Диалоговый код против кодграббера

В последнее время мы все чаще слышим, что команду, которую посылает брелок сигнализации, можно перехватить специальным прибором - так называемым кодграббером или сканером, а потом снять машину с охраны незаметно для владельца. Как этому противостоят современные системы?

Начнем с того, что кодграбберы появились еще в прошлом веке, практически одновременно с первыми электронными охранными системами. Тогда использовался фиксированный код, подобрать который при том уровне техники было невероятно сложно. Но неизменный код легко занести в память специального радиоприемника (кодграббера) – достаточно один раз оказаться неподалеку от «родного» брелока в момент постановки или снятия с охраны. А воспроизвести команду, само собой, уже в отсутствие хозяина.

В качестве ответной меры появился динамический код, который при каждой посылке изменялся по особому алгоритму, заложенному в память брелока и сигнализации. Поэтому воспроизведение однажды записанного кода уже не могло помочь угонщикам. Но они не стояли на месте. Не будем вдаваться в математические тонкости дешифровки, заметим лишь, что, записав несколько последовательно переданных с одного брелока команд, можно расшифровать алгоритм формирования «секретной» части динамического кода – это вопрос времени.

На сегодняшний день (и надолго вперед) **полноценную защиту от электронного взлома обеспечивает только диалоговый код с индивидуальными ключами шифрования.** Система, приняв динамически кодированную команду («пароль»), не выполняет ее сразу, а посылает запрос на подтверждение – некое случайное число, также динамически кодированное. Брелок его принимает и при помощи секретного ключа и сложного алгоритма формирует «отзыв», снова динамически перекодирует и шлет системе. Если отзыв верен, то система выполняет команду, причем процесс занимает доли секунды. В отличие от брелока кодграббер в руках даже самого матерого угонщика не знает алгоритма изменения кода, ключа шифрования и не способен сформировать отзыв за отведенное на это время. Но и эти меры – еще не предел защиты.

«Диалоговый код»

Особенности диалогового кода, реализованного в сигнализациях и иммобилайзерах StarLine, гарантируют абсолютную защиту от взлома с помощью любых известных кодграбберов. В каждой системе используется индивидуальный ключ шифрования, передаваемый единственный раз при регистрации брелока в системе. Длина ключа — 128 бит, что дает $3{,}4*10^{38}$ комбинаций. Даже если перебирать миллиарды вариантов в секунду, чтобы разгадать задачу, потребуется больше времени, чем существует Вселенная. При существующих сегодня вычислительных средствах решить эту задачу «в лоб» невозможно.

При формировании отзыва в диалоговом коде использован аппаратный генератор случайных чисел, дополнительно защищающий от взлома кода. Кроме того, передача пакетов информации сопровождается короткими паузами, а рабочая частота передачи внутри цикла авторизации скачкообразно изменяется.

Эти меры затрудняют как перехват, так и расшифровку команды – при том что подбор индивидуального ключа вообще невозможен. Короче говоря, смерть Кощея - в игле, игла - в яйце, яйцо - в утке, утка - в зайце, заяц - в сундуке, сундук - на дубе…

Компания StarLine настолько уверена в своем детище, что официально предлагает всем специалистам в области исследования криптостойкости долгосрочный контракт на сумму 5 000 000 рублей – пусть попробуют взломать!