Обзор протоколов безопасного осуществления транзакций в электронной торговле

Кузнецов Алексей Игоревич, 9.04.2005

Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

В наше время отрасль, связанная с электронной коммерцией, переживает настоящий бум. Тому есть несколько причин, но основная – это уникальная возможность представить товар или услугу перед необходимой целевой аудиторией, минимизировав при этом накладные расходы. Основное техническое препятствие на пути развития электронной торговли – необходимость обеспечить конфиденциальность и безопасность платежей, как для покупателя, так и для продавца. Очевидно, что безопасность осуществления сделок (транзакций) неразрывно связана с риском, который берут на себя участники операции, и, следовательно, влияет на размер этого рынка.

До создания протоколов, осуществляющих шифрование передаваемой информации на основе асимметричных алгоритмов, данные, необходимые для оплаты, приходилось передавать открытым текстом, что представляло собой значительную угрозу их перехвата, изменения или подделки при передаче по незащищенным каналам (например, по сети Интернет).

Первым из достаточно распространённых протоколов, которые изменили ситуацию к лучшему, стал SSL (Secure Socket Layer). Это универсальный протокол, применяемый не только в электронной торговле. Являясь протоколом транспортного уровня, он не привязывается к конкретному протоколу уровня приложения, поэтому может шифровать, например, как данные HTTP (протокол HTTP, работающий поверх SSL, называется HTTPS), так и данные других протоколов. SSL решает несколько задач:

- обеспечение конфиденциальности сообщения (даже если злоумышленник перехватит его на пути от клиента к серверу, он не сможет его прочитать);
- обеспечение целостности сообщения (злоумышленник не может изменить сообщение);
- аутентификация сторон (злоумышленник не может обмануть клиента, представившись сервером).

Конфиденциальность в SSL обеспечивается шифрованием передаваемых данных с помощью симметричных алгоритмов (DES, Triple-DES, RC4), при этом ключ шифруется открытыми ключами участников сделки по алгоритму RSA, либо формируется посредством алгоритма открытого распределения ключей Диффи-Хеллмана (Diffie-Hellman). Целостность сообщения достигается использованием криптографических хеш-функций (MD5, SHA-1), а аутентификация – использованием сертификатов, подписанных доверенными организациями.

Протокол SSL предоставляет необходимый минимум для осуществления электронных сделок, однако, с ним связаны две проблемы:

- в то время как подлинность продавца проверяется с помощью сертификата, невозможно определить подлинность покупателя;

- секретные данные, необходимые для осуществления платежа, становятся доступными продавцу. В случае использования кредитной карты нет никакой гарантии, что он не снимет со счета больше денег, чем нужно.

Эти недостатки привели к появлению протоколов, специально созданных для электронной торговли. Наиболее распространенные из них можно условно подразделить на следующие категории:

- системы осуществления электронных платежей по кредитной карте;
- «электронные монеты».

Эти два подхода различаются как по технологии защиты платежа, так и по целевому рынку. Первые являются полноценными криптографическими протоколами с аутентификацией сторон и ограничением доступа участников к данным кредитной карты. Однако, платеж с помощью кредитной карты представляет определенный риск, поэтому данная схема обычно используется при крупных переводах.

«Электронные монеты», применяемые в основном при мелких операциях, обычно представляют собой токены, подписанные эмитентами. Каждый токен имеет определенный номинал. При платеже покупатель передает его продавцу, тот проверяет его цифровую подпись и затем представляет к оплате организации, его выпустившей. При этом эмитент заносит серийный номер токена в свою базу как «погашенный», чтобы предотвратить повторное использование.

Далее мы рассмотрим несколько примеров протоколов обоих видов, обращая особое внимание на их отличия друг от друга.

SET

SET (Secure Electronic Transactions) является, по-видимому, одним из наиболее широко известных и применяемых протоколов осуществления электронных платежей по кредитной карте. Он был разработан компаниями Visa и MasterCard. Протокол описывает механизм взаимодействия между четырьмя субъектами:

- покупатель (cardholder);
- продавец (merchant);
- банк покупателя (issuer);
- организация, обеспечивающая связь продавца с банком получателя, обычно банк продавца, используемая как шлюз платежей (payment gateway).

