

Разработка виртуального HSM для платформы Linux

Выполнили: Карташов Д. А., Савенко С. А.

Руководитель: Кринкин К. В.

Кафедра математических и информационных технологий
Санкт-Петербургский Академический университет

2013

Введение

Криптография в приложениях:

- ▶ хранение секретных данных
- ▶ вычисления с их использованием

Проблемы безопасности:

- ▶ компрометация секретных данных

Решение:

- ▶ исключить попадание секретных данных на диск и/или в память компьютера

Цели и задачи проекта

Цель

Разработать решение, предоставляющее функциональность HSM в виртуальном окружении

Задачи

- ▶ поиск и анализ существующих решений;
- ▶ изучение стандартов HSM;
- ▶ изучение приложений, поддерживающих HSM;
- ▶ разработка прототипа VHSM.

Существующие решения

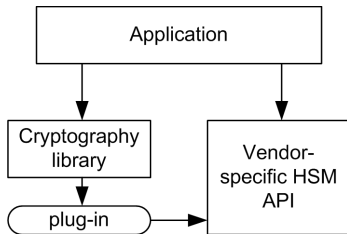
Существующие решения:

- ▶ Amazon CloudHSM:
<http://aws.amazon.com/cloudhsm/>

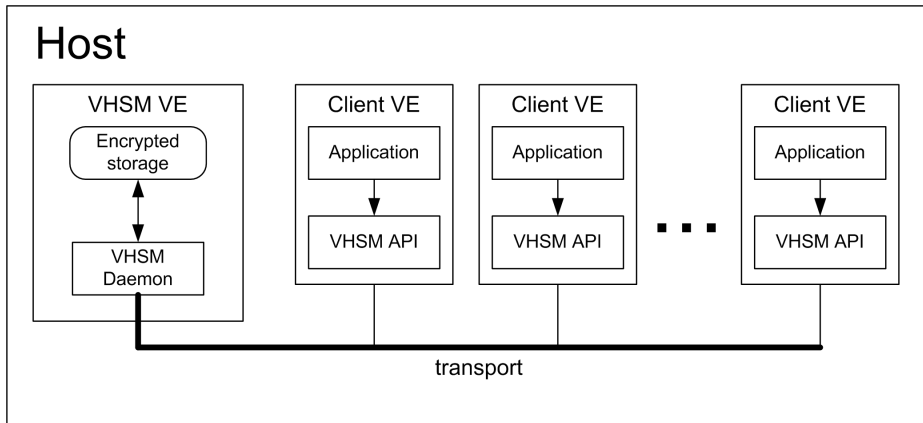
Стандарты HSM:

- ▶ pkcs#11:
<http://www.rsa.com/rsalabs/node.asp?id=2133>

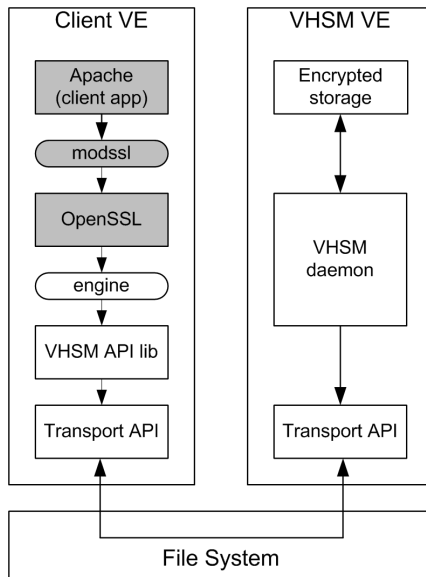
Использование HSM в приложениях:



Общая архитектура решения



Детали реализации



Использованные решения

- ▶ Протокол:
 - ▶ Google protobuf
- ▶ Транспорт:
 - ▶ файловая система
- ▶ Защищенное хранилище:
 - ▶ файловая система
 - ▶ AES
- ▶ Криптография:
 - ▶ crypto++

Итоги

- ▶ Реализован прототип:
 - ▶ MAC
 - ▶ хэш-функции
 - ▶ управление ключами
 - ▶ OpenSSL engine
- ▶ Изучены технологии:
 - ▶ криптография
 - ▶ protobuf
 - ▶ OpenSSL
 - ▶ pkcs#11
 - ▶ crypto++
 - ▶ OpenVZ
 - ▶ netlink

Ссылки

- ▶ Репозиторий проекта:
`https://github.com/OSLL/vhsm`
- ▶ wiki проекта:
`http://osll.spb.ru/projects/vhsm/wiki`