Разработка виртуального HSM для платформы Linux

Карташов Д. А., Орлов А. В., Азаров А. И.
Руководитель: Кринкин К. В.

Кафедра математических и информационных технологий
Санкт-Петербургский Академический университет

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

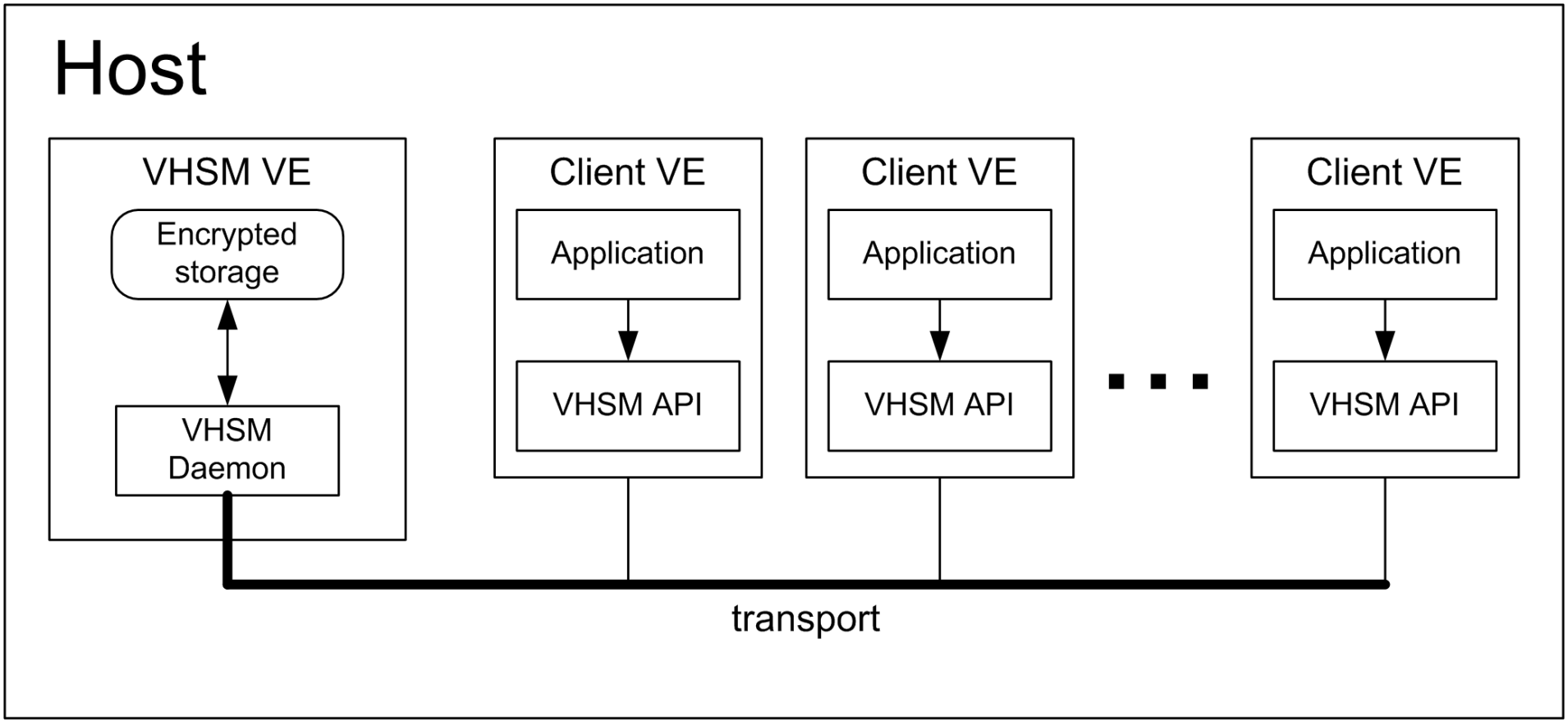
Цель

Разработать решение, предоставляющее функциональность HSM в виртуальном окружении

Задачи

- поиск и анализ существующих решений;
- изучение стандартов HSM;
- разработка прототипа VHSM:
  - клиентский API;
  - защищенное хранилище;
  - транспорт;
- формирование конечного продукта:
  - система сборки;
  - unit и интеграционные тесты;
  - пакетирование.

