Обзор платежных систем в Internet

Студент: *Пупкова Мария Викторовна*
Группа: *115 группа*
Курс: *“Защита информации”*

г. Долгопрудный
2005 г.

Введение

Конец 20 века ознаменовался телекоммуникационным бумом. Не только потому, что выросли скорости передачи данных, появились новые протоколы и технологии, на рынке возникли новые операторы связи, увеличилось число пользователей глобальной сети, но изменилась сама жизнь людей – она стала тесно связана с Internet. Сегодня нам кажется обычной возможность размещения рекламы, покупка товаров, услуг или информации в Internet. Электронная коммерция стала широко распространенным явлением. Качественный электронный бизнес возможен лишь тогда, когда человек - пользователь глобальной сети, может совершить покупку, не отходя от своего компьютера, произведя заказ и оплату одновременно. На этом этапе возникает множество проблем и главная из них – как обеспечить безопасность финансовых транзакций, как сделать так, чтобы и покупатель и продавец были уверены, что ни та, ни другая сторона их не обманет, или в процесс не вмешается третья сторона. Перейдем к описанию основных платежных систем в современной сети Internet.

Выделяют два вида платежных систем в Internet: карточные системы (платежные карты) и некарточные платежные системы (электронные деньги и системы управления счетом).

Некарточные платежные системы

Более привычным для человека при покупке является использование банковских карт. Но это способ имеет ряд важных недостатков, когда дело касается покупок в сети Internet, а именно, он не обеспечивает безопасность ни продавцу, ни покупателю. Например, при покупке в сети покупателю необходимо ввести полную информацию о своей карте: номер карты, pin – код, срок её действия, информацию о себе и т.д. В этом случае ему остается только положиться на порядочность продавца и на то, что формы для ввода, заполненные им в Internet – магазине, отсылают данные нужному адресату. Продавцу же важно, чтобы карточный номер вводился “истинным” владельцем карты, потому что если это не так, то ему придется отдать полученные деньги, и к тому же заплатить штраф (так называемый chargeback) банку. Конечно, в этой торговой цепочки есть и другие звенья: доставка товара, сам процесс заказа, но самым слабым является оплата.

Необходимо использовать более “продвинутый” механизм оплаты, который не имеет вышеперечисленных недостатков и о котором речь пойдет ниже.

Выделяют два вида альтернативных способов оплаты:

- электронные деньги;
- управление счетом через Internet (системы банк - клиент).

Система банк – клиент

Системы такого типа позволяют производить управление счетом через Internet. Клиент может передать запрос банку с целью перевода денег с одного счета на другой, например, для оплаты покупки в Internet - магазине. По принципу работы такие системы близки к клубным системам работы с карточками. Система должна гарантировать выполнение следующих пунктов:

- клиент должен быть уверен, что соединяется именно с сервером своего банка, а не с подставным сервером;
- к серверу банка не может подключиться злоумышленник;
- злоумышленник не может получить доступ к информации, передаваемой между клиентом и банком;
- злоумышленник не может передавать в банк информацию от имени клиента;
- злоумышленник не может внести в передаваемую информацию изменения.

Большинство систем криптографической защиты систем банк – клиент используют протокол SSL.

К сожалению, существует ряд ограничений из-за которых такие системы не получили большого распространения:

- При покупке товара через Internet счета продавца и покупателя могут находиться в разных банках. Расчет между банками бывает затруднен, так как один банк должен получить доступ к счетам другого банка, а это плохо для безопасности банковских систем.
- Можно перевести все деньги, находящиеся на счете, одновременно. Злоумышленник, получивший доступ к счету, может этим легко воспользоваться.
- При “виртуальной” покупке товаров нет возможности составить договор купли – продажи, и, как следствие, невозможно составить паспорт сделки.
- Так как информация о платежах и счетах хранится в банке, то ей может воспользоваться как злоумышленник, взломавший систему, так и недобросовестный сотрудник банка, решивший заработать на этой информации свой первый миллион.

