М. В. Кузин

ПЕРСПЕКТИВЫ ВНЕДРЕНИЯ EMV В США

1. Проблема мошенничества с платежными картами

По определению *платежная карта* является средством доступа к некоторому счету — так, банковская карта, являясь платежной, используется как инструмент для совершения безналичных операций по счету клиента в банке-эмитенте [1]. 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 [2]:
- 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).

Потери от мошенничества с платежными картами в мире составляют миллиарды долларов США в год [2], только в США в 2009 г. потери составили 6,89 млрд, а ожидаемые в 2015 г. — 10 млрд [3]. Крупнейшие из известных взломов автоматизированных систем также связаны с компрометацией данных платежных карт.

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. А в 2009 г. злоумышленники получили доступ к более чем 100 млн платежных карт в результате взлома процессингового центра Heartland Payment Systems [3]. Всего же, по данным компании Verizon Business, только в 2008 г. были скомпрометированы 285 млн единиц данных, из которых 98 % относились к данным платежных карт [4]. Следует заметить, что упомянутые инциденты с TJX и Heartland произошли в США, при этом они — крупнейшие за всю историю известные случаи компрометации подобных данных. По некоторым оценкам, стоимость принятия мер по каждому факту компрометации данных платежной карты в США составляет 202 доллара США, так что только в 2008 г. на устранение последствий атак был потрачен 1 трлн долларов США.

Для противодействия мошенничеству с платежными картами США выступили активными сторонниками стандарта безопасности индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard), разработанного и введенного в 2006 г. Следует отметить, что взломанный процессинговый центр Heartland Payment Systems был сертифицирован на соответствие стандарту PCI DSS на момент атаки. Хотя PCI DSS стремится защитить данные магнитной полосы платежной карты, он лишь пытается бороться с последствиями принципиальной уязвимости и небезопасности магнитной полосы [3, 5].

Другой путь противодействия мошенничеству — внедрение современных технологий, позволяющих обеспечить безопасность платежных операций на приемлемом уровне. К таким технологиям относятся микропроцессорные карты стандарта EMV [6].

2. EMV сегодня

Стандарт микропроцессорных карт EMV является международным и был представлен в 1995 г. для противодействия экспоненциально растущему мошенничеству с платежными картами. В мире более 60 стран внедрили EMV и приняли правила локального и глобального переноса ответственности (liability shift) по мошенничеству с платежными картами. Перенос ответственности означает, что эмитенты и эквайреры, не отвечающие требованиям EMV к определенной устанавливаемой дате, обязаны нести финансовые потери от проводимых мошеннических операций. На практике это означает, что мошенничество из стран, где EMV активно внедряется, мигрирует в сеть Интернет (это относится к мошенничеству без присутствия карты) и страны, где EMV внедрен слабо или не применяется вовсе. Так, спецификация микропроцессорных карт EMV получила широкое распространение в Европе (76 % карт, 85 % торговых терминалов и 95 % банкоматов) [7], Азии и Латинской Америке, а это означает, что США являются чрезвычайно привлекательной для злоумышленников страной, где можно использовать скомпрометированные данные платежных карт путем изготовления поддельных карт с магнитной полосой [3]. При этом, поскольку спецификация EMV полностью не вытеснила магнитную полосу, платежные карты эмитируются одновременно и с микропроцессором, и с магнитной полосой для совместимости и удобства клиентов, уязвимости карт с магнитной полосой по-прежнему актуальны и активно используются злоумышленниками. В связи с тем, что в ближайшее время США не собираются внедрять EMV, Европейский Центробанк предписал эмитировать новые карты с 2012 г. по умолчанию только с микропроцессором и не использовать магнитную полосу для проведения операций [7].

К настоящему моменту в мире финансовыми институтами было выпущено более 1 млрд микропроцессорных EMV-карт. США являются единственной страной из G20 («Большая двадцатка» наиболее экономически развитых стран мира), не начавшей миграцию платежных карт на EMV и до сих пор использующей технологию магнитной полосы, которой исполнилось 50 лет [3].

