1 Лекция No.4

2 “Электронные платежи”

2.0.1 Юрий Лифшиц*

2.0.2 11 октября 2005г.

Законспектировал В. Васильев

“И он сделает то, что всем – малым и великим, богатым и нищим, свободным и рабам – положено будет начертание на правую руку их или на чело их, И что никому нельзя будет ни покупать, ни продавать, кроме того, кто имеет это начертание, или имя зверя, или число имени его. Здесь мудрость. Кто имеет ум, тот сочти число зверя, ибо число это человеческое; число его шестьсот шестьдесят шесть.”

Откровение Святого Иоанна Богослова, глава 13.

План лекции:

Классификация электронных платежей: требования к электронным платежам, их типы.

Криптографические ингредиенты: цифровые сертификаты, слепая подпись.

Электронные наличные.

2.0.3 I

Основные достоинства электронных денег по сравнению с традиционными – это дешевизна банковских операций, анонимность (это свойство выполняется не для всех типов электронных денег), защищенность от подделки и возможность использования в электронном бизнесе.

Каковы требования и характеристики платежных систем?

По части безопасности: невозможность подделать, невозможность превысить кредит при оплате, невозможность двойной платы, анонимность, аппаратная и/или криптографическая стойкость.

По части эффективности должны быть снижены вычислительная трудоемкость, коммуникационная стоимость и стоимость обслуживания.

Платежные системы должны обладать следующими возможностями: переносимость, делимость (возможность заплатить любое количество денег без сдачи), универсальность (возможность использования в любой

стране, в любых условиях, даже когда нет связи с представителями банка (в том числе с банкоматами)) и возможность удаленной оплаты.

Заметим, что каждый человек может делать свои собственные деньги, которые он сам будет обеспечивать.

Сравним некоторые системы оплаты:

Кредитная карта – она хранит имя владельца и максимальную сумму единоразового платежа. При такой системе оплаты можно брать кредит у банка. Магазины и банкоматы отправляют информацию в банк в конце рабочего дня, значит за день можно "уйти в минус"

Дебетная карта – аналог бумажника: карта хранит только остаток денег, который обновляется при каждом использовании кассовыми аппаратами. Можно использовать украденную дебетную карту. Нельзя "уйти в минус". Пример – таксофонные карты, магнитные карты метро.

Чеки – бумажный аналог кредитной карты. На них написана максимальная сумма единоразового платежа.

Наличные.

Существуют и другие системы электронных платежей.

Рассмотрим подробнее наши 4 системы.

Дебетные карты. Как ими пользоваться? Первый шаг: кладем деньги на карту. Второй шаг: сумма записывается на карту. Далее потраченные деньги вычитаются с карты.

Если сделать аппарат, который может записывать на карту любую сумму, то система будет взломана. Украденную карту можно использовать, как и обычные деньги.

Кредитная карта. Здесь алгоритм использования такой: заводим счет в банке, потом деньги снимаются со счета.

Минусы этой системы: нарушается анонимность, т к банк обналичивает каждый платеж и может следить сколько денег и где мы тратим; высокая себестоимость (обслуживание банкоматов).

Криптографическая основа – протокол SET (Secured Electronic Transactions)

Микроплатежи – оплата услуг мобильной связи и пр. Этот вид платежей обладает некоторыми особенностями:

Здесь не требуется анонимности

Необходимо минимизировать вычисления (всвязи с большим количеством платежных операций)

Современные решения – это системы Millicent и Payword.

Электронные наличные

Здесь банк каждый раз проверяет корректность платежей

2.0.4 II

Перейдем к собственно криптографии. Что используется в электронных платежах?

Аутентификация сообщений – гарантирует целостность

Шифрование – гарантирует секретность от посторонних

Цифровой сертификат – защита от мошенников (аналог паспорта; доказывает, что тот, кто платит – на самом деле тот, кем назвался)

Слепая подпись – применяется только для электронных наличных.

Рассмотрим цифровую подпись. Существуют два ключа: секретный (он есть только у владельца подписи) и открытый (используется любым желающим для проверки подлинности подписи). Для создания подписи генерируются секретный и открытый ключи, открытый ключ посылается в глобальную базу данных ("правительство", "милиция"). Для проверки подлинности надо скачать из нее этот ключ. (картинка). Здесь есть соединение продавца с базой данных. Как можно обойтись без него? Например, так. Я хочу создать себе подпись. Я отправлю в "правительство" открытый ключ, мне возвращают сертификат (слепок моей подписи), подписанный правительством (подпись правительства всем известна). Теперь я посылаю сертификат и подпись, сгенерированную секретным ключом, вместе с посланием. Как избавить правительство от большого объема работы? Можно ввести иерархическую структуру: правительство сертифицирует подписи "отделов милиции", те сертифицируют более мелкие "отделения милиции", а они – конечных пользователей.

