Ученые записки Таврического национального университета имени В.И. Вернадского
Серия «Экономика и управление». Том 27 (66). 2014 г. № 4. С. 39-43.

УДК 004.056.5

АЛГОРИТМЫ ИДЕНТИФИКАЦИИ ПЛАТЕЖНЫХ КАРТ

Бойченко О.В., Знаменская Ю. А.

Таврический национальный университет имени В.И. Вернадского, Симферополь, Республика Крым
E-mail: bolek61@mail.ru

В статье рассматриваются современные проблемы идентификации платежных карт в решении задачи безопасности электронной коммерции. Проанализированы основные методики использования PIN-кода для идентификации владельца карты. Предложен перечень требований к схемам проведения транзакции ЭК, обеспечивающим необходимый уровень ее безопасности.
Ключевые слова: платежные карты, идентификация, электронная коммерция, транзакция, безопасность.

ВВЕДЕНИЕ

Для России киберпреступность характеризуется не только возможностью мошенников для скорого обогащения, но и их способностью довольно хорошо скрывать преступные действия, что делает данный вид преступной деятельности практически ненаказуемым.

Арсенал хакеров для обхода существующих систем безопасности становится все долее изощренным, а вредоносные программы направленного действия, обеспечивающие несанкционированный доступ к конфиденциальной информации и распространения вирусов, легко преодолевают любую сигнатурную систему защиты.

Так, согласно отчетам Европейского агентства по сетевой и информационной безопасности (ENISA) и сведениям Европейской группы по безопасности банкоматов (EAST), только в 2009 г. количество преступлений со взломом банкоматов увеличилось на 149% по сравнению с предыдущим годом. Проблему обостряет то, что традиционные скимминговые атаки постепенно заменяются атаками с использованием специальных вредоносных программ, направленных как на сети банкоматов, так и по сами банкоматы [1].

Кроме того, существенное повышение риска уязвимостей электронной коммерции (ЭК) создает переход от закрытых систем обработки транзакций к открытым. Это приводит к неосуществимости частых обновлений и перезагрузки системы для работы традиционных средств защиты от вредоносных программ в целях обеспечения непрерывной защиты в автоматических системах, таких как банкоматы, кассовые терминалы, системы электронного голосования.

Отдельные вопросы проблематики безопасности транзакций ЭК в вопросах безопасности платежей в Интернет и разработке стандартов безопасности ЭК в Интернет рассматривались в работах таких ученых как Баутов А., Голдовский И., Скородумов Б. и других [3].

Однако, решение проблемы безопасности схем проведения транзакции ЭК является достаточно актуальной задачей современности, что требует проведения дальнейших научных исследований.

Цель исследования состоит в анализе проблематики схем транзакций электронной коммерции и разработке требований к схемам проведения транзакции ЭК, обеспечивающим необходимый уровень ее безопасности.

ИЗЛОЖЕНИЕ ОСНОВНОГО МАТЕРИАЛА

С самого начала внедрения ЭК стало очевидно, что методы идентификации владельца карты, применяемые в обычных транзакциях, являются неудовлетворительными для транзакций ЭК.

В мире пластиковых карт с магнитной полосой самым надежным способом защиты транзакции от мошенничества является использование PIN-кода для идентификации владельца карты его банком-эмитентом.

Секретной информацией, которой обладает владелец карты, является PIN-код, предстающий собой последовательность, состоящую из 4-12 цифр, известную только владельцу карты и его банку-эмитенту.

Более того, общая тенденция развития платежных систем – более активное использование PIN-кода для операций «покупка» по дебетовым картам. Казалось бы, использование подобного идентификатора могло бы помочь решить проблему безопасности в ЭК, однако в приложении к ЭК этот метод в классическом виде неприменим.

Это связано с тем, что использование PIN-кода должно производиться таким образом, чтобы этот секретный параметр на всех этапах обработки транзакции оставался зашифрованным (PIN-код должен быть известен только владельцу карты и ее эмитенту) [2].

