Еще раз о фроде...

Очередные шаги международных платежных систем, направленные на повышение безопасности карточных операций

Игорь Голдовский, генеральный директор ЗАО «Платежные технологии»

В течение уже более чем 5 лет банковский мир местами весьма активно мигрирует на технологию микропроцессорных карт. Особо дружной эту миграцию назвать трудно, но тем не менее на сегодняшний день каждая пятая карта ведущих платежных систем содержит чип, а каждый третий в мире POS-терминал умеет с ним работать. Этот результат достигнут главным образом усилиями европейских стран, а также стран Азиатско-Тихоокеанского региона (где сегодня эмитировано примерно в 3 раза меньше микропроцессорных карт, чем в Европе) и Латинской Америки (разрыв с Европой примерно оценивается как девятикратный). В самой же Европе сегодня содержит микропроцессор каждая вторая платежная карта, а работать с такими картами способны две трети POS-терминалов. Это, в свою очередь, означает, что примерно треть всех операций в Европе ($\frac{1}{2}\cdot\frac{2}{3}=\frac{1}{3}$) выполняется с использованием микропроцессорной технологии.

Главным стимулом банков для миграции на чип по-прежнему остается повышение безопасности карточных операций. Безусловно, микропроцессор позволяет поднять этот показатель на качественно новый уровень. Результаты миграции на новую технологию являются хорошим тому подтверждением. В странах, мигрировавших на чип, уровень такого вида мошенничества, как операции по поддельным картам, значительно снизился. В странах, где используется технология Chip&PIN, кроме того, заметно снизилось число случаев мошенничества по украденным/потерянным картам. Обо всем этом я уже рассказывал в своем материале «Легкая поступь EMV-миграции, или Куда уходит фрод?», опубликованном в «ПЛАС» №4/2006.

Цель настоящей статьи – оценить реальную безопасность операций по микропроцессорным картам в сегодняшних условиях, т. е. несколько лет спустя после упомянутой публикации, а также рассказать о новых шагах, предпринимаемых платежными системами с целью повышения безопасности карточных операций. Подчеркну, что речь в данной статье идет об оценке безопасности операций именно в сегодняшних условиях, характеризующихся перечисленными ниже особенностями:

- неравномерностью миграции на чип различных страновых/региональных рынков;
- гибридным характером микропроцессорных карт, содержащих как магнитную полосу, так и чип;
- наличием значительного количества терминалов, не поддерживающих чиповую технологию (примерно 2/3 всех установленных в мире POS-терминалов);
- наличием значительного количества терминалов, не способных поддерживать офлайновую проверку картой значения ПИН-кода;
- тем фактом, что подавляющее большинство эмитированных микропроцессорных карт не поддерживают динамическую офлайновую аутентификацию карты (точнее, финансового приложения карты), т. е. являются SDA-картами.

Все эти особенности сегодняшнего дня мы подробнее рассмотрим чуть позже, а пока остановимся на существующих угрозах безопасности операций для микропроцессорных карт.

На основе опыта платежных систем (МПС) к таким угрозам в сфере эмиссии относятся:

- «клонирование» магнитной полосы;
- «клонирование» чипа;
- CNP-фрод;
- украденные/потерянные карты;
- виртуальное «клонирование» чиповой карты;
- модификация диалога карты и терминала.

К основным угрозам в сфере обслуживания карт следует отнести:

- ложный ключ МПС;
- замену терминала с целью кражи информации держателей карт;

- некорректную реализацию метода Enciphered PIN Offline;
- подделку торговой точкой типа криптограммы в презентментах.

Мошенничество в сфере эмиссии карт

Остановимся на отмеченных выше угрозах и способах борьбы с ними подробнее. Начнем с эмиссии микропроцессорных карт. Предметом наших дальнейших исследований является гибридная карта, содержащая одновременно магнитную полосу и чип.

«Клонирование» магнитной полосы гибридной карты

Ниже мы будем условно называть терминал магнитным, если он способен обрабатывать операции только по «магнитным» картам, и гибридным, если он обрабатывает операции и по «магнитным», и по чиповым картам. Аналогичные определения будем использовать и в отношении самих платежных карт.

Под «клонированием» магнитной полосы гибридной карты понимается процедура создания мошенниками аналога банковской карты (на основе данных реальной карты, эмитированной некоторым банком системы) с целью несанкционированного использования этого аналога (поддельной карты) в терминальной сети платежной системы по технологии карты с магнитной полосой. При этом очевидно, что конечной целью несанкционированного использования аналога карты является получение мошенниками материальной выгоды (услуг, товаров, денежных средств).

Важно отметить, что воспользоваться аналогом банковской карты (поддельной картой) преступники могут в зависимости от ситуации по-разному. Например, у мошенника не возникает проблем при использовании аналога гибридной карты в магнитном терминале. Но такая проблема возникнет, если мошенник обратится с поддельной картой, содержащей только магнитную полосу, в гибридный терминал. Гибридный терминал, распознав по коду обслуживания, прочитанному с магнитной полосы карты, что карта содержит чип, должен требовать проведения операции по чиповой технологии. Чтобы обойти это препятствие, мошенники пользуются дополнительными мерами, речь о которых пойдет ниже. Здесь важно подчеркнуть, что когда мы говорим о «клонировании» карты, то речь идет о создании некоторого аналога реальной карты, который может успешно с точки зрения мошенников применяться в определенном множестве терминалов. При этом каждый раз мы будем четко определять область применения созданного аналога.

Очевидно, для «клонирования» магнитной полосы гибридной карты мошенникам сначала необходимо получить данные, записанные на магнитной полосе некоторой реальной карты, с тем чтобы впоследствии перенести эти данные (возможно, модифицировав их определенным образом) на заготовку карты, предназначенную для создания аналога карты. Эти данные можно получить в результате их считывания (часто несанкционированного) с магнитной полосы реальной карты, в результате кражи данных в каналах связи при передаче данных в процессинговый центр (ПЦ) или в результате кражи данных о магнитной полосе из POS-терминала или ПЦ.

Самым распространенным способом кражи данных о реальной карте является скимминг (skimming). Существует большое количество способов скимминга. Самый простой из них – это использование кассиров торговых предприятий, вступивших в сговор с преступниками и снабженных специальными устройствами, способными считывать и запоминать информацию, хранящуюся на магнитной полосе карты.

