МИНИСТЕРСТВО РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ И КОМУНИКАЦИИ РЕСПУБЛИКИ УЗБЕКИТСАН

НУКУССКИЙ ФИЛИАЛ ТАШКЕНСТКОГО УНИВЕРСИТЕТА ИНФОРМАЦИОННЫХ ТЕХНОЛОГИИ

Факультет: Компьютерный инжиниринг

Группа: 201-15 КИ рус (2в КИ)

Самостоятельная работа

По предмету:_____

На тему:_ Защита информации в электронных платежных системах

Сдал : _____

Принял(а) : _____

ЗАЩИТА ИНФОРМАЦИИ В ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМАХ

Содержание

ВВЕДЕНИЕ

Одновременно с изобретением денег как абстрактного представления ценности, сформировались и различные платежные системы. Однако, с течением времени число способов абстрактного представления ценности росло, и каждый виток развития экономики привносил в эту область новые элементы, обеспечивая тем самым развитие и систем проведения платежей. Начав с бартера, общество прошло через введение банкнот, платежных поручений, чеков, а в последнее время еще и кредитных карт, и, наконец, вступило в эпоху электронных платежных систем. Стремительное развитие электронной коммерции привело к разработке множества самых различных электронных платежных систем, функциональные возможности которых постоянно расширяются и усложняются. Специалисты предсказывают, что до стабилизации рынка и установления на нем очевидных лидеров, тенденция роста числа предложений сохранится.

Присутствующие сегодня на рынке электронные платежные системы можно разделить на ряд категорий - как по поставщикам, так и согласно особенностям реализации. Каждая категория имеет своих лидеров и аутсайдеров, но пока ясно, что компаний, доминирующих на всем рынке в целом, еще нет, а наличные деньги, чеки и реальные кредитные карты широко используются параллельно своим электронным аналогам. Банки же традиционно осторожны к экспериментам с различными новыми решениями. Тем не менее, ожидается, что финансовые институты сыграют решающую роль в признании этих решений рынком электронных платежных систем. Актуальными пока остаются проблемы безопасности в электронных системах, традиционно являющиеся одним из ключевых вопросов финансового бизнеса. Кроме того, для всех этих предложений пока не разработана жесткая система стандартов, которые так же повлияли бы на развитие и принятие электронных платежных систем. Пока организационная часть данной отрасли находится в стадии становления, и ее участки еще нуждаются в серьезной защите.

ПОСТАНОВКА ЗАДАЧИ

Изучить основные понятия, алгоритмы, способы защиты информации в электронных платежных системах. Реализовать метод генерации PIN кода из номера счета клиента.

РЕАЛИЗАЦИЯ

Общий процесс генерации назначаемого PIN из номера банковского счета показан на рис.3. Сначала номер счета клиента дополняется нулями до 16 шестнадцатеричных цифр (8 байт). Затем генерируется псевдослучайное число, которое тоже дополняется нулями до 16 шестнадцатеричных цифр (8 байт). Полученные числа переводятся в двоичную систему счисления и складываются по модулю 2. Из полученного числа длиной 8 байт поочередно выделяют 4-битовые блоки, начиная с младшего байта. Если число, образуемое этими битами, меньше 10, то полученная цифра включается в PIN, иначе это значение не используется. Таким путем обрабатывают все 64 бита (8 байт) Если в результате обработки не удалось получить сразу требуемое количество десятичных цифр, то обращаются к неиспользованным 4-битовым блокам, из

которых берут остаток от деления на 10. Реализацию алгоритма можно увидеть в приложение 6.

Для функционирования программы достаточно, чтобы программное обеспечение включало операционную систему

Интерфейс программы прост в использование (см. рис.6). Пользователь должен ввести номер банковской карточки и выбрать длину PIN-кода, и на выходе он получит PIN-код, выбранной длины.

ПРИНЦИПЫ ФУНКЦИОНИРОВАНИЯ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ СИСТЕМ

Электронной платежной системой называют совокупность методов и реализующих их субъектов, обеспечивающих в рамках системы использование банковских пластиковых карт в качестве платежного средства.

