PayMe Protocol

Горохов Александр

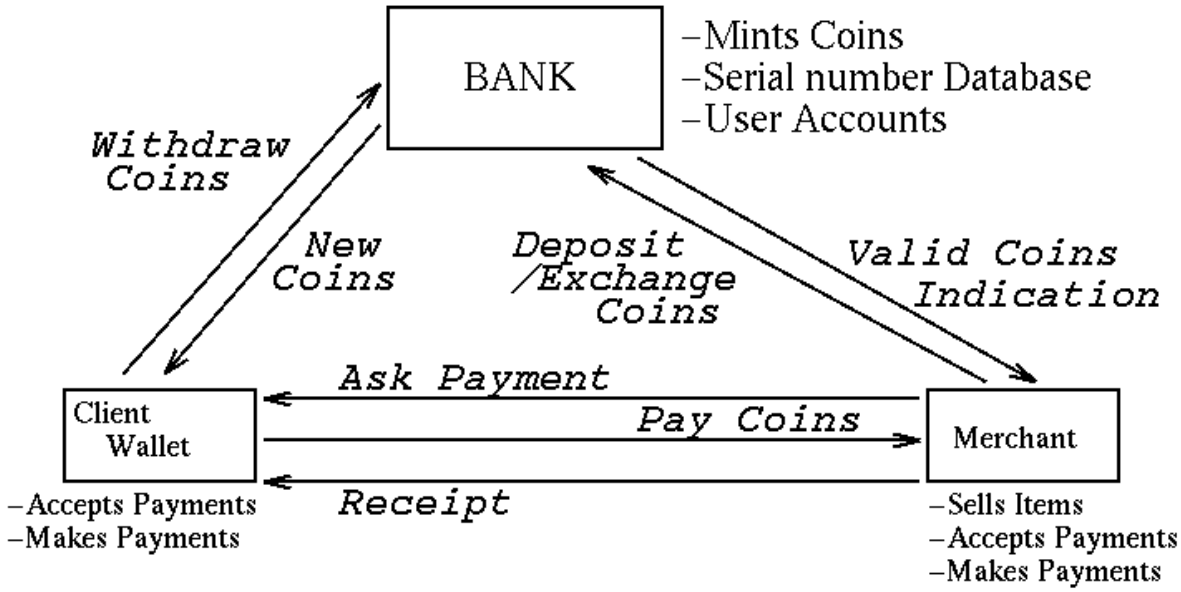
911 группа

Протокол PayMe

Главной целью, которая ставилась при создании протокола PayMe, было обеспечение анонимности в сочетании с масштабируемостью (т.е. возможностью системы работать с несколькими банками и множеством пользователей). Ниже будет рассмотрена общая структура протокола, а также его работа на примере платежа по сети. Будет также подробно описано представление денежных средств и примитивов протокола во время web транзакции.

PayMe – это онлайновая система электронной оплаты. В рамках этой системы пользователи и банки взаимодействуют между собой. Пользователи могут выступать как покупатели или как продавцы, они могут производить или принимать платежи либо осуществлять операции с банком. Каждый банк обладает своей собственной электронной валютой с серийными номерами. Монеты, находящиеся в обращении, банк заносит в базу данных, предотвращая таким образом двойное использование денежных средств.

Простая модель, демонстрирующая базовую функциональность системы PayMe, показана на рисунке:



Могут использоваться как симметричная схема шифрования, так и схема шифрования с открытым ключом. Каждый участник имеет свою собственную пару ключей (открытый и закрытый).

Система PayMe использует свой собственный защищённый протокол взаимодействия участников – PayMe Transfer Protocol (PMTP). Это обеспечивает безопасность и средства взаимодействия без привлечения Web протокола HTTP. Такой

подход был принят для разработки полного прототипа, который можно использовать с любым стандартом безопасности Web.

Представление денежных средств

Монеты – это некоторая информация, обладающая денежной ценностью внутри системы PayMe. Для того чтобы получить силу, монеты должны быть подписаны банком по схеме шифрования с открытым ключом. Каждая монета имеет серийный номер, который заносится в базу данных банка, когда монета пускается в обращение. Монеты содержат в себе следующие поля: ценность, серийный номер, идентификатор банка, имя хоста и номер порта банка и дата, до которой монета имеет силу.

PayMe Transfer Protocol (PMTP)

PMTP – это набор защищённых сообщений, разработанный для обеспечения необходимых взаимодействий в системе PayMe. Он использует как симметричное шифрование, так и систему схему шифрования с открытым ключом. PMTP содержит 6 типов сообщений запрос-ответ. Для каждого из этих типов возможны 3 различных идентификатора – запрос, ответ и отказ, соответственно. В запросе содержится требование выполнить какое-либо действие. Ответ посылается как подтверждение того, что действие выполнено, и тело сообщения содержит результат этого действия. Отказ посылается, когда выполнение запрошенного действия невозможно, и тело сообщения может содержать причину отказа.

