Contribution ID : **18** Type : **not specified**

Threshold-Cryptography Distributed HSM

Friday, 1 April 2016 09:30 (30)

In the 20th DNS-OARC workshop, we showed a virtual HSM based on threshold cryptography. This system has the purpose to be used with OpenDNSSEC in order to provide a low cost solution to DNS record signing automation. But that system had a single point of failure: the key manager. Single points of failure are undesirable, even more in a fault tolerant distributed system. After a reengineering during the last year, we solved this problem by implementing the whole protocol within the PKCS #11 API. The communication now is done directly between the application that uses the system and the nodes, without the need of any centralised subsystem. This reengineering not only help us to have a really fault tolerant system but to improve the performance by reducing the latency of the operations.

In this presentation, we will walk through the main features of the system, how simple is to integrate it with currently working systems, and how the system might help to improve the number of deployed DNSSEC systems when a secure low-cost cryptographic solution is needed.

Summary

Primary author(s) : Mr. CIFUENTES, Francisco (NIC Chile Research Labs)

Co-author(s) : Dr. HEVIA, Alejandro (Computer Science Department (DCC), Universidad de Chile); Dr. BUSTOS-JIMÉNEZ, Javier (NIC Chile Research Labs (NICLabs). Universidad de Chile)

Presenter(s) : Mr. CIFUENTES, Francisco (NIC Chile Research Labs)

Session Classification : Public Workshop: Tools & Measurements

Track Classification : Public Workshop