Пластиковая карта - это персонифицированный платежный инструмент, предоставляющий пользующемуся этой картой лицу возможность безналичной оплаты товаров и услуг, а также получения наличных средств в банковских автоматах и отделениях банков. Предприятия торговли и сервиса и отделения банков, принимающие карту в качестве платежного инструмента, образуют приемную сеть точек обслуживания карты.

При создании платежной системы одной из основных решаемых задач является выработка и соблюдение общих правил обслуживания карт, выпущенных входящими в платежную систему эмитентами, проведения взаиморасчетов и платежей. Эти правила охватывают как чисто технические аспекты операций с картами - стандарты данных, процедуры авторизации, спецификации на используемое оборудование и другие, так и финансовые аспекты обслуживания карт - процедуры расчетов с предприятиями торговли и сервиса, входящими в состав приемной сети, правила взаиморасчетов между банками и т.д.

С организационной точки зрения ядром платежной системы является ассоциация банков, объединенная договорными обязательствами. Кроме того, в состав электронной платежной системы входят предприятия торговли и сервиса, образующие сеть точек обслуживания. Для успешного функционирования платежной системы необходимы и специализированные организации, осуществляющие техническую поддержку обслуживания карт: процессинговые и коммуникационные центры, центры технического обслуживания и т.п.

Обобщенная схема функционирования электронной платежной системы представлена на рис.1. Банк, заключивший соглашение с платежной системой и получивший соответствующую лицензию, может выступать в двух качествах - как банк-эмитент и как банк-эквайер. Банк-эмитент выпускает пластиковые карты и гарантирует выполнение финансовых обязательств, связанных с использованием этих карт как платежных средств. Банк-эквайер обслуживает предприятия торговли и сервиса, принимающие к оплате карты как платежные средства, а также принимает эти платежные средства к обналичиванию в своих отделениях и через принадлежащие ему банкоматы. Основными неотъемлемыми функциями банка-эквайера являются финансовые операции, связанные с выполнением расчетов и платежей точками обслуживания.

Технические атрибуты деятельности банка-эквайера (обработка запросов на авторизацию; перечисление на расчетные счета точек средств за товары и услуги, предоставленные по картам; прием, сортировка и пересылка документов, фиксирующих совершение сделок с использованием карт и т.п.) могут быть делегированы эквайером процессинговым центрам.

Неавтоматизированная процедура приема платежа с помощью карты сравнительно проста. В первую очередь кассир предприятия должен убедиться в подлинности пластиковой карты. При оплате предприятие должно перенести реквизиты пластиковой карты клиента на специальный чек с помощью копировальной машины-импринтера, занести в чек сумму, на которую была совершена покупка или оказана услуга, и получить подпись клиента. Оформленный подобным образом чек называют слипом.

В целях обеспечения безопасности операций платежной системы рекомендуется не превышать нижние лимиты сумм для различных регионов и видов бизнеса, по которым можно проводить расчеты без авторизации. При превышении лимитной суммы или в случае возникновения сомнения в личности клиента предприятие должно проводить процедуру авторизации. При авторизации предприятие фактически получает доступ к информации о состоянии счета клиента и может установить принадлежность карты клиенту и его платежную способность в размере суммы сделки. Одна копия слипа остается на предприятии, вторая передается клиенту, третья доставляется в банк-эквайер и служит основанием для возмещения суммы платежа предприятию со счета клиента.

В последние годы широкую популярность приобрели автоматизированные торговые POS-терминалы (Point-Of-Sale - оплата в точке продажи) и банкоматы. При использовании POS-терминалов нет необходимости в заполнении слипов. Реквизиты j пластиковой карты считываются с ее магнитной полосы на встроенном в POS-терминал считывателе. Клиент вводит в терминал свой PIN-код (Personal Identification Number - персональный идентификационный номер), известный только ему. Элементы PIN-кода включаются в общий алгоритм шифрования записи на магнитной полосе и служат электронной подписью владельца карты. На клавиатуре POS-терминала набирается сумма сделки.