Слепая подпись: один подписывает документ другого, но не знает, что в нем написано. Для лучшего понимания можно рассмотреть такую модель: я кладу в конверт документы, а между ними – копировальную бумагу, заклеиваю его и посылаю тому, кто подписывает. Он ставит свою подпись на наружной стороне конверта, не заглядывая внутрь. С помощью копировальной бумаги она отпечатывается на всех документах. Он отправляет конверт обратно мне, теперь у меня есть подписанные документы, о содержании которых никто ничего не знает. В RSA слепая подпись реализуется так: пусть у нас есть сообщение M, секретный ключ d и открытый ключ e. Подпись – это $\mathrm{S}{=}\mathrm{M}^d$. Проверка подлинности: $\mathrm{S}^e{=}\mathrm{M}$? В протоколе Шаума: Боб выбирает случайное число r. Он посылает Алисе $\mathrm{M}' = \mathrm{M} * \mathrm{r}^{\mathrm{e}}$. Алиса подписывает M' и посылает $\mathrm{S}' = \mathrm{M}^{\mathrm{d}} * \mathrm{r}^{\mathrm{e*d}} = (\mathrm{M}')^{\mathrm{d}}$. Боб получает исходную подпись $\mathrm{S}' = \mathrm{S} * \mathrm{r}^{-1}$.

2.0.5 III

Как реализовать систему “электронные наличные” с помощью слепой подписи? Рассмотрим “наивный протокол”.

Обналичивание: сначала мы просим банк выдать некоторую сумму, например, \$153. Банк присылает чек. Мы проверяем подпись – Ok

Оплата: мы посылаем чек продавцу. Продавец проверяет подпись – Ok

Получение денег продавцом по нашему чеку: продавец посылает чек в банк. Банк проверяет подпись, высылает деньги продавцу – Ok.

Недостатки “наивного протокола”:

Нет анонимности – банк может следить за нашими платежами

Возможна двойная трата (использовать чек в 2 магазинах)

Первый недостаток исправляется введением слепой подписи для банка. Но тогда банк может подписать любую сумму, в т ч сумму, большую, чем имеется у нас на счете.

Этот недостаток исправляется введением выборочной проверки. Мы посылаем банку много (например, 1000) чеков. Банк проверяет большую часть (999 чеков). Если на них написана сумма, не превышающая имеющуюся на нашем счете, то с большой вероятностью сумма на 1000-м чеке тоже “хорошая”, и банк подписывает его вслепую и отсылает нам. Теперь соблюдается анонимность, т к банк не знает серийного номера чека, значит не может следить за клиентами.

Также для исправления этого недостатка можно использовать систему ключей. В таком случае у банка существует набор ключей-подписей (например, для обозначения \$10, \$100 и т п.). По результатам большого числа (например, 999) проверок определяется наиболее вероятная сумма на чеке, и банк подписывает эту сумму с помощью набора ключей.

Как исправить второй недостаток – возможность двойной платы? Для этого можно использовать online и offline контроль. Online–контроль – это связь продавца с банком в момент оплаты с целью выяснить, является ли действительным предъявляемый чек. Этот метод абсолютно надежен (если, конечно, банк не жульничает), но обладает многими недостатками: необходима постоянная связь продавца с банком, медленная скорость обслуживания. Offline–контроль – “продавец связывается с банком вечером”.

Рассмотрим подробнее offline–контроль. Мы хотим, чтобы имя покупателя осталось неизвестным, если он потратил чек, а если он исполь-

зовал его более одного раза, то мы хотим его узнать. Для этого можно поступить так:

Участники (покупатели) генерируют $x_1 \dots x_k, y_1 \dots y_k$ по правилу: имя участника $ID = x_i \oplus y_i$ для каждого i.

Участники посылают банку хэш-функции от этих значений и включают хэш-значения в текст чека.

К каждой электронной купюре добавляют набор из k значений x_i или y_i по выбору продавца (то есть продавец говорит покупателю: "Дай мне x_1, y_2, y_3, x_4".)

Если деньги тратили 2 раза, то можно с вероятностью $1–2^{-k}$ установить нарушителя: у продавцов окажутся половинки имени (x_i и y_i), и они будут разными с большой вероятностью.

Истинность ID проверяется выборочной проверкой. С вероятностью 2^{-k} магазин может получить убыток при двойной оплате.

2.0.6 IV. Итоги.

Если не запомните ничего другого:

Типы платежей: кредитные карты, электронные наличные, микроплатежи.

Электронные наличные основаны на слепой подписи.

Два метода борьбы с двойной тратой – online и offline методы.

Список источников:

Ященко:
http://www.cryptography.ru/db/msg.html?mid=1161235&uri=node21.html
Electronic Payments: where do we go from here?
http://www.gemplus.com/smart/rd/publications/pdf/JMTY99ec.pdf
Koleva
http://www.crg.cs.nott.ac.uk/people/Boriana.Koleva/Teaching/IDB/lecture15.pdf
Глава 11 Goldwasser-Bellare
http://www.cs.ucsd.edu/users/mihir/papers/gb.html
Damgard & Co
http://www.daimi.au.dk/~ivan/ecash.pdf