А. О. Меньшенин, А. В. Кораблин

ЗАЩИЩЕННЫЙ ПРОТОКОЛ ВЗАИМОДЕЙСТВИЯ «ХОСТ – СЧИТЫВАТЕЛЬ NFC»

В настоящее время услуги платежей на базе мобильных технологий получают все более широкое распространение в Европе, а в странах Азии уровень распространения подобных услуг уже достаточно высок. В России технология мобильных платежей еще только начинает развиваться.

Мобильные платежи — перспективная область, имеющая важное преимущество перед платежами через Интернет: уровень распространения Интернета на большей части территории России остается низким, тогда как охват услуг сотовой связи приближается к 100 %. Также мобильные платежи имеют преимущество и перед пластиковыми картами: в нашей стране они используются недостаточно активно. По данным российского Центробанка, 93 % всех операций по картам в России — это снятие наличных.

Одна из наиболее распространенных технологий, используемых в мобильных платежах, — Near Field Communication (NFC, коммуникация ближнего радиуса действия) [1]. Она представляет собой сочетание бесконтактной идентификации и беспроводной коммуникации мобильных устройств. Таким образом, телефон с технологией NFC можно использовать в качестве «карты для банкомата». Нужно всего лишь поднести устройство к банкомату, и он в течение нескольких секунд распознает владельца устройства и считает все необходимые данные для выдачи наличных. Помимо использования в банкомате, можно найти множество разнообразных применений технологии NFC, в том числе для оплаты товаров и услуг. Например, в Японии, приложив телефон к считывающему устройству, можно проходить в метро, оплачивать парковку или заправку автомобиля, делать мелкие покупки в небольших уличных магазинах, рассчитываться в закусочных, покупать билеты в кино и на другие массовые мероприятия. А в некоторых случаях телефоны с поддержкой технологии NFC используются вместо ключа от квартиры или автомобиля.

При совершении транзакций с помощью технологии мобильных платежей информация, отправляемая по сетям передачи данных, содержит чувствительные данные: баланс электронного кошелька, идентификатор покупателя. В связи с этим необходимо обеспечить безопасность передаваемых сообщений в части конфиденциальности, целостности и защиты от атак типа повтора.

Также необходимо обеспечить аутентичность взаимодействующих частей системы. Выполнение данных требований возможно только с использованием криптографических методов защиты информации.

Типовая инфраструктура мобильных платежей в торговой точке состоит из следующих компонентов (см. рис. 1):

- POS-терминал;
- управляющий сервер;
- бесконтактные считыватели с поддержкой технологии NFC.

Бесконтактные считыватели подключаются последовательно по интерфейсу RS-485 [2] к управляющему серверу. Управляющей сервер взаимодействует с POS-терминалами по локальной сети TCP/IP торговой точки. На управляющем сервере установлен web-сервис, благодаря которому происходит обмен данными между POS-терминалом и бесконтактным считывателем. Соответственно, основной обмен данными в системе происходит по двум каналам, изображенным на рис. 1:

- между POS-терминалом и управляющим сервером по сети с использованием стека протоколов TCP/IP (команды приложения и ответы сервера);

- между сервером и бесконтактным считывателем через интерфейс RS-485 (опрос считывателя и ответы от него).

Рис. 1. Схема обмена данными в информационной системе торговой точки

Обеспечение заданных требований безопасности в канале между POS-терминалом и управляющим сервером достигается за счет использования стандарта WS-Security, специально разработанного для обеспечения безопасности web-сервисов.

Безопасность бесконтактного канала передачи данных «электронный кошелек — считыватель» обеспечивается протоколом CRYPTO1 [3], разработанным компанией NXP Semiconductors.

Далее рассматривается предлагаемый протокол взаимодействия управляющего сервера с бесконтактными считывателями, обеспечивающий заданные требования безопасности.

Обмен данными со считывателем осуществляется согласно ГОСТ Р МЭК-870-5-1-95 по протоколу FT1.2 с переменной длиной кадра в режиме «команда— ответ». Инициатором обмена может быть только хост системы. На команду, составленную в соответствии с протоколом, считыватель обязан выдать ответ, если адрес команды нулевой или совпадает с адресом считывателя. При обнаружении считывателем хотя бы одного несоответствия в команде кадр бракуется, команда не выполняется, ответ не выдается, а перед повтором команды хост должен выдержать интервал спокойного состояния линии. Если хост не получил ответа в соответствии с протоколом, команда передается повторно по окончании интервала спокойного состояния линии с прежним номером кадра. Если считыватель получил команду, совпадающую с предыдущей по номеру кадра и коду команды, и выполнил предыдущую, то повторную он не выполняет, а только повторяет ответ на нее.