Если сделка осуществляется в отделении банка и в ее процессе происходит выдача клиенту наличных денег, помимо банковских POS-терминалов может быть использован электронный кассир-банкомат. Конструктивно он представляет автоматизированный сейф со встроенным POS-терминалом. Терминал через встроенный модем обращается за авторизацией в соответствующую платежную систему. При этом используются мощности процессингового центра, услуги которого предоставляются торговцу банком-эквайером.

Процессинговый центр представляет собой специализированную сервисную организацию, которая обеспечивает обработку поступающих от банков-эквайеров или непосредственно из точек обслуживания запросов на авторизацию и протоколов транзакций - фиксируемых данных о произведенных посредством пластиковых карт платежах и выдачах наличными. Для этого процессинговый центр ведет базу данных, которая, в частности, содержит данные о банках-членах платежной системы и держателях пластиковых карт. Процессинговый центр хранит сведения о лимитах держателей карт и выполняет запросы на авторизацию в том случае, если банк-эмитент не ведет

собственной базы данных (off¬line банк). В противном случае (on-line банк) Процессинговый центр пересылает полученный запрос в банк-эмитент авторизируемой карты. Очевидно, что Процессинговый центр обеспечивает и пересылку ответа банку-эквайеру.

Выполнение банком-эквайером своих функций влечет за собой расчеты с банками-эмитентами. Каждый банк-эквайер осуществляет перечисление средств точкам обслуживания по платежам держателей карт банков-эмитентов, входящих в данную платежную систему. Поэтому соответствующие средства должны быть затем перечислены банку-эквайеру банками-эмитентами. Оперативное проведение взаиморасчетов между эквайерами и эмитентами обеспечивается наличием в платежной системе расчетного банка (одного или нескольких), в котором банки-члены системы открывают корреспондентские счета. На основании накопленных за операционный день протоколов транзакций процессинговый центр готовит и рассылает итоговые данные для проведения взаиморасчетов между банками-участниками платежной системы, а также формирует и рассылает банкам-эквайерам и непосредственно в точки обслуживания стоп-листы (перечни карточек, операции по которым по разным причинам приостановлены). Процессинговый центр может также обеспечивать потребности банков-эмитентов в новых картах, осуществляя их заказ на заводах и последующую персонализацию.

Особенностью продаж и выдач наличных по пластиковым картам является то, что эти операции осуществляются магазинами и банками "в долг", т.е. товары и наличные предоставляются клиентам сразу, а средства на их возмещение поступают на счета обслуживающих предприятий через некоторое время (не более нескольких дней). Гарантом выполнения платежных обязательств, возникающих в процессе обслуживания пластиковых карт, является выпустивший их банк-эмитент. Характер гарантий банка-эмитента зависит от платежных полномочий, предоставляемых клиенту и фиксируемых видом карточки.

По виду расчетов, выполняемых с помощью пластиковых карт, различают кредитные и дебетовые карты.

Кредитные карты являются наиболее распространенным видом пластиковых карт. К ним относятся карты общенациональных систем США Visa и MasterCard, American Express и ряда других. Эти карты предъявляют на предприятиях торговли и сервиса для оплаты товаров и услуг. При оплате с помощью кредитных карт банк покупателя открывает ему кредит на сумму покупки, а затем через некоторое время (обычно 25 дней) присылает счет по почте. Покупатель должен вернуть оплаченный чек (счет) обратно в банк. Естественно, подобную схему банк может предложить только наиболее состоятельным и проверенным из своих клиентов, которые имеют хорошую кредитную историю перед банком или солидные вложения в банк в виде депозитов, ценностей или недвижимости.

Держатель дебетовой карты должен заранее внести на свой счет в банке-эмитенте определенную сумму. Размер этой суммы определяет лимит доступных средств. При осуществлении расчетов с использованием этой карты соответственно уменьшается и лимит. Контроль лимита выполняется при проведении авторизации, которая при использовании дебетовой карты является обязательной. Для возобновления или увеличения лимита держателю карты необходимо вновь внести средства на свой счет. Для страхования временного разрыва между моментом осуществления

платежа и моментом получения банком соответствующей информации на счете клиента должен поддерживаться неснижаемый остаток.

