Securing PKCS#11 HSM Deployments

Hardware-based cryptography is a core technology for controlling risk in potentially hostile environments such as mobile, cloud and Internet of things.

However, choosing, configuring, deploying and securely using a cryptographic device like a Hardware Security Module (HSM) is far from simple. A small mistake in the details can lead to a complete loss of security.

Cryptosense software ensures the ongoing security of your system with comprehensive testing and monitoring tools.

Key Features

Formal Methods technology

The combination of automated fuzzing, model inference and model-checking makes the power of formal analysis techniques available to everyone.

Out of the box functionality

Cryptosense Analyzer requires no configuration to produce insights into the security of a PKCS#11 deployment.

Available as a Product or Service

Cryptosense analysts can complete a full audit of a PKCS#11 installation for you using our toolsuite.

Ongoing monitoring

Once best practice has been established, Cryptosense Monitor can be installed to ensure configurations stay unchanged and keys remain secure.

Comprehensive Testing Suite

Our adaptative mutation-based fuzzing engine explores the corner-cases of the PKCS#11 standard as implemented in the device under test. The results are passed through more than 100 compliance and vulnerability filters to detect anomalies and weaknesses like CVE-2015-5464 and CVE-2015-6924. This facilitates security testing of vendors equipment before procurement as well as evaluation of firmware updates and configuration changes.

Access to the latest applied crypto research results

Our App Tracer software records the way an application uses the PKCS#11 interface during run-time. Afterwards, it applies logical rules to the trace to test security. These rules are based on the latest academic research results (Cryptosense is a spin-off from INRIA Team Prosecco that recently discovered the FREAK, LOGJAM and SLOTH vulnerabilities) as well as our own vulnerability research and recommendations from standards institutes like NIST, ENISA and PCI. Key-length and approved algorithm rules can be customized to company policy to leverage existing internal expertise.

Alerts that integrate with your existing systems

Cryptosense Monitor makes regular tests on your HSM and the keys it contains. If the configuration has changed since the last test, or if the keys are not protected in the same way, an alert is created. The alerts can be customized to integrate with existing security incident management systems to ensure efficient treatment.

Technical Specifications

- Runs on Windows, Mac, Linux, AIX and Solaris - 32 or 64 bit.
- Supports any PKCS#11 compatible device including HSMs and smartcards.
- No need to consult a cloud-based database of vulnerabilities, so can be used in sensitive internal network environments.

