Аппаратные алгоритмы

В этой части подробно описаны аппаратные алгоритмы: для защиты от каких методов взлома они нужны, каково их устройство, как с их помощью можно преобразовать данные и усложнить логику работы ключа.

Важная информация

1. Хотя дескрипторы аппаратных алгоритмов и являются частным случаем защищенных ячеек, аппаратные алгоритмы являются основным защитным механизмом, предоставляемым электронными ключами. Поэтому понимание сути работы аппаратных алгоритмов и правильное использование их для защиты программного обеспечения играет решающую роль в построении надежных систем защиты и повышает защищенность приложений на порядки
2. Обратите особое внимание на устройство алгоритмов и на особенности методов преобразования данных с их помощью.

Назначение

Аппаратные алгоритмы ключей Guardant предназначены для преобразования информации. С их помощью можно шифровать любые данные, используемые защищенным приложением. При правильной организации защиты, использование аппаратных алгоритмов делает бессмысленным удаление хакером вызовов функций Guardant API из кода приложения: в этом случае попросту нечем будет декодировать данные. Кроме того, при правильном использовании аппаратных алгоритмов можно достичь достаточно высокой степени защищенности от эмуляции.

Эмулятор – это программный модуль или драйвер, умеющий воспроизводить процесс обмена с тем или иным ключом и «подсовывающий» защищенному приложению те данные, которые оно ожидает получить. То есть программный эмулятор, по сути, становится полноценной заменой (с точки зрения защищенного приложения, конечно) электронного ключа.

Важная информация

Единственный эффективный путь борьбы с эмуляцией – это усложнение логики работы с ключом. Только в том случае, если ключ обменивается с приложением большими объемами каждый раз разных данных на протяжении как можно больших периодов времени, написание эмулятора становится слишком трудоемким. Только в том случае, если эти данные невозможно ни подсмотреть, ни вычислить заранее, написание эмулятора становится задачей очень трудно реализуемой.

К ним относятся симметричные алгоритмы типа GSII64 и AES128, однонаправленные алгоритмы HASH64 и SHA256, вычисляющие хэш-функцию от исходных данных, алгоритм электронной цифровой подписи на базе эллиптических кривых ECC160, алгоритм генерации случайных чисел RND64.

Особенности

Аппаратные алгоритмы ключей Guardant имеют следующие особенности:

- Преобразование данных происходит не в приложении, а в электронном ключе, что исключает возможность изучения алгоритмов при помощи отладчика и делает бессмысленным удаление из программы модулей защиты.
- Данные преобразуются стойким алгоритмом, секретный ключ которого находится в памяти электронного ключа и не покидает его при выполнении преобразования. Стойкость алгоритма подразумевает, что даже если удастся извлечь сам алгоритм, то на подбор секретного ключа уйдет много вычислительных ресурсов, а вычислить его аналитическими методами не удастся.
- Разработчику приложения известен только секретный ключ шифрования аппаратного алгоритма, а создателям ключей только вид микропрограммы, обрабатывающей этот дескриптор. Таким образом, конкретный вид аппаратного алгоритма, не может быть известен никому.
- Одно и то же защищенное приложение может использовать несколько уникальных дескрипторов аппаратных алгоритмов для преобразования разной информации. Это заставит хакера подбирать вид каждого из них.