3. «Мифы» о EMV в США

Из-за упрощений и некоторой дезинформации общественность в США имеет неверное представление о стандарте EMV и практике его внедрения [3]. Основные «мифы» заключаются в следующем:

1. снижение прибыли эмитентов за счет снижения комиссии по операциям (interchange);

2. EMV не препятствует мошенничеству, переход на данную технологию не исключит несанкционированные операции;

3. мошенничество в США недостаточно велико, чтобы мигрировать на чип;

4. EMV не является безопасным стандартом, есть информация о практически реализованных атаках;

5. EMV слишком медленный.

Отмеченные заблуждения могут быть достаточно легко опровергнуты.

1. Стандартом EMV предусматриваются различные способы аутентификации держателя карты эмитентом, что определяется на этапе персонализации карты в поле Cardholder Verification Method (CVM List) [6]. В связи с этим эмитент сам выбирает предпочтительный способ проверки подлинности держателя карты и таким образом может влиять на общую стоимость транзакции по карте своего клиента.

2. Замена платежных карт с магнитной полосой микропроцессорными полностью не искоренит мошенничество хотя бы потому, что злоумышленники смогут по-прежнему совершать несанкционированные операции без присутствия карты, например в Интернете, причем объем мошеннических операций такого типа вырастет. Действительно, в настоящий момент подделать чип EMV-карты злоумышленники не пытаются, потому что есть гораздо более слабые способы проведения операций, в том числе в Интернете, из-за чего в ряде стран, например в Великобритании, где процесс миграции на EMV идет очень активно, мошенничество смещается от подделок (Counterfeit Cards) к операциям без присутствия карты (Card Not Present мошенничество). Однако в настоящий момент есть способы обеспечения большей безопасности операций без присутствия карты, к которым относятся технологии 3-D Secure, Chip Authentication Program (CAP), динамические пароли.

3. Справедливо, что карты с магнитной полосой существенно дешевле микропроцессорных — так, карта с магнитной полосой стоит около 20 центов, в то время как цена EMV-карты варьируется от 2 до 10 долларов США. Тем не менее микропроцессорную карту можно рассматривать как актив, поскольку для ее обновления можно просто переписать данные на чипе, а не заново выпускать карту на новом пластике [3, 6].

Торговые предприятия, самостоятельно владеющие торговыми терминалами, столкнутся с необходимостью вкладывать средства в их замену для возможности приема микропроцессорных карт. В случае, если терминал принадлежит банку-эквайреру, то затраты на обновление оборудования часто перекладываются на торговое предприятие в виде комиссий по операциям с платежными картами в данной точке.

Большинство банкоматов, торговых терминалов и терминалов самообслуживания, как правило, используются в течение 3—5 лет, после чего заменяются полностью или модернизируются. Регулярное проведение работ по замене криптографических ключей терминальных устройств и обновление ПО (в том числе для соответствия требованиям стандартов безопасности, таких как PCI DSS) может быть совмещено с работами по обеспечению приема EMV-карт.

Все упомянутое приведет к необходимости инвестиций в EMV для эквайреров и торговых предприятий. Кроме того, потребуется поддержка EMV со стороны эмитентов и процессинговых центров в США. Возможно в таком случае, что переход на EMV экономически не оправдан?

В 2009 г. потери от мошенничества с использованием платежных карт в США составили 6,89 млрд долларов, при этом стоимость миграции на EMV оценивается в 8,6 млрд долларов США [3]. С учетом всего отмеченного переход на EMV является, очевидно, целесообразным.