Процесс оплаты состоит из трех частей: покупка (purchase process), авторизация платежа (payment authorization) и осуществление платежа (payment capture). Протокол устроен таким образом, что продавец не получает секретных данных кредитной карты, а шлюз платежей и банк получателя не получают информации о том, что именно клиент покупает.

На первом этапе (покупка) между собой взаимодействуют покупатель и продавец. Покупатель инициирует соединение, продавец посылает ему сертификаты (свой и шлюза платежей) и уникальный идентификатор транзакции (transaction identifier). Покупатель проверяет сертификаты, помещает идентификатор транзакции в информацию о заказе (order information) и в данные о кредитной карте (payment information), шифрует их симметричными шифрами со случайными ключами, а сами ключи шифрует с помощью публичных ключей продавца и шлюза соответственно. Затем эта информация хешируется, подписывается и отправляется продавцу.

На втором этапе (авторизация платежа) предполагается взаимодействие между продавцом и шлюзом. Основная цель этапа – убедится, что у покупателя действительно есть деньги на счету. Продавец передает шлюзу запрос на авторизацию, содержащий идентификатор транзакции и данные о кредитной карте, зашифрованные покупателем, вместе с секретным ключом, зашифрованным с помощью открытого ключа шлюза. Шлюз расшифровывает информацию о карте и проверяет, разрешена ли операция банком получателя. В случае успеха шлюз создает токен, который передает продавцу. Все сообщения между продавцом и шлюзом шифруются, хешируются и подписываются.

В третьем, заключительном, этапе, продавец использует полученный токен, чтобы перевести деньги на свой счет.

Особого внимания заслуживает иерархическая система сертификации продавцов. Каждый продавец имеет сертификат, подписанный сертификатором продавцов (MCA - Merchant Certification Authority). Сертификат MCA подписывается BCA – Brand Certificate Authority, сертификат которой, в свою очередь, подписывается RCA – Root Certificate Authority.

В протоколе SET используются симметричный алгоритм шифрования DES, хеш SHA-1 и ассиметричный алгоритм RSA.

CPTP

CPTP (Customer Payment Transactions Protocol) в чем-то похож на SET, но здесь в транзакции принимают участие не четыре, а три стороны: покупатель, продавец и посредник (intermediation server), связанный с банковской инфраструктурой. Процесс состоит из следующих фаз:

- продавец направляет покупателю PRT (Payment Request Ticket), представляющее собой предложение покупателю, подписанное продавцом, которое он не может аннулировать задним числом;
- покупатель перенаправляет PRT посреднику;
- покупатель получает от посредника информацию о возможных способах платежа, вместе с PRT, заверенную цифровой подписью посредника;
- покупатель выбирает способ платежа, помещает в сообщение секретные данные о счете, шифрует и направляет посреднику;
- посредник проверяет возможность осуществления операции и, в случае успеха, выдает покупателю PPT (Payment Proof Ticket), который затем передается продавцу в качестве подтверждения факта платежа.

Интересно заметить, что в этом протоколе для обеспечения аутентификации покупателя применяются не сертификаты, а PIN-код. Такое решение было принято создателями протокола исходя из риска кражи секретного ключа с машины покупателя. В то же время, аутентичность продавца по-прежнему определяется с помощью сертификатов.

В протоколе не определено конкретных средств шифрования, в нем могут использоваться любые алгоритмы, как симметричные, так и асимметричные.

MPTP

Протокол MPTP (Micro Payment Transfer Protocol), как можно догадаться из названия, основан на идее «электронных монет». В нем предполагается взаимодействие между покупателем, продавцом и «брокером» - организацией, контролирующей обмен.

Предполагается, что покупатель имеет некий счет у брокера. Подлинность клиента подтверждается сертификатом, подписанным брокером. При необходимости заплатить покупатель формирует набор сообщений $m_1,\dots m_n$, и подписывает обязательство, связанное с этим набором. Сообщения связаны соотношением $m_i=H(m_{i+1})$, где H – односторонняя хеш-функция. Со всеми сообщениями ассоциируется один и тот же номинал.

