СИСТЕМА КОНТРОЛЯ ДОСТУПА С ПРОПУСКАМИ НА ОСНОВЕ ТОКЕНИЗИРОВАННЫХ EMV КАРТ

Ермолович И.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шамына А.Ю. – магистр техн. наук, ассистент каф. ПОИТ

В работе описывается программное и аппаратное средство, которое способно эмулировать платежный терминал и считывать номера токенизированных EMV[1] карт (прим. Apple Pay, Samsung Pay, Google Pay). Программное средство позволяет вести базу пользователей с номерами их карт и контролировать возможность посещения клиентом организации. Программное средство создано для того, чтобы уменьшить расходы компаний на содержание программных средств и закупку персональных карт, уменьшить количество карт у клиентов, а также снизить количество пластикового мусора в мире.

Все существующие системы контроля доступа при детальном изучении довольно сильно переусложнены и неудобны. Они требуют выпуска отдельных карт, установки программ, обучения персонала, запоминания последовательности действий с мастер-картами. Такое программное средство подходит для крупных организаций, но такие решения избыточны для небольших компаний в сфере обслуживания, которые имеют один проходной пункт и не требуют разделения зон доступа.

Создаваемое программное средство должно быть просто в подключении, поддерживать разные операционные системы и не требовать специального обучения для персонала. В качестве платформы для программного средства было решено использовать веб-браузер.

Для связи программного и аппаратного средства был выбран стандарт WebUSB[2], который позволяет связывать веб-сайт с USB устройствами. В качестве аппаратного средства была выбрана Arduino Pro Micro, для чтения NFC карт был выбран микроконтроллер PN532, поскольку он способен отправлять на NFC карту APDU команды[3] для активации программ на EMV картах.

Все платежные инструменты работают по протоколу EMV. Бесконтактные EMV-карты позволяют без авторизации считать данные, такие как: имя владельца, номер карты, срок действия, лог транзакций по карте. PAN номер (номер карты) не изменяется на протяжении всего срока действия карты, поэтому он будет использован в качестве идентификатора пользователя.

Безопасность работы с номерами карт осуществляется самой платежной системой. Платежная система генерирует токен при добавлении виртуальной карты на устройство. Токен это такой же PAN номер, но он не соответствует реальному номеру карты, а является его эквивалентом. Запросы POS-терминалов по этому виртуальному номеру будут рассмотрены платежной системой, как норм физической карты. При таком подходе, даже потенциально скомпрометированный терминал не видит реального номера карты — токен можно использовать только для платежей на POS-терминалах.

Начало общения с EMV-картой всегда происходит с чтения файла PPSE[4] (Payment System Environment) командой чтения. В ответ на команду чтения карта должна вернуть FCI (File Control Information) со списком приложений, существующих на карте. В ответе FCI нам необходимо найти идентификатор платежного приложения (AID), который содержит информацию о платежной системе.

В ответ на запуск платежного приложения карта может затребовать от считывателя PDOL (Processing Options Data Object List). Это набор параметров POS-терминала — поддерживаемые протоколы и стандарты, валюта, дата, случайное число для криптографии, и т.д. Сложность состоит в том, некоторые карты могут отказаться работать без корректного ответа PDOL. Карта ожидает ответ на PDOL в том же порядке, в котором следуют запросы, и той длины, которая указана после каждого параметра PDOL. Так как наше средство не собирается списывать деньги, то его задача — сформировать самый простой ответ PDOL, который удовлетворит карту. Экспериментальным путем было получено, что почти на все запросы PDOL можно ответить нулями, кроме Terminal Transaction Qualifiers (TTQ).

После этого программное средство сравнивает номер карты с базой и в случае наличия записей производит проверку возможности доступа пользователя в организацию при этом сигнализируя оператору о статусе проверке и, в случае возникновения ошибки, описания возникших проблем.

Разработанное программное и аппаратное средство позволяет в течении 5 минут настроить систему доступа и не требует дополнительных затрат на установку и подключение, поскольку подключается в USB порт компьютера. Также разработанное средство способно сэкономить средства организации на обслуживании оборудования и закупке персональных карт для клиентов. При этом у самих клиентов уменьшается количество персональных карт.

Список использованных источников:

1. EMV Payment Tokenisation [Электронный ресурс]. – Режим доступа: https://www.emvco.com/emv-technologies/payment-tokenisation/. – Дата доступа: 05.04.2021.

2. WebUSB API [Электронный ресурс]. – Режим доступа: https://wicg.github.io/webusb/. – Дата доступа: 05.04.2021.

3. ISO/IEC 7816-4:2005 [Электронный ресурс]. – Режим доступа: https://www.iso.org/36134.html – Дата доступа: 5.4.2021.

4. Contactless Specifications for Payment Systems [Электронный ресурс]. – Режим доступа: https://www.emvco.com/wp-content/uploads/2017/05/BookB_Entry_Point_Specification_v2_6_20160809023257319.pdf – Дата доступа: 05.04.2021.