Security : a snapshot from W3C

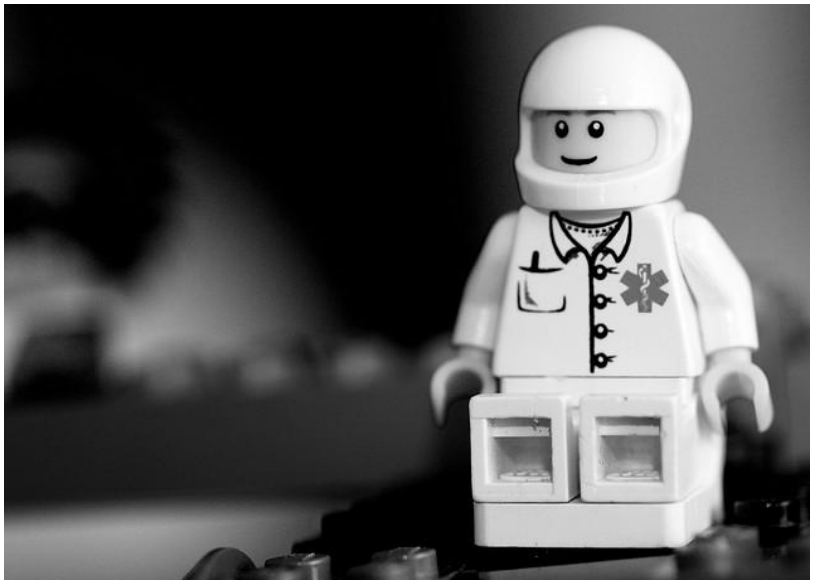
Virginie GALINDO
July 2014

Menu ? 30 minutes to taste web, standard and security cocktail

(no drone, no demo, no hack, no code, just gossips)

gemalto

Virginie Galindo ...



gemalto

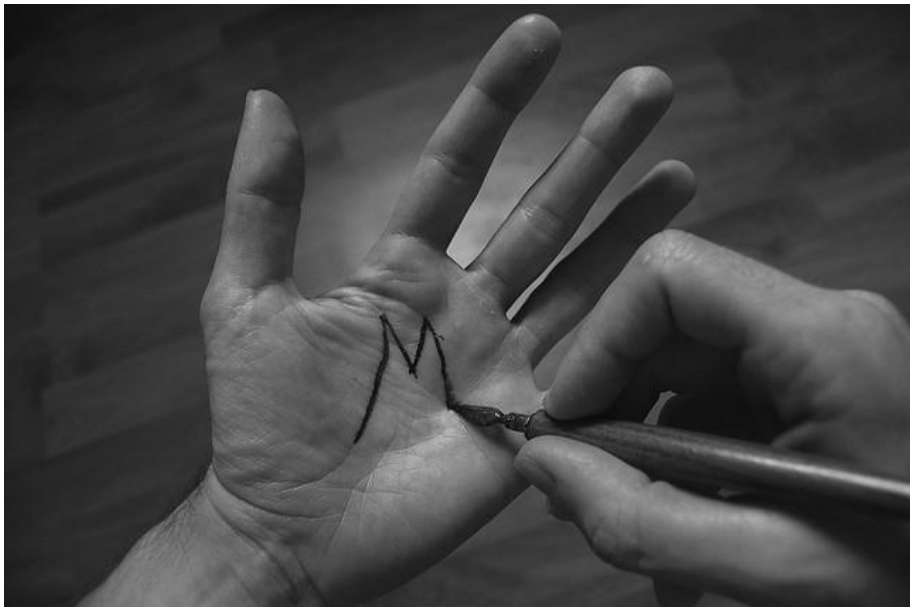
Web Security ?

Cumulating hardware, firmware, software , and servers holes

gemalto

But, everyones going web...

Payment** with e-commerce, **Social** with collaborative web, **Content protection** (boooo), and **Mobile



Protecting business on the web is a real job, and a bit of coordinated effort may help...

gemalto

Standards

gemalto

Web Standards

IETF (basements)

OWASP (firemen)

W3C (browser temple)

FIDO, OASIS, ... (market specific)


MASSACHVSETTS
77
AVENVE

Google, Microsoft, Mozilla, Apple, Opera, Adobe, Qualcom, Hachette, LG, Samsung, IBM, Akamai, Alcatel Lucent, Netflix, AT&T, Baidu, BlackBerry, Bloomberg, Boeing, BT, Canon, CDT, Dell, China mobile CISCO, DT, Dolby, Ebay, EFF, Facebook, Fujitsu, Genivi, Huawei, Ingenico, Intel, Irdeto, Jaguar, JQuery, KDDI, Mitsubichi, NEC, NTT, Nokia, Oracle, Pierson, Red Hat, SAP, Siemens, Sony, Standord University, Tencent, Apache Software Foundation, Toshiba, Twitter, Verisign , Verizon...

