max (cor) A_x = 0,65;
max (cor) A_y = 0,35;
max (cor) A_z = 0,31;
max (cor) G_x = 0,23;
max (cor) G_y = 0,37;
max (cor) G_z = 0,76.

Можно заметить, что некоторые коэффициенты уменьшились более в чем два раза. Также примечательно, что в некоторых случаях оси A_x и G_z также показывали значения корреляции порядка 0.7, что близко к значениям, полученным при сравнении попыток одного человека. Однако остальные оси A_y, A_z, G_x G_y также продолжали сохранять двукратную разницу значений.

1. Лебедев А.Н., Онуфриев С.В., Степанов Б.А., Способ строгой многофакторной аутентификации. // «Безопасные информационные технологии». Сборник трудов Седьмой всероссийской научно-технической конференции / под ред. Матвеева В.А. – М.: НУК «Информатика и системы управления» МГТУ им. Н. Э. Баумана, 2017. – С. 194–196.

УДК 004.021

ЗАЩИТА КАНАЛОВ ПЕРЕДАЧИ ИНФОРМАЦИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ АТАК JACKPOTTING

Максимов Р.Л., Рафиков А.Г.
Московский государственный технический университет имени Н. Э. Баумана
Москва, Российская Федерация

Введение. Классическими примерами автоматизированных систем, которые стали неотъемлемой частью жизни каждого современного человека и требующие защиты от злоумышленников, являются банкоматы, платежные терминалы, терминалы самообслуживания, билетопечатающие автоматы.

Несмотря на постоянный интерес к банковскому сектору со стороны злоумышленников, представители этого бизнеса неохотно тратят дополнительные средства на дорогостоящие решения по защите банковских автоматов от атак на информацию. Если раньше практически всегда объектами атак становились клиенты банков, то в последнее время зачастую такими объектами становятся непосредственно системы банковского обслуживания и банковские автоматы (банкоматы, платежные терминалы).

Банкомат представляет особенный интерес для злоумышленников как хранилище денежных средств. Несмотря на то, что деньги хранятся в защищенном сейфе, злоумышленники находят способы добраться и до них.

Помимо радикальных методов, например, подрыва газом или кражи банкомата, имеют место и более высокотехнологичные атаки на уровне аппаратного и программного обеспечений, сетевого взаимодействия, подсистемы управления периферийным оборудованием. К ним относятся, так называемые, атаки jackpotting, одна из реализаций которых заключается в скрытом размещении внутри банкомата некоторого устройства (black box) и его непосредственном подключении к шинам или портам банковского автомата, что позволяет злоумышленнику удаленно контролировать все периферийные устройства. Это приводит к возможности анализа, перехвата и изменения команд при работе с диспенсером, что, в конечном счете, обеспечивает беспрепятственный несанкционированный вывод денежных средств из сейфа атакуемого объекта.

Основными проблемами, при этом, являются: использование стандартных интерфейсов (USB, RS232, SDC) и незащищенных коммуникационных каналов, в частности, для связи «хост-диспенсер», отсутствие механизмов аутентификации, авторизации и регистрации действий злоумышленников во время проведения jackpotting-атаки.

Широкому распространению атак на информацию банкоматов также способствует доступная злоумышленнику документация банкоматов с описанием протоколов и формата команд управления.

Относительно простым и недорогим решением по защите банкоматов от jackpotting-атак с использованием black box, может стать устройство на базе криптоконтроллера, имеющего нановаттное энергопотребление, возможность подключения батареи резервного питания, аппаратную поддержку криптографических алгоритмов для защиты каналов информационного обмена и реализующего функции блокирования наиболее критических периферийных устройств при обнаружении кибератаки. Таким образом, «блокиратор» использует алгоритмы взаимной аутентификации модулей устройства и шифрования потока управляющих команд для обнаружения атак, защиты и снижения ущерба от них путем блокирования соответствующего модуля.

К критическим (с точки зрения безопасности) периферийным устройствам банкоматов относятся: защищенная EPP-клавиатура (encrypting PIN pad), устройство для чтения карт (card reader), диспенсер (dispenser) и устройство для внесения наличных денег (cash-in).

Однако разработать высокоэффективный, быстродействующий, надежный криптографический алгоритм для решения поставленной

задачи в контексте сформулированных требований – серьезная задача.