Общая архитектура решения

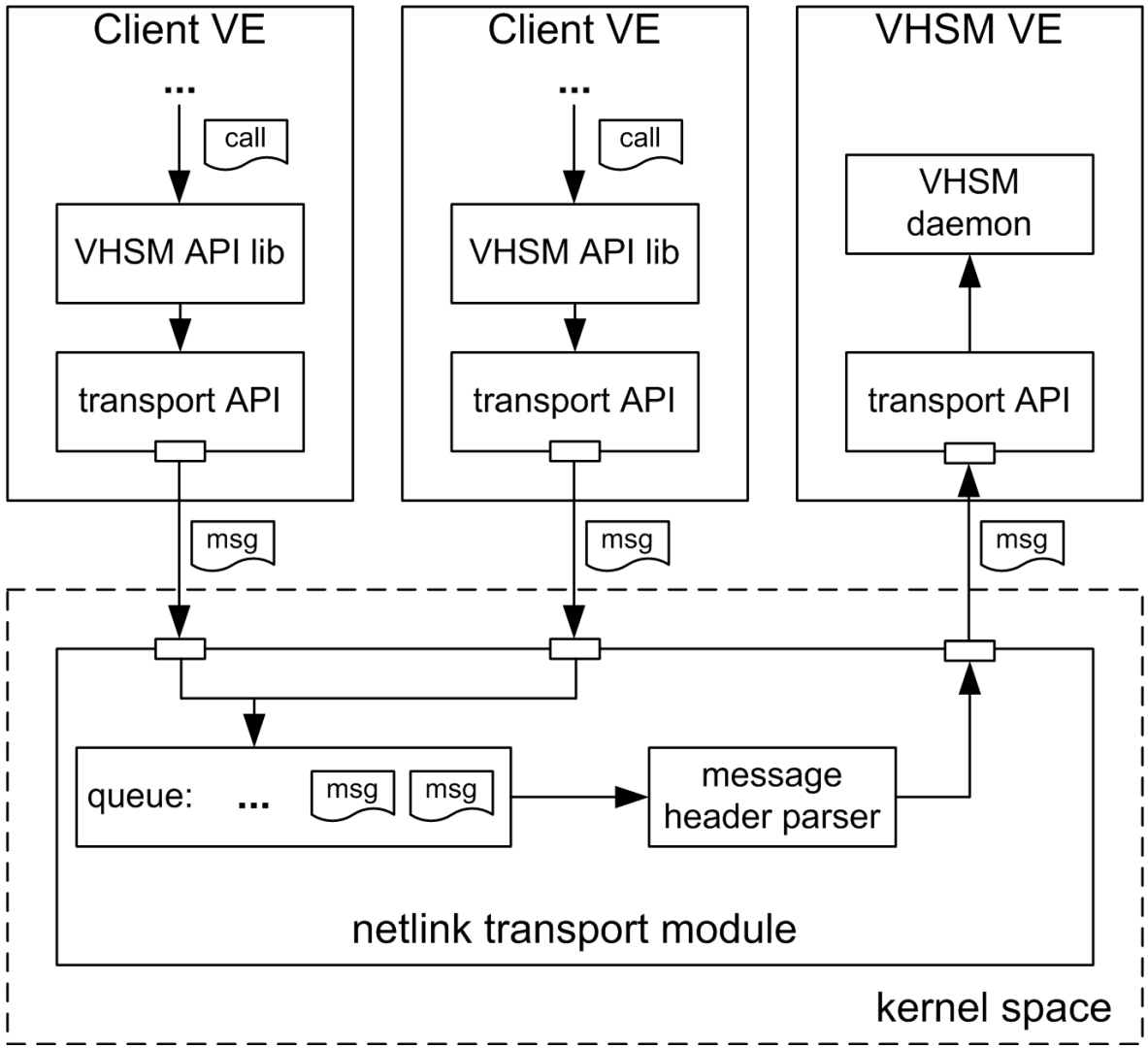


Основные компоненты

- **Transport**
  - пересылка сообщений
  - идентификация контейнеров
- **VHSM API**
  - передача запросов на выполнение криптографических операций через транспорт
  - получение результатов операций
- **VHSM daemon**
  - аутентификация
  - выполнение криптографических операций с использованием секретных данных
- **Encrypted storage**
  - хранение секретных данных пользователя

