Рекомендации по повышению устойчивости к взлому охранных систем на базе технологии KeeLoq.

Несмотря на надежность и устойчивость к «взлому» систем с «прыгающим» кодом, существует методика по их вскрытию. Основывается она на подмене кода и работает приблизительно следующим образом:

Рассмотрим такую ситуацию: Выходя из автомобиля, владелец нажимает кнопку на брелке «поставить на охрану». При этом ничего не происходит. Автомобилист, естественно, еще раз нажимает на эту же кнопку. Система нормально срабатывает и автомобиль становится на охрану, как и положено. Автомобилист думает, что в первый раз «что-то где-то не сработало», и уходит по своим делам.

А на самом деле произошло вот что:
Когда автомобилист первый раз нажимал на кнопку, находящийся неподалеку злоумышленник со специальным устройством - граббером перехватывает кодовую посылку, передаваемую с брелка владельца, и записывает ее в свою память. При этом сам граббер передает помеху, которая препятствует нормальной работе приемника в автомобиле, в результате система не срабатывает на эту последовательность. Когда же видя, что система не сработала, владелец автомобиля повторно нажимает кнопку «поставить на охрану», граббер злоумышленника так же «захватывает» передаваемый код и записывает в свою память, но одновременно с этим передает из своей памяти предыдущую записанную кодовую последовательность.

Приемник срабатывает, система взята на охрану, довольный владелец уходит. Но в памяти граббера остался последний ПРАВИЛЬНЫЙ код, передав который, злоумышленник может спокойно открыть автомобиль!!

Для повышения устойчивости к взлому охранных систем с использованием «интеллектуальных грабберов» рекомендуется:

1. Самый простой и эффективный способ - реализовывать включение режимов снятия\постановки на охрану РАЗНЫМИ КНОПКАМИ на брелке - т.е. поставить на охрану -одной кнопкой, снять с охраны - второй кнопкой. В этом случае даже захватив последний правильный код граббер сможет лишь повторно поставить систему на охрану, т.к. команда снятия с охраны имеет другой код.
2. (дополнениние к пункту 1) В кодовой посылке KeeLoq код передаваемой команды (кнопки) содержится в двух местах - в некодированном (явном) виде и в закодированном виде внутри «прыгающей» части кодовой последовательности. Так вот, система должна реагировать только на команды, полученные после декодирования прыгающей части кода, а так же проверять, что она одинакова с командой в некодированной части посылки. (на случай подмены кода команды в фиксированной части посылки).
3. По возможности использовать более совершенные кодеры семейства HCS36X с дополнительными битами CRC (разумется, что надо не только заменить кодер, но и переписать алгоритм декодера, добавив контроль CRC).
4. Идеальный вариант - использовать специальный алгоритм ОТЛОЖЕННОГО ИНКРЕМЕНТА. В этом случае через (например) 20 сек, и кодер (брелок), и декодер (приемник) автоматически увеличивают значение счетчика синхронизации. Соответственно, если взломщик с помощью граббера захватил последний доступный код, то через эти 20 сек. этот код уже перестает быть правильным. Полностью такой режим поддерживается только кодерами (транскодерами) HCS4XX. Теоретически можно использовать и недорогие HCS2XX/HCS30X, но в этом случае система будет срабатывать лишь на второе нажатие кнопки, так как автоматический инкремент будет производиться только декодером (приемником), а в недорогих моделях HCS20X/HCS30X эта функция не предусмотрена. В этом случае система будет ожидать прихода двух последовательных правильных команд, и только в этом случае срабатывать, что вынуждает владельца дважды нажимать на кнопку.
5. И, наконец, производителям охранных систем необходимо помнить, что чем лучше хранится в тайне мануфактурный код, записываемый при изготовлении в чип кодера (брелка), тем меньше вероятность вскрытия злоумышленниками охранной системы.