Ещё раз о фроде...

Часть II. Мошенничество в сфере обслуживания карт

Игорь Голдовский, генеральный директор ЗАО «Платёжные технологии»

Ложный ключ МПС

Одной из серьёзных «дыр» в модели безопасности операций, выполненных с использованием микропроцессорной карты, является практическая возможность заведения мошенниками в POS-терминал ложного открытого ключа платёжной системы. Изготовив под ложным ключом сертификаты ключа «мнимого» эмитента, далее можно выпустить поддельные карты, которые будут успешно работать в терминалах с загруженным в них ложным ключом.

Естественным способом борьбы с такого рода мошенничеством является создание подписи вводимых в терминал ключей платёжной системы на ключе обслуживающего банка (возможно, на симметричном ключе). Такая подпись обеспечивает целостность ключевой информации системы на терминале. В этом случае, не обладая ключом обслуживающего банка, невозможно успешно завести/использовать ложный открытый ключ системы на терминале.

К сожалению, чтобы обойти упомянутую защиту открытых ключей системы, преступник может и не идти по пути компрометации секретного ключа обслуживающего банка. Для совершения мошенничества ему достаточно загрузить на терминал фальшивый исполняемый модуль, который в отличие от приложения обслуживающего банка не станет проверять подпись используемого ключа. В этом случае описанная выше защита не работает.

Чтобы лишить мошенника возможности замены приложения терминала, требуется подключить ресурсы операционной системы и криптопроцессора терминала. Мы не будем останавливаться здесь на проблеме обеспечения целостности приложения терминала. Отметим только, что для терминалов, принимающих микропроцессорные карты, эта проблема решается с использованием специальной микропроцессорной карты, выполняющей функцию контроля доступа к операциям, например, удаления/загрузки исполняемых файлов.

В то же время заметим, что проблема обеспечения целостности приложения терминала не является надуманной. По мнению экспертов в области безопасности карточных операций, по мере повышения защищенности карт внимание мошенников во всевозрастающей степени будет обращаться на среду их обслуживания. Терминал является близким окружением карты и потому, несомненно, станет мишенью для атак. Поскольку терминал сегодня фактически представляет собой персональный компьютер, то для атак будут использоваться те же методы, что и в случае PC. В частности, применение специальных программ (аналог программ spyware, Trojan horse, keyboard/screen logger, вирусов) позволит мошеннику получать интересующую его информацию о карте (например, запись второй дорожки магнитной полосы карты, значение случайной последовательности терминала и случайного числа карты, используемых для шифрования ПИН-блока, значение зашифрованного ПИН-блока и т. п.).

Подмена POS-терминала

Важна также и проблема подмены настоящего POS-терминала банка терминалом, установленным мошенниками, к которой мы уже обращались*. Стоимость терминала невелика – 400–600 долл. Поэтому подобная подмена является весьма правдоподобной при сговоре мошенника с кассиром торгового предприятия (известны случаи установки даже ложных банкоматов!). Возможны также случаи, когда мошенническое торговое предприятие использует конкретный POS-терминал только с целью сбора информации о картах.

В случае применения ложного терминала может записываться не только содержимое

* См. первую часть материала Игоря Голдовского «Ещё раз о фроде… Мошенничество в сфере эмиссии карт», ПЛАС № 1/2009.

магнитной дорожки карты, но и значение ПИН-кода держателя карты. С учётом использования на практике гибридных карт, имеющих магнитную полосу, получив информацию о магнитной дорожке карты и значение ПИН-кода, мошенник может изготовить «белые» карты для их использования в банкомате. Для решения проблемы ложного терминала при обработке операций в онлайновом режиме необходимо повсеместно внедрять коды MAC для сообщений, циркулирующих между терминалом и хостом обслуживающего банка. Это обеспечит целостность информационного обмена и аутентификацию POS-терминала.

Между тем использование кодов MAC позволяет эффективно решить проблему только для онлайновых операций. Информация об офлайновых транзакциях, выполненных на терминале, также может подписываться для передачи в обслуживающий банк. Однако мошеннический терминал может и не передавать информацию о транзакциях в банк достаточно долго или вообще никогда. В случае, когда терминал действует в офлайновом режиме, к сожалению, кроме организационных мер для борьбы с подобного рода мошенничествами, предложить пока нечего.