В последнее пятилетие большой популярностью стал пользоваться банкоматный скимминг. Еще одним источником кражи данных магнитной полосы являются некоторые POS-терминалы и процессинговые центры. В этом случае необходимые для клонирования магнитной полосы данные можно получить не только с магнитной полосы, но и с чипа. Дело в том, что чип содержит информацию второй дорожки магнитной полосы (Track2 Equivalent Data). Это делается для того, чтобы обеспечить прием микропроцессорной карты в устройстве обслуживающего банка, работающего в режиме Partial Grade Acquirer. Кроме того, наличие элемента данных Track2 Equivalent Data в авторизационных запросах упрощает адаптацию приложений хостов эмитентов и обслуживающих банков под технологию чипа.

Обмен информацией между микропроцессорной картой и ридером в основном не защищен, что позволяет мошенникам получать интересующую их информацию Track2 Equivalent Data через терминалы. То же касается и процессинговых центров. Существует возможность перехвата межхостового сообщения или сообщения от терминала, после чего можно легко извлечь из него информацию о второй дорожке магнитной полосы. Напомним, что хранение информации о второй дорожке карты на терминалах и процессинговых центрах строго запрещено стандартом PCI DSS. Но ни у кого нет сомнения в том, что далеко не все терминалы и процессинговые центры удовлетворяют этому требованию. Поэтому похищать данные Track2 Equivalent Data иногда возможно из лог-файлов/БД терминалов и процессинговых центров.

Для борьбы с кражей чиповых данных Track2 Equivalent Data в терминалах и ПЦ с целью дальнейшего использования этих данных для клонирования магнитной полосы ведущие платежные системы ввели обязательное использование отдельного значения CVC/CVV (Chip CVC/iCVV) в приложении на чипе. Это отдельное значение вычисляется по стандартному алгоритму вычисления CVC/CVV при значении кода обслуживания 999. В MasterCard Europe это нововведение стало обязательным с 1 января 2008 г., в VISA CEMEA – с 1 января 2009 г. (напомним, что именно к этим регионам относится и Россия). Сегодня

использование украденных данных Track2 Equivalent Data в России для клонирования магнитной полосы остается возможным только для карт, выпущенных до указанных выше сроков.

Очевидно, что «клонирование» магнитной полосы имеет смысл для мошенников до тех пор, пока в мире остаются «магнитные» карты и терминалы. Действительно, представим себе два крайних случая. В первом случае все терминалы в мире являются гибридными. Тогда по магнитной полосе в них могут обрабатываться только «магнитные» карты, имеющие значение кода обслуживания 1XX или 5XX.

Во втором крайнем случае все карты являются гибридными (значение кода обслуживания таких карт 2XX или 6XX). Такие карты могут обрабатываться (с оговорками, о которых будет рассказано ниже) по магнитной полосе только в магнитных терминалах. Поскольку модификация кода обслуживания в большинстве случаев мошенникам не под силу (целостность кода защищена использованием криптографических величин CVC/CVC, хранящихся на магнитной полосе карты), то действительно, необходимым условием целесообразности для мошенников клонирования магнитной полосы является одновременное использование банками платежной системы «магнитных» карт и терминалов.

Именно поэтому платежные системы предпринимают значительные (но, к сожалению, как показывает практика, все еще недостаточные) усилия к ускорению процесса миграции банков на технологию микропроцессорных карт. Для этого помимо работы с банками и разъяснения преимуществ новой технологии платежные системы используют правила переноса ответственности на «нечиповую» сторону (Chip Liability Shift) и изменения межбанковских платежей в пользу банков, мигрировавших на EMV. О сегодняшнем положении дел с Chip Liability Shift в рамках MasterCard Worldwide можно судить по данным таб. 1.

LS Applicability	Europe	LAC	SAMEA	AP	US & Canada
MC POS Chip	✔	✔	✔	✔	✗
MC POS Chip & PIN	✔	✗	✗	✗	✗
MA POS Chip	✔	✔	✗	✗	✗
ATM Chip	✔	✔	✗	✗	✗
Includes domestic txns	✔	✗*	✗	✔	✗
Interchange incentive	✔	✔	✔	✔	✗
Opted-in to Inter-regional LS	✔	✗	✗	✗**	✗

On a per country basis: Brazil, Mexico, Colombia, Venezuela (July 2009)

*** Malaysia and Taiwan only for MC POS Chip only*

Таблица 1. *Перенос ответственности в MasterCard Worldwide*

Как демонстрирует таблица, полноценный Chip Liability Shift в MasterCard имеет место только в регионе MasterCard Europe. Только здесь правило переноса ответственности действует для всех карточных продуктов платежной системы и на всех типах терминальных устройств (банкоматы и POS-терминалы). Например, во втором с точки зрения масштабов миграции на чип регионе – Азиатско-Тихоокеанском – Chip Liability Shift действует только для операций, выполненных по картам MasterCard в POS-терминалах, и не касается ни карт Maestro, ни операций в банкоматах.

Другая особенность Chip Liability Shift – его преимущественно внутрирегиональный характер. Действительно, с точки зрения применения правила переноса ответственности к операциям, выполненным по картам MasterCard (не Maestro!) на POS-терминалах, к региону MasterCard Europe на сегодняшний день присоединились лишь Малайзия и Тайвань.

Иногда Chip Liability Shift действует внутри региона, но не работает на уровне отдельных стран региона. Так происходит в MasterCard для стран Латинской Америки, где перенос ответственности для внутристрановых транзакций начнет действовать с июля 2009 г. лишь в отдельных странах – в Бразилии, Мексике, Колумбии и Венесуэле.

Похожая ситуация сложилась и в Visa Inc. Chip Liability Shift введен в регионах AP, CEMEA, Europe, LAC по всем карточным продуктам Visa. В 2010 г. ожидается введение данного правила в Канаде. Существует соглашение о межрегиональном переносе ответственности (Bilateral Liability Shift) между регионами Europe и CEMEA. В октябре 2010 г. к нему должна присоединиться Канада.

Кроме того что Chip Liability Shift носит внутрирегиональный характер, сама миграция на чип происходит очень неравномерно, и существуют целые рынки (например, крупнейший в мире карточный рынок США), на которых она фактически и не начиналась. Неравномерность процесса приводит к образованию больших «островов», на которых магнитная технология является преобладающей, что влечет за собой миграцию на эти рынки фрода из других стран и регионов мира. В результате страдают и эмитенты чиповых карт, операции по которым проводятся на данных «островных» рынках. Трудно назвать нормальной ситуацию, когда банк сделал все, что от него требовала платежная система, – перевел свои карты и терминалы на чиповую технологию – и тем не менее продолжает страдать от фрода, причем в значительной степени из-за того, что банки на других рынках остаются «магнитными». На этом фоне платежным системам как инициаторам миграции на новую технологию следует проводить более жесткую политику в отношении «магнитных» банков с целью придания Chip Liability Shift глобального характера.