В первую очередь проблема связана с использованием распространенных алгоритмов шифрования и со статистическими свойствами информации, используемой банкоматом в процессе работы. Суть заключается в том, что команды, при помощи которых производится управление периферийным оборудованием, диспенсером в частности, представляют собой ограниченный набор команд, а их перечень может быть получен из соответствующей документации. Следовательно, применение криптографических алгоритмов с использованием неизменного ключа шифрования будет приводить к ситуации, когда каждой одинаковой из заданных команд, будет соответствовать один и тот же шифртекст.

В некоторых случаях, с определенной долей вероятности, этого можно избежать, используя разнообразные режимы алгоритмов шифрования, но существует другая, не менее значимая в данном контексте проблема, заключающаяся в существенных дополнительных затратах вычислительных ресурсов и времени, необходимых для реализации известных (классических) криптографических алгоритмов.

Для сравнения, алгоритм DES (Data Encryption Standard) в самом схематичном виде использует начальную и финальную перестановки и 16 раундов шифрования, каждый из которых представляет собой итерационный блочный шифр Фейстеля, генерацию цикловых ключей и сложение результатов по модулю 2. Как результат (без учета перестановок и получения ключа шифрования) – около 200 операций для получения одного шифртекста и наличие достаточного объема памяти для хранения S-блоков.

Также стоит отметить, что алгоритм симметричного шифрования DES подвержен ряду известных атак (полный перебор, дифференциальный криптоанализ, линейный криптоанализ), а из-за небольшого числа возможных ключей (всего 2^{56}), появляется возможность их полного перебора на быстродействующей вычислительной технике за реальное время. Конечно, существует более стойкая реализация – Triple DES (3DES), но по очевидным причинам скорость ее работы ниже скорости работы DES более чем в три раза.

Работа алгоритма Rijndael (Advanced Encryption Standard, AES) в простейшем случае (128-битный ключ шифрования) включает в себя 10 раундов, на каждом из которых происходит четыре основных преобразования: выбор ключа итерации и побитовое сложение с элементами состояния, замена элементов матрицы состояния используя таблицу замен (S-box), сдвиг строк состояния, умножение каждого столбца полученной матрицы на матрицу особого вида. Как результат (без учета получения исходного ключа шифрования) – около 300 операций для получения одного шифртекста и необходимость наличия достаточного объема памяти для хранения таблиц замен.

Асимметричные алгоритмы не рассматриваются по причине еще более сложных математических преобразований, по сравнению с симметричными алгоритмами, требующих более высокой вычислительной мощности и временных затрат как для аппаратной, так и программной реализации.

Предлагаемое решение предполагает наличие аппаратной и программной составляющих. Аппаратная часть состоит из платы расширения системного блока сервисной зоны банкомата и модуля защиты периферийных устройств, в частности диспенсера, располагаемого в сейфе банкомата. Программная часть включает разработку и реализацию алгоритма. Важно отметить, что среди дополнительно предъявляемых требований к алгоритму, в данном случае, рассматриваются: снижение вычислительных затрат, повышение быстродействия за счет уменьшения общего количества преобразований и их упрощения.

Алгоритм предполагает наличие массива ключей, который хранится на обеих сторонах устройства. Массив ключей может быть достаточно большим; размер его определяется объемом памяти. Получение сеансовых ключей производится из исходного массива с помощью генератора истинно случайных чисел, мастер-ключа, блоков преобразований F_1, F_2 и F_3, генератора псевдослучайных чисел (рис. 1).

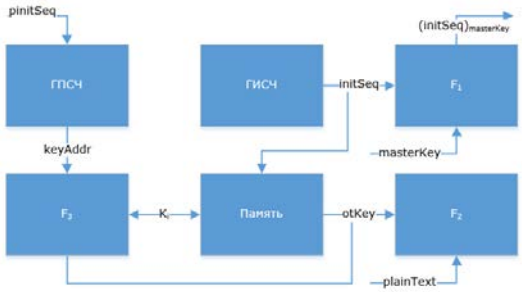

Рисунок 1 – Упрощенная схема алгоритма

На первом этапе работы алгоритма генератор истинно случайных чисел (ГИСЧ) вырабатывает последовательность initSeq, которая также отправляется ответной стороне, используя симметричный секретный ключ masterKey и преобразование F_1, и служит в качестве заполнения имеющегося объема Памяти. В обычном режиме работы из Памяти каждого модуля извлекается очередной сеансовый ключ otKey и используется для формирования шифртекста из открытого текста plaintext с помощью преобразования F_2. В качестве открытого текста может выступать, например, набор команд управления периферийными устройствами. Длина открытого текста plaintext всегда не превышает длину сеансового ключа otKey.

При истощении ключевого набора Памяти раньше, чем выполнится очередная синхронизация модулей, используется преобразование F_3, которое позволяет существенно расширить набор сеансовых ключей с небольшим понижением их криптографических характеристик и обеспечить непрерывность работы.