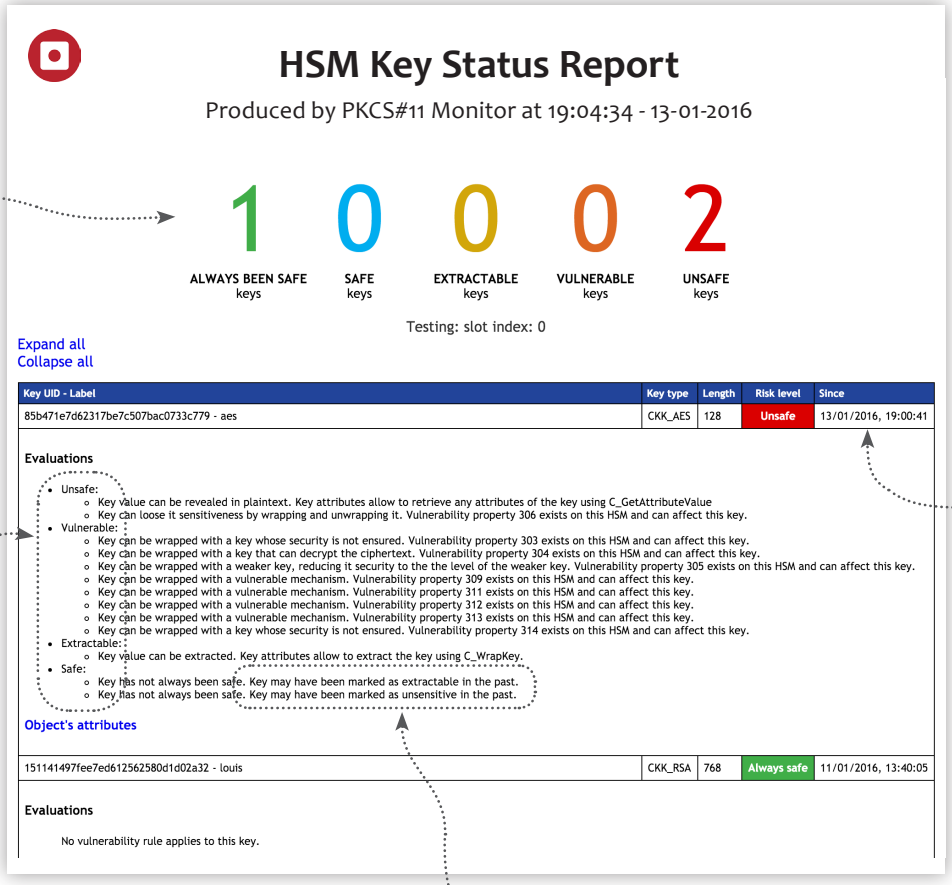
About Cryptosense

Cryptosense's founders combine more than 40 years experience in research and industry. Based in Paris, France, Cryptosense provides its security analysis solutions to an international clientele in particular in the financial, industrial and government sectors.

Cryptosense

Securing PKCS#11 HSM Deployments

Summary
Quickly get an overview of risk level by key.



HSM Key Status Report

Produced by PKCS#11 Monitor at 19:04:34 - 13-01-2016

1	0	0	0	2
ALWAYS BEEN SAFE keys	SAFE keys	EXTRACTABLE keys	VULNERABLE keys	UNSAFE keys

Testing: slot index: 0

Expand all
Collapse all

Key UID - Label	Key type	Length	Risk level	Since
85b471e7d62317be7c507bac0733c779 - aes	CKK_AES	128	Unsafe	13/01/2016, 19:00:41

Evaluations

- Unsafe:
  - Key value can be revealed in plaintext. Key attributes allow to retrieve any attributes of the key using C_GetAttributeValue
  - Key can loose it sensitiveness by wrapping and unwrapping it. Vulnerability property 306 exists on this HSM and can affect this key.
- Vulnerable:
  - Key can be wrapped with a key whose security is not ensured. Vulnerability property 303 exists on this HSM and can affect this key.
  - Key can be wrapped with a key that can decrypt the ciphertext. Vulnerability property 304 exists on this HSM and can affect this key.
  - Key can be wrapped with a weaker key, reducing it security to the the level of the weaker key. Vulnerability property 305 exists on this HSM and can affect this key.
  - Key can be wrapped with a vulnerable mechanism. Vulnerability property 309 exists on this HSM and can affect this key.
  - Key can be wrapped with a vulnerable mechanism. Vulnerability property 311 exists on this HSM and can affect this key.
  - Key can be wrapped with a vulnerable mechanism. Vulnerability property 312 exists on this HSM and can affect this key.
  - Key can be wrapped with a vulnerable mechanism. Vulnerability property 313 exists on this HSM and can affect this key.
  - Key can be wrapped with a key whose security is not ensured. Vulnerability property 314 exists on this HSM and can affect this key.
- Extractable:
  - Key value can be extracted. Key attributes allow to extract the key using C_WrapKey.
- Safe:
  - Key has not always been safe. Key may have been marked as extractable in the past.
  - Key has not always been safe. Key may have been marked as unsensitive in the past.

Object's attributes

151141497fee7ed612562580d1d02a32 - louis	CKK_RSA	768	Always safe	11/01/2016, 13:40:05

Evaluations

No vulnerability rule applies to this key.

Customized Rules
Specific vulnerability rules are derived from your HSM and its configuration.

Risk Level
Reports give risk level and record when this status was first seen.

Historical Analysis
Properties record not just current status, but also past security of the key.

Contact us

To find out how your organization can use Cryptosense to discover and mitigate unknown vulnerabilities in cryptography, contact us at **sales@cryptosense.com** or go to **https://cryptosense.com**

Cryptosense