Первые три типа сообщений используются владельцем банковского счёта для снятия денег со счёта, внесения средств на счёт и получения информации о состоянии счёта.

- Снятие денег со счёта

  Требует идентификатор аккаунта, соответствующее имя аккаунта, пароль и количество, подписанные пользователем.

- Внесение средств

  Сначала банк делает проверку, имеют ли силу денежные средства. Для проведения операции требуются идентификатор аккаунта, имя и цифровая сигнатура. Депозит может быть сделан в любом банке, в котором у пользователя есть аккаунт. Если денежные средства не являются внутренней валютой данного банка, он свяжется с соответствующим банком, чтобы признать монеты действительными. У каждого банка есть аккаунты в остальных, и таким образом осуществляется учёт межбанковский долгов.

- Получение информации о состоянии счёта

Для проведения операция требуется цифровая сигнатура для удостоверения владельца аккаунта.

- Обмен монет на новые

  Процесс обмена монет на другие анонимный, но безопасный. Банку известен только адрес, откуда поступили денежные средства. Если полученные банком монеты имеют силу, пользователю взамен будут возвращены новые. Необязательно иметь аккаунт в банке, для того чтобы произвести обмен, однако, обмен должен производиться в банке, в котором данные денежные средства являются внутренней валютой.

  Покупатель и продавец могут использовать этот механизм для обеспечения своей анонимности. Когда пользователь берёт деньги в банке, банк мог бы записывать номера монет и получателя. В последствии, когда продавец кладёт деньги в банк, можно было бы проверить, от кого он их получил. Однако, когда продавец меняет деньги, а не кладёт их в банк сразу, банк не может определить, кто произвёл обмен.

- Запрос на оплату

  Последние два типа сообщений используются при взаимодействии двух пользователей (например, покупателя и продавца). Сообщение ask_payment посылается пользователю как запрос оплатить определённую сумму. Во время заказа покупатель остаётся неизвестным продавцу. Сначала покупатель должен получить открытый ключ продавца. Однако, этот ключ посылается в запросе. С этим связан некоторый риск, поскольку третья сторона может подменить ключ продавца своим собственным. Пользователь может принять в этом случае новый ключ или нет.

  ask_payment запрос: {PAYMENT_REQ<количество>:K_M:{<метка>}K_M^{-1}};

  ask_payment ответ: такой же, как и pay_coins запрос;

  ask_payment отказ: {PAYMENT_REFUSAL<количество>:<метка>}K_M.

  (K_M – ключ продавца)

- Оплата

  Покупатель остаётся неизвестным продавцу. Продавец знает только сетевой адрес покупателя.

  pay_coins запрос: {PAY_COINS_REQ<монеты>:<SK>:<метка>}K_M;

  pay_coins ответ: {PAY_COINS_RESPONSE<подтверждение>:<метка>}SK;

  pay_coins отказ: {PAY_COINS_REFUSAL<причина>:<метка>}SK.

  (SK – сессионный симметричный ключ)

Безопасность PMTP

Сообщения PMTP защищены от атак прослушивания, подмены, повторения и выдачи себя за другого.

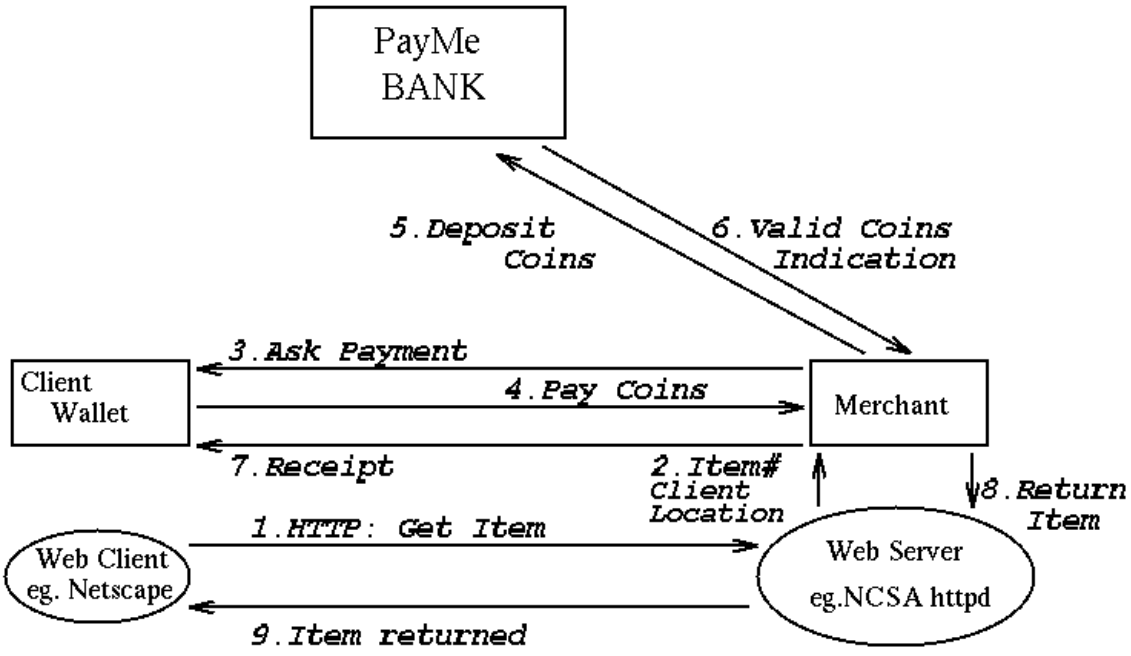
Атакующая сторона не может получить содержание SMTP сообщения, так как сообщение зашифровано либо открытым ключом получателя, либо сессионным ключом, сгенерированным общающимися сторонами заранее. Единственное исключение – ответ ask_payment. Так как покупатель должен оставаться неизвестным, это сообщение передаётся открытым текстом.