Легко показать, что уровень мошенничества по поддельным картам с точки зрения эмиссии банка (выраженный в базисных пунктах) определяется выражением: $F = (f_1 a + f_2 b)(1 - A) + f_3 c(1 - AB)$, где

A – доля EMV-карт рассматриваемого банка, B – доля POS-терминалов, принимающих EMV-карты в «чужих» для банка регионах, f_1, f_2, f_3 – соответственно, внутристрановые, внутрирегиональные и межрегиональные уровни мошенничества по поддельным картам, a, b, c – соответственно, вероятности того, что карта банка применяется внутри страны, внутри региона и за пределами региона. Из приведенной формулы легко видеть, что даже если все карты банка являются микропроцессорными $(A=1)$, то уровень фрода с точки зрения эмиссии карт банка в общем случае не будет нулевым из-за наличия второго слагаемого в правой части выражения для F. Более того, как предсказывали аналитики и показывает сегодняшний опыт, для стран, продвинувшихся в процессе миграции на чиповую технологию, величина f_3 будет расти, поскольку у преступников останется возможность осуществления мошенничества только из стран с плохо развитой инфраструктурой приема чиповых карт. Так, по данным MasterCard, в той же Великобритании за последние три года размер межрегионального фрода вырос на 250%!

После того как аналог карты изготовлен, он может быть использован мошенниками различным образом. Самый простой способ – использование поддельной карты в магнитных терминалах.

Использование поддельной карты в магнитном терминале. Очевидно, при использовании поддельной карты, клонирующей магнитную полосу реальной гибридной карты в магнитном терминале, шансы мошенников на успех велики (достаточно, чтобы реальная карта на данный момент была активна и было достаточно средств на счете, связанном с картой).

Сегодня в качестве магнитных терминалов для использования клонированных по магнитной полосе карт все чаще выступают банкоматы. Понятно, что при использовании банкомата мошеннику достаточно знать реквизиты второй дорожки реальной карты и ПИН-код. При этом аналог карты можно изготовить на «белом пластике», что облегчает и удешевляет деятельность мошенников.

Для повышения безопасности операций снятия наличных в банкоматах МПС рассматривают возможность применения для таких операций следующих видов защиты:

- Использование CVC2/CVV2/ CAP Token при выполнении банкоматных транзакций в магнитных терминалах;
- Применение офлайновой динамической аутентификации приложения карты в банкоматах для обслуживающих банков, работающих в режиме Partial Grade Acquirers (без передачи в сеть элемента DE55, содержащего «чиповые» данные).

Очевидно, внедрение таких технологий потребует от банков значительных усилий – им придется модернизировать приложения на банкомате, а также изменить форматы авторизационных запросов. В этой связи у обслуживающих банков существует более разумная альтернатива – осуществить миграцию своих банкоматов на чип.

Кроме того, платежные системы для борьбы с банкоматным мошенничеством традиционно рекомендуют банкам:

- Ускорить миграцию банкоматов и карт на чип;

КАЛЕЙДОСКОП

«Энвижн Груп» и ArcSight: партнерство в области безопасности

Компания «Энвижн Груп» (NVision Group) объявила о заключении партнерских отношений с ArcSight (США), разработчиком решений для контроля инцидентов безопасности и степени выполнения норм отраслевого регулирования.

Выбор «Энвижн Груп» в пользу ArcSight был сформирован рядом конкурентных технологических возможностей ее продуктов. Флагманом продуктовой линейки ArcSight является решение ArcSight Enterprise Security Solution, ядром которого служит модуль ArcSight ESM Enterprise Security Manager. Данный модуль обеспечивает сбор, обработку и хранение гетерогенных событий безопасности, генерируемых практически любой информационной системой. ArcSight ESM поддерживает интеграцию с максимальным количеством прикладных систем и устройств (всего более 300) и поставляется с несколькими тысячами предустановленных правил корреляции. ArcSight ESM является единственной системой на рынке, обладающей уникальным механизмом интеграции с любым бизнес-приложением. Гибкая архитектура ArcSight ESM позволяет развернуть решение даже в территориально-распределенной информационной системе с «узкими» каналами связи. ArcSight ESM поставляется в программном и программно-аппаратном виде, что выгодно отличает ее от других систем корреляции.

Партнерство с ArcSight позволит «Энвижн Груп» расширить продуктовый портфель и предложить заказчикам сбалансированный комплекс средств в области построения центров мониторинга и управления информационной безопасностью (Security Operation Center – SOC), поднять на качественно новый уровень эффективность работы систем класса Compliance-Management и т. д.

Кроме того, с расширением собственного портфеля продуктов в области информационной безопасности за счет партнерства с компанией ArcSight, «Энвижн Груп» сможет предлагать финансовым компаниям комплексные решения в области сертификационного аудита информационных систем на соответствие стандарту PCI DSS.

- Использовать SMS-уведомления клиентов о совершенных ими операциях;
- Предпринимать меры по защите ПИН-кода в банкоматах и POS-терминалах.

Чуть подробнее остановимся на краже ПИН-кодов в POS-терминалах. Несмотря на то что производители POS-терминального оборудования уверяют нас в реализации надежных механизмов защиты ПИН-кода на POS-терминалах, количество случаев компрометации ПИН на этих устройствах быстро растет. Известно, что в 2006 г. компания Shell приостановила прием карт на своих 600 терминалах (из 1000) в связи с возникшим подозрением на то, что некоторые из них использовались для кражи ПИН-кодов и других реквизитов карт. В дальнейшем было подтверждено, что мошенники по договоренности с персоналом торгово-сервисных точек модифицировали ПИН-пады на трех заправочных станциях Shell с целью кражи данных карты и ПИН-кода.

К сожалению, факт прохождения терминалом сертификации на соответствие требованиям PCI Pin Entry Device не является достаточным условиям для того, чтобы чувствовать себя уверенно в отношении сохранности ПИН-кодов в таких терминалах. В частности, исследователи из Великобритании показали на нескольких моделях терминалов, как можно заменой всего двух-трех внутренних компонентов терминала получить устройство, полностью контролируемое мошенниками.

Тревогу вызывают и недавно опубликованные данные о том, что в ряде POS-терминалов нескольких очень известных моделей, произведенных в Китае, была вставлена «закладка», с помощью которой информация о карте, ПИН-коде и данные магнитной полосы карты передавались по GSM-каналу мошенникам.

Ну и, наконец, нельзя забывать, что POS-терминалы – устройства относительно недорогие. Тем более что в последнее время все чаще используются переносные модели. Поэтому в отличие от банкомата заменить POS-терминал на специальное устройство, способное записывать интересующую мошенников информацию, не составляет труда.

