DNS-OARC
Domain Name System Operations Analysis and Research Center

Contribution ID : **22** Type : **not specified**

Low-Cost Threshold Cryptography HSM for OpenDNSSEC

Monday, 13 October 2014 11:50 (20)

The DNS Security Extensions (DNSSEC) add a new layer of security based on public-key infrastructure: each DNS record is digitally signed to verify the authenticity of the answer. However, the introduction of DNSSEC has an impact in the operational workflow of DNS systems: (i) signatures have an expiration date, hence the records must be periodically signed and (ii) key management tasks can be overwhelming. These are problems specially for DNS zones with several records (for instance a Top Level Domain).
The adoption of Hardware Security Module (HSM) is an option to provide highly secured keys and signature management. Nevertheless HSM is expensive and hardware can fail. We present a novel system based on threshold cryptography to support the operational signing workflow of DNSSEC. This approach significantly improves security and availability of the overall system since the secret key is never stored in a single place; it is spread among the nodes of the
system.

Summary

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

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

Session Classification : Monday Joint OARC/Tech Day

Track Classification : Joint OARC/Tech Day