Как кредитная, так и дебетовая карты могут быть не только персональными, но и корпоративными. Корпоративные карты предоставляются компанией своим сотрудникам для оплаты командировочных или других служебных расходов. Корпоративные карты компании связаны с каким-либо одним ее счетом. Эти карты могут иметь разделенный или неразделенный лимит. В первом случае каждому из держателей корпоративных карт устанавливается индивидуальный лимит. Второй вариант больше подходит небольшим компаниям и не предполагает разграничения лимита.

В последние годы все большее внимание привлекают к себе электронные платежные системы с использованием микропроцессорных карт. Принципиальным отличием микропроцессорных карт от всех перечисленных выше является то, что они непосредственно несут информацию о состоянии счета клиента, поскольку являются в сущности транзитным счетом. Все транзакции совершаются в режиме off-line в процессе диалога карта-терминал или карта клиента - карта торговца. Такая система является почти полностью безопасной благодаря высокой степени защищенности кристалла с микропроцессором и полной дебетовой схеме расчетов. Кроме того, хотя карта с микропроцессором дороже обычной, платежная система оказывается дешевле в эксплуатации за счет того, что в режиме off-line нет нагрузки на телекоммуникации.

Для обеспечения надежной работы электронная платежная система должна быть надежно защищена. С точки зрения информационной безопасности в системах электронных платежей существуют следующие уязвимые места:

пересылка платежных и других сообщений между банком и клиентом и между банками;

обработка информации внутри организаций отправителя и получателя сообщений;

доступ клиентов к средствам, аккумулированным на счетах.

Одним из наиболее уязвимых мест в системе электронных платежей является пересылка платежных и других сообщений между банками, между банком и банкоматом, между банком и клиентом. Пересылка платежных и других сообщений связана со следующими особенностями:

внутренние системы организаций отправителя и получателя должны быть приспособлены для отправки и получения электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);

взаимодействие отправителя и получателя электронного документа осуществляется опосредовано - через канал связи. Эти особенности порождают следующие проблемы:

взаимное опознавание абонентов (проблема установления взаимной подлинности):

защита электронных документов, передаваемых по каналам связи (проблемы обеспечения конфиденциальности и целостности документов);

защита процесса обмена электронными документами (проблема доказательства отправления и доставки документа);

обеспечение исполнения документа (проблема взаимного недоверия между отправителем и получателем из-за их принадлежности к разным организациям и взаимной независимости).

Для обеспечения функций защиты информации на отдельных узлах системы электронных платежей должны быть реализованы следующие механизмы защиты:

управление доступом на оконечных системах;

контроль целостности сообщения;

обеспечение конфиденциальности сообщения;

взаимная аутентификация абонентов;

невозможность отказа от авторства сообщения;

гарантии доставки сообщения;

невозможность отказа от принятия мёр по сообщению;

регистрация последовательности сообщений,

контроль целостности последовательности сообщений.

ЭЛЕКТРОННЫЕ ПЛАСТИКОВЫЕ КАРТЫ

Применение POS-терминалов и банкоматов возможно при использовании некоторого носителя информации, который мог бы идентифицировать пользователя и хранить определенные учетные данные. В качестве такого носителя информации выступают пластиковые карты.

Пластиковая карта представляет собой пластину стандартных размеров (85,6х53,9х0,76 мм), изготовленную из специальной, устойчивой к механическим и термическим воздействия пластмассы. Одна из основных функций пластиковой карты - обеспечение идентификации использующего ее лица как субъекта платежной системы. Для этого на пластиковую карту наносят логотипы банка-эмитента и платежной системы, обслуживающей эту карту, имя держателя карты, номер его счета, срок действия карты и т.п. Кроме того, на карте может присутствовать фотографий держателя и его подпись. Алфавитно-цифровые данные - имя номер счета и др. - могут быть эмбоссированы, т.е. нанесены рельефным шрифтом. Это дает возможность при ручной обработке принимаемых к оплате карт быстро перенести данные на чек с помощью специального устройства - импринтера, осуществляющего "прокатывание" карты (аналогично получению второго экземпляра при использовании копировальной бумаги).

По принципу действия различают пассивные и активные пластиковые карты. Пассивные пластиковые карты всего лишь хранят информацию на том или ином носителе. К ним относятся пластиковые карты с магнитной полосой.