Ниже будет рассказано об идее создания специальных каналов взаимодействия карты и терминала, позволяющих избегать кражи ПИН-кодов (т. н. Customer Trustworthy Channel). К сожалению, возможность использования таких каналов пока только обсуждается, и до их массовой реализации на практике может пройти немало времени.

Использование поддельной карты в гибридном терминале. В этом случае терминал должен требовать выполнения операции по чиповой технологии, поскольку код обслуживания карты равен 2XX или 6XX и указывает терминалу на поддержку картой чиповой технологии, являющейся более приоритетной по сравнению с технологией магнитной полосы. Однако в некоторых реализациях приложение терминала позволяет кассиру обойти это требование МПС, и в результате мошенники имеют шансы на успех.

Однако с таким мошенничеством можно успешно бороться. Эмитенту чиповой карты MasterCard/Maestro рекомендуется отклонять транзакции, в авторизационных запросах которых DE 61 (POS Data) указывает на то, что терминал может выполнить операцию по чипу, но проводит ее по магнитной полосе и при этом POS Entry Mode (DE22) не равен 80X (случай fallback).

Эмитенту чиповой карты Visa рекомендуется отвергать транзакции, в которых одновременно выполняются условия:

DE22.1 = “90” or “02” (magnetic stripe read);
DE60.2 = “5” (chip capable terminal);
DE60.3 ≠ “1”(Fallback. No info about chip read error on previous transaction in that terminal) or “2” (Fallback. There was chip read error on previous transaction in that terminal),

что указывает на то, что терминал может выполнить операцию по чипу, но проводит ее по магнитной полосе и не в режиме fallback.

Однако и в случае, когда терминал работает корректно и не позволяет кассиру провести транзакцию по магнитной полосе с кодом обслуживания 2XX/6XX, у мошенников имеются как минимум два способа добиться успеха.

При первом способе мошенник просто меняет код обслуживания на магнитной полосе на значение 1XX или 5XX и рассчитывает на проведение операции в режиме floor limit. Такая прореха в безопасности чиповой технологии считалась платежными системами самой вопиющей (действительно, и терминал гибридный, и карта гибридная, а все-таки ее «клонирование» по магнитной полосе оказывается результативным!). Поэтому в регионах MasterCard Europe и Visa CEMEA, к которым принадлежит и Россия, было принято решение о том, что все операции в online-capable терминалах по магнитной полосе должны проводиться исключительно в online. Отметим, что это решение до сих пор носит локальный характер и не принято во всех регионах платежных систем.

При втором способе мошенник использует заготовку с определенным образом персонализированной микросхемой и магнитной полосой, содержащей информацию, скопированную с реальной гибридной карты. В этом случае заготовка обойдется преступникам чуть дороже (примерно на 50 центов). Зато благодаря специальному способу персонализации микросхемы терминал при обработке транзакции примет решение о переходе на режим запасной (обязательно онлайновой) авторизации по магнитной полосе (т. н. fallback). Этот режим был принят МПС для обеспечения необходимого уровня качества приема карт в ситуациях, когда программное обеспечение терминала и/или карты не в полной мере отвечает требованиям соответствующих спецификаций платежной системы.

Для борьбы с этим видом мошенничества MasterCard придерживается политики постепенного отказа от режима fallback по мере того, как уровень совместимости карт и терминалов возрастает.

По данным MasterCard Europe, на конец 2008 г. в Европе уровень fallback составляет около 2% (год назад – 3,2%, два года назад – 4,8%). Примерно треть всех fallback (по данным Visa – четверть) связаны с мошенничеством. На этом фоне MasterCard Europe принял следующие важные решения:

- С 1 января 2007 г. fallback в банкоматах банков, действующих в регионе MasterCard Europe, возможен под ответственность обслуживающего банка;
- С 1 января 2008 г. страновые/региональные рынки по согласованию с MasterCard имеют возможность отказываться от fallback на магнитную полосу на POS-терминалах;
- С 1 января 2011 г. для стран SEPA fallback на магнитную полосу будет запрещен на POS-терминалах.

Visa Inc. в настоящее время не планирует принимать аналогичные решения по отказу от fallback, делая акцент на обеспечение высокого уровня качества приема карт.

«Клонирование чипа» гибридной карты

Под «клонированием» чипа гибридной карты понимается процедура создания мошенниками аналога банковской карты (на основе данных реальной карты, эмитированной некоторым банком системы) с целью несанкционированного использования этого аналога в терминальной сети платежной системы по чиповой технологии. Очевидно, область применения клонированных карт – некоторое подмножество гибридных терминалов.

Несколько лет назад в своей книге «Микропроцессорные карты стандарта EMV» [1] я подробно рассказал о том, каким образом можно «клонировать» любую SDA-карту с целью ее использования в офлайновом режиме авторизации (онлайновая авторизация по клонированной SDA-карте не будет успешно авторизована). Стоимость клонирования SDA-карты невелика и составляет 5–10 долл. Данные таких карт, необходимые для клонирования реальной карты по чипу, могут собираться на специальным образом «обработанных» POS-терминалах или в устройствах, аналогичных тем, что используются для клонирования магнитной полосы. Опасная особенность правильно изготовленной «клонированной» SDA-карты заключается в том, что эмитент не может заблокировать ее через Script Processing (заблокировать SDA-карту можно только с помощью стоп-листов на терминале). «Правильная» «клонированная» SDA-карта вообще никогда не принимает участия в онлайновых операциях. Как только терминал требует выполнения операции в online, SDA-карта завершает операцию отказом в авторизации.

Тот факт, что SDA-карта может требовать офлайновой проверки ПИН-кода, так же очевидно не является ограничением для успешного выполнения мошенничества с использованием ее «клона».

Следует отметить, что, по данным МПС, уже были зафиксированы случаи использования «клонированных» SDA-карт британских банков в Португалии и Турции. На этом фоне проблеме «клонирования» SDA-карт МПС уделяют особое внимание. Несколько лет назад в МПС появились Планы экстренных действий (т. н. Contingency Plan) на случай массовой компрометации SDA-карт. Наличие на рынке большого количества SDA-карт привело к тому, что значения floor limit на терминалах для операций по микропроцессорным картам с проверкой PIN Offline все еще не принимают бесконечного значения (например, для карт Maestro).

МПС всегда рекомендовали использовать SDA-карты преимущественно в режиме онлайновой авторизации. Однако в ближайшее время будут приняты более определенные решения на эту тему. С 1 января 2011 г. все новые микропроцессорные карты в MasterCard Europe и Visa CEMEA/Europe должны будут поддерживать методы динамической офлайновой аутентификации (DDA, CDA) и будет запрещена поддержка этими картами метода SDA. На последнее решение (запрет поддержки SDA) следует обратить особое внимание, поскольку в Visa сегодня существует требование поддержки SDA для карт с динамической офлайновой аутентификацией (очевидно, в целях обеспечения высокого уровня качества приема карт). В России сегодня примерно 80% эмитированных карт являются картами с динамической аутентификацией, одновременно поддерживающими метод SDA.

