М. В. Кузин

СОВРЕМЕННЫЕ МЕТОДЫ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВУ С БАНКОВСКИМИ КАРТАМИ

По данным международной платежной системы Visa, переход к электронным платежам добавил объему мировой экономики 1,1 трлн долларов США с 2003 по 2008 г., что составило 0,5 % мирового ВВП и позволило создать 4,9 млн рабочих мест по всему миру [1]. Доля Visa на мировом рынке платежных систем составляет 28,6 %, MasterCard — 20 %, а крупнейшей в настоящий момент является China UnionPay — 29,2 %. По прогнозам, общее число платежных карт вырастет с 8 млрд в 2010 г. до 10,1 млрд к 2015 г. В настоящее время 62 % платежных карт являются дебетовыми, 28 % — кредитными [2]. В России общее число эмитированных карт выросло за 2011 г. на 38 % и составило около 200 млн штук, при этом порядка 50 % карт являются активными, т. е. срок их действия не истек и по ним совершаются транзакции. Количество операций по банковским картам в 2011 г. выросло на 32 % до 4 млрд, объем операций составил 17 трлн рублей, что на 36 % больше, чем в 2010 г. [3]. Следует также отметить, что российский рынок банкоматов является крупнейшим в Европе: так, в 2011 г. общее число установленных устройств составило более 130 тыс. (для сравнения: в Великобритании — 65 тыс., в Германии и Испании — по 58 тыс.) [4]. К 2016 г. общее число установленных в мире банкоматов вырастет на 42 % и достигнет 3,2 млн устройств [5].

Постоянный рост числа карт, устройств их обслуживания и объемов совершаемых операций привлекает злоумышленников к сфере платежных карт. Так, по результатам расследований крупнейших инцидентов информационной безопасности, связанных с компрометацией данных [6], в 2011 г. 48 % инцидентов и 3 % всех скомпрометированных данных были связаны с данными платежных карт, причем в предыдущие несколько лет данные платежных карт составляли более 90 % от всех скомпрометированных. Относительное снижение числа компрометаций данных платежных карт объясняется лишь с существенным ростом скомпрометированных данных других типов. Ниже перечислены крупнейшие инциденты, относящиеся к компрометации данных платежных карт [7–8]:

- в 2005 г. в результате взлома процессингового центра *Card Systems Solutions* было скомпрометировано 40 млн платежных карт;
- в 2007 г. хакеры похитили 45 млн записей с данными платежных карт в результате атаки на крупную розничную сеть TJX;
- в 2008 г. был взломан *RBS Worldpay*, что привело к компрометации данных 1,5 млн держателей карт;
- в 2009 г. злоумышленники получили доступ к более чем 100 млн данных платежных карт в результате взлома процессингового центра *Heartland Payment Systems*;
- в марте 2012 г. стало известно о компрометации около 1,5 млн платежных карт, обслуженных в процессинговом центре *Global Payments*.

По определению *платежная карта* является средством доступа к некоторому счету — так, банковская карта, будучи платежной, используется как инструмент для совершения безналичных операций по счету клиента в банке-эмитенте [9]. Относительно обеспечения безопасности данный инструмент:

- может быть скомпрометирован и использован злоумышленником для несанкционированного доступа к счету владельца инструмента;
- может быть использован ненадлежащим образом самим клиентом.

Мошенническая операция относительно платежной системы — это операция с использованием банковской карты или ее реквизитов, не инициированная или не подтвержденная ее держателем.

В соответствии с общепринятой классификацией, различают следующие виды мошенничества с платежными картами [10]:

- утерянные и украденные карты (Lost and Stolen Cards);
- неполученные карты (Never-Received-Issue — NRI);
- поддельные карты (Counterfeit Cards);
- карта не присутствует (Card Not Present);
- несанкционированное использование персональных данных держателя карты и информации по счету (Card ID Theft — Application Fraud, Account Take-over);
- другие виды мошенничества (miscellaneous).

Мошенничество с платежными картами для банка связано с определенными рисками. Так, для банка-эмитента, осуществляющего выпуск карт, любое лицо, запрашивающее доступ к банковскому счету с целью выполнения финансовой операции и (или) для получения информации о статусе счета, на момент запроса доступа к счету является только лицом, совершающим операцию. Поэтому корректность аутентификации лица, совершающего операцию с использованием банковской карты, является критически важной для обеспечения безопасности проводимой операции. От того, насколько применяемые процедуры позволяют банку-эмитенту карты быть уверенным в том, что операция выполнена с использованием эмитированной банком карты и совершается держателем, которому карта была выдана на основе договора с банком, зависит безопасность операции. Для банка-эквайрера, обеспечивающего прием карт в торгово-сервисных предприятиях для оплаты товаров и услуг и в банкоматах и пунктах выдачи наличных для получения наличных денежных средств, риски связаны с возможностью опротестования операций, совершенных несанкционированно, в рамках установленных в платежной системе процедур.

Потери от мошенничества с платежными картами в мире составляют миллиарды долларов США в год [10], только в США в 2009 г. потери составили 6,89 млрд, а ожидаемые в 2015 г. — 10 млрд [11]. В 2010 г. мировые потери от мошенничества с платежными картами крупнейших международных платежных систем составили 7 млрд долларов США, или 9,6 цента на каждые 100 долларов оборота. В регионе Центральной и Восточной Европы, куда входит Россия, потери, по данным крупнейших международных платежных систем, составили всего 2—3 %, однако темпы роста несанкционированных операций в России существенно превышают рост оборота по картам. За первое полугодие 2011 г. по сравнению с аналогичным периодом 2010 г. объем всех операций в стране вырос на 37 % и составил 7,8 трлн рублей, а общая *сумма мошеннических операций удвоилась*: за 2010 г. злоумышленники похитили 1,396 млрд рублей с помощью платежных карт, за первое полугодие 2011 г. — больше 1 млрд рублей, при этом годовой прогноз составляет 2,4 млрд рублей. Особенностью мошенничества в России является то, что 40 % несанкционированных операций совершаются в банкоматах, в то время как в мире — лишь 5 %. Компрометация данных также часто происходит в банкоматах: злоумышленники устанавливают накладки на устройства считывания данных с магнитной полосы карт и ПИН-клавиатуры, а также внедряют специализированное вредоносное ПО в программную среду банкомата для получения данных платежных карт. В 2009 г. потери только от скимминга (несанкционированное считывание данных магнитной полосы платежной карты) в банкоматах РФ составили 248 млн рублей, в 2010 г. — 558 млн рублей, за первое полугодие 2011 г. рост составил 250 % [12].

Упомянутые многочисленные факты компрометации данных платежных карт и их последующего использования злоумышленниками свидетельствуют о существенных уязвимостях

применяемых в настоящее время платежных технологий. Операции по поддельным картам становятся возможными из-за использования платежных карт на основе магнитной полосы, данные которой могут быть легко скопированы при передаче, хранении или простом считывании с помощью специального устройства (скиммера). Реквизиты карты (такие, как номер, срок окончания действия, код верификации CVC2/CVV2), будучи скомпрометированными, могут быть использованы для проведения операций без присутствия карты, прежде всего в сети Интернет, на тех сервисах, которые не обеспечивают дополнительную аутентификацию держателя карты (3D Secure). Принципиальных решений в связи с этим может быть два:

1) замена уязвимых технологий, миграция на более безопасные;

2) сохранение существующих уязвимых технологий и защита их дополнительными методами и системами.

Первое решение связано с миграцией на микропроцессорные карты стандарта EMV для предотвращения несанкционированного копирования (скимминга) магнитной полосы карты и посредством внедрения более надежных систем аутентификации держателя карты при проведении операций без присутствия карты, причем в последнем случае в ряде решений также может использоваться EMV-карта. Несмотря на то что EMV разрабатывался и развивался с середины 90-х годов прошлого века и во многих странах началась миграция на смарт-карты этого стандарта, повсеместного перехода на микропроцессорные карты до сих пор не произошло. Это объясняется, прежде всего, тем, что США до недавнего момента не были вовлечены в процесс миграции на микропроцессорные карты, но летом 2011 г. ситуация изменилась. Международная платежная система Visa установила для эквайреров и торгово-сервисных предприятий США обязательства по обеспечению принятия EMV карт к оплате для торгово-сервисных предприятий с 1 октября 2012 г., для процессинговых центров — с 1 апреля 2013 г. [13]. Тем не менее о полном отказе от платежных карт на основе магнитной полосы пока не говорится, и крупнейшие международные платежные системы пока не установили никаких сроков и временных ограничений. Поскольку полного отказа от магнитной полосы как основы платежных карт до настоящего времени не произошло, компрометация данных магнитной полосы карт и их последующее использование злоумышленниками остаются возможными как для карт только с магнитной полосой, так и для комбинированных, содержащих и магнитную полосу (для возможности использования карты в регионах, не поддерживающих обслуживание смарт-карт), и микропроцессор.

Основных стимулов перехода на смарт-карты два — это размещение различных приложений с возможностью хранения (в том числе и в защищенной области памяти) и обработки данных на карте и лучшая защищенность карты от подделки. Последний тезис подтверждается опытом Великобритании, где переход на EMV с одновременной обязательной аутентификацией держателя карты по ПИН-коду (программа Chip & PIN) позволил существенно снизить потери от операций по поддельным картам в стране — с 39 % от всего объема потерь в 2001 г. до 11 % в 2011 г. [14]. Следует отметить, что внимание злоумышленников сместилось в область операций без присутствия карты (прежде всего в Интернете), где часто используются уязвимые технологии, не обеспечивающие дополнительной аутентификации лица, представляющего реквизиты карты для проведения платежной операции.

Безопасность операций без присутствия карты в настоящее время достаточно эффективно обеспечивается технологией 3D Secure, поддерживающей дополнительную аутентификацию держателя карты эмитентом при проведении операции без присутствия карты в Интернете. Помимо реквизитов карты, которые держатель карты предоставляет для совершения операции (номер карты, срок окончания действия карты, код безопасности CVC2/CVV2), эмитент запрашивает заранее согласованную аутентификацию пользователя, которая может включать в себя статический пароль, динамический пароль в виде СМС на мобильный телефон пользователя, динамический пароль, получаемый с

использованием токенов (One Time Password — OTP), динамический пароль на основе схемы «запрос-ответ» (challenge-response) и пр. На сегодняшний день 3D Secure является наиболее безопасной схемой аутентификации держателя карты в Интернете, поддерживаемой международными платежными системами [14]. Уровень поддержки данной технологии эквайрерами и эмитентами достаточно высок, но возникли трудности с привлечением держателей карт к ее использованию. Для того чтобы держатель карты некоторого банка, обеспечивающий со своей стороны поддержку 3D Secure, мог осуществить платежную транзакцию с использованием дополнительной аутентификации, от него потребуется предварительная регистрация на сервере эмитента (enrollment server). В общем случае держатели карт недостаточно активно подключаются к данной услуге, поскольку с их стороны требуются некоторые действия, непосредственно не приносящие им очевидной выгоды или удобства.

Второй путь состоит в защите существующих уязвимых технологий (прежде всего — платежных карт с магнитной полосой). Для разработки повышенных требований к обеспечению безопасности данных платежных карт в 2006 г. был создан специальный Совет стандартов безопасности индустрии платежных карт (Payment Card Industry Security Standards Council), в который вошли American Express, Discover Financial Services, JCB, MasterCard Worldwide, Visa International. Совет к настоящему времени выпустил ряд документов, среди которых базовым является Стандарт безопасности данных индустрии платежных карт Payment Card Industry Data Security Standard (PCI DSS, далее — Стандарт). Стандарт (в настоящий момент версия 2.0) определяет требования безопасности для защиты информации, относящейся к платежной карте, и должен использоваться тогда, когда номер карты хранится, обрабатывается или передается.

Стандарт устанавливает требования по следующим шести категориям [13]:
построение и обеспечение безопасности сети;

1. защита данных о держателях карт;
2. обеспечение программы менеджмента уязвимостей;
3. реализация строгих механизмов контроля доступа;
4. регулярный мониторинг и тестирование сетей;
5. обеспечение политики информационной безопасности.

Всего определяется 12 основных требований по всем категориям:

- установить и поддерживать конфигурацию межсетевого экранирования;
- не использовать пароли и другие параметры безопасности, определяемые поставщиками по умолчанию;
- защищать хранимые данные;
- шифровать передаваемые данные о держателях карт по открытым каналам;
- использовать и регулярно обновлять антивирусное ПО;
- разрабатывать и поддерживать безопасные системы и приложения;
- ограничивать доступ к данным на основе принципа необходимого знания;
- назначить уникальный идентификатор каждому субъекту доступа к информации;
- ограничить физический доступ к данным о держателях карт;
- осуществлять мониторинг доступа к сетевым ресурсам и данным о держателях карт;
- регулярно тестировать системы и процессы безопасности;
- поддерживать политику информационной безопасности.

Приведенные требования призваны обеспечить безопасность данных платежных карт через повышение защищенности автоматизированных систем, в которых эти данные обрабатываются. Соответствие требованиям Стандарта должно означать, что система защищена и компрометация данных в ней произойти не может. Однако практика его внедрения показывает, что даже для соответствующих его требованиям организаций безопасность не обеспечивается — так, упомянутые

выше компании RBS WorldPay (2008 г.), Heartland Payment Systems (2009 г.) и Global Payments (2012 г.) до взломов своих автоматизированных систем проходили аудит и получили статус соответствия Стандарту. Практика показывает, что следование Стандарту не обеспечивает достаточной защиты данных платежных карт. Кроме того, по результатам проведенного анализа автор формулирует следующие принципиальные недостатки и противоречия Стандарта.

1. *Попытка сокрытия идентификатора (номера карты) принципиально невыполнима.* Безопасность доступа к счету карты не основывается на сокрытии идентификатора, а должна находиться в области усовершенствования процедур и средств аутентификации. Стандарт предназначен для тех организаций и процессов, в которых номер карты передается, обрабатывается или хранится. Номер карты предназначен для обеспечения соответствия счету держателя карты, т. е. является его идентификатором. Безопасность такого доступа обеспечивается процедурами аутентификации держателя карты, которые должны препятствовать несанкционированному доступу к счету. Логично предположить, что для обеспечения безопасности доступа к счету, при наличии фактов несанкционированного использования карты как инструмента доступа, необходимо усовершенствовать процедуры аутентификации. Такое усовершенствование может включать в себя внедрение механизмов многофакторной аутентификации, например, Chip&PIN, CAP-EMV. Однако Стандарт предполагает сокрытие идентификатора (номера карты) как обязательное условие обеспечения безопасности доступа. Очевидно, что принципиально невозможно отказаться от полного сокрытия идентификатора — для проведения транзакции по карте номер необходим, так как является идентификатором счета держателя карты. При современных технологиях платежных карт номер карты не относится к критически важным данным — проведение несанкционированной операции возможно либо при нарушении требований безопасности (хранение полного содержимого магнитной полосы карты и/или результатов криптографического преобразования ПИН-кодов — ПИН-блоков), либо при отставании от передовых технологий, таких как EMV и 3D Secure.

2. *Стоимость реализации требований Стандарта может превысить величину потерь от нарушения безопасности защищаемых активов, что сделает такую защиту неэффективной и в принципе нецелесообразной.* Стоимость защиты должна быть приемлемой и как минимум не превышать убытков в случае ее отсутствия, однако таких оценок при разработке Стандарта не проводилось.

3. *Внедрение требований Стандарта* потребует дополнительных затрат со стороны эквайреров и торговых предприятий, *что может привести к замедлению развития бизнеса*, если не к полной остановке (например, в российских условиях, где рентабельность и так невелика).

Реализацией мер по принуждению к прохождению процедур сертификации на соответствие Стандарту и выдачей сертификатов на его соответствие занимаются платежные системы. Процессинговые центры и эквайреры имеют договорные отношения с платежными системами и вследствие этого обязаны выполнять все требования Стандарта. Торговые предприятия членами платежных систем не являются, гражданско-правовые отношения они имеют только с эквайрерами. Поэтому ответственность за соответствие торговца требованиям Стандарта возложена на эквайрера, т. е. эквайрер считается соответствующим его требованиям, если все его торговцы прошли процедуры сертификации в платежных системах. Расходы на обеспечение соответствия требованиям могут состоять из затрат на проведение аудита, пентеста, ежеквартальных сканирований сети, мероприятий по приведению автоматизированной системы торговца в соответствие с требованиями, в том числе приобретение оборудования, программного обеспечения (соответствующего, помимо прочего, требованиям стандарта безопасности для платежных приложений PA-DSS), принятие в штат или обучение сотрудников.

4. *Существует ряд юридических аспектов в РФ для банков, которые следует отметить.* По требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных

данных» и Стандарта Банка России СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», носящего в настоящее время рекомендательный характер, банки и так внедряют системы защиты данных в соответствии с этими требованиями, причем сами требования принципиально не отличаются от требований Стандарта. Это означает, что общая стоимость защиты различных используемых банком автоматизированных систем еще более возрастет, однако целесообразность этого не является бесспорной и достаточно обоснованной применительно к российским условиям.

5. *После успешного прохождения аудита на соответствие требованиям Стандарта компания, его прошедшая, не получает никаких гарантий безопасности ни от аудиторов, ни от платежных систем*. В случае же взлома такой компании в дальнейшем статус сертифицированной организации будет, как показывает практика, пересмотрен (отозван).

6. *В Стандарте нет метрик, позволяющих судить об эффективности применения его требований*. Организация может либо соответствовать Стандарту после прохождения аудита (compliance), либо не соответствовать.

7. Наконец, *платежные карты на основе магнитной полосы и традиционные платежи без присутствия карты* (с использованием только номера карты, срока действия и кода верификации карты CVC2/CVV2) *принципиально уязвимы ввиду уязвимостей самих технологий*. Обеспечить же безопасность принципиально уязвимых технологий невозможно.

К настоящему моменту индустрия платежных карт выбрала оба упомянутых пути обеспечения безопасности — и миграцию на современные технологии, и защиту существующих уязвимых технологий. Последний подход, очевидно, является вспомогательным и временным решением и, как показывает практика, недостаточен и весьма дорог. В современные технологии безопасности платежей, такие как EMV и 3D Secure, уже вложены значительные средства. Таким образом, за безопасность платежных карт банки фактически платят дважды.

К перспективным технологиям относится технология беспроводной высокочастотной связи Near Field Communication (NFC), встраиваемой, в том числе, в мобильный телефон. Мобильный телефон является самым распространенным устройством в мире — сегодня у населения находится более 3 млрд устройств [15]. Большинство аппаратов имеют ОС (Blackberry OS, Android OS, iOS, Windows Phone OS и пр.), в среде которой работают многочисленные приложения. В связи с этим актуальной является защита операционной среды телефона и исполняемых приложений от вредоносного ПО, решение которой связано, помимо прочего, с использованием аппаратного модуля безопасности SIM/UICC. Поскольку мобильный телефон находится под контролем держателя, то при условии его достаточной защищенности NFC-модули позволят дополнительно решить следующие задачи:

- обеспечить безопасность мобильного банка;
- обеспечить безопасность операций электронной коммерции;
- поддерживать получение новых приложений с новыми функциями;
- создать новую безопасную технологию платежей без уязвимостей старых технологий.

Технологии, применяемые в индустрии платежных карт в настоящее время и планируемые к внедрению в ближайшей перспективе, предоставляют и предоставят пользователям многочисленные функции и сервисы, безопасность которых необходимо обеспечивать.

СПИСОК ЛИТЕРАТУРЫ:

1. Цифровая валюта и экономическое влияние [Электронный ресурс]: Валюта будущего // Visa. URL: http://currencyofprogress.ru (дата обращения 28.06.2012).

2. UnionPay становится крупнейшей платежной системой в мире [Электронный ресурс]: Журнал ПЛАС. URL: http://www.plusworld.ru (дата обращения 01.09.2011).
3. Число эмитированных в России карт выросло за 2011 год на 38 % и составило около 200 млн штук [Электронный ресурс]: Бизнес ТАСС. URL: http://www.biztass.ru (дата обращения 28.06.2012).
4. European ATM Crime Report 2011 [Электронный ресурс]: European ATM Security & Fraud Prevention. URL: https://www.european-atm-security.eu (дата обращения 28.06.2012).
5. Global ATM Market And Forecasts to 2016 [Электронный ресурс]: Retail Banking Research. URL: http://www.rbrlondon.com (дата обращения 20.06.2012).
6. 2012 Data Breach Investigations Report [Электронный ресурс]: Verizon Enterprise Solutions. URL: http://www.verizonbusiness.com (дата обращения 15.05.2012).
7. *Алексанов А. К., Демчев И. А., Доронин А. М. и др.* Безопасность карточного бизнеса: бизнес-энциклопедия. М.: Московская финансово-промышленная академия; ЦИПСиР, 2012.
8. *Krebs B.* Global Payments: 1.5 MM Cards 'Exported' [Электронный ресурс]: Krebs on Security. URL: http://krebsonsecurity.com (дата обращения 22.05.2012).
9. Положение ЦБ РФ № 266-П от 24.12.2004. Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт [Электронный ресурс]: законодательство РФ: кодексы, законы, указы, постановления, нормативные акты // Консультант Плюс. URL: http://www.consultant.ru (дата обращения 28.06.2012).
10. *Авакова Ю. М., Быстров Л. В., Воронин А. С. и др.* Платежные карты: бизнес-энциклопедия. М.: Маркет ДС, 2008.
11. *Vermeulen W.* Six Myths Preventing EMV Migration in the U.S. [Электронный ресурс]: Smart Token Management Software. URL: http://www.bellid.com (дата обращения 15.06.2012).
12. *Хуторных Е.* Крупный проигрыш. С платежных карт россиян воруют всё больше [Электронный ресурс]: Бизнес // Московские новости. URL: http://mn.ru (дата обращения 10.10.2011).
13. *Кузин М. В.* PCI DSS: стандарт безопасности и реальная безопасность // Безопасность информационных технологий. 2011. № 4. С. 120–125.
14. *Голдовский И.* «Легкая» поступь EMV-миграции, или Куда уходит фрод? [Электронный ресурс]: Журнал ПЛАС. URL: http://www.plusworld.ru (дата обращения 05.05.2006).
15. *Голдовский И. М.* NFC-модуль: ключ к созданию платежных систем нового поколения // Журнал ПЛАС. 2012. № 2. С. 9–12.