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

Платежные системы. Безопасность осуществления платежей (дебетовые и кредитные системы).

Студент: Пидоненко Вадим Леонидович.
Группа: 211.
Дата: 12.04.2006 г.

г. Долгопрудный, 2006 г.

План:
1)Условия, которые должны быть реализованы в платежной системе.
2)Дебетовые системы, электронные деньги, схемы работы.
3)Кредитные системы, схема работы.
4)Атаки на платежные системы (краткий обзор).

В настоящее время Интернет используется в огромном количестве областей нашей жизни. В настоящее время он может служить не только как система всеобщего доступа к информации, но и как система частного доступа к определенной информации. Многие обыденные процессы были перенесены в электронное пространство, тем самым, получив преимущества в скорости и масштабности. Так возникла электронная коммерция, целью которой было моментальное осуществление электронных платежей и торговля. Но сразу же возникает огромное количество вопросов связанных с безопасностью платежей, аутентификацией сторон, гарантии рисков, и т.д. В этой статье будут рассмотрены основные условия, накладываемые на современные платежные системы, осуществление платежей и их безопасность, а также некоторые из видов атак.

Итак, сама по себе платежная система – это система проведения расчетов в Интернете между различными организациями и пользователями в процессе купли/продажи товаров и сервисов. Разумеется здесь и далее под термином «платежная система» будет иметься в виду платежная система, действующая в Интернете. Преимущества такой системы очевидны: скорость и удобство осуществления платежей. Она позволяет заказчику совершать покупки и заказы, не выходя из дома или не покидая рабочего места. А продавцу создать не просто электронный магазин с наглядным каталогом всех товаров, но и осуществлять сделки или обрабатывать заказы в считанные минуты.

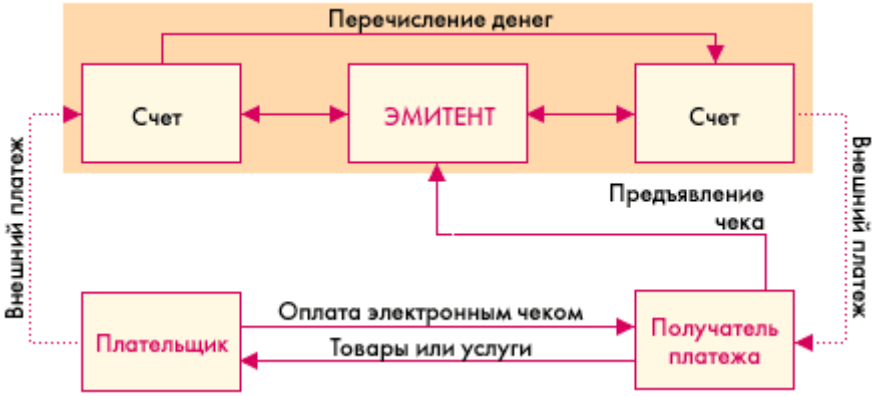
Следующие условия должны быть соблюдены в любой из современных платежных систем:

1) Конфиденциальность. Данные заказчика, например номер кредитной карты, должны быть известны только соответствующим организациям, участвующим в процессе осуществления платежа.
2) Сохранение целостности информации. Информация о покупки и данные транзакции должны быть защищены от несанкционированного изменения.
3) Аутентификация сторон. Обе стороны должны быть уверены, что имеют дело именно с тем лицом, за которое оно себя выдает.
4) Широкий выбор средств оплаты. Покупатель может оплачивать сделки любыми доступными ему денежными средствами.
5) Авторизация. Проверка аутентифицированного пользователя на возможность осуществления сделки(например платежеспособность).
6) Гарантия рисков. Продавец должен иметь гарантии от множества рисков связанных с использованием платежной системы. Например, отказ от товара. Риски определяются и документируются в соглашениях между провайдером платежной системы и других участвующих в процессе организаций.
7) Минимизация оплаты транзакции. Оплата обработки заказа, очевидно, будет входить в стоимость операции и она должна быть, по возможности, минимизирована. Оплата, также оплачивается даже, в том случае, когда покупатель отказывается от приобретаемого товара.

Платежные системы подразделяются на дебетовые(электронные деньги и чеки) и кредитные(кредитные карточки).

Дебетовая система.