Пользовательские байты кадра обмена называются фреймом. Форматы фрейма команды и фрейма ответа отличаются друг от друга. Для обеспечения заданных требований безопасности информации при обмене данными некоторые команды доступны только в закрытом режиме передачи команд и/или ответов. При таком обмене используется алгоритм шифрования данных AES-128 в режиме CBC с переменным начальным вектором.

Начальный вектор алгоритма шифрования первоначально вычисляется в процессе выполнения аутентификации хоста и считывателя, а затем обновляется по следующему правилу: после каждой операции зашифрования или расшифрования начальным вектором становится последний шифрованный блок. В считывателе хранятся ключи шифрования двух типов. Все они недоступны для чтения. Первый тип ключей используется для защиты обмена данными при работе с бесконтактными картами. Эти ключи можно обновлять. Перед началом работы с картами необходимо выполнить аутентификацию с использованием одного из этих ключей. Количество ключей первого типа ограничивается размером флэш-памяти считывателя. Второй тип содержит один ключ и используется для защиты обмена данными при обновлении ключей первого типа. Перед началом обновления этих ключей необходимо выполнить аутентификацию с использованием ключа второго типа и стереть память ключей.

Целостность информации при передаче шифрованных данных проверяется с помощью контрольной суммы CRC32. В случае несовпадения значений вычисленной и принятой

контрольной суммы команда не выполняется, происходит сброс состояния аутентификации хоста и считывателя и выдается сообщение об ошибке (см. рис. 2).

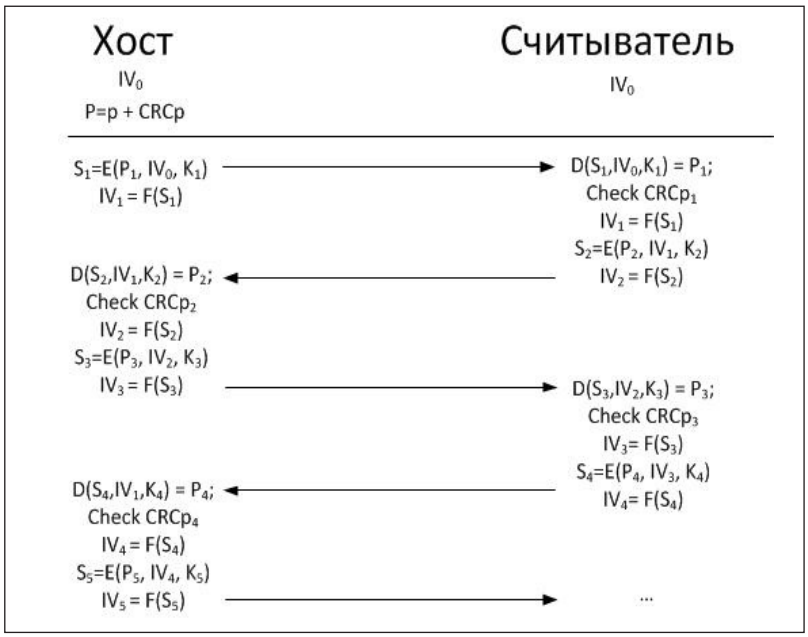

Рис. 2. Схема обмена данными «Хост — Считыватель»

Фрейм команды содержит следующие данные:

— адрес считывателя;
— режим команды;
— длина команды;
— номер кадра;
— код команды;
— режим ответа;
— параметры команды;
— контрольная сумма CRC32.

Обмен данными при выполнении команд происходит либо в открытом режиме, либо в закрытом. Нулевое значение в поле «режим команды» соответствует открытому режиму, для закрытого режима его значение соответствует номеру ключа шифрования. В закрытом режиме после параметров команды следуют 4 байта контрольной суммы CRC32. При обмене данными без ошибок номера кадров у любой пары следующих друг за другом команд должны различаться (например, увеличиваться на единицу). Ответ на команду может передаваться как в открытом, так и в закрытом режиме. Режим ответа определяется в поле «режим ответа». Нулевое значение этого байта соответствует открытому режиму ответа. Для закрытого режима ответа значение данного поля соответствует номеру ключа шифрования.

Некоторые команды доступны только после выполнения двухпроходной процедуры аутентификации между хостом и считывателем. В процессе аутентификации используется шифрование в соответствии с алгоритмом AES-128 CBC с нулевым начальным вектором.

Порядок выполнения процедуры аутентификации выглядит следующим образом (см. рис. 3):

1. Хост посылает команду первой фазы аутентификации, содержащую номер ключа шифрования.