Достаточно эффективным способом борьбы с подменой терминалов стало бы введение в стандарт EMV процедуры взаимной аутентификации карты и терминала. Заведение в терминал пары секретного и открытого асимметричных ключей обслуживающего банка и сертификата этого ключа на ключе платёжной системы, а также поддержка картой процедуры аутентификации терминала и хранение на карте хэш-функций открытых ключей системы стало бы хорошим решением проблемы подмены терминала. Хранение на карте хэш-функций открытых ключей системы необходимо для того, чтобы избежать ситуации, когда мошенник сам придумывает ложный ключ системы и генерирует для заведения в терминал пару ключей обслуживающего банка с сертификатом, вычисленным на ложном ключе системы.

Конечно, хранение хэш-функций ключей системы (очевидно, что придется хранить информацию о ключах, сгенерированных впрок, чтобы не получилось так, что во время жизненного цикла карты на терминалах появятся ключи системы, неизвестные карте) предъявляет повышенные требования к размеру памяти EEPROM. Терминал должен хранить до 6 ключей системы. Поэтому с учетом ключей, заводимых впрок, и размера значения хэш-функции SHA-1, равного 20 байтам, потребуется зарезервировать около 200 байтов памяти EEPROM для одного приложения одной платёжной системы.

Для процедуры аутентификации терминала крайне важной является проблема формирования CRL-листов (Certificate Revocation List) и их распространения. Очевидно, хранить такие листы на карте не получится. Функция контроля таких листов должна быть возложена на обслуживающий банк и в данном случае – включать в себя выезд сотрудников банка на место работы терминала с целью изъятия терминала/ замены в нем ключей.

Некорректная реализация процедуры проверки PIN Offline

Об этом виде мошенничества подробно рассказано в моей книге[1]. Случайная последовательность, генерируемая терминалом и добавляемая к ПИН-блоку до его шифрования, должна быть закрытой для терминала (последовательность должна генерироваться модулем безопасности терминала). В противном случае возможно вскрытие ПИН-кода методом перебора возможных значений ПИН-кода с помощью Code Book Attack.

Подделка типа криптограммы

Рассмотрим еще один вид мошенничества со стороны недобросовестного торгового предприятия. В упрощенном виде он выглядит следующим образом.

Когда в мошенническое ТСП обращается за покупкой держатель микропроцессорной карты, ТСП завершает любое решение терминала/карты отклонением транзакции. При этом держатель карты либо уходит из торгового предприятия ни с чем, либо расплачивается за товар наличными.

Далее мошенническое ТСП отправляет обслуживающему банку данные по неуспешной транзакции как данные об операции, выполненной успешно в офлайновом режиме. При этом обслуживающему банку предъявляются все доказательства того, что транзакция была выполнена успешно: подделанное значение Cryptogram Information Data, указывающее на завершение операции генерацией картой криптограммы TC, значение криптограммы (независимо от ее типа – TC, ARQC, AAC), значение ICC Dynamic Number. Все эти данные (за исключением Cryptogram Information Data) могли быть сформированы только реальной микропроцессорной картой.

Обслуживающий банк на основе полученных данных формирует презентменты, которые отправляет в платёжную систему, и возмещает торговому предприятию средства по «выполненным» в нем операциям.

Через некоторое время отдельные держатели карт инициируют chargeback по мошенническим операциям, выполненным с использованием их карт. Однако эмитенту будет сложно их инициировать, поскольку обслуживающий банк предъявил в презентменте или по запросу эмитента (сообщение retrieval request) криптограмму TC.

В данном случае разобраться в ситуации поможет платёжная система, которая через некоторое время обнаружит, что возникшая странная ситуация (клиенты жалуются, но клиринговые сообщения, переданные обслуживающим банком, выглядят убедительно) необыкновенно часто случается в одной и той же конкретной торговой точке. Однако чтобы расследовать каждый прецедент, платёжной системе потребуется время. За это время мошенническое предприятие успеет скрыться.

Другой способ борьбы с описанным выше мошенничеством – использование метода CDA для офлайновой аутентификации приложения карты и принятие МПС

требования к торговому предприятию, которое состояло бы в следующем: ТСП должно предоставлять в распоряжение обслуживающего банка элемент Signed Dynamic Application Data, а не просто криптограмму. В этом случае обслуживающий банк извлекает из элемента Signed Dynamic Application Data правильное значение объекта Cryptogram Information Data, и описанная ранее схема мошенничества перестанет работать.