Transport

- протокол — Google Protobuf
- реализован на основе netlink



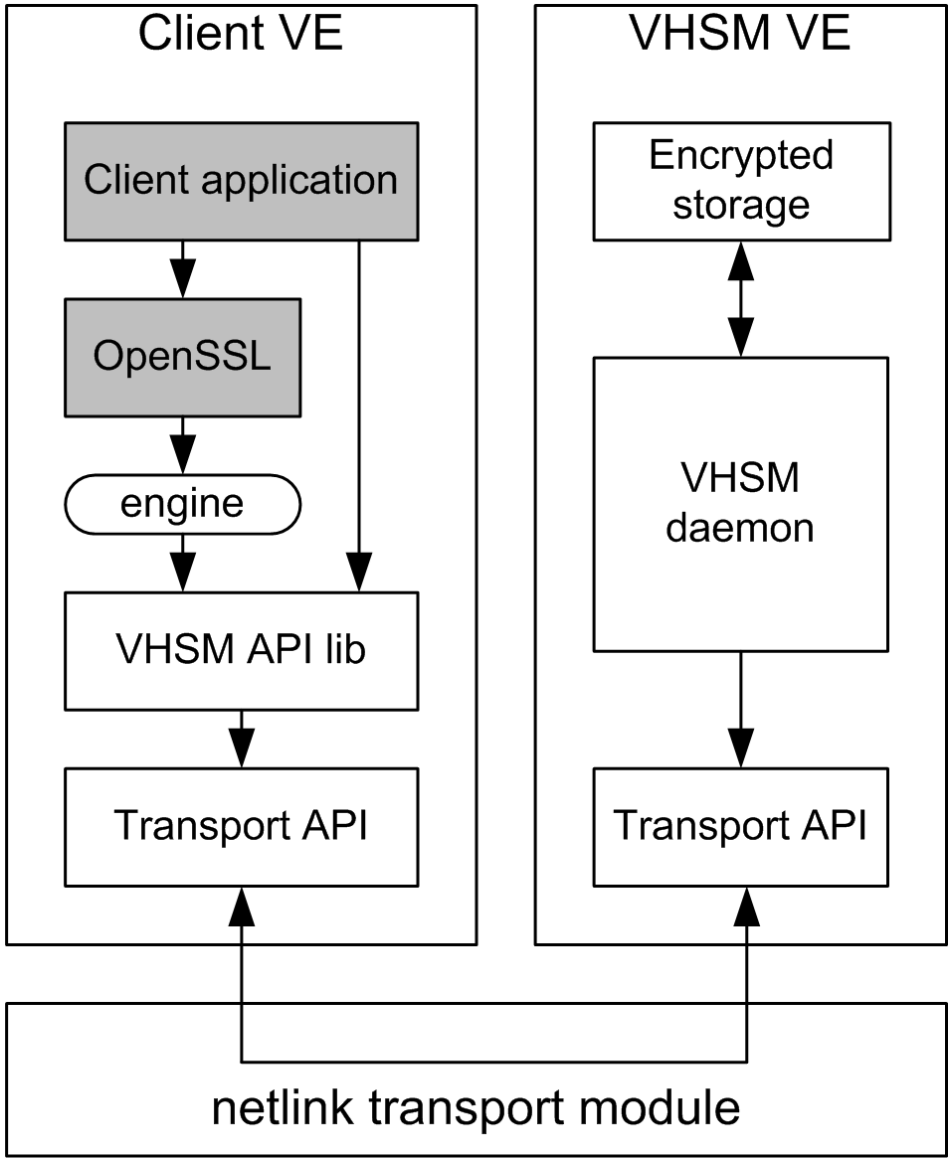
VHSM API

- управление сессиями
  - открытие/завершение сессии;
  - аутентификация пользователя;
- управление ключами
  - импорт;
  - генерация;
  - удаление;
- хэширование и MAC
  - стандартные функции: `init`, `update`, `final`

VHSM daemon & encrypted storage

- вычисление криптографических функций
- хранение пользовательских данных:
  - база данных SQLite;
  - пользовательские ключи хранятся в зашифрованном виде;
  - шифрование AES в режиме GCM;
  - ключ шифрования генерируется функцией PBKDF2 на основе пароля пользователя;

Пример использования



Тестирование

- Unit-тесты
- Интеграционные тесты:
  - установка и инициализация контейнеров;
  - создание пользователя;
  - вход и выход из системы;
  - операции с ключами;
  - HMAC.

Система сборки и пакетирование

- Система сборки:
  - cmake;
- Генерация пакетов:
  - rpm;
  - deb;
- Пакеты:
  - client;
  - server;
  - host.

Итоги и планы

Итоги:

- реализована система, состоящая из нескольких компонентов:
  - клиентская библиотека;
  - транспортный модуль;
  - VHSM и хранилище;
- внедрена система сборки;
- проведены unit и интеграционные тесты;

Планы на будущее:

- расширение функциональности VHSM;
- введение прав пользователей и уровней доступа.

Ссылки

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