Карты с магнитной полосой являются на сегодняшний день наиболее распространенными - в обращении находится свыше двух миллиардов карт подобного типа. Магнитная полоса располагается на обратной стороне карты и, в соответствии со стандартом ISO 7811, состоит из трех дорожек. Из них первые две предназначены для

хранения идентификационных данных, а на третью дорожку можно записывать информацию (например, текущее значение лимита дебетовой карты).

Однако из-за невысокой надежности многократно повторяемого процесса записи и считывания запись на магнитную полосу обычно не практикуется, и такие карты используются только в режиме считывания информации.

Карты с магнитной, полосой относительно уязвимы для мошенничества. Для повышения защищенности своих карт системы Visa и MasterCard/Europay используют дополнительные графические средства защиты: голограммы и нестандартные шрифты для эмбоссирования. Платежные системы с подобными картами требуют on-line авторизации в торговых точках и, как следствие, наличия разветвленных, высококачественных средств коммуникации (телефонных линий). Поэтому с технической точки зрения подобные системы имеют серьезные ограничения по их применению в странах с плохо развитыми системами связи.

Отличительная особенность активных пластиковых карт - наличие встроенной в нее электронной микросхемы. Принцип пластиковой карты с электронной микросхемой запатентовал в 1974 г. француз Ролан Морено. Стандарт ISO 7816 определяет основные требования к картам на интегральных микросхемах или Чеповым картам. В недалеком будущем карты с микросхемой вытеснят карты с магнитной полосой. Поэтому остановимся более подробно на основных типах карт с микросхемой.

Карты с микросхемой можно классифицировать по нескольким признакам. Первый признак - функциональные возможности карты.

Здесь можно выделить следующие основные типы карт:

карты-счетчики;

карты с памятью;

карты с микропроцессором.

Второй признак-тип обмена со считывающим устройством:

карты с контактным считыванием;

карты с индукционным считыванием.

Карты-счетчики применяются, как правило, в тех случаях, когда та или иная платежная операция требует уменьшения остатка на счете держателя карты на некоторую фиксированную сумму. Подобные карты используются в специализированных приложениях с предоплатой (плата за использование телефона-автомата, оплата автостоянки и т.д.) Очевидно, что применение карт со счетчиком ограничено и не имеет большой перспективы

Карты с памятью являются переходными между картами со счетчиком и картами с процессором. Карта с памятью - это в сущности перезаписываемая карта со счетчиком, в которой приняты меры, повышающие ее защищенность от атак злоумышленников. У простейших из существующих карт с памятью объем памяти может составлять от 32 байт до 16 килобайт. Эта память может быть реализована или в виде программируемого постоянного запоминающего устройства ППЗУ которое допускает однократную запись и многократное считывание, или в виде электрически стираемого программируемого постоянного запоминающего устройства ЭСППЗУ допускающего многократную запись и многократное считывание.

Карты с памятью можно подразделить на два типа с незащищенной (полнодоступной) и защищенной памятью.

В картах первого типа нет никаких ограничений на чтение и запись данных Их нельзя использовать в качестве платежных, так как специалист средней квалификации может их достаточно просто "взломать".

Карты второго типа имеют область идентификационных данных и одну или несколько прикладных областей. Идентификационная область карт допускает лишь однократную запись при персонализацию и в дальнейшем доступна лишь для считывания. Доступ к прикладным областям регламентируется и осуществляется только при выполнении определенных операций, в частности при вводе секретного PIN-кода.

Уровень защиты карт с памятью выше, чем у магнитных карт, и они могут быть использованы в прикладных системах, в которых финансовые риски, связанные с мошенничеством, относительно невелики. В качестве платежного средства карты с памятью используются для оплаты таксофонов общего пользования, проезда в транспорте, в локальных платежных системах (клубные карты) Карты с памятью применяются также в системах допуска в помещения и доступа к ресурсам компьютерных сетей (идентификационные карты). Карты с памятью имеют более низкую стоимость по сравнению с картами с микропроцессором

Карты с микропроцессором называют также интеллектуальными картами или смарт-картами (smart cards). Карты с микропроцессором представляют собой по сути микрокомпьютеры и содержат все соответствующие основные аппаратные компоненты центральный процессор (ЦП), оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ) и электрически стираемое программируемое ПЗУ (ЭСППЗУ) (рис.2).