Цикл формирования сеансовых ключей повторяется необходимое количество раз. Обновление набора сеансовых ключей происходит аналогичным образом.

В некоторых случаях качестве преобразований F_1 и F_2 (в зависимости от требуемых свойств информации) может выступать одно из простейших преобразований: побитовое сложение, арифметическое сложение (по mod 2^n), операция циклического сдвига, – или их комбинации, что позволяет существенно повысить производительность алгоритма по сравнению с известными алгоритмами шифрования и обеспечить при этом достаточную стойкость. При использовании более сложного набора преобразований стоит учитывать, что необходимый объем вычислений приводит к потере производительности всей системы в целом.

Несмотря на отсутствие у представленного алгоритма аналога S-блокам, требуется значительный объем дополнительной памяти для хранения сеансовых ключей шифрования. Однако при использовании функции расширения это можно расценивать и как преимущество, т.к. большой объем исходной ключевой последовательности позволяет значительно увеличить количество сеансовых ключей, хранящихся в Памяти.

Необходимость процедуры синхронизации возникает только в том случае, если произошел сбой в канале связи, нарушен протокол обмена, обнаружены атаки на подсистему. Благодаря сопутствующей функции взаимной аутентификации легко обнаруживаются нарушения нормального функционирования информационного обмена.

Заключение. Представленный алгоритм имеет малое количество операций, что повышает общее быстродействие устройства, снижает энергопотребление; позволяет синхронизировать сеансовые ключи.

Применение методов расширения ключевой последовательности в большинстве случаев позволит избежать преждевременной процедуры обновления набора ключей.

Предлагаемый алгоритм может служить концептуальной и логической основой для построения эффективной подсистемы защиты информации в каналах передачи и позволит эффективно распознавать и предотвращать различные кибератаки, включая jackpotting-атаки.

1. Шеннон К. Работы по теории информации и кибернетике. Теория связи в секретных системах. – М.: ИЛ, 1963. – С. 333-369.
2. Жуков А.Е. Легковесная криптография. Часть 1 // Вопросы кибербезопасности. – 2015. – № 1 (9). – С. 26–43.
3. Жуков А.Е. Легковесная криптография. Часть 2 // Вопросы кибербезопасности. – 2015. – № 2 (10). – С. 2–10.
4. Островский Д.Е., Рафиков А.Г. Криптозащищенный микроконтроллер // 3-я Международная научно-техническая конференция. – М., 2012.
5. Островский Д.Е., Рафиков А.Г. Генератор истинно случайных чисел // 3-я Международная научно-техническая конференция. – М., 2012.
6. Rukhin A, Soto J, Nechvatal J. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST special publication 800-22, 2010.
7. Сабанов А.Г. Обзор технологий идентификации и аутентификации // Документальная электросвязь. – 2006. – № 17. – С. 23–27.
8. Сабанов А.Г. Аутентификация как часть единого пространства доверия // Электросвязь. – 2012. – С. 40–44.
9. Деднев М.А., Дыльнов Д.В. и др. Защита информации в банковском деле и электронном бизнесе. – М.: КУДИЦ-ОБРАЗ, 2012. – 512 с.
10. Кривченко И. Аппаратно-защищенные микросхемы семейства Crypto Authentication: потенциальные применения ATSHA204A // Компоненты и технологии. –2015. – № 10. – С. 87–93.
11. Jan Axelson. USB Complete: The Developer's Guide (Complete Guides series). Lakeview Research, English, 2015. ISBN/ASIN: 1931448280, ISBN13: 9781931448284.
12. NIST S. Guide to Integrating Forensic Techniques into Incident Response. 2006. – P. 80-86.

УДК620.130

ГИСТЕРЕЗИСНЫЕ МЕТОДЫ КОНТРОЛЯ ОБЪЕКТОВ В ИМПУЛЬСНЫХ МАГНИТНЫХ ПОЛЯХ

Павлюченко В.В., Дорошевич Е.С.
Белорусский Национальный Технический Университет
Минск, Республика Беларусь

Контроль свойств объектов с помощью пленочных преобразователей магнитного поля и расчеты магнитных полей описаны в [1–4]. Определение удельной электропроводности и магнитной проницаемости объектов, а также их толщины и параметров дефектов в них осуществлено в работах авторов в импульсных магнитных полях с применением разработанных гистерезисных методов контроля [5–8]. Целью работы является повышение точности измерения магнитных полей и контроля свойств объектов путем использования численных расчетов,