Вместо послесловия

Резюмируя сказанное выше, можно сделать вывод о том, что с увеличением количества микропроцессорных карт и расширением инфраструктуры их приёма уровень карточного фрода (но отнюдь не его объем!) будет неукоснительно снижаться. Использование микропроцессорной технологии доказало свою высокую эффективность с точки зрения борьбы с мошенничеством. Великобритания, осуществившая практически полную миграцию на технологию чиповых карт, поддерживающих офлайновую проверку ПИН-кода, стала ярким тому примером.

С точки зрения технологий МПС проводят активную политику, направленную на максимально возможное повышение безопасности карточных операций. В зависимости от текущего состояния зрелости карточного рынка принимаются упреждающие решения, целью которых является уменьшение уровня карточного мошенничества. Именно к таким решениям следует отнести последние шаги МПС по расширению применения надежных методов аутентификации карты, использованию PIN Offline на картах и терминалах, оптимизацию правил перехода на альтернативную авторизацию по магнитной полосе и т. п.

В то же время вполне очевидно, что криминальные структуры не смирятся с потерей своих доходов от карточного мошенничества и будут адаптироваться к новым «условиям игры» в мире чиповых карт. К сожалению, для этого у них остается немало возможностей.

Самой серьёзной брешью в технологии микропроцессорных карт остается отсутствие синхронности и должных темпов миграции банков на чип. Даже если банки какой-либо страны полностью мигрируют на чип, но при этом останутся страны, где данный процесс идет медленно, мигрировавшие на чип банки будут страдать от деятельности мошенников в менее продвинутых с точки зрения миграции странах. Поэтому европейские страны, достигшие значительных результатов в миграции на чип, не может не беспокоить ситуация с положением дел в некоторых регионах и особенно в США. Действительно, все усилия европейского банка, выпустившего микропроцессорную карту, аннулируются возможностью выполнения операции по мошеннической карте, изготовленной на основе данных магнитной полосы этой микропроцессорной карты в магнитном терминале американского банка. Здесь МПС должны действовать более жёстко и решительно, управляя Chip Liability Shift внутри регионов и между регионами, а также заставляя банки внедрять разные межбанковские комиссии в зависимости от способности участников операции поддерживать микропроцессорную технологию. ПЛАС

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

КАЛЕЙДОСКОП

ЛАНИТ: модернизация банкоматов в соответствии с EMV-требованиями

ЛАНИТ продолжает реализацию проекта по модернизации банкоматов Diebold серии iX в соответствии с EMV-требованиями. Проект модернизации банкоматов Diebold iX, стартовавший в 2003 г., вступил в заключительную стадию. Она предусматривает установку на банкоматы нового программного обеспечения «Agilis XV IX + Windows», которое позволяет обслуживать чиповые карты клиентов. В ходе модернизации операционная система банкоматов меняется с OS/2 на Windows, а прикладное программное обеспечение TCS – на специальную версию Agilis для банкоматов серии iX.

Основные разделы нового прикладного ПО банкоматов серии iX унифицированы с ПО банкоматов серии Opteva. По мнению разработчика, это позволит значительно упростить эксплуатацию банкоматов серий iX и Opteva. Стоит отметить, что проведение заключительного этапа модернизации банкоматов позволит банкам довести функциональные возможности их парка оборудования Diebold серии iX до уровня банкоматов Diebold Opteva с минимальными дополнительными затратами.

В ходе первых двух этапов проекта была проведена большая подготовительная работа. По требованию производителя при проведении модернизации были заменены следующие узлы банкоматов:

- Клиентская клавиатура заменялась на EPP4.
- Картридер для работы только с магнитной полосой менялся на EMV-ридеры Sankyo моделей 101861E или 101861F.
- Заменялись системные блоки с тактовой частотой ниже 566 Мгц. Для работы с программным обеспечением, поддерживающим EMV-приложения, требуются системные блоки банкоматов с тактовыми частотами процессора G5-566 Мгц., G5-866 Мгц., HTP-700 Мгц., G5t-1200 Мгц.
- Объем оперативной памяти увеличивался до 512 Мб.