В настоящее время в смарт-карты устанавливают:

микропроцессоры с текстовой частотой 5 МГц;

оперативное ЗУ емкостью до 256 байт,

постоянное ЗУ емкостью до 10 Кбайт;

энергонезависимое ЗУ емкостью до 8 Кбайт.

В ПЗУ записан специальный набор программ, называемый операционной системой карты COS (Cards Operation System). Операционная система поддерживает файловую систему, базирующуюся в ЭСППЗУ (емкость которого обычно находится в диапазоне 1.8 Кбайт, но может достигать и 64 Кбайт) и обеспечивающую регламентацию доступа к данным. При этом часть данных может быть доступна только внутренним программам карточки.

Смарт-карта обеспечивает обширный набор функций:

разграничение полномочий доступа к внутренним ресурсам (благодаря работе с защищенной файловой системой);

шифрование данных с применением различных алгоритмов;

формирование электронной цифровой подписи;

ведение ключевой системы;

выполнение всех операций взаимодействия владельца карты, банка и торговца.

Некоторые карты обеспечивают режим "самоблокировки" при попытке несанкционированного доступа. Смарт-карты позволяют существенно упростить процедуру идентификации клиента. Для проверки PIN-кода применяется алгоритм, реализуемый микропроцессором на карте. Это позволяет отказаться от работы POS-терминала и банкомата в режиме реального времени и централизованной проверки PIN. Отмеченные выше особенности делают смарт-карту высокозащищенным платежным инструментом, который может быть использован в финансовых приложениях, предъявляющих повышенные требования к защите информации. Именно поэтому микропроцессорные смарт-карты рассматриваются в настоящее время как наиболее перспективный вид пластиковых карт.

По принципу взаимодействия со считывающим устройством различают карты двух типов:

карты с контактным считыванием;

карты с бесконтактным считыванием.

Карта с контактным считыванием имеет на своей поверхности 8.10 контактных пластин. Размещение контактных пластин, их количество и назначение выводов различны у разных производителей и естественно, что считыватели для карт данного типа различаются между собой.

В последние годы начали широко применяться карты с бесконтактным считыванием. В них обмен данными между картой и считывающим устройством производится индукционным способом. Очевидно, что такие карты надежнее и долговечнее.

Персонализацию карты осуществляется при выдаче карты клиенту. При этом на карту заносятся данные, позволяющие идентифицировать карту и ее держателя, а также осуществить проверку платежеспособности карты при приеме ее к оплате или выдаче наличных денег.

Под авторизацией понимают процесс утверждения продажи или выдачи наличных по карте. Для проведения авторизации точка обслуживания делает запрос платежной системе о подтверждении полномочий предъявителя карты и его финансовых возможностей. Технология авторизации зависит от типа карты, схемы платежной системы и технической оснащенности точки обслуживания. Исторически сложилось так, что первоначальным способом персонализации карт было эмбоссирование.

Эмбоссирование - это процесс рельефного тиснения данных на пластиковой основе карты. На картах банков-эмитентов эмбоссируются, как правило, следующие данные: номер карты; даты начала и окончания срока ее действия; фамилия и имя владельца. Некоторые платежные системы, например Visa, требуют тиснения двух специальных символов, однозначно идентифицирующих принадлежность банка-эмитента к платежной системе. Эмбоссеры (устройства для тиснения рельефа на карте) выпускает ограниченный круг изготовителей. В ряде стран Запада законодательно запрещена свободная продажа эмбоссеров. Специальные символы, подтверждающие принадлежность карты к той или иной платежной системе, поставляются владельцу Эмбоссеры только с разрешения руководящего органа платежной системы. Эмбоссированная карта может служить средством платежа при использовании импринтера - устройства для прокатки слипа (чека), подтверждающего совершенную платежную операцию.

К персонализации карт относится также кодирование магнитной полосы либо программирование микросхемы.