386 in total ...

gemalto

W3C scope and operations...

- All about interoperable browsers (browser feature, web apps, APIs, ...), independently from the underlying platform
- Advisory Council, Advisory Board, W3C team
- IP free (all specs can be implemented for free)
- Working in public (even on github sometimes)
- Some specs documentation are starting to be issued in CC

"[...] When submitting an extension specification to the Working Group, individuals may propose that W3C publish the document under the Creative Commons Attribution 3.0 Unported License (CC-BY) as well as the W3C Document License (Dual License). [...]"

There is a security roadmap in W3C

gemalto

Snowden effect...

gemalto

Business on the web …

gemalto

The W3C groups dealing with security

XML Security WG

Web App Sec WG

Web Crypto WG

Web Security IG

All is here http://www.w3.org/Security/wiki/Main_Page

XML Security WG – the xlm guys

This is all about syntax and process for signature and encrypted data in XML

All is done, they rock …

Web App SecWG – security core

Challenging Same Origin Policy and creating new security features

- CSP level 1, level 2, user interface security directives

http://www.w3.org/TR/CSP11/ and http://www.w3.org/TR/UISecurity/

- CORS

http://www.w3.org/TR/cors/

- SubRessource Integrity

http://www.w3.org/TR/SRI/

Web App SecWG

CORS

Recommendation

CSP 1.0

User Interface Security Directives CSP

Candidate Recommendation

SRI

CSP 1.1

Last Call Working Draft

Public Working Draft

gemalto

CORS implementation …

Cross-Origin Resource Sharing - Recommendation

Method of performing XMLHttpRequests across domains

*Usage stats:	Global
Support:	82.6%
Partial support:	7.06%
Total:	89.66%

Show all versions	IE	Firefox	Chrome	Safari	Opera	iOS Safari	Opera Mini	Android Browser	Blackberry Browser	IE Mobile
								2.1		
								2.2		
						3.2		2.3		
						4.0-4.1		3.0		
	8.0					4.2-4.3		4.0		
	9.0					5.0-5.1		4.1		
	10.0	29.0	34.0			6.0-6.1		4.2-4.3	7.0	
Current	11.0	30.0	35.0	7.0	22.0	7.0-7.1	5.0-7.0	4.4	10.0	10.0
Near future		31.0	36.0	8.0	23.0	8.0		4.4.3		
Farther future		32.0	37.0		24.0					
3 versions ahead		33.0	38.0							

Notes | Known issues (3) | Resources (5) | Feedback — Edit on GitHub

Supported somewhat in IE8 and IE9 using the XDomainRequest object (but has limitations)

Source : Can I Use http://caniuse.com/#search=cors

gemalto

Web Crypto WG – crypto trolls

Trying to make available crypto to web apps

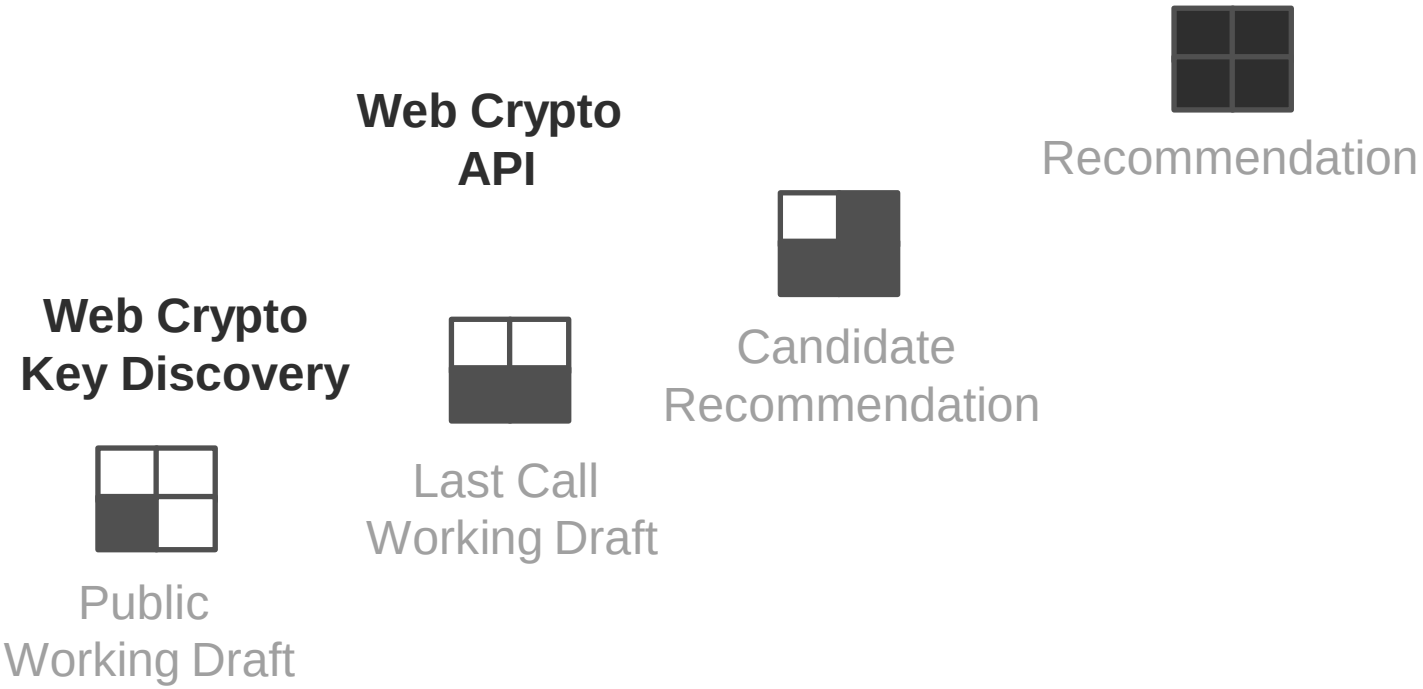
Web Crypto API

http://dvcs.w3.org/hg/webcrypto-api/raw-file/tip/spec/Overview.html

Web Crypto Key Discovery

https://dvcs.w3.org/hg/webcrypto-keydiscovery/raw-file/tip/Overview.html

Web Crypto WG



gemalto

Web Crypto API : first implementations

Netflix – NfWebCrypto project blog and github

Google – statement and corresponding issue by the Chromium team.

Internet Explorer – Developer documentation for IE11 preview and plugin for other browsers

WebKit – Implementation is tracked as bug 122679

Firefox – Implementation is tracked under bug 865789

Web Crypto API in few lines

With the Web Crypto API one can

- Generate a random
- Generate a key
- Derive key (or bits)
- Import or export 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-1
- 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

But this is not the end...

- Questions about key storage, dynamic algorithms, other algorithms, certificate management, integration of hardware token...
- Will be part of 2015 work...

Web Security IG – labs and research

To strengthen the open web platform and clarify the next steps

- Security reviews

- W3C next steps

Security reviews

Process under construction

Aims to make systematic security reviews

Candidates – but no resources

- EME
- HTML5
- Manifest
- Web RTC

Next steps

Collect W3C members wishes

- Protocol Security Enablers
- Device Trusted Enablers
- Securing resources
- User Security Indicators

By the way, privacy is also a hot W3C topic

Tracking Protection WG

Privacy Interest Group

All is here http://www.w3.org/Privacy/

Did you hear that ?

Webizen ....

https://www.w3.org/wiki/Webizen

gemalto

Thanks!

Keep in touch

@poulpita
virginie.galindo@gemalto.com

gemalto

Credit photos

Lake by Stephane (slide 28)
Trees and Circle by Naty (slide 27)
Pupils protest (slide 13), techno parad (slide 30) by Philipe Leroyer
Grubling of the tigers (slide 7) by Yoann
Caffeinated (slide 2) by Ross Pollack
L'enfant au chapeau (slide 4) by Martine Lanchec Girard
On the road (slide 12) by Ki2
Alignement de cabine de plage (slide 15) by Nomad Photography
Lego (slide 14) by Josselin Lioust
L'indémodable (slide 3) by EquinoxeFr
Parc du boisé de Saint Sulpice (slide 26) , Hamac (slide 33) by Bob August
Mortel (slide 5) by Angelus Yodasson
Jardin des Plantes Nantes (slide 6) by Gwen
Lettres (slide 31) by Daoro

Source : Flickr, all pictures in Creative Commons

gemalto

gemalto