www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.3.4

УДК 004.9:621.395.721.5
ББК 32.971.321.422

БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ МОБИЛЬНЫХ ПЛАТЕЖЕЙ

Оксана Сергеевна Слепова

Преподаватель высшей категории кафедры экономики и управления,
Волгоградский институт бизнеса
vib@volbi.ru
ул. Качинцев, 63, 400010 г. Волгоград, Российская Федерация

Аннотация. Последние модели смартфонов облегчают жизнь своим покупателям. Мобильный банк в смартфонах уже не новость, а вот к возможности оплатить покупку прикосновением гаджета к терминалу по технологии бесконтактного платежа пользователи только привыкают.

Переход в цифровой мир чреват иллюзией безопасности: умный гаджет сам за себя постоит. Но это так лишь отчасти – безопасность зависит в первую очередь от поведения самого пользователя. Поэтому, какие бы финансовые приложения не устанавливались на смартфон, прежде необходимо освоить технику безопасности мобильных платежей.

Ключевые слова: смартфон, безопасность, конфиденциальность, Secure Element, микропроцессорный чип, Near Field Communication, электронный кошелек, Apple Pay, Google Pay, Samsung Pay, мобильный платеж, Hands Free, биометрическая аутентификация.

Современные смартфоны давно и успешно совмещают в себе не только средство связи, фотоаппарат и плеер, но также проездной и даже кошелек. Это несомненно заставляет задуматься о безопасности хранения данных на них. Сначала необходимо разобраться насколько тщательно смартфоны защищают конфиденциальную информацию.

Главным по защите данных смартфона выступает миниатюрный чип под названием Secure Element (далее – SE). Это микропроцессорный чип, который может хранить конфиденциальные данные и запускать защищенные приложения, такие как платежи. Он действует как хранилище, защищая то, что внутри SE (приложения и данные), от атак вредоносных программ, которые типичны для хоста (то есть операционной системы устройства). Защищенные элементы обрабатывают все виды приложений, которые жизненно важны для современной цифровой жизни:

1. Аутентификация. Вместо имени пользователя и пароля доступ к онлайн-сервису может быть защищен механизмом строгой аутентификации, основанным на учетных данных, хранящихся и обрабатываемых в защищенном элементе. Таким образом, чтобы войти в виртуальную частную сеть (VPN) или пользовательскую электронную почту, в фоновом режиме может быть задействован безопасный элемент, чтобы убедиться в правильности аутентификации.

2. Цифровая подпись. Приложения могут использовать SE для цифровой подписи документа или любых данных с помощью ключа, хранящегося в этом защищенном элементе. - Этот ключ помогает SE разблокировать зашифрованные данные, чтобы их можно было про-

читать. Опять же это используется, чтобы доказать, что пользователь именно тот, за кого себя выдает. Таким образом, программа электронной почты может использовать подключение к защищенному элементу для цифровой подписи отправляемых пользователем электронных писем, или правительственное веб-приложение может получить к нему доступ, когда используются их цифровые услуги.

3. Управление жизненным циклом. Крайне важно, чтобы встроенные в SE устройства были безопасны на протяжении всего жизненного цикла.

4. Мобильные платежи. Здесь SE надежно хранит данные карты / владельца карты и управляет чтением зашифрованных данных. Во время платежной транзакции она действует как бесконтактная платежная карта, использующая стандартную технологию, которая помогает авторизовать транзакцию. Защитный элемент может быть встроен в телефон или в SIM-карту.

SE в смартфоне – это примерно тот же самый чип, что и в пластиковых картах. На нем работает отдельная операционная система. Вся необходимая информация записывается в память этого чипа, откуда ее нельзя ни прочитать, ни скопировать, – доступа к ней нет даже у родной операционной системы смартфона.

С недавних пор смартфонами можно пользоваться вместо пластиковых карточек. Это стало возможным с возникновением функции Near Field Communication (далее – NFC), которая была изобретена 11 лет назад.

NFC это технология беспроводной высокочастотной связи малого радиуса действия (до 3–5 см), позволяющая осуществлять бесконтактный обмен данными между мобильными телефонами, смарт-картами, платежными терминалами, системами контроля доступа и прочими устройствами.

По принципу действия NFC походит на технологии Bluetooth и RFID, однако в сравнении с ними обладает целым рядом важных преимуществ: более высокими скоростью и уровнем безопасности, чем Bluetooth, и более широкими функциональными возможностями, чем RFID.

Точно так же работает эта технология в пластиковых карточках MasterCard PayPass и Visa payWave со специальным чипом, который позволяет совершать покупки, просто прикладывая карту к платежному терминалу, не вставляя ее вовнутрь и не проводя магнитной полосой. Аббревиатура NFC вызывает ассоциации с игрой Need for Speed (NFS), и можно сказать, что это довольно правильные ассоциации, – все происходит быстрее.

На данном этапе развития технологий смартфон можно использовать как универсальную бесконтактную карту, оплачивая покупки, услуги или проезд в общественном транспорте, в качестве билета на массовое мероприятие. При посещении фастфуда или кинотеатра всегда есть возможность открыть меню заведения прямо на смартфоне и с него же сделать и оплатить заказ. Все эти, а также многие другие возможности доступны пользователям уже сегодня благодаря технологии NFC. Но, как и у любой другой технологии, которая набирает обороты популярности, у NFC есть достоинства и недостатки.

Плюсы: мобильные кошельки сейчас находятся в центре внимания, и основная борьба развернется среди поставщиков оборудования, необходимого для реализации NFC. Например, ожидается появление оборудования, позволяющего заменить только SIM-карту для использования NFC, вместо модернизации всего мобильного телефона. Сначала NFC-кампании будут проводиться с использованием QR-кодов.

Минусы: общее проникновение NFC будет оставаться ниже нормы. Также ожидается рост плохо продуманных маркетинговых компаний.

Технология NFC не возникла на пустом месте. Она органично использует принципы RFID и коммуникационных технологий, максимально увеличивая положительный эффект от их использования.

Итак, идея объединить телефон с кредитной картой старше, чем может показаться. Первые модели мобильных телефонов с встроенным SE были еще кнопочными – особой популярности они не приобрели. Пытались с помощью гаджетов имитировать и магнитную ленту, однако реальным конкурентом привычной пластиковой карты смартфоны стали сравнительно недавно, а именно – в 2014 г., когда компания Apple анонсировала платежную систему Apple Pay.

Успех производителя iPhone привлек внимание его конкурентов, и в 2015 г. аналогичный сервис появился у Samsung. Кстати, обе эти системы подразумевают использование встроенного чипа SE (именно поэтому старые iPhone и недорогие модели Samsung не поддерживают бесконтактные платежи).

А еще через несколько месяцев Google представила систему Android Pay, которая в начале 2018 г. была переименована в Google Pay.

Apple Pay, Google Pay и Samsung Pay уже сравнительно давно работают в России, но до сих пор есть люди, которые боятся оплачивать покупки телефоном. Самый большой страх пользователей новомодных технологий в том, что данные банковских карточек могут попасть к третьим лицам и привести к потерям на счетах.

Мобильный платеж – это вид финансовой сделки, которая проводится при помощи персонального компьютера, планшета, телефона или другого мобильного устройства посредством сети Интернет. Осуществлять такие платежи удобнее всего при покупке товаров и услуг в интернет-магазинах.

Существует три типа мобильных платежей. Первый – это когда покупатель заходит на веб-сайт, добавляет товар в корзину, оформляет заказ и получает свою покупку вместе с чеком. Еще есть бесконтактные платежи – когда информация о транзакции хранится на устройстве и для ее завершения требуется ввести PIN-код. И, наконец, мобильные кошельки, которые способны заменить традиционный кошелек и хранят всю информацию по совершенным платежам.