Кодирование магнитной полосы производится, как правило, на том же оборудовании, что и эмбоссирование. При этом часть информации о карте, содержащая номер карты и период ее действия, одинаковая как на магнитной полосе, так и на рельефе. Однако бывают ситуации, когда после первичного кодирования требуется дополнительно занести информацию на магнитную дорожку. В этом случае применяются специальные устройства с Функцией "чтение-запись". Это возможно, в частности, когда PIN-код для пользования картой не формируется специальной программой, а может быть выбран клиентом по своему усмотрению.

Программирование микросхемы не требует особых технологических приемов, но зато оно имеет некоторые организационные особенности. В частности, для повышения безопасности и исключения возможных злоупотреблений операции по программированию различных областей микросхемы разнесены территориально и разграничены по правам различных сотрудников, участвующих в этом процессе.

Обычно эта процедура разбивается на три этапа:

на первом рабочем месте выполняется активация карты (ввод ее в действие);

на втором рабочем месте выполняются операции, связанные с обеспечением безопасности;

на третьем рабочем месте производится собственно персонализация карты.

Традиционно процесс авторизации проводится либо "вручную", когда продавец или кассир передает запрос по телефону оператору (голосовая авторизация), либо автоматически, когда карта помещается в POS-терминал, данные считываются с карты, кассиром вводится сумма платежа, а владельцем карты со специальной клавиатуры - секретный PIN-код. После этого терминал осуществляет авторизацию, либо устанавливая связь с базой данных платежной системы (on-line режим), либо реализуя дополнительный обмен данными с самой картой (off-line авторизация). В случае выдачи наличных денег процесс носит аналогичный характер, с той лишь особенностью, что деньги в автоматическом режиме выдаются специальным устройством - банкоматом, который и проводит авторизацию. Для защиты карт от подделки и последующего несанкционированного применения используются различные методы и способы. Например, для персонализации карт может применяться нанесение на пластиковую основу черно-белой или цветной фотографии владельца карты методом термопечати. На любой карте всегда существует специальная полоска с образцом подписи владельца карты. Для защиты карты, как таковой, различные платежные сообщества применяют специальные объемные изображения на лицевой и оборотной стороне карты (голограммы).

ПЕРСОНАЛЬНЫЙ ИДЕНТИФИКАЦИОННЫЙ НОМЕР

Испытанным способом идентификации держателя банковской карты является использование секретного персонального идентификационного номера PIN. Значение PIN должно быть известно только держателю карты. Длина PIN должна быть достаточно большой, чтобы вероятность угадывания злоумышленником правильного значения с помощью атаки полного перебора значений была приемлемо малой. С другой

стороны, длина PIN должна быть достаточно короткой, чтобы дать возможность держателям карт запомнить его значение. Рекомендуемая длина PIN составляет 4.8 десятичных цифр, но может достигать 12.

Предположим, что PIN имеет длину четыре цифры, тогда противник, пытающийся подобрать значение PIN к банковской карте, стоит перед проблемой выбора одной из десяти тысяч возможностей. Если число попыток ввода некорректного значения PIN ограничивается пятью на карту в день, этот противник имеет шансы на успех менее чем 1: 2000. Но на следующий день противник может попытаться снова, и его шансы увеличиваются до 1: 1000. Каждый следующий день увеличивает вероятность успеха противника. Поэтому многие банки вводят абсолютный предел на число неверных попыток ввода PIN на карту, чтобы исключить атаку такого рода. Если установленный предел превышен, считается, что данная карта неправильная, и ее отбирают.

Значение PIN однозначно связано с соответствующими атрибутами банковской карты, поэтому PIN можно трактовать как подпись держателя карточки. Чтобы инициировать транзакцию, держатель карты, который использует POS-терминал, вставляет свою карту в специальную Щель считывателя и вводит свой PIN, используя специальную клавиатуру терминала. Если введенное значение PIN и номер счета клиента, записанный на магнитной полосе карты, согласуются между собой, тогда инициируется транзакция.

