One of our Algorithms is Missing

Crypto APIs in 2014

Cryptosense

Graham Steel

Most **Real World Crypto™** is delivered by APIs.

APIs are often standardised.

Standards can lag behind advances in crypto...

...in 2014 some progress was made.

PKCS#11

Describes Cryptoki, most widely-used API for crypto hardware **smartcards, HSMs** (see session 9 tomorrow)

Latest version (v2.20) - 2004(!)

In 2012, the standard moved from RSA to OASIS

v2.40 approved in **December 2014**

v2.20	v2.40
No authenticated encryption mode	GCM+CCM
No MAC mode secure for variable-length messages	CMAC + GMAC
PBKDF2 with SHA-1 only	PBKDF2 with SHA-256 and SHA-512
Broken legacy crypto	Less broken legacy crypto
Secure key management difficult	Secure key management difficult

Webcrypto

Native crypto available in the browser.

Some good crypto, some less good crypto.

https://github.com/cryptosense

A simple (free) analysis tool

Secure key management difficult

More in: Cairns & Steel 2014, "Webcrypto Analysis Highlights"

More on secure use of PKCS#11
and Webcrypto at:

http://cryptosense.com/blog

@cryptosense