В каждом PMTP сообщении содержится метка времени. Стороны хранят недавно полученные временные метки. Если атакующая сторона попытается повторить одно из сообщений в течение промежутка времени, когда оно будет воспринято как верное, это будет выявлено по повторяющимся временным меткам.

Везде, где возможно, сообщения заверяются цифровыми подписями. Снятие денег со счёта также требует пароля на банковский аккаунт. В анонимных сообщениях используется симметричное шифрование.

PayMe в Web'е

PayMe используется с любыми Web клиентами и серверами. При заказе товаров или услуг используется следующая комбинация PMTP сообщений:



1. Для заказа товара или услуги пользователь выбирает соответствующий URL.

2. Программному обеспечению PayMe продавца передаются свойства выбранного элемента, сетевой адрес покупателя, а также дополнительная информация (адрес доставки для доставки товара).
3. Определяется стоимость товара и пользователю отправляется ask_payment запрос.
4. Покупатель уведомляется о запросе и принимает (посылает pay_coins_request) или отклоняет (ask_payment_refusal) его. В случае принятия запроса электронный кошелёк пользователя выбирает монеты для передачи и передаёт их продавцу. Сдача в этом случае не возвращается, поскольку это могло бы нарушить анонимность покупателя в случае, если продавец вступил бы в сговор с банком.
5. Продавец проверяет подлинность монет, либо анонимно обменивая их на новые монеты, либо делая депозит в банке. Обмен должен производиться в том банке, где данные денежные средства являются внутренней валютой. Этот банк проверяет наличие серийных номеров монет в своей базе данных. В случае их наличия монеты считаются подлинными. После этого записи, соответствующие этим монетам, удаляются из базы данных, таким образом, лишая их ценности. Взамен продавец получает новые монеты.
6. Продавец получает от банка уведомление о подлинности монет. В случае положительного ответа – это exchange_coins_response (если производился обмен) или deposit_coins_response (если делался вклад).
7. Покупатель извещается о получении платежа (pay_coins_response).
8. Заказанный элемент отправляется от продавца на Web сервер.
9. Сервер отсылает заказ клиенту.

Реализация и использование

Система была реализована в окружении C++/Unix на кластере машин Sun. Для реализации схемы шифрования с открытым ключом используется RSA, и IDEA для симметричной схемы шифрования.

Для уменьшения подверженности системы сбоям хранятся копии монет и ведутся лог-файлы.

Протокол PayMe объединяет в себе свойства нескольких протоколов (NetCash, Ecash, Magic Money, Netbill и др.), обеспечивая анонимность, возможность масштабируемости, безопасность, возможность широкого использования с любым web-

клиентом; он не требует привлечения средств на уровне hardware (таких, как смарт-карты).

Используемая литература

[1] Michael Peirce, Donal O'Mahony. Scaleable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set
http://www.w3.org/Conferences/WWW4/Papers/228/

[2] D.Chaum, A.Fiat, and M.Naor. Untraceable Electronic Cash,
http://www.wisdom.weizmann.ac.il/~naor/PAPERS/untrace.ps

[3] Gennady Medvinsky and B.Clifford Neuman. Electronic Currency for the Internet. Electronic Markets Vol 3. No. 9/10, October 1993
http://www.isi.edu/people/bcn/papers/pdf/9311_netcash-medvinsky-neuman-cccs93.pdf

[4] Gennady Medvinsky and B. Clifford Neuman. NetCash: A design for practical electronic currency on the Internet. In Proceedings of the First ACM Conference on Computer and Communications Security, November 1993.
http://www.isi.edu/people/bcn/papers/pdf/9311_netcash-medvinsky-neuman-cccs93.pdf

[5] B. Clifford Neuman and Gennady Medvinsky. Requirements of Network Payment: The NetCheque Perspective. In Proceedings of IEEE Compcon'95, San Francisco, U.S.A., March 1995.
http://www.isi.edu/people/bcn/papers/pdf/
9503_netcheque-neuman-medvinsky-compcon95.pdf