Защита персонального идентификационного номера PIN для банковской карты является критичной для безопасности всей платежной системы. Банковские карты могут быть потеряны, украдены или подделаны. В таких случаях единственной контрмерой против несанкционированного доступа остается секретное значение PIN. Вот почему открытая форма PIN должна быть известна только законному владельцу карты. Она никогда не хранится и не передается в рамках системы электронных платежей. Очевидно, значение PIN нужно держать в секрете в течение всего срока действия карты.

Метод генерации значения PIN оказывает существенное влияние на безопасность электронной платежной системы. Вообще, персональные идентификационные номера могут формироваться либо банком, либо держателями карт. В частности, клиент различает два типа PIN:

PIN, назначенный ему банком, выдавшим карту;

PIN, выбираемый держателем карты самостоятельно.

Если PIN назначается банком, банк обычно использует один из двух вариантов процедур генерации PIN.

При первом варианте PIN генерируется криптографически из номера счета держателя карточки. Процесс генерации назначаемого PIN из номера счета показан на рис.3. Сначала номер счета клиента дополняется нулями или другой константой до 16 шестнадцатеричных цифр (8 байт). Затем получившиеся 8 байт шифруются по алгоритму DES с использованием секретного ключа. Из полученного шифр-текста длиной 8 байт поочередно выделяют 4-битовые блоки, начиная с младшего байта. Если число, образуемое этими битами, меньше 10, то полученная цифра включается в PIN, иначе это значение не используется. Таким путем обрабатывают все 64 бита (8 байт) Если в результате обработки не удалось получить сразу требуемое количество деся-

тичных цифр, то обращаются к неиспользованным 4-битовым блокам, из которых вычитают 10.

Очевидное достоинство этой процедуры заключается в том, что значение PIN не нужно хранить внутри электронной платежной системы. Недостатком этого подхода является то, что при необходимости изменения PIN требуется выбор либо нового счета клиента, либо нового криптографического ключа Банки предпочитают, чтобы номер счета клиента оставался фиксированным. С другой стороны, поскольку все PIN вычисляют, используя одинаковый криптографический ключ, изменение одного PIN при сохранении счета клиента неизбежно влечет за собой изменение всех персональных идентификационных номеров

При втором варианте банк выбирает значение PIN случайным образом, сохраняя значение этого PIN в виде соответствующей криптограммы. Выбранные значения PIN банк передает держателям банковских карт, пользуясь защищенным каналом

Использование PIN, назначенного банком, неудобно для клиента даже при небольшой его длине Такой PIN трудно удержать в памяти, и поэтому держатель карты может записать его куда-нибудь Главное - это не записать PIN непосредственно на карту или какое-нибудь другое видное место Иначе задача злоумышленника будет сильно облегчена.

Для большего удобства клиента используют значение PIN, выбираемое самим клиентом. Такой способ определения значения PIN позволяет клиенту:

использовать один и тот же PIN для различных целей;

задавать PIN как совокупность букв и цифр (для удобства запоминания).

Когда PIN выбран клиентом, он должен быть доведен до сведения банка. PIN может быть передан в банк заказной почтой или отправлен через защищенный терминал, размещенный в банковском офисе, который немедленно его шифрует. Если банку необходимо использовать выбранный клиентом PIN, тогда поступают следующим образом. Каждую цифру выбранного клиентом PIN складывают по модулю 10 (без учета переносов) с соответствующей цифрой PIN, выводимого банком из счета клиента. Получаемое десятичное число называется "смещением" Это смещение запоминается на карте клиента. Поскольку выводимый PIN имеет случайный характер, то выбранный клиентом PIN невозможно определить по его "смещению".

Главное требование безопасности состоит в том, что значение PIN должно запоминаться владельцем карты и никогда не должно храниться в любой читабельной форме. Но люди несовершенны и очень часто забывают свои значения PIN. Поэтому банки должны заранее заготовить специальные процедуры для таких случаев. Банк может реализовать один из следующих подходов. Первый основан на восстановлении забытого клиентом значения PIN и отправке его обратно владельцу карты. При втором подходе просто генерируется новое значение PIN.

При идентификации клиента по значению PIN и предъявленной карте используются два основных способа проверки PIN. неалгоритмический и алгоритмический. Неалгоритмический способ проверки PIN не требует применения специальных алгоