Virtual HSM Implementation in OpenVZ Containers

Dmitry Kartashov, Kirill Krinkin
Saint-Petersburg Academic University of Russian Academy of Sciences
Saint-Petersburg, Russia
mapseamoff@mail.ru

Abstract—**Hardware Security Module (HSM) is a physical device that can keep digital keys and other security data and provide traditional cryptography operations like encryption/decryption and so on. Such modules usually physically connected to the computer or server. Our project aims to create Virtual HSM based on linux container technology OpenVZ [1] and provide HSM functionality in virtual environment (usually used in data centers).**

Keywords—OpenVZ, Virtual HSM, Linux Containers.

I. SUMMARY

Traditional HSM provides next main functionality: secure cryptographic key generation, secure cryptographic key storage and management, etc. The main idea is to encapsulate all sensitive data and operations outside of server. Nowadays, virtual infrastructure is being used for providing traditional server functionality. Virtual servers are being run on real hardware of data centers and end user cannot use HSM in this case. We suggest to use Linux Containers for HSM functionality implementation.

Suggested solution has layered architecture. Key components are:

- virtual HSM environment (VHSM VE) – separated OpenVZ container, which encapsulates HSM logic;
- secured transport – implementation of the HSM protocol over netlink interface.

Currently we published [2] preliminary solution which can be downloaded.

REFERENCES

[1] OpenVZ Linux Containers Wiki, Web: http://openvz.org.
[2] VHSM repository, Web: https://github.com/OSLL/vhsm.