Данное требование реализуется за счет использования в устройствах ввода транзакции специальных физических устройств, называемых PIN-PAD и содержащих Hardware Security Module (аппаратно-программные устройства, позволяющие хранить и преобразовывать некоторую информацию весьма надежным способом). Эти устройства хранят специальным способом защищенный секретный коммуникационный ключ, сгенерированный обслуживающим банком данного торгового предприятия (ТП). Когда владелец карты вводит значение PIN-кода, оно немедленно закрывается (шифруется) коммуникационным ключом и отправляется внутри авторизационного запроса на хост обслуживающего банка.

Точнее говоря, шифруется не сам PIN-код, а некоторый электронный «конверт», в который код помещается. На хосте обслуживающего банка зашифрованный идентификационный код перекодируется внутри Hardware Security Module хоста (хост обслуживающего банка также имеет свое устройство шифрования) в блок, зашифрованный на коммуникационном ключе платежной системы, и передается в сеть для дальнейшего предъявления эмитенту. Однако, для того чтобы следовать классической схеме обработки PIN-кода, каждый владелец карты должен хранить криптограммы коммуникационных ключей всех обслуживающих банков, что на практике невозможно [3].

Классическую схему можно было бы реализовать с помощью применения асимметричных алгоритмов с шифрованием PIN-кода владельца карты открытым

ключом ТП. Но для представления PIN-кода в платежную сеть его необходимо зашифровать, как это принято во всех платежных системах, симметричным ключом.

Однако, на сегодняшний день, проблематичным является решение задачи выполнения трансляции PIN-кода, зашифрованного с помощью асимметричного криптоалгоритма, в PIN-код, зашифрованный на симметричном алгоритме шифрования по технологии стандартного Hardware Security Module .

Существует другое, неклассическое решение по использованию PIN-кода. Например, можно на компьютере владельца карты шифровать PIN-код и некоторые динамически меняющиеся от транзакции к транзакции данные на ключе, известном только эмитенту и владельцу карты.

Такой подход потребует решения задачи распределения секретных ключей, что является весьма непростой задачей, решение которой имеет смысл для других, более эффективных, по сравнению с проверкой PIN-кода, методов идентификации владельца карты.

Альтернативой является методика проверки PIN-кода для повышения безопасности транзакций ЭК по картам, базы данных (БД) которых хранятся на хосте процессора STB CARD [4].

В общих чертах STB CARD реализует следующую схему:

1. Владельцы карт, эмитенты которых держат свою БД карточек на хосте STB CARD, могут получить дополнительный PIN-код, называемый ПИН2. Этот код представляет собой последовательность из 16 шестнадцатеричных цифр, которая распечатывается в PIN-конверте, передаваемом владельцу карты (специальный бумажный конверт, используемый банком-эмитентом для хранения в нем секретной информации, относящейся к эмитированной карте). ПИН2 вычисляется эмитентом с помощью симметричного алгоритма шифрования, примененного к номеру карты и использующего секретный ключ, известный только эмитенту карты.

2. Во время проведения транзакции ЭК на одном из ТП, обслуживаемом банком STB CARD, у владельца карты в процессе получения данных о клиенте запрашивается информация по ПИН2. Клиент вводит значение кода ПИН2 в заполняемую форму и возвращает ее ТП (владелец карты в действительности ведет диалог в защищенной SSL-сессии не с ТП, а с виртуальным POS-сервером, через который работает ТП (система STB CARD на сервере Assist). При этом ПИН2 играет роль секретного ключа этого алгоритма шифрования, а шифруемые данные получаются в результате применения хэш-функции к номеру карты, сумме и дате транзакции, а также случайному числу £,, генерируемому ТП. Таким образом, в заполненной владельцем карты форме присутствует только результат шифрования перечисленных выше данных о транзакции на ключе ПИН2.

3. ТП формирует авторизационное сообщение, передаваемое на хост обслуживающего банка, содержащее помимо «стандартных» данных о транзакции еще результат шифрования и случайное число £,.

