УЯЗВИМОСТИ СИСТЕМ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

Лагутина Евгения Алексеевна
НИЯУ МИФИ, студент
la.evgeniya@gmail.com

В настоящее время существенно возрастает роль и интенсивность использования мобильных платежей, что обусловлено рядом объективных причин.

Электронные платежи являются выгодной альтернативой традиционным способам оплаты товаров и услуг. Причем можно предположить, что мобильные платежи (схема оплаты, в которой хотя бы один этап транзакции осуществляется с помощью мобильного устройства) в ближайшем будущем будут наиболее востребованными среди существующих способов оплаты. Это обусловлено доступностью мобильных устройств и широкими возможностями реализации приложений, предоставляющих клиенту доступ к его счету.

Следовательно, ввиду популяризации мобильных платежей их безопасность приобретает ключевое значение, и первым шагом проектирования мобильной платежной системы должен быть анализ угроз безопасности, возникновение которых возможно на всех уровнях реализации.

В данной статье проводится анализ существующих уязвимостей, которые необходимо закрыть в процессе создания системы мобильных платежей.

Любая система мобильных платежей представляет собой совокупность объектов, которые могут взаимодействовать по двум основным схемам: удаленного платежа (Remote M-Payment System) и бесконтактного платежа (Proximity Payment Systems). В зависимости от выбора схемы определяется набор технологий, использование которых возможно для передачи данных.

Очевидно, что для обеспечения стойкости системы мобильных платежей, необходимо рассмотреть защищенность использованных при ее построении стандартов, технологий, протоколов и платформ.

Таким образом, все уязвимости можно разделить согласно уровню их реализации: нижний уровень – протокол GSM, операционная система, технология передачи (RFID) и уровень программного обеспечения. Рассмотрим уязвимости нижнего уровня.

Уязвимости протокола GSM

Безопасность системы GSM основана на разделении секрета мобильной станцией и её базовой приёмопередающей станцией, для чего используются следующие три алгоритма:

- алгоритм аутентификации A3;
- алгоритм генерации ключа A8;
- алгоритм шифрования A5.

1) Алгоритмы A3 и A8

Для исключения несанкционированного использования ресурсов системы связи вводятся механизмы аутентификации. У каждого подвижного абонента есть стандартный модуль подлинности абонента (SIM-карта), которая содержит алгоритм аутентификации (A3), и генерации сеансового ключа (A8). В настоящее время известны следующие стандартной реализацией алгоритма A3/A8 является COMP128. Хотя существуют альтернативы COMP128, но этот протокол по-прежнему поддерживается в подавляющем большинстве сетей GSM.

Можно выделить следующие проблемы безопасности:

- Активные атаки — злоумышленник исполняет роль сетевого элемента.
- Небезопасная передача ключевой информации: аутентификационные данные передаются в явном виде внутри и между сетями.
- Односторонняя аутентификация: обеспечивается только аутентификация пользователя для сети, нет средств аутентификации сети для пользователя.
- Слабые алгоритмы шифрования. Длина ключа слишком мала, в то время как скорости вычислений растут

2) Алгоритм шифрования A5 реализуется в самой мобильной станции, а не в SIM-карте, и зависит от производителей оборудования базовых и мобильных станций.

В настоящее время используется модификация A5/3, базой для которой служит алгоритм KASUMI, утвержденный для использования в качестве ядра для алгоритмов конфиденциальности и целостности информации. В настоящее время данный поточный шифр обеспечивает требуемую криптостойкость.

Уязвимости технологии передачи (RFID)

В качестве одного из возможных сценариев реализации уязвимости технологии RFID можно рассмотреть следующий: при потере телефона любой человек, нашедший данное устройство, имеет возможность (при наличии необходи-

мого оборудования) скопировать смарт-карту, содержащую идентификационные данные пользователя. Таким образом, очевидно, могут быть осуществлены операции, инициированные не законным владельцем телефона, а злоумышленником.

Уязвимости ОС (на примере Google Android)

Одной из последних уязвимостей, обнаруженных в Android-смартфонах, является следующая: уязвимость позволяет любому приложению, имеющему разрешение на доступ в интернет, собирать и передавать личные данные пользователя, в том числе данные СМС: номера телефонов и зашифрованный текст сообщений.

Помимо программы, собирающей для HTC пользовательские данные, в новых прошивках также присутствует приложение, не только имеющее доступ ко всей вышеперечисленной информации, но и способное предоставить её любому неавторизованному пользователю по запросу на локальный порт, при этом не требуется никаких специальных разрешений, кроме доступа в интернет (это разрешение, помимо всего прочего, позволит передать полученные данные куда и кому угодно).

Таким образом, получили список уязвимостей нижнего уровня, которые могут нанести ущерб безопасности создаваемой нами системы. Соответственно, данный список дает возможность при реализации системы мобильных платежей предотвратить несанкционированный доступ к конфиденциальной информации посредством перечисленных уязвимостей.

Список источников

1. Security Issues in Mobile Payment Systems. Shivani Agarwal , Mitesh Khapra , Bernard Menezes , Nirav Uchat.

2. Анастасия Мясникова. Реализация алгоритма A5/3 (GSM). URL: ftp://cs.usu.edu.ru/crypto/A5_3/ReadMe.htm