При i-м платеже покупатель передает продавцу обязательство сообщение m_i. Очевидно, что продавец не может самостоятельно вычислить m_{i+1}. В конце дня он передает брокеру обязательство покупателя и сообщение m_k, где k – число осуществленных данным клиентом платежей, таким образом обналичивая деньги.

MicroMint

MicroMint – другая система, основанная на принципе «электронной монеты». Набор участников такой же, как и в предыдущем протоколе.

Монета должна быть легко проверяемой, но её должно быть трудно сформировать. В данном протоколе решение этой проблемы основано на сложности поиска коллизии криптографических хеш-функций.

Брокер, обладающий мощным оборудованием, перебирает возможные сообщения и находит те из них, которые вызывают k-кратную коллизию (k – параметр протокола), т.е. k сообщений, таких, что $H(m_1)=\dots=H(m_k)$. Эти сообщения и есть «монета». Срок действия монет истекает через месяц, поэтому считается, что злоумышленник не успеет сгенерировать достаточное количество монет, чтобы это принесло серьёзный урон.

Millicent

В этой системе платежную функцию снова выполняют электронные монеты. В отличие от других систем, здесь нет третьей стороны, покупатель общается напрямую с продавцом.

Монета содержит следующую информацию:

- идентификатор покупателя, для которого она была изготовлена;
- идентификатор продавца, который её изготовил;
- номинал;
- sequence number – для борьбы с повторным использованием монеты;
- цифровую подпись изготовителя монеты.

Таким образом, необходимо, чтобы покупатель заранее открыл счет у продавца, с которым собирается работать. После этого он получает «монету» определенного номинала. При покупке он отправляет продавцу эту монету и сумму, которую хотел бы потратить, продавец проверяет её подлинность, уменьшает её номинал на сумму покупки, и возвращает покупателю.

IOTP

IOTP – Internet Open Trading Protocol – это больше, чем протокол осуществления электронного платежа. Он охватывает не только области, традиционные для обычных протоколов (от формирования заказа на машине покупателя до передачи продавцу подтверждения осуществления перевода), но обеспечивает и другие операции, такие, как, например, возврат, отзыв платежа и доставку.

IOTP определен в рекомендации RFC-2801.

IOTP предлагает стандартные средства инкапсуляции протоколов осуществления электронных платежей, в том числе SET, Millicent и другие. Это означает его независимость от конкретной платежной системы, что, в свою очередь, делает его более универсальным и конкурентоспособным.

Разработчики протокола перенесли на электронную торговлю модель обычной торговли. В IOTP определены следующие роли:

- покупатель (consumer);
- продавец (merchant);
- кассир (payment handler);
- агент доставки (delivery handler);
- агент обслуживания (customer care provider).

Необходимо подчеркнуть, что это именно роли, а не организации. Одна организация в протоколе IOTP может исполнять несколько ролей.

Рассмотренные протоколы по-разному решают задачи обеспечения конфиденциальности, невозможности повторного использования одного и того же сообщения (replay attack), и другие. Однако, любая платежная система основывается на доверии участников центру, осуществляющему операции (банку, эмитенту электронных монет или payment gateway). Здесь можно провести аналогию с обычными бумажными деньгами, когда участники сделок доверяют государству.

Ссылки:

1. Secure Electronic Transactions: Credit Card Payment on the Web in Theory and Practice, http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg244978.html?Open
2. Cryptography and SET, http://www-306.ibm.com/software/genservers/commerce/payment/cryptset.html
3. A Formal Presentation of Electronic Commerce Protocols, http://www.cs.utexas.edu/ftp/pub/techreports/tr02-33.pdf
4. Телекоммуникационные технологии, http://book.itep.ru
5. RFC-2801
6. Payment Protocols: Cache on Demand: from Information Security Magazine, http://infosecuritymag.techtarget.com/articles/october00/features2.shtml
7. Introduction to the SSL Technology, http://e-docs.bea.com/tuxedo/tux80/security/publicke.htm