2. Считыватель в ответ посылает криптограмму — последовательность из 16 случайных чисел RndB, зашифрованную заданным ключом.

4. Хост расшифровывает принятую криптограмму и получает RndB.

5. RndB сдвигается на 1 байт влево с кольцевым переносом, в результате чего получается RndB'.

6. Хост формирует последовательность из 16 случайных чисел RndA, добавляет к ней справа RndB' и зашифровывает, в результате чего получается криптограмма размером 32 байта.

7. Хост посылает команду второй фазы аутентификации, содержащую обязательно тот же номер ключа шифрования, что и в первой фазе.

8. Считыватель расшифровывает принятую криптограмму и сравнивает полученную последовательность RndB' со своей случайной последовательностью RndB с учетом сдвига на 1 байт. Если совпадения не произошло, процедура аутентификации прекращается.

9. RndA сдвигается на 1 байт влево с кольцевым переносом, в результате чего получается RndA'. Считыватель зашифровывает RndA' и полученную криптограмму посылает в ответ хосту.

10. Хост расшифровывает принятую криптограмму и сравнивает полученную последовательность RndA' со своей случайной последовательностью RndA с учетом сдвига на 1 байт.

11. Если произошло совпадение, процедура аутентификации считается выполненной успешно и производится формирование начального вектора для шифрования данных при выполнении последующих команд.

Начальный вектор IV[16] состоит из четырех фрагментов по 4 байта.

IV[0-3] – это первые 4 байта RndA[0-3];

IV[4-7] – это исключающее ИЛИ: RndA[4-7] ^ RndB[4-7];

IV[8-11] – это инверсия исключающего ИЛИ: ~(RndA[8-11] ^ RndB[8-11]);

IV[12-15] – это последние 4 байта RndB[12-15].

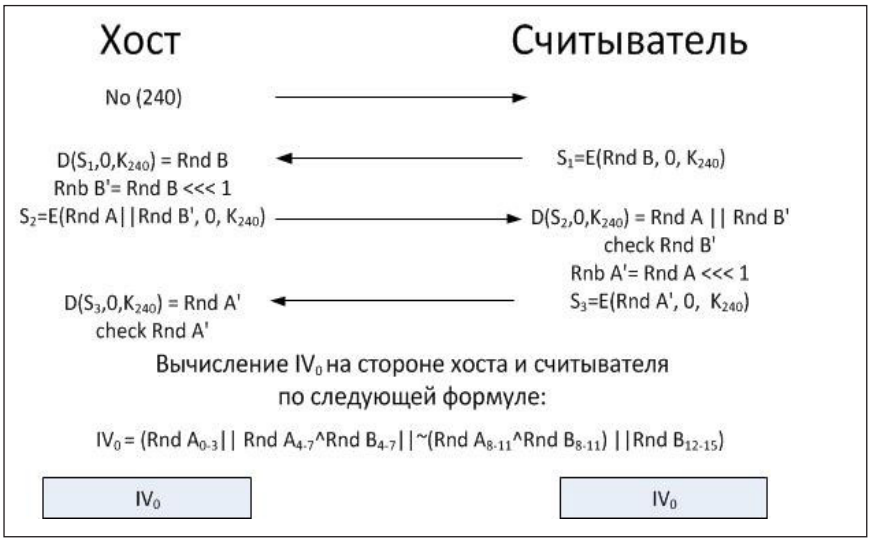

Рис. 3. Схема аутентификации «Хост – Считыватель»

Конфиденциальность передаваемых данных обеспечивается использованием симметричного алгоритма шифрования AES-128. Целостность передаваемых данных обеспечивается добавлением контрольной суммы CRC32 к каждому фрейму, передаваемому в закрытом режиме. Защита от атак типа повтора обеспечивается использованием переменного начального вектора, который зависит от передаваемых данных и изменяется после каждой операции зашифрования или расшифрования. Аутентичность хоста (управляющего сервера) и бесконтактного считывателя обеспечивается с помощью двухпроходной процедуры двухсторонней аутентификации.

Таким образом, разработанный протокол позволяет обеспечить требуемый уровень безопасности в канале передачи данных между сервером и бесконтактным считывателем через интерфейс RS-485 при совершении мобильных платежей.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO/IEC 18092:2004 Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1).
2. *Яшкардин В.* RS-485 рекомендованный стандарт электрических характеристик генераторов и приемников для использования в балансных многоточечных системах. URL: http://www.softelectro.ru/rs485.html.
3. *Courtois N. T., Karsten N., O'Neil S.* Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. Cryptology ePrint Archive. URL: http://eprint.iacr.org/2008/166.