В моей книге [1] уже было рассказано о том, что при неправильной персонализации клонировать можно и карту с динамической аутентификацией, если эта карта поддерживает также метод SDA (карта содержит объект данных Tag '93' Signed Static Application Data; заметим, что Visa пока требует поддержки метода SDA и в случае поддержки картой DDA). Под неправильной персонализацией в данном случае понимается отсутствие на карте составного объекта данных SDA Tag List, содержащего единственный объект данных AIP (Application Interchange Profile), определяющий, в частности, методы аутентификации, поддерживаемые картой. Целостность объекта AIP обеспечивается наличием на карте объекта данных SDA Tag List.

Если SDA Tag List на карте отсутствует, то, модифицировав AIP такой карты на AIP, указывающий на поддержку картой только статической аутентификации, можно «создать» SDA-карту, которая будет успешно применяться в режиме SDA при выполнении офлайновых операций.

Таким образом, при поддержке картой метода SDA приложение должно хранить объект данных SDA Tag List! Если метод SDA приложением карты не поддерживается (отсутствует объект данных Signed Static Application Data), хранить SDA Tag List на карте не обязательно, но желательно. Это связано с тем, что этот объект данных содержит другую критическую информацию (например, информацию о поддержке картой верификации держателя карты и необходимости для терминала вы-

полнения процедур управления рисками), которой мошенники могут воспользоваться в очень экзотических случаях.

Итак, общее направление борьбы МПС с «клонированием» чипа заключается в переходе на динамические методы аутентификации (использование DDA/CDA). В этой связи МПС принимают следующие важные решения, касающиеся России:

- С 1 января 2011 г. в регионах MasterCard Europe и Visa CEMEA/Europe новые карты должны поддерживать метод DDA/CDA (заметим, что во Франции это правило действует с 1 января 2007 г.);
- С 1 января 2011 г. в рамках MasterCard по всем регионам все новые гибридные offline capable терминалы должны поддерживать метод CDA (DDA поддерживается с 1 января 2005 г., сегодня более 70% терминалов поддерживают CDA; в Visa вопрос о принятии подобного решения пока не обсуждался).

CNP-фрод

Как и предсказывали аналитики, с расширением применения микропроцессорной карточной технологии CNP-мошенничество стремительно растет. На конец 2007 г. в Европе на этот вид мошенничества приходилось более половины всего фрода (51%). Причем в Великобритании этот показатель достигал 54%, что в два раза превышало уровень мошенничества по поддельным картам (27%). Последний вид мошенничества сейчас занимает второе «почетное» место, хотя еще 5 лет назад являлся уверенным лидером, на который приходилось около 35% всего карточного фрода.

CNP-фрод следовало бы отнести в рамках данной публикации в раздел, посвященный «клонированию» общих реквизитов карты (номера карты и срока ее действия), одинаковых для магнитных и гибридных карт. Однако в силу важности этого вида мошенничества мы отводим ему отдельную главу.

Сегодня ведущие платежные системы признают единственный протокол безопасной электронной коммерции – 3D Secure (в Visa этот протокол продвигается под брендом Verified by Visa, а в MasterCard – под брендом MasterCard SecureCode). По мнению экспертов, повсеместное использование этого протокола торговыми предприятиями, обслуживающими банками и эмитентами карт способно снизить общий уровень фрода в области электронной коммерции (ЭК) не менее чем на 80%, доведя его до уровня 5–7 базисных пунктов.

К концу 2007 г. в среднем по миру 12% всех операций ЭК производились в онлайновых магазинах, поддерживающих 3D Secure. Из этих 12% операций только 28% являлись полностью аутентифицированными в соответствии с 3D Secure (протокол поддерживается держателями карт). Таким образом, только 3,36% всех операций ЭК выполнялось по протоколу 3D Secure как со стороны торговой точки, так и со стороны держателя карты.

Для стимулирования внедрения протокола 3D Secure платежные системы ввели правило переноса ответственности (merchant only liability shift), в соответствии с которым при поддержке торговой точкой протокола 3D Secure ответственность за мошенничество в ЭК, связанное с отказом держателя карты от совершенной операции, возлагается на эмитента. В Visa merchant only liability shift носит глобальный характер. В MasterCard глобальный перенос

КАЛЕЙДОСКОП

Альфа-Банк и «Северная Казна» объединили АТМ-сети

Альфа-Банк и банк «Северная Казна» объявили о запуске с 23 декабря 2008 г. процесса объединения своих банкоматных сетей.

Таким образом, клиенты двух банков получают ряд новых преимуществ от интеграции банковских структур. В частности, держателям карт Visa Inc. и MasterCard Worldwide, эмитированных банком «Северная Казна», предоставлена возможность снятия наличных и получения информации о балансе карты в АТМ Альфа-Банка на тех же условиях, что и в банкоматах своего банка. Аналогичную возможность – прием и обслуживание карт международных платежных систем в сети АТМ банка «Северная Казна» по тарифам Альфа-Банка – получают клиенты Альфа-Банка.

INPAS открывает полноценный филиал в Казахстане

Собранием акционеров «Инлайн технолоджиес групп» было принято решение о преобразовании представительства компании INPAS в Республике Казахстан в филиал INPAS. Данные изменения открывают больше возможностей для работы с партнерами, а также закрепляют позиции ИНПАС на рынке стран бывших союзных республик.

В сферу деятельности филиала будут входить не только организация продаж, но и вопросы оказания полноценного гарантийного и негарантийного сервисного обслуживания поставляемого в регион оборудования, а также заключение прямых договоров с банками на сопровождение программного обеспечения INPAS.

Данным шагом INPAS усиливает свое присутствие на рынке Средней Азии, упрощает схемы финансовых взаимоотношений с клиентами компании и расширяет спектр оказываемых услуг.

Экономический эффект от создания на рынке Казахстана полноценного филиала INPAS уже сегодня становится весьма заметен. Сегодня доля компании на местном рынке POS-терминального оборудования составляет порядка 65–75%. В клиентскую базу INPAS входят сегодня практически все кредитные организации в республике.