4. Эмитент карты, получив сообщение ТП, по номеру карты вычисляет значение ПИН2, и далее по номеру карты, сумме и дате транзакции, а также по случайному числу %, вычисляет результат шифрования этих данных на ключе ПИН2. Если полученная величина совпадает с аналогичной величиной из

сообщения ТП, верификация PIN-кода считается выполненной успешно. В противном случае транзакция отвергается.

В результате технология проверки PIN-кода, принятая в системе STB CARD, в действительности обеспечивает не только динамическую аутентификацию клиента, но еще и гарантирует «сквозную» целостность некоторых данных о транзакции (сумма транзакции, номер карты).

Методика STB CARD довольно стабильна в решении проблем безопасности транзакций ЭК по картам, однако характеризуется рядом недостатков:

1. Сужение области применения STB CARD в относительно небольшом множестве ТП ввиду того, что для реализации схемы проверки значения PIN-кода необходимо четкое формирование ТП соответствующей формы с Java-апплетом;
2. Использование длинного (шестнадцать шестнадцатеричных цифр) ключа, что делает его применение на практике крайне неудобным для владельца карты.
3. Низкая эффективность защиты от подставки (форма, запрашивающая ПИН2, предоставляется владельцу карты не ТП, а мошенником, желающим узнать значение ПИН2), которая основана на надежности аутентификации клиентом сервера ТП, а также на подписании апплета секретным ключом сервера ТП.

Решение проблемы надежной защиты от подставки обеспечивает электронный бумажник клиента на основе специального программного обеспечения, заменяющего по своей функциональности Java-апплет в форме ТП. Такой электронный бумажник может использовать сколь угодно мощные средства шифрования данных, а секретные ключи владельца карты могут держаться в порядке повышения надежности их хранения на диске компьютера, дискете или микропроцессорной карте [5].

ВЫВОДЫ

В результате проведенного анализа сформированы основные требования к схемам проведения транзакции ЭК, обеспечивающим необходимый уровень ее безопасности.

Эти требования сводятся к следующему:

1. Аутентификация участников покупки (покупателя, ТП и его обслуживающего банка). Под аутентификацией покупателя (продавца) понимается процедура, доказывающая (на уровне надежности известных криптоалгоритмов) факт того, что данный владелец карты действительно является клиентом некоторого эмитента-участника (обслуживающего банка-участника) данной платежной системы. Аутентификация обслуживающего банка доказывает факт того, что банк является участником данной платежной системы;

2. Реквизиты платежной карты (номер карты, срок ее действия, CVC2/ CVV2 и т.п.), используемой при проведении транзакции ЭК, должны быть конфиденциальными для ТП;

3. Невозможность отказа от транзакции для всех участников транзакции ЭК, то есть наличие у всех участников неоспоримого доказательства факта совершения покупки (заказа или оплаты).

Полученные результаты могут быть использованы для проведения дальнейших научных исследований в разработке требований к безопасным схемам проведения транзакций ЭК.

Список литературы

1. Калиниченко М. Эффективная защита информационной среды банкоматов: будущее за проактивными технологиями / М. Калиниченко // Information Security. – 2010. - № 3. - [Электронный ресурс]. – Режим доступа: http://www.itsec.ru
2. Голдовский И. Безопасность платежей в Интернете / И. Голдовский. – С-Пб: Питер, 2006. – 240 с.
3. Скородумов Б.И. Стандарты для безопасности электронной коммерции в сети Интернет / Б.И. Скородумов // [Электронный ресурс]. – Режим доступа: http://www.bre.ru/security/21627.html
4. Баутов А. Эффективность защиты информации / А. Баутов // [Электронный ресурс]. – Режим доступа: http://www.bre.ru/security/19165.html
5. Бойченко О.В. Проблемы информационной безопасности платежных средств / О.В. Бойченко // Ученые записки Таврического национального университета им. В.И. Вернадского. – Симферополь, 2014. - Т. 27(66). – № 1. – С.12-17.

Статья поступила в редакцию 11. 11. 2014 г