Со вступлением в игру все большего количества крупных брендов, рынок мобильных платежей претерпевает значительные изменения. Продавцы используют новейшие технологии и адаптируют свои приложения для обеспечения максимально комфортного осуществления мобильных платежей. Например, недавно Google представила новое приложение Hands Free. Оно использует для работы как Bluetooth, так и Wi-Fi, а особенность заключается в том, что телефон можно не доставать из кармана. В Google также проводится работа с системой идентификации личности по чертам лица.

Эксперименты, проводимые в Google, не являются чем-то исключительным; обеспечение максимального удобства и безопасности платежей – это главная тенденция в индустрии мобильных платежей. Что касается опции «оплатить», Apple, Google и Samsung – не более чем верхушка айсберга. Все больше и больше информационно-технологических компаний разрабатывают свои собственные платформы для мобильных платежей.

Сотни тысяч людей уже освоили и оценили Apple Pay, Google Pay и другие аналогичные системы, пришедшие в Россию осенью 2016 года. Однако есть и те, кто уверен, что данные карточки могут попасть или к производителю смартфона, или к оператору, или вообще к хакерам, которые моментально опустошат счет.

Исследования ISACA показывают, что отношение к безопасности мобильных платежей в среде ИТ- и ИБ-специалистов скептическое – только 23 % из опрошенных считают их безопасными. Однако исследования компании Ovum говорят, что в 2019 г. количество мобильных плательщиков превышает 1 млрд (против 44,5 млн в 2014 г.), поэтому необходимо серьезно задуматься о безопасности данных пользователей мобильных платежей.

По мнению специалистов международной ассоциации ИБ-аудиторов ISACA, представление о безопасных платежах смещается в сторону бесконтактных транзакций, осуществляемых с помощью мобильных устройств. Происходящие там улучшения информационной безопасности делают эти технологии как более безопасными, так и открывающими дополнительные возможности для пользователей и бизнеса.

Наборы приложений для безопасных мобильных платежей во время транзакций вместо номера банковской карты позволяют передавать платежному терминалу (или в сеть) случайным образом сгенерированный набор данных – токен. Токен может быть сконфигурирован с таким расчетом, чтобы отвечать специальным критериям: точному моменту времени, конкретному ритейлеру, определенному размеру платежа. И только выпустивший токен банк и авторизованные клиенты и партнеры банка могут отождествить его с конкретной платежной картой. Так образуется еще один рубеж защиты чувствительных пользовательских данных.

Шифрование данных производится с таким расчетом, чтобы привязать платежи к устройству, принадлежащему владельцу карты. Шифрограмма устройства отправляется на платежный терминал вместе с токеном. Это образует защиту транзакционных данных в случае их перехвата и попытки использовать на других устройствах.

Двухфакторная аутентификация организуется по традиционной схеме: что-то, что пользователь знает (пароль), что-то, чем он располагает физически (устройство, платежная карта), и биометрические данные (отпечатки пальцев, голос, распознавание лица).

Если владелец устройства не хранит на нем данные платежной карты, то для предлагаемой схемы защиты утеря устройства не страшна, тем более, что память устройства может быть очищена дистанционно. Однако следует учитывать, что предлагаемая схема требует строгой аутентификации при доступе к набору платежных приложений. Эксперты ISACA рекомендуют использовать для этого сильные пароли и биометрию. Интеграция технологий мобильных платежей с мерчант-бизнесом позволяет повысить безопасность платежей (например, через геолокацию устройства плательщика) и развивать программу лояльности клиентов.

Рассмотрим основные опасные моменты, связанные с использованием мобильных платежей и в частности бесконтактных платежей.

Основная опасность кроется в утере или краже телефона. Если злоумышленнику удастся получить доступ к системе, вред, который может быть нанесен пользователю, будет сравним с кражей бумажника с картами и с запиской с пин-кодами внутри него: деньги могут быть украдены с помощью перевода на чужой счет, например, или потрачены в ближайшем магазине. Но получить доступ к мобильной банковской карте, привязанной к смартфону, не так-то просто. Это возможно в двух случаях:

1. Имитировать отпечаток пальца (практически невозможный вариант).

2. Узнать пароль (при должной бдительности владельца карты и смартфона это не так легко).

Чтобы избежать реализации мошенниками второго варианта, единственная рекомендация для владельцев: стараться не вводить пароль у всех на виду (как и при стандартной оплате банковской картой) и, естественно, не записывать его в доступных местах (на бумажке в бумажнике и т. п.).

Получается, что физический взлом систем Samsung Pay, Apple Pay и Google Pay почти невозможен, особенно, если в качестве защиты был выбран ввод отпечатка пальца. Но не стоит забывать и о других опасностях.

Технологии Apple Pay, Samsung Pay и Google Pay фактически делают телефон картой оплаты, поэтому пользователи могут столкнуться с традиционными видами мошенничества в этой сфере. Например, карту могут украсть физически или с помощью программ-зловредов, собирающих данные, а использовать ее злоумышленники будут, привязав к своему телефону.

Бесконтактные платежи в онлайн-торговле и в обычных магазинах значительно облегчили работу кардеров. Привязав данные украденной карты к телефону премиум-класса, они могут приобретать товары в магазинах, вызывая намного меньше подозрений.

Кроме того, плохую службу может сослужить и история операций, если станет доступной карточным ворам.

Еще одной потенциальной угрозой может стать хакерская атака. В этой ситуации злоумышленникам не нужны ни карта, ни телефон. По словам экспертов в области предотвращения киберпреступлений, технологии бесконтактных платежей с помощью смартфонов пристально изучаются экспертами по информационной безопасности с момента их публичного анонса. Еще летом 2016 г. на конференции BlackHat в США были выделены возможные угрозы систем Samsung Pay, Apple Pay и Google Pay:

1. Социальная инженерия.

2. Создание помех для MST сигнала. При использовании телефона для оплаты в терминалах, работающих с магнитной полосой.

3. Изменение функции кодирования / декодирования.

4. Подбор следующего номера токена.

Пока это скорее потенциальные, чем реально существующие риски. Однако злоумышленники тоже не дремлют и активно исследуют новые технологии.

Основным способом защиты данных в мобильных платежах является развитие биометрических методов аутентификации платежа. Наиболее серьезно на безопасность платежных операций, которые проводятся с использованием смартфона (а это не только Apple Pay / Google Pay, а также мобильные банки, приложения платежных сервисов и т. д.), влияют конкретные программные наработки самого смартфона, а не возможности приложений. Производители смартфонов заинтересованы в том, чтобы лучше конкурентов превращать смартфон в основной платежный инструмент своих пользователей. В средней и длинной перспективе это не просто дополнительное преимущество, build-in функция для каждого бренда, рассчитывающего на успех своего продукта. Исследование, проводимое Juniper Research, прогнозирует, что количество пользователей этих software-based методов будет расти с примерно 429 млн чел. в 2018 г. до более чем 1,5 млрд чел. в 2023 году. Иными словами – начинается эпоха, когда аутентификация мобильных платежей будет обеспечиваться за счет множества биометрических данных, которые учитывают подробную шаблонизацию, заданную на устройстве конкретного пользователя.

Дальнейшее использование биометрической аутентификации, от очевидных Touch ID до активно внедряемого Face ID или голосовых датчиков, будет лишь способствовать росту мобильных платежей. Сначала они будут охватывать флагманские линейки смартфонов, затем внедряться во всех более низких ценовых диапазонах.

Рост мобильных платежей с биометрическим подтверждением составит, по прогнозам аналитиков, где-то 76 % в год по всему миру. Основной рост этого произойдет из Азии, использование их в Северной Америке составит всего 46 % в год.