1. К настоящему моменту известны некоторые уязвимости стандарта EMV и уже реализованные атаки на конкретные терминалы и карты [8, 9], тем не менее стандарт постоянно совершенствуется, от слабых и уязвимых реализаций протоколов безопасности постепенно отказываются в пользу более защищенных. Так, от статической аутентификации карты (Static Data Authentication — SDA) постепенно, по требованиям платежных систем, осуществляется обязательный переход к более безопасной динамической (Dynamic Data Authentication — DDA) или комбинированной (Combined Data Authentication — CDA) [6]. Кроме того, описанные исследователями из Кембриджа атаки на терминалы и карты [8, 9] возможны только при некоторых допущениях и ограничениях и в общем случае являются сложными для использования злоумышленниками, либо обнаруженные уязвимости в протоколах и системах могут быть устранены доработкой параметров персонализации карт, а также дополнительными проверками при авторизации операций по EMV-картам.

2. Транзакция по микропроцессорной EMV-карте действительно занимает больше времени, поскольку требуется чтение данных с чипа, выполнение ряда криптографических и иных процедур, затратных во временном отношении. Тем не менее скорость проведения этих контактных операций постоянно увеличивается, при этом появляются и получают широкое распространение технологии бесконтактных платежей и технология связи в ближнем поле NFC (Near Filed Communication).

В случае же использования собственноручной подписи на чеке терминала для аутентификации держателя карты именно этот этап транзакции занимает основное время, и оно никак не зависит от микропроцессора карты [3].

4. Будущее EMV в США

Несмотря на то что официально старт миграции на чип в США еще не дан, определенные шаги в этом направлении рядом компаний уже делаются. Так, крупнейшая организация розничной торговли Walmart заявила о намерении обеспечить повсеместный прием EMV-карт в своей сети к концу 2011 г. Один из крупнейших кредитных союзов в США United Nations Federal Credit Union начал выдавать EMV-карты более чем 80 тысячам своим членов. Некоторые эмитенты в США предлагают микропроцессорные карты своим клиентам, которые совершают заграничные поездки, поскольку граждане США часто испытывают неудобства при использовании своих платежных карт в Европе. Так, за последние 4 года около половины держателей карт из США, посещавших Европу, столкнулись с какими-либо проблемами при попытке расплатиться своими картами (в некоторых случаях держателям карт было отказано в проведении операций) [3].

С учетом ранее отмеченной экономической целесообразности перехода на микропроцессорные EMV-карты для США при текущем и прогнозируемом уровнях ежегодного мошенничества стоимость внедрения может быть компенсирована уже через год-два за счет снижения потерь [3]. Если же к этому добавить дополнительные ежегодные расходы участников платежных систем на обеспечение требований стандарта PCI DSS, спасающего уязвимые технологии платежей наподобие магнитной полосы, то внедрение EMV является единственным разумным ответом мошенничеству с платежными картами.

СПИСОК ЛИТЕРАТУРЫ:

1. Положение ЦБ РФ № 266-П от 24.12.2004. Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт // «Консультант Плюс»: законодательство РФ: кодексы, законы, указы, постановления, нормативные акты. URL: http://www.consultant.ru.
2. *Быстров Л. В. и др.* Пластиковые карты. М.: Издательская группа «БДЦ-пресс», 2005. — 624 с.
3. *Vermeulen W.* Six Myths Preventing EMV Migration in the U.S. URL: http://www.bellid.com.
4. *Кузин М. В.* Исследование Verizon Business: компрометация данных в 2008 г. // Безопасность информационных технологий. 2009. № 4. С. 111.
5. *Кузин М.* PCI DSS и реальная безопасность платежных карт // ПЛАС. 2010. «Дайджест'2009». С. 16–18.
6. *Голдовский И. М.* Микропроцессорные карты стандарта EMV. М.: Издательская группа «БДЦ-пресс», 2006. — 544 с.
7. Single Euro Payments Area October 2010. Seventh Progress Report. Beyond Theory into Practice. URL: http://www.ecb.eu.
8. *Drimer S., Murdoch J.* Tamper Resistance of Chip & PIN (EMV) Terminals // The Computer Laboratory. URL: http://www.cl.cam.ac.uk.
9. *Drimer S., Murdoch J.* Keep Your Enemies Close: Distance Bounding against Smartcard Relay Attacks // The Computer Laboratory. URL: http://www.cl.cam.ac.uk.