Архитектура ключей

Современная линейка ключей Guardant (**Guardant Sign / Time / Sign Net /Time Net**) обладает энергонезависимой памятью общим объемом 4096 байт.Часть этой памяти недоступна ни для чтения, ни для записи, часть доступна только для чтения, часть может изменяться только специальными операциями. Остальная память доступна для чтения и записи. При необходимости можно создавать области памяти, защищенные от чтения и (или) записи.

Современные ключи Guardant с загружаемым кодом (**Guardant Code / Code Time**) имеют 128 Кбайт Flash-памяти для загружаемого кода, а также энергонезависимую память общим объемом 4096 байт, предназначенную, в основном, для хранения данных защищенного приложения.

Адресация памяти	Режимы адресации памяти электронных ключей Guardant
Карта памяти Guardant Sign	Описание полей памяти современной линейки электронных ключей Guardant

Протокол обмена драйвера с ключом традиционно является одним из уязвимых звеньев программно-аппаратной защиты. Его изучение – один из основных этапов создания эмуляторов электронных ключей.
Разработчики электронных ключей тратят много сил на улучшение стойкости протоколов обмена. Протокол обмена с современными ключами Guardant имеет ряд оригинальных свойств, повышающих его стойкость.

Свойства протокола обмена с ключом

Шифрование трафика. Все данные, курсирующие между Guardant API и электронным ключом Guardant, непрерывно шифруются при помощи алгоритма AES-128. Это значительно осложняет задачу анализа протокола обмена.
Использование сеансовых ключей. Для противодействия атакам типа «man-in-the-middle» (MITM) на протокол обмена между электронным ключом и Guardant API используется принцип сеансовых ключей. Для каждого сеанса работы с электронным ключом вырабатывается уникальный ключ, на котором и производится шифрование трафика. В течение сеанса периодически вырабатывается новый сеансовый ключ. Таким образом, даже при обмене одинаковыми данными трафик не повторяется и задача построения табличного эмулятора не может быть решена.
Взаимная аутентификация. Кроме собственно шифрования трафика, протокол обеспечивает взаимную аутентификацию электронного ключа и Guardant API, основанную на использовании асимметричного криптографического алгоритма на базе эллиптических кривых ECC160, для защиты от атак типа MITM.

Устройство ключей Sign и Time

Современные электронные ключи Guardant базируются на высокопроизводительном 32-разрядном микроконтроллере. По сравнению с предшественниками, новые ключи получили гораздо больше вычислительных ресурсов и обеспечивают в несколько раз большую производительность и высокую скорость обмена данными с компьютером по шине USB.

Этот факт открывает множество новых возможностей защиты, как, например, вычисление хэш-функций, шифрование данных симметричными алгоритмами, электронная цифровая подпись на основе эллиптических кривых.

Благодаря наличию микроконтроллера электронный ключ Guardant представляет собой интеллектуальное устройство, способное обрабатывать данные по сложным алгоритмам. На этапе изготовления ключа в память его микроконтроллера "прошивается" специальная микропрограмма, реализующая следующие функции:

- Доступ к функциям ключа по трем 32-битным паролям - кодам доступа
- Интерфейсные функции, организация защищенного протокола обмена с драйвером
- Вычисление функций преобразования данных (симметричное шифрование, хэш-функции, асимметричное шифрование и ЭЦП) при помощи аппаратных алгоритмов
- Защита содержимого памяти: аппаратные запреты

Для электронных ключей используются микроконтроллеры, защищенные от считывания и модификации микропрограммы. Согласно идеологии такого микроконтроллера, его микропрограмма и расположенная в нем память **(EEPROM** и **RAM)** недоступны ни для считывания, ни для модификации. Таким образом, микроконтроллер представляет собой "черный ящик", скрывающий все происходящие в нем процессы.

- EEPROM-память
    - Адресация памяти