УДК 004.056.55

Обзор аппаратных решений для хранения долей пороговых подписей Elliptic Curve DSA.

Салихов М.Р. (Университет ИТМО)
Научный руководитель – доцент, кандидат технических наук, Таранов С.В.
(Университет ИТМО)

Введение. Ведущую роль в системах защиты информации занимают методы управления и хранения криптографических ключей. От данных методов напрямую зависит стойкость криптографических систем шифрования, устойчивость протоколов к атакам. Управление ключами играет важнейшую роль в криптографии как основа для обеспечения конфиденциальности обмена информацией, идентификации и целостности данных. Как бы ни была сложна и надежна сама криптосистема, она основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в системе, где количество пользователей составляет десятки и сотни управление ключами, – это серьезная проблема. Под ключевой информацией понимается совокупность всех действующих в системе ключей. Если не обеспечено достаточно надежное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации.

Основная часть. Рассматриваются аппаратные решения для хранения долей пороговых подписей Elliptic Curve DSA, такие как Hardware Security Module(HSM), Trusted Platform Module(TPM). HSM – это физическое устройство, которое само хранит цифровые ключи или другие секретные данные, управляет ими, генерирует их, а также производит с их помощью криптографические операции. HSM защищает ваши приватные ключи и берет на себя выполнение всех криптографических операций, позволяя вашим узлам и клиентам подписывать и подтверждать транзакции без риска раскрытия их приватных ключей. Модули TPM сами по себе не новы, но всё чаще их используют для защиты закрытых ключей. Доверенный платформенный модуль можно использовать для хранения (или переноса) корневого ключа и защиты дополнительных ключей, созданных приложением. Ключи приложений нельзя использовать без TPM, что делает его очень полезным методом аутентификации для оконечных точек, таких как ноутбуки, серверы и производители устройств Интернета вещей.

Выводы. Проведен обзор существующих аппаратных решений для хранения долей пороговых подписей.

Список использованных источников:

1. Habr [Электронный ресурс] URL: https://habr.com/ru/company/globalsign/blog/352626/
2. Demos [Электронный ресурс] URL: https://www.demos.ru/vendors/crypto/hsm/