The Problem with Cryptography

Crypto is:

- Ubiquitous
- Powerful
- Complex
- Fragile

How can a company find and remove weaknesses, and then demonstrate its systems are secure?
Solution

- **Cryptosense**: software tools for vulnerability management of cryptographic systems.
- Vision: treat all enterprise crypto
- First step: focusing on HSMs and associated applications.
- **Cryptosense Analyzer** for PKCS#11 HSMs in use at two European national security agencies and two top five European banks.
- Currently developing/testing Thales (payment API), MS CAPI/CNG and OpenSSL versions.
How it Works

Cryptosense Analyzer

command
attack
response

October 2014  CRYPTOSENSE
Vulnerability scanning vs Cryptosense

<table>
<thead>
<tr>
<th>Standard vuln scanner</th>
<th>Cryptosense</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks “fingerprint” of system against database of known vulns</td>
<td>Infers a model of specific system and config under test, searches this model for “new” attacks</td>
</tr>
<tr>
<td>Typically many false positives + negatives</td>
<td>Attacks found are executable, all attacks of a particular class can be found</td>
</tr>
<tr>
<td>Not useful for custom apps</td>
<td>Works just fine on custom apps</td>
</tr>
<tr>
<td>Usually accesses a cloud-based DB of vulns</td>
<td>Autonomous: no need to connect to an external network</td>
</tr>
</tbody>
</table>
Vulnerabilities Cryptosense Analyzer finds

1. **Implementation discrepancies**
   PKCS#11 is a 407 page document with 303 footnotes, many of which are security critical (e.g. CVE-2010-3321)

2. **Configuration problems**
   Even correct implementations may expose *combinations* of commands that are insecure.

3. **Application incoherencies**
   Even if the HSM is secure, the application can misuse it.
Cryptosense solution

1. Security audit of existing infrastructure
   ◦ using Analyzer

2. Secure configuration
   ◦ using App Tracer to check applications

3. Regular automatic testing of HSM infrastructure
   ◦ using Cryptosense Monitor
   ◦ to prove to auditors (internal or external) that risks are identified, controls are in place and implemented (weekly reports)
Compliance testing

Get a free demo at http://cryptosense.com
PKCS#11 Future

In early 2013 PKCS#11 moved from RSA to OASIS.

v2.40 now in public draft at http://docs.oasis-open.org/pkcs11

Some significant changes to available crypto - see blog articles at http://cryptosense.com/tag/pkcs11

v3.0 (2015) brief is to address key protection, multiple user profiles/authentication, updated crypto mechanisms..
W3C Web Crypto API

"..expose trusted cryptographic primitives from the browser. This will promote higher security insofar as Web application developers will no longer have to create their own or use untrusted third-party libraries for cryptographic primitives."

April 2012: Group Formation

April 2014: Last call on v1.0

October 2013: Exit Last Call (?)

Jan 2015: Expected Recommendation (?)
Cryptosense W3C API Tracer

Get it from https://github.com/cryptosense
More information

Video demo and various details at cryptosense.com

White paper on PKCS#11 vulnerabilities available graham@cryptosense.com