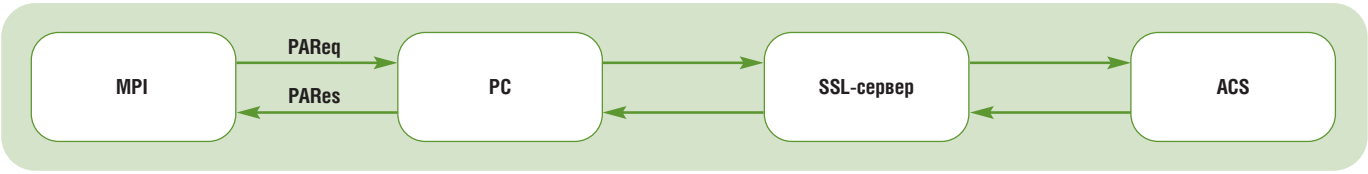

Рис. 1. *Атака «man-in the-middle» для CNP-операции, выполненной в соответствии с протоколом 3D Secure*

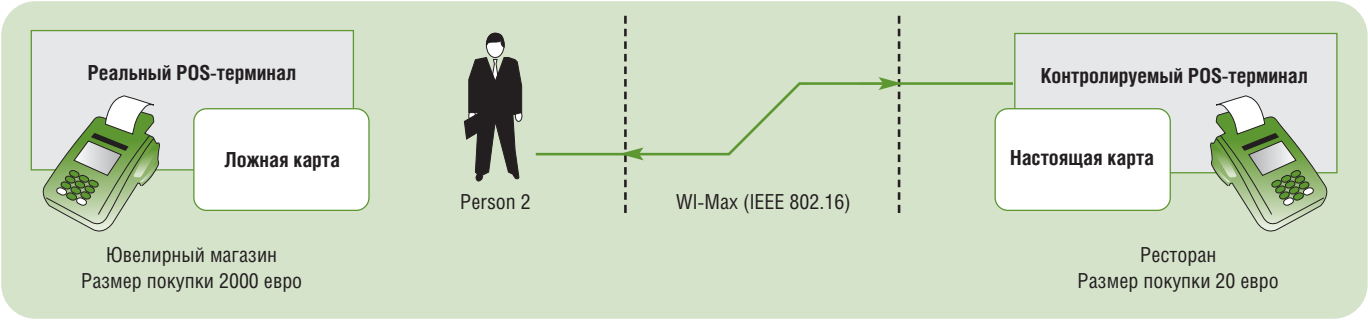

Рис. 2. *Виртуальное клонирование карты*

ответственности (global merchant only liability shift) касается всех регионов за исключением США, где ответственность за результат операции по картам американских банков перекладывается на эмитента только в случае поддержки 3D Secure всеми участниками транзакции ЭК – онлайновым магазином, обслуживающим банком, банком-эмитентом и держателем карты (так называемая Full Authentication авторизация).

Напомним, что для CNP-транзакций без использования защищенного протокола ответственность за мошенничество возлагается на обслуживающий банк. Таким образом, в случае использования торговой точкой 3D Secure восстанавливается традиционное распределение ответственности, характерное для платежных операций других типов.

Наиболее серьезной проблемой безопасности протокола 3D Secure является его беззащитность перед атаками типа «man-in the-middle». Например, при использовании держателем карты протокола 3D Secure мошеннические онлайновые магазины могут применять следующую процедуру компрометации пароля держателя карты (см. рис. 1).

Сервер Merchant Plug-In (MPI) мошеннического магазина, получив ответ VERes, содержащий динамический адрес (URL) страницы аутентификации сервера эмитента Access Control Server (ACS), направляет запрос на аутентификацию держателя карты PAReq не по указанному адресу, а на адрес своего SSL-сервера. Затем SSL-сервер перенаправляет данный запрос на URL ACS эмитента карты, тем самым эмулируя для ACS компьютер держателя карты. В результате ACS принимает ложный сервер за персональный компьютер держателя карты и передает на ложный сервер свою страничку, предназначенную для аутентификации держателя карты. Эта страничка содержит сообщение Personal Assurance Message, с помощью которого в схеме 3D Secure клиент аутентифицирует свой банк. Обладая страничкой для аутентификации, мошеннический сервер теперь может играть роль ACS для настоящего клиента банка, запрашивая у последнего значение статического пароля.

Чтобы защититься от подобных краж статических паролей, были предложены различные схемы генерации и использования динамических или, как их еще называют, разовых паролей (One Time Password, OTP). Примером распространенного в банковской сфере алгоритма генерации OTP является метод Chip Authentication Program (CAP) разработанный MasterCard и принятый для использования в Visa под брендом Dynamic Passcode Authentication (DPA).

Для реализации метода CAP клиент должен обладать микропроцессорной картой с EMV-приложением, поддерживающим PIN Offline, а также специальным картридером, способным инициировать генерацию пароля OTP и отображать его значение на дисплее ридера. Стоимость такого ридера может составлять 5–10 евро в зависимости от производителя и объема закупаемой партии устройств. Помимо дополнительных расходов на обеспечение ридерами держателей карт, другим недостатком такого подхода является тот факт, что за картридером клиенту необходимо прийти в банк. Кроме того, для совершения операции ридер нужно иметь под рукой, что не всегда удобно, поскольку размеры устройства значительно превышают размеры банковской карты, и в бумажнике такой ридер не помещается. Впрочем, сегодня на рынке уже предлагаются ультратонкие модели ридеров, позволяющие хранить их в бумажнике вместе с картой.

На начало II квартала 2008 г., по данным MasterCard, в Европе продано 22 млн ридеров, инициирующих генерацию пароля

OTP. Более того, поскольку не все эмитированные микропроцессорные карты поддерживают метод PIN Offline, обсуждается идея расширения алгоритма CAP. В соответствии с данным расширением протокола (Enhanced CAP) каждый ридер будет иметь свое значение ПИН-кода, которое будет сообщаться клиенту при получении им ридера. Таким образом, двухфакторная аутентификация держателя карты станет возможной и в том случае, когда PIN Offline картой не поддерживается.

Украденные/потерянные карты

Люди теряли, теряют и будут терять свои карты. Иногда в таких случаях они утверждают, что карты были украдены. Иногда это соответствует действительности.

Известно, что наиболее эффективным методом борьбы с мошенничеством по потерянным/украденным картам является использование проверки ПИН-кода. Кроме того, не нужно забывать о том, что поддержка картой PIN Offline сегодня пока еще по-прежнему является необходимым условием для использования алгоритма аутентификации CAP (MasterCard Chip Authentication Program и Visa Data Passcode Authentication). Поэтому общая тенденция в решениях МПС – принуждать банки к более широкому применению проверки ПИН-кода и особенно метода PIN Offline, поскольку он является универсальным для онлайновых и офлайновых операций. В результате МПС приняли следующие решения по использованию проверки ПИН-кода:

- С 1 января 2008 г. в регионе VISA CEMEA все online capable терминалы должны поддерживать PIN Offline, а online only терминалы должны поддерживать PIN Online, если они не поддерживают PIN Offline;
- С 1 января 2011 г. в рамках MasterCard по всему миру все новые гибридные терминалы должны поддерживать PIN Offline (более 70% сертифицированных платежной системой моделей терминалов поддерживают PIN Offline).