Электронные деньги

Для начала стоит сказать о том, что аналитики рынка денежных средств не склонны считать, что электронные деньги являются альтернативой “бумажным”, тем более что когда-нибудь электронные деньги вытеснят обычные с рынка. Скорее электронные деньги являются дополнением к обычным деньгам и кредитным карточкам, особенно, когда использование последних невозможно или затруднительно, например, при совершении операций в сети Internet.

Электронные деньги являются широким понятием. Обычно они представляют собой файл – сертификат, хранимый на компьютере пользователя. В этом файле содержится обязательство банка выплатить предъявителю сертификата определенную сумму, например с целью оплаты покупки в Internet.

Рассмотрим основные системы, существующие в Internet.

Система Mondex

Платежная система Mondex работает с цифровыми наличными, носителем которых является смарт – карта, представляющая собой микропроцессор с частотой 10 МГц, который состоит из 8 – битного CPU, 16 – килобайтного ROM, 512 – байтного RAM и 8 Кбайт энергонезависимой памяти для хранения данных. Наличность зачисляется на смарт – карту путем “замены” “реальных” денег на цифровые. После зачисления электронных денег на смарт - карту отследить их перемещение между пользователями невозможно, в этом смысле смарт – карты представляют собой полный эквивалент бумажных денег.

Передача денег между пользователями может осуществляться через телефон, подключенный к Mondex или при помощи специального оборудования. Для передачи данных между картами существует специальное устройство – бумажник, кроме того, существует специальный карманный считыватель, который позволяет определять остатки на карте.

Смарт – карта Сбербанка

Если смарт – карты Mondex это европейское изобретение, то первым проектом внедрения смарт – карт в России стал проект Сбербанка России – Сберкарт, использующий смарт – карты BGS Smartcard AG. Для защиты смарт – карты держатель может установить два пароля: один на зачисление денежных средств на карту, другой для списания денежных средств с карты. По принципу работы эти смарт – карты аналогичны картам Mondex: пользователь хранит деньги в памяти компьютера и может передавать их из одного кошелька в другой с помощью кассы. Сдерживающим фактором для развития этих смарт – карт является высокая стоимость устройств для связи смарт – карт и компьютеров, а

также то, что на сегодняшний день существует всего один Internet – магазин, принимающий платежи с этих смарт – карт.

DigiCash

DigiCash - это голландская компания, основанная в 1990 году. Это была первая компания, создавшая систему защищенных электронных сертификатов – цифровых денег. Основной проект компании - система eCash, использующая электронные деньги для оплаты товаров и услуг в режиме реального времени через Internet с помощью e-mail. Для использования системы необходимо открыть счет у одного из финансовых агентов, производящих операции с eCash. При этом пользователь получает известный только ему пароль. Система представляет денежные знаки в цифровой форме, как последовательность цифр. Пользователь может производить различные операции с электронными монетами: посылать их по Internet, продиктовать по телефону, послать по факсу или с помощью e-mail, сохранять монеты на жестком диске. Для обеспечения безопасности система использует технологию цифровой подписи и шифрование с открытым ключом. Продавец получает цифровую монету и предоставляет её в банк для авторизации. После того, как банк авторизует монету, на счет продавца зачисляется необходимая сумма, а сама монета помещается в список использованных и запрещенных к дальнейшему использованию монет. Преимуществом данной системы является высокая степень анонимности: при совершении транзакций клиенту не нужно указывать никаких данных о себе, ему необходимо только ввести пароль, позволяющий ему использовать счет. Недостатком является то, что клиент вынужден доверять банку, он не может проверить, использовалась ли ранее цифровая монета или нет. Таким образом, существует вероятность обмана банком клиентов путем присваивания банком цифровых денег клиента.

PayCash

На данный момент на базе технологии PayCash работают 4 платежные системы, одна из них хорошо известна в России – Яндекс.Деньги. Преимуществами этой платежной системы является невозможность обмана участниками друг друга. Для работы с системой необходимо установить программу управления счетом – Кошелек. Необходимо сразу оговориться, что любая операция в системе PayCash подтверждается электронными цифровыми подписями участников. Кроме работы с электронными деньгами, система может хранить и передавать информацию обо всех транзакциях, совершенных в системе, например договор о купли – продажи, подписанный электронными цифровыми подписями участников. Таким образом, система обеспечивает связь между “виртуальной” и “реальной транзакцией”.

Пользователь системы должен сам нести ответственность за сохранность кошелька, а значит и своего счета. Пользователь системы может создать так называемую платежную книжку, на которую через банк он будет перечислять определенную сумму электронных денег. Кроме того, пользователь может снимать со своего счета любую сумму в пределах той, что находится на книжке, для оплаты через Internet и делать это по частям. Банк должен подтверждать любые изменения счета, в противном случае, пользователь может их отменить или через определенное время эти изменения аннулирует сама система.

WebMoney

Пожалуй, это наиболее известная платежная система в России. Принципы её работы аналогичны принципам работы PayCash. Пользователь системы работает с виртуальным счетом, которым он может управлять через электронный кошелек. В системе существует три вида валюты, которые соответствуют рублям, долларам и евро. Расчеты производятся через банки, в том числе и западные. Это обеспечивает большой спектр предоставляемых операций и размер пользовательской аудитории.

Платежные карты

Несмотря на появление альтернативных способов оплаты через Internet, таких как электронные обязательства (деньги), бо́льшая часть платежей на сегодняшний день происходит с использованием карточек. Этот способ является более привычным для человека, так как он больше приближен к реальной торговой операции. Вместе с тем этот способ имеет существенный недостаток, а именно, он не позволяет аутентифицировать человека, производящего оплату с помощью карты. Internet - магазин, в котором пользователь производит оплату, может только проверить платежеспособность карты, но не может проверить действительно ли карта принадлежит пользователю.

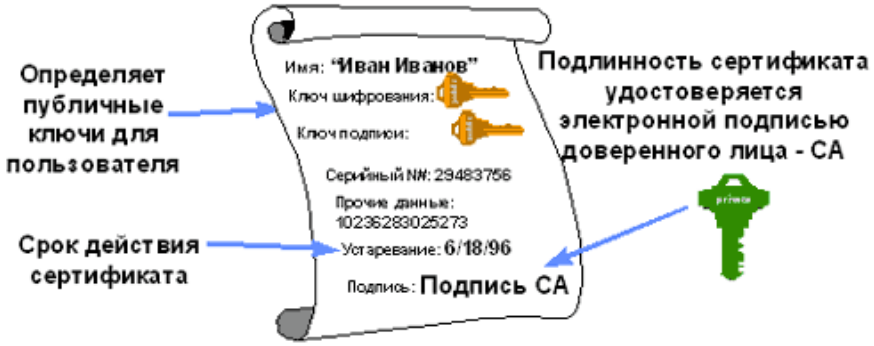
В таком случае у недобросовестного пользователя может возникнуть мысль получить данные карты, без согласия её владельца. Несет убытки, как продавец, так и истинный владелец карты. Истинный держатель карты вынужден опротестовывать сделку, которую совершил злоумышленник, что отнимает время и силы. Только таким образом можно получить от продавца компенсацию. Продавцу, кроме выплаты компенсации из страхового фонда, придется заплатить штраф банку. Вследствие всех этих причин увеличивается стоимость транзакций и сокращается область обслуживания Internet – магазина и платежной системы.

Есть несколько способов получения данных о карте:

- Одним из самых распространенных и эффективных способов мошенничества является “фишинг” (phishing - искаженное английское слово fishing - рыбалка). “Фишинг” является одной из разновидностей спама. Авторы рассылки подделывают обратные адреса, выдавая себя за представителей банков, финансовых структур, операторов связи и пр., предлагая отправить по определенному адресу данные о карте или номере счета или зайти на сайт, внешний вид которого копирует дизайн известных ресурсов, например, с целью подтвердить регистрацию аккаунта. В некоторых случаях достаточно лишь открыть письмо, чтобы скрипт, содержащийся в нем, подменил адреса банков на адреса поддельных сайтов. Конечно, банки стараются защитить своих клиентов и информируют их о необходимости соблюдения мер безопасности и внимательности при работе с почтой или браузером, но существует печальная статистика, которая говорит о том, что на уловки фишеров попадаются до пяти процентов пользователей, иными словами, каждый двадцатый становится жертвой мошенников.
- Перехват данных о карте при передаче их через Internet. В таком случае злоумышленник должен иметь доступ к трафику и уметь его отфильтровывать. Достаточно сложная задача, к тому же большинство Internet – магазинов используют протокол защиты SSL (Security Socket Layer). Этот протокол представляет собой некую надстройку над протоколом HTTP, которая позволяет идентифицировать стороны на основе сертификатов, шифровать передаваемую информацию и подтверждать правильность передачи данных. Протокол использует 2 схемы шифрования: ассиметричная (используется при установке сеанса связи) и симметричная (используется для шифрования передаваемой информации). Но использование такого механизма потребует дополнительных (пусть и небольших) капиталовложений, к тому же магазин должен предоставить центру сертификации информацию, подтверждающую его деловую репутацию и благие намерения.
- Создание поддельных сайтов с целью получения информации о карте. При заполнении формы на сайте данные о карте могут быть отосланы злоумышленнику. В последнее время такой способ получает все большее распространение.
- Взлом Internet – магазина.
- “Физическое” получение данных о карте. Каким-то образом злоумышленнику становится доступным сама карта и её pin – код.

Существуют способы и решения, которые позволяют снизить риск всех вышеперечисленных мошенничеств. Сначала о способах:

- Покупать товары и услуги только через проверенные Internet – магазины, которые хорошо себя зарекомендовали и работают на рынке Internet – услуг довольно давно.
- Передавать данные о карте только при наличии протокола SSL. Во всех остальных случаях существует вероятность, что данные получит злоумышленник.
- Сертификат для SSL – протокола должен быть выдан солидной организацией, занимающейся сертификацией. Наиболее известные: RSA Data Security, Thawte, VeriSign. Вот как выглядит сертификат, выдаваемый такой организацией:



Альтернативных решений существует не так уж много. Основные:

- Создание закрытых клубных систем. Все участники такой системы проходят специальную регистрацию с внесением вступительного взноса и размещают средства в страховом фонде. Таким образом, в обмен на полное раскрытие персональной информации клиентам предоставляются гарантии безопасности при совершении транзакций через Internet. Примеры таких систем: "Ассист" (система используется в крупнейшем Internet – магазине oЗон), банк "Платина", Internet Billing Company.
- Специализированные Internet – карты. Используются специально для совершения операций в сети Internet. Эти карты не имеют вид пластиковых карт, они фактически представляют собой подписанный банком номер, но в то же время они имеют все атрибуты пластиковых карт: срок действия, номер, данные о пользователе. На таких картах удобно хранить сбережения, используемые для оплаты покупок в Internet. Но при всех своих плюсах, такие карты также имеют риск быть украденными.
- Использование одноразовых карт. Пока существует лишь в виде концепции. Принцип работы заключается в создании одноразовой карты с суммой на счете, равной сумме платежа. С течением времени такая карта блокируется, тем самым вышеперечисленные способы мошенничества становятся неэффективными. Вместе с тем, это бы потребовало перестройки всех платежных систем, поскольку современные системы не поддерживают быстрое и дешевое создание таких карт.

Список литературы

[1] С. Волков, В. Достов, "Платежные механизмы современного Интернета", "Мир Internet", #5 (44), май 2000.
http://www.iworld.ru/magazine/index.phtml?fnct=page&p=9999999

[2] В. Достов, "Интернет–платежи в России: состояние и тенденции", "Аналитический и информационный журнал Документальная Электросвязь", №10 январь 2003.
http://www.paycash.ru/files/page.htm

[3] В. В. Сенкевич, "Электронные деньги в Internet".
http://www.marketer.ru/articles/index.95.html