Биометрическая аутентификация отпечатком пальца становится все более распространенной: к 2023 г. она будет доступной в 4,5 млрд смартфонов. Это станет необходимым минимумом для бюджетных моделей. Но на каком-то этапе ее применение будет спадать – с выходом iPhone X Apple открыла дорогу использованию лицевой аутентификации. К 2023 г. названные 4,5 млрд девайсов будут составлять лишь 9/10 всех смартфонов.

В результате проведенного исследования необходимо сделать вывод о том, что платежным приложениям не стоит задумываться над собственными решениями, а лишь необходимо правильно настраивать работу предустановленных в смартфонах решений. Пользователям также рекомендуется:

1) регулярно проверять устройства на наличие вредоносного программного обеспечения;

2) не вводить данные карты на чужих компьютерах и смартфонах;

3) пользоваться магазинами, которые используют защищенное HTTPS-соединение;

4) для оплаты интернет-покупок лучше пользоваться не своей основной картой, а завести виртуальную карточку.

СПИСОК ЛИТЕРАТУРЫ

1. Безопасность мобильных платежей: тренды защиты транзакций на ближайшие 5 лет. – Электрон. текстовые дан. – Режим доступа: https://blogs.korrespondent.net/blog/business/4008692. – Загл. с экрана.

2. Вместе с экспертами разбираемся в безопасности Samsung Pay, Apple Pay и Android Pay. – Электрон. текстовые дан. – Режим доступа: https://bankinform.ru/news/singlenews.aspx?newsid=87426. – Загл. с экрана.

3. Про безопасность мобильных платежей. – Электрон. текстовые дан. – Режим доступа: https://www.itweek.ru/security/blog/security/8774.php. – Загл. с экрана.

4. Технология Near Field Communication (NFC). – Электрон. текстовые дан. – Режим доступа: https://www.top-technologies.ru/ru/article/view?id=34148. – Загл. с экрана.

REFERENCES

1. *Bezopasnost mobilnykh platezhey: trendy zashchity tranzaktsiy na blizhayshie 5 let* [Mobile Payment Security: Transaction Security Trends for the Next 5 Years]. URL: https://blogs.korrespondent.net/blog/business/4008692.

2. *Vmeste s ekspertami razbiraemsya v bezopasnosti Samsung Pay, Apple Pay i Android Pay* [Together with Experts We Understand the Security of Samsung Pay, Apple Pay and Android Pay]. URL: https://bankinform.ru/news/singlenews.aspx?newsid=87426.

3. *Pro bezopasnost mobilnykh platezhey* [About Mobile Payment Security]. URL: https://www.itweek.ru/security/blog/security/8774.php.

4. *Tekhnologiya Near Field Communication (NFC)* [Near Field Communication (NFC) Technology]. URL: http://www.top-technologies.ru/ru/article/view?id=34148.

SECURITY AND PRIVACY OF MOBILE PAYMENTS

Oksana S. Slepova

Highest Category Lecturer, Department of Economics and Management,
Volgograd Institute of Business
vib@volbi.ru
Kachintsev St., 63, 400010 Volgograd, Russian Federation

Abstract. The latest smartphones make life easier for their customers. Mobile banking in smartphones is no longer news, but users are just getting used to the opportunity to pay for a purchase by touching the gadget to the terminal using the contactless payment technology.

Going into the digital world is fraught with the illusion of security: a smart gadget stands up for itself. But this is true only partly – security depends primarily on the behavior of the user. Therefore, no matter what financial applications are installed on your smartphone, you first need to master the safety technique of mobile payments.

As a result of the study, it is necessary to conclude that payment applications should not think about their own solutions, but only need to properly configure the work of pre-installed solutions in smartphones, as well as: 1) regularly check your devices for malicious software; 2) do not enter card data on other people's computers and smartphones; 3) use stores that use a secure HTTPS connection; 4) to pay for online purchases, it is better not to use your main card, but to have a virtual card.

Key words: smartphone, security, privacy, Secure Element, microprocessor chip, Near Field Communication, electronic wallet, Apple Pay, Google Pay, Samsung Pay, mobile payment, Hands Free, biometric authentication.