Виртуальное «клонирование» гибридной карты

Данный метод мошенничества применим к любым картам (SDA, DDA, CDA), в том числе поддерживающим проверку защищенного ПИН-кода. Суть мошенничества состоит в следующем.

Мошенники контролируют терминал в некотором ТСП (например, в ресторане). Одновременно они изготавливают специальную чиповую карту, поддерживающую EMV, стандартный контактный интерфейс в соответствии с ISO 7816 и радиоинтерфейс, работающий в соответствии с одним из распространенных протоколов для радиоканалов на расстоянии от нескольких десятков сантиметров до нескольких метров (например, ISO 15693, ISO 18000). С помощью такого радиоинтерфейса карта может обмениваться данными со специальным оборудованием, которое помимо установления связи с картой обеспечивает организацию удаленного радиоканала (например, в соответствии с протоколом Wi-Max (IEEE 802.16).

Мошенник, вооружившись описанными выше специальной картой и специальным оборудованием, приходит, например, в ювелирный магазин и выбирает украшение стоимостью 2000 евро. В это время в ресторане завершает трапезу ничего не подозревающий держатель карты, которую он предъявляет официанту для оплаты обеда. Официант, являющийся сообщником преступника, посетившего ювелирный магазин, звонит ему и предупреждает, что у него в руках реальная карта. Дальше оба действуют следующим образом. Официант вставляет карту в контролируемый мошенниками терминал, вводит в терминал стоимость обеда и ждет. Мошенник в ювелирном магазине передает кассиру для оплаты украшения свою поддельную карту, которую кассир вставляет в настоящий терминал. Далее все команды терминала через карту мошенника, его специальное оборудование и мошеннический терминал транслируются реальной карте пообедавшего в ресторане господина (см. рис. 2).

При этом некоторые команды требуют преобразования содержащихся в них данных. Например, если реальная карта потребует выполнения проверки ПИН-кода, то мошенник в ювелирном магазине введет на терминале произвольную последовательность, и когда команда будет транслирована на мошеннический терминал, этот терминал затребует ПИН-код реального держателя карты, который введет его, после чего реальная карта посчитает, что аутентификация прошла успешно, и примет соответствующее решение по продолжению обработки транзакции.

Очевидно, что помехой для успешного выполнения мошеннической транзакции не является и проведение операции в онлайновом режиме. В этом случае реальная карта сгенерирует ARQC, который будет передан на хост эмитента, и, наоборот, ответ эмитента (Issuer Authentication Data) будет транслирован по радиоинтерфейсу на мошеннический терминал для передачи этих данных реальной карте.

Результат такого виртуального «клонирования» может оказаться весьма печален для держателя реальной карты. Если у него в данный момент было достаточно средств на счете, 2000 евро будут со счета дебетованы. При этом он получит чек на стоимость обеда и, вероятнее всего, будет находиться в неведении о случившемся до получения справки о состоянии своего банковского счета в конце месяца.

Шансы вовремя распознать мошенничество повышаются для господина из ресторана, если эмитент его карты предоставляет услугу SMS-уведомления о выполненных операциях. Впрочем, последняя эффективно работает только в том случае, если операция была выполнена в онлайновом режиме.

Если проанализировать описанную выше ситуацию, то станет ясно: мошенничество оказалось возможным из-за отсутствия прямого взаимодействия (диалога) держателя карты и самой карты.

Действительно, в идеальном случае держатель должен был бы «ввести» не-

посредственно на карте реквизиты операции, и карта (возможно, с участием эмитента) приняла бы решение о том, может ли держатель получить интересующие его услугу/товар или нет. Но между держателем и картой всегда стоит посредник – терминал, который может исказить информацию об операции таким образом, что держатель карты в процессе обработки операции этого не заметит. Этот посредник, помимо прочего, может и украсть важную информацию карты, включая ПИН-код ее держателя.

Другими словами, проблему можно решить, если организовать прямой надежный канал взаимодействия между картой и ее держателем (т. н. Customer Trustworthy Channel). Реализовать это можно несколькими способами. Например, предоставить в распоряжение держателя карты простейшее устройство, имеющее, с одной стороны, контактную площадку стандартной смарт-карты, а с другой – ридер для работы со смарт-картой. Такое устройство может обладать экраном и клавишами для ввода ПИН-кода. Экран используется для отображения суммы и валюты транзакции, данные о которых отправляются терминалом карте, а клавиши – для того, чтобы клиент мог ввести свой ПИН-код не на терминале, а на личном устройстве, которому держатель карты доверяет. В предлагаемом решении устройство должно уметь по поручению терминала выполнять верификацию держателя карты по его ПИН-коду в офлайновом режиме (PIN Offline), для чего оно должно поддерживать выполнение команд Get Challenge и Verify. Кроме того, устройство должно в команде Generate AC к данным команды добавлять криптографическую хэш-функцию (для этого используется ключ, известный карте и устройству) от размера операции и случайного числа карты, полученного с помощью команды Get Challenge. Тогда карта, получив от терминала команду Generate AC, проверит значение хэш-функции и после этого стандартным образом обработает полученную команду.

К сожалению, реализация подобного решения потребует небольшого изменения стандарта EMV как на стороне карты, так и на стороне терминала.

Очевидно, имей держатель реальной карты в своем распоряжении подобное устройство, описанный выше «ресторанно-ювелирный» фрод оказался бы невозможен. У мошенника в магазине нет устройства, необходимого для использования карты, а использовать значение криптографической функции, сгенерированное реальным держателем карты, не получится, поскольку оно соответствует другому значению суммы транзакции.

Другое решение состоит в использовании ридеров, которые выполняют двухфакторную аутентификацию держателя карты и генерируют криптографический токен как функцию от размера транзакции и номера транзакции. В этом случае приложение карты должно проверить значение токена. Для генерации токена используется отдельный ключ, отличный от ключа карты для генерации криптограммы. Преимущество этого метода заключается в том, что верификация держателя выполняется и на терминалах, не имеющих ПИН-пада. Для реализации метода также требуется незначительное изменение стандарта EMV.