Рассмотрим дебетовую систему осуществления платежей на примере электронных чеков. Электронные чеки – это аналог бумажных чеков. То есть это некоторый запрос о переводе наличности со счета плательщика на счет получателя. Электронные чеки, в отличие от реальных чеков, выдаются в электронном виде и подписываются электронной цифровой подписью. Ниже приводится схема осуществления платежей посредством электронных чеков:



В этой схеме можно выделить следующие этапы:
1) Выписка чека. Плательщик выписывает чек и подписывает его электронной цифровой подписью, затем отсылает его получателю. Чековый номер может быть, для обеспечения дополнительной безопасности, закодирован открытым ключом банка.
2) Предъявление к оплате. Получатель платежа предъявляет чек платежной системе, которая в свою очередь осуществляет проверку электронной подписи чека.
3) Начисление денег. В случае подлинности чека, происходит перевод денежных средств со счета клиента на счет продавца, заказанный товар поставляется.

Простота схемы проведения платежей, к сожалению, компенсируется сложностями ее внедрения в России. Здесь чековые схемы пока не получили распространения и не имеется сертификационных центров. Несколько слов о последних. Для реализации электронной цифровой подписи используется схема с открытым ключом. При этом секретный ключ находится у пользователя, а открытый ключ, для проверки, доступен всем. Открытые ключи удобно хранить в виде сертификатов – открытый ключ + информация о владельце. Для хранения сертификатов используются сертификационные центры, с помощью которых происходит распространение сертификатов.

Пример системы: eCheck

Эта система была разработана по аналогии с обычными бумажными чеками. eCheck составляется используя специальный язык FSML(Financial Services Markup Language), это язык использующий тэги, как HTML или XML. Тэги включают в себя информацию о чеке(подобную обычным чекам). FSML определяет блоки подписей, которые позволяют поддерживать добавление или удаление информации из чека, совместную подписку, прикрепление документов (в том числе и зашифрованных). Для того, чтобы прочерить кому принадлежит подпись используются x.509 сертификаты. Электронные чеки могут передаваться и по e-mail и по http (для совместимости с этими и другими протоколами передачи верхних уровней, в FSML используются только кодировка ASCII в комбинации с ограничением длины строк).

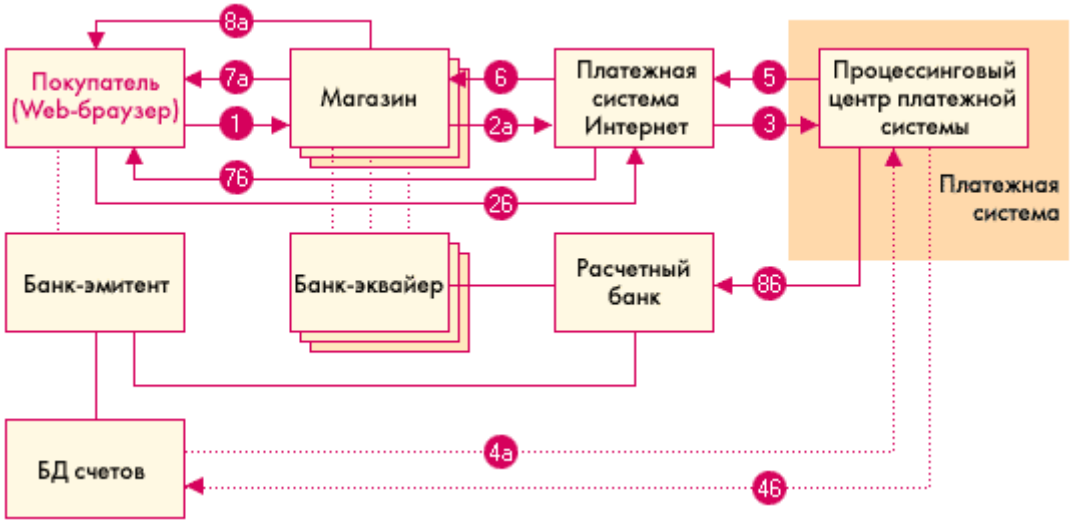
Пример тэгов в eCheck:

<account>	Данные о банковском счете плательщика
<action>	Действия получателя чека
<attachment>	Прикрепленные документы
<cert>	Информация о сертификате X.509
<signature>	Блок подписей
<check>	Данные чека: сумма, дата и т. д.

Блоков <signature> в документе может быть несколько, каждый из них подписывает свои определенные блоки.

Кредитные системы.

Кредитные платежные системы созданы по аналогии реальных систем, использующих кредитные карточки. Схема проведения платежей отличается, в виду необходимости осуществления безопасности платежей и аутентификации.
Рассмотрим схему осуществления платежей:



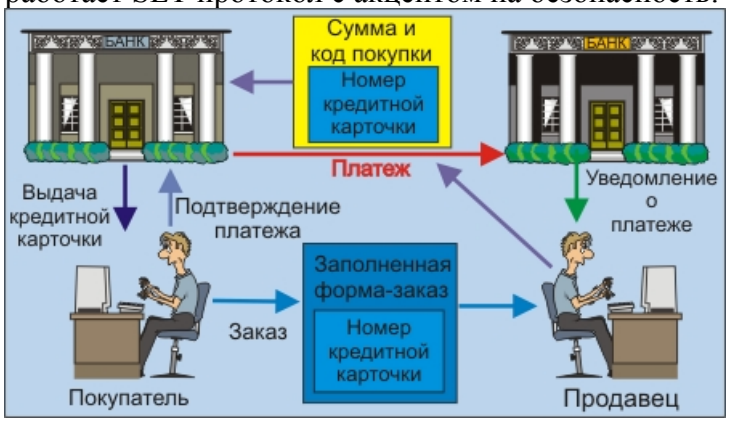
В этой схеме:
Банк-эквайер – банк, в котором продавец держит расчетный счет.
Банк-эмитент – банк, в котором находится расчетный счет покупателя.

1) Покупатель делает запрос магазину на приобретение товара в магазине.
2) Передача своих данных (номер кредитной карты, имя, дата окончания действия кредитной карты) платежной системе. Это совершается либо через сайт магазина(2a), либо непосредственно на сервере платежной системы. Второй путь предпочтительнее первого с точки зрения безопасности. При передаче данных через магазин, повышается не только вероятность перехвата данных по каналам, но и есть риск, что сервер магазина был плохо защищен, и данные могут быть перехвачены. Самым распространенным способом защиты данных является использования протокола SSL (Secure Socket Layer), он использует алгоритм RSA для шифрования данных. В настоящее время более надежным алгоритмом является SET (Secure Electronic Transaction), который был призван на смену SSL в платежных системах. Минусами использования SET является его высокая стоимость и сложность реализации.

3-8) Процессинговый центр осуществляет стандартную авторизацию пользователя в системе, результат авторизации передается магазину, пользователю и платежной

системе. В зависимости от результата авторизации магазин либо поставляет услугу/товар пользователю(и деньги со счета покупателя переводятся на счет магазина), либо сообщает о невозможности проведения операции.

В большинстве случаев такие системы реализованы в виде электронных кошельков(программа, устанавливаемая пользователю). Рассмотрим схему, по которой работает SET протокол с акцентом на безопасность:



1) Покупатель выбирает товар и заполняет бланк заказа на сервере продавца. При заказе на стороне покупателя запускается установленное программное обеспечение, где хранятся данные о покупателе или покупатель вводит их самостоятельно.
2) Программа отсылает на сервер продавца сообщение о заказе в виде двух шифрованных сообщений: заполненная форма заказа и номер кредитной карточки; и хэшей к ним. Форма заказа шифруется используя открытый ключ продавца, а номер кредитной карточки – используя открытый ключ банка (в котором открыт счет кредитной карты). Программа также генерирует хэш к обоим сообщением используя секретный ключ покупателя, это делается для того, чтобы проконтролировать целостность данных(так как секретный ключ известен только покупателю).
3) Сообщение получает web-сервер продавца. Он формирует запрос к банку, в котором хранится счет продавца. Этот запрос подписывается электронной подписью продавца, таким образом, сервер может его идентифицировать.
4) Банк идентифицирует продавца и проверяет действительность кредитной карточки. Действительность кредитной карточки проверяется запросом к банку, выпустившего карту (запрос снабжается электронной подписью).
5) Банк, выпустивший карточку, проверяет данные карточки и сообщает о результате банку, сделавшему запрос (ответ снабжается соответствующей электронной подписью)
6) После авторизации операции банком, отсылается подтверждение web-серверу продавца.
7) Продавец извещает покупателя о статусе транзакции.
8) Покупатель осуществляет подтверждение операции своему банку.

На каждом шаге операции используется, аутентификация, тем самым, делая невозможность повлиять на ход транзакции сторонними лицами. В приведенной выше схеме, очевидно, что все участники должны разослать свои открытые ключи. Протокол SET включает в себя не только эти, но и ряд других функций.

Теперь, когда рассмотрены основные стороны платежных систем, а также методы осуществления безопасности платежей на примере протоколы SET, можно рассмотреть, основные виды существующих сегодня атак.

1) Фишинг – создание точной копии веб-сайта с целью завладеть секретной информацией клиента. Время существования таких сайтов не велико. Обычно для увеличения числа покупателей, цены снижаются, но это не смущает пользователей, так как сайт является, в основном, точной копией какого-нибудь широко доверяемого сайта. Обычно пользователей «ловят» запросив, например, ввести свои данные на сайте заново. Это осуществляется, например, через почтовую рассылку.
2) DDoS атака (Destributed Denial of Service). Это атака направлена на остановку работы сервера (либо другое ее нарушение) жертвы посредством отсылки большого кол-ва пакетов на него. Это осуществляется путем использования некоторого количества компьютеров (в основном, ничем не повинных пользователей). Например, троянская программа, попавшая на компьютеры обычных пользователей, может быть запрограммирована на атаку в определенное время на определенный сервер. Сервер не может справиться с обслуживанием такого кол-ва пакетов и становится нефункционирующим.
3) Фарминг. Атака схожая с фишингом. Она основана на перенаправлении DNS адреса на сервер с поддельной, точной копией атакуемого. Это более опасная атака, так как пользователь вводит в окне настоящий адрес сервера, но попадает на поддельную страницу, которую сложно отличить от настоящего сайта. Такая атака осуществляется, например, с помощью изменения файла hosts в OS Windows, который отвечает за кэширование соответствия DNS IP адресу. Файл может быть изменен с помощью Трояна, который сделает в файле запись, производящую перенаправление с реального адреса на IP сервера хакеров.

Существует большое количество других атак, которые производятся на машины, на которые установлены веб-серверы. Такие атаки позволяют злоумышленникам заполучить все возможные данные, которые хранятся на сервере. Известны случаи, когда удавалось осуществить атаки на серверы платежных систем, которые обрабатывают огромное кол-во платежей по всему миру. Посредством таких атак было украдено большое количество номеров кредитных карточек. Пример этому нашумевшая атака на сервер VISA. Эти атаки подрывают доверие к электронным платежным системам. Хотя сама по себе система сильно защищена. Подводят уязвимости в программном обеспечении или операционных системах серверов, а также недостаточно квалифицированный персонал.

Несмотря на все сложности внедрения и осуществления мер по безопасности, платежные системы активно развиваются и распространяются, облегчая и ускоряя торговлю в Интернет.

Литература:

1. Linda Jean Camp “PRIVACY & RELIABILITY IN INTERNET COMMERCE”, A Dissertation submitted to the Graduate School in Carnegie Mellon University, 1996 http://reports-archive.adm.cs.cmu.edu/anon/1996/CMU-CS-96-198.ps
2. Семенов Ю.А. “Telecommunication technologies - телекоммуникационные технологии (v2.1)”, статья на основе материалов книг автора "Протоколы и ресурсы Интернет" (Радио и связь, М. 1996), "Сети Интернет. Архитектура и протоколы" (Синъ, М. 1998), "Протоколы Интернет. Энциклопедия" ("Горячая линия - Телеком", М. 2001) http://www.podgoretsky.com/ftp/Docs/Internet/Semenov/4/6/set_66.htm
3. Феномены интернета: фишинг http://www.webplanet.ru/news/focus/2004/6/15/phishing.html
4. Платежные средства в Интернет - понятие, технология и виды http://business.rin.ru/cgi-bin/search.pl?action=view&num=341384&razdel=26&w=0

5. The Electronic Check Architecture, Milton M. Anderson
http://www.echeck.org/library/wp/ArchitectualOverview.pdf