sign, verify a signature, create a digest
- A key is characterized by
  - Key type
  - Key usage (encrypt, sign, …)
  - Key algorithm (from registered algorithms)
  - Extractable or not

Recommended algorithms

- The specification describes how to manage operations with a large number of algorithms
  - https://dvcs.w3.org/hg/webcrypto-api/raw-file/tip/spec/Overview.html#algorithms

- But recommends some of them to be implemented by UA – while this not being normative
  - HMAC using SHA-256
  - RSASSA-PKCS1-v1_5 using SHA-1
  - RSA-PSS using SHA-256 and MGF1 with SHA-256.
  - RSA-OAEP using SHA-256 and MGF1 with SHA-256.
  - ECDSA using P-256 curve and SHA-256
  - AES-CBC

Few specificities to keep in mind

- This spec “does not attempt to provide a mitigation for existing threats to the web security model, such as script injection or hostile intermediaries”
- Some features are left to implementations
  - Implemented algorithms
  - Key store and method for storage
  - Extractability guarantee
- Entropy of the random numbers is not monitored

Few specificities to keep in mind

- The wrap/unwrap proposal is finetuned for JWK objects
- The maintenance of the algorithm is planned to be done by W3C
  - Deprecating algorithms, adding new ones

Web Crypto API Key Discovery - overview

- Editor's draft https://dvcs.w3.org/hg/webcrypto-keydiscovery/raw-file/tip/Overview.html
- Editors
  - Mark Watson (Netflix)
- Implementers
  - Microsoft (based on previous version)
- Experiments
  - none

Web Crypto API Key Discovery - overview

- Issue review
  - No more issue
- Bug review
  - No bug
- Reviewers
  - PING review : done
  - TAG review : on going right now ;)

Web Crypto API Key Discovery - overview

- Timeline
  - Expecting Web Crypto API to go for Last Call

Future Work in Web Crypto WG

- Specification evolution
  - Include streams (if happening)
  - Include new algorithms (SEED, …)
  - Potentially adapt to future Web RTC and Payment requirements
- New features
  - Certificate management
  - Dealing with hardware token
    - Potential workshop to be organized

Anything we can do ?

- To help to finalize the specification review ?
- To better synch ?

Inputs for W3C Security Roadmap

… my recent security discussions

Who is discussing security in W3C ?

- WebApp Security WG
- Web Crypto WG
- SysApp WG
- Web Security IG
- W3C AC rep’

Several trends on security

- ‘Pervasive monitoring’
  - Make the old web more robust
  - Make sure next technology will be trusted (a la Web RTC)
- High value services on the open web platform
  - Payment, content protection
- New usages and privacy by design
  - Peer to peer, BYOD

Echoes from W3C members (1)

- Discussions happened with W3C members
  - during the TPAC 2013 meeting (Nov 2013)
    - http://www.w3.org/wiki/TPAC2013/security
  - During last Web Security IG call (Dec 2013)
    - http://www.w3.org/2013/12/18-websec-minutes.html

- Executive summary is that W3C can do more…

Echoes from W3C members (2)

- Security community
  - To maintain knowledge
  - To understand how other bodies are dealing with security features
- Process to review security specifications
  - HTML EME, Promise, …
- Security features
  - Client side
  - Certificate management
  - Session management
- Educational material to web developers and end users

Suggested actions

- Start building a community (or bringing back the security expert on board) by creating places for discussion and knowledge sharing
  - Workshops, Conferences
- Write down and advert the security value proposition of W3C
  - White papers, WebPlatform
- Include security review in the process and/or culture of W3C
- (Hire people)
- …

Thanks