Можно предложить и другие варианты, например, когда роль ридера играет сотовый телефон со специально загруженным на него мидлетом, и т. д. У всех этих методов имеется один общий принцип. На руках у держателя карты должно быть устройство, которому он доверяет (оно выдано банком держателя и постоянно находится под его контролем) и которое обладает разделяемым с картой секретом. С помощью этого секрета устройство (и только оно) способно сгенерировать некоторую криптовеличину, которую карта может проверить. Тот факт, что криптовеличину может сгенерировать только предоставленное держателю устройство, гарантирует, что транзакцию совершил держатель карты. Тот факт, что устройство находится под контролем держателя, гарантирует, что введенные через него значения размера транзакции и ПИН-кода держателя не будут модифицированы/украдены.

В последнее время появились карты с крошечным цифровым экраном (display equipped cards), которые также могут частично решить описанную выше проблему. Однако стоимость таких карт, надежность их работы и отсутствие клавиатуры все еще препятствуют широкому распространению данной инновации.

Модификация диалога карты и терминала

Виртуальное «клонирование» карты является хитроумным примером модификации диалога карты и терминала. Существуют другие, более простые схемы модификации диалога карты и терминала, обеспечивающие проведение мошеннической транзакции. Самая простая и известная схема – «схема с двумя чипами». При применении этой схемы мошенники используют печатную плату с двумя чипами: один чип – банковский, а второй – так называемый чип-посредник. Чип-посредник контролирует обмен данными между банковским чипом и терминалом, при необходимости модифицируя диалог карты с терминалом (например, изменяет размер транзакции, результат проверки PIN Offline, значение Cryptogram Information Data в ответе на команду Generate AC). Чип-посредник принято еще называть wedge device, он может располагаться не только на карте, но и на POS-терминале.

Для защиты диалога карты и терминала используются два метода:

- метод подписи чувствительных с точки зрения важности статических данных карты;
- метод CDA.

Как подробно рассказано в моей книге [1], суть CDA состоит в следующем. Приложением карты с использованием закрытого ключа для офлайновой аутентификации приложения формируется подпись в ответе на команду Generate AC под

данными, включающими в себя IDN (ICC Dynamic Data), CID (Cryptogram Information Data), криптограмму, хэш-функцию от данных PDOL, CDOL1, CDOL2, ответа на CDOL1. Таким образом, имеется возможность проверить целостность CID и реквизитов транзакции (размер транзакции, валюта транзакции и т.п.) непосредственно приложением терминала. Если проверка подписи терминалом по каким-либо причинам «провалилась» (failed), транзакция отвергается на уровне терминала.

Важно понимать, что метод CDA обеспечивает целостность обмена транзакционными данными, которыми терминал и карта обмениваются при обработке команд Get Processing Options и Generate AC. Целостность данных, читаемых терминалом с помощью команд Read Record, обеспечивается механизмом статической подписи наиболее важных данных приложения, например, объектов данных Application Usage Control, CDOL1,CDOL2, CVM List, AIP и т. п. Например, если объект CVM List не входит в список подписываемых данных, то при его чтении терминалом он может быть модифицирован с помощью wedge device. В результате, например, вместо метода верификации держателя PIN Offline будет использоваться обычная подпись держателя карточки на чеке, что очевидно снижает безопасность операций по такой карте. Например, мошенник может воспользоваться украденной картой, в которой PIN Offline является приоритетным способом верификации держателя карты, используя ее чип в схеме «атака двумя чипами» и изменяя CVM List при чтении данных терминалом (повторюсь, CDA не защищает данные команды Read Record).

Сегодня используются два механизма подписи статических данных: если карта поддерживает SDA, то имеется отдельный объект данных, представляющий собой подпись чувствительных данных приложения. Если же карта поддерживает методы офлайновой динамической аутентификации (DDA, CDA), то чувствительные данные подписываются в рамках сертификата открытого ключа карты и, возможно, в виде описанного выше отдельного объекта данных.

У метода CDA имеются следующие важные ограничения:

- Модуль ключа карты при использовании CDA может быть ограничен сверху 205 байтами;
- Если на терминале отсутствует ключ платежной системы, с использованием которого создан сертификат ключа эмитента карты, то все операции по этой карте будут отклоняться в данном терминале.

ПЛАС

О таких методах мошенничества в сфере обслуживания карт, как ложный ключ МПС, подмена POS-терминала и т. д., а также о современной ситуации в области противостояния фроду читайте во второй части материала Игоря Голдовского в следующем номере журнала «ПЛАС».

[1] **Голдовский И. М.** Микропроцессорные карты стандарта EMV. – М.: Издательская группа «БДЦ-Пресс», 2006.– 544 с.

КАЛЕЙДОСКОП

Харьковский метрополитен выпустит 300 тыс. бесконтактных карт

В 2009 г. руководство Харьковского метрополитена планирует вдвое увеличить количество бесконтактных карт, находящихся в обороте. На сегодняшний день электронными картами пользуется 25% пассажиров метро (порядка 150 тыс. карт в обороте). В I квартале 2009 г. также планируется внедрить универсальные автоматы для пополнения счета электронной карты, которые позволят осуществлять и другие электронные платежи. Автоматами будут оснащены станции с наибольшим пассажиропотоком. Бесконтактные карты были введены в Харьковском метро летом 2007 г.

INPAS модернизирует продуктовый ряд ПИН-падов, предлагаемых в России и СНГ

За прошедшие 6 лет основная модель интеллектуального ПИН-пада VeriFone SC5000 несколько раз обновлялась в соответствии с требованиями международных платежных систем. ПИН-пады SC5000 установлены в России более чем в 140 тыс. точек и обслуживают карты с магнитной полосой и микропроцессором. Однако в настоящее время уровень развития эквайринговых услуг в России потребовал новых возможностей как от самих устройств, так и от работающего на них программного обеспечения. В ответ на возросший уровень требований INPAS выводит на рынок новый ПИН-пад Vx810 и завершает продажи ПИН-пада SC5000 в апреле 2009 г.

Новый продукт VeriFone Vx810 построен на платформе Vx Solutions и пользуется всеми возможностями безопасной защищенной операционной системы Verix V. Благодаря общей с терминалами платформе Verix V банки и эквайеры могут быстро и с минимальными затратами интегрировать Vx810 в сеть по приему пластиковых карт.

Vx810 впервые в линии ПИН-падов VeriFone предоставляет широкие возможности подключения – последовательный порт, USB или, опционально, Ethernet. Таким образом, торговая точка может подключить ПИН-пад к терминалу, кассе, компьютеру или локальной сети, обеспечивая максимальную гибкость подключения и удобство в работе. Порт расширения Secure Digital Input/Output (SDIO) обеспечивает простой путь наращивания конфигурации – например, присоединение модуля для бесконтактной оплаты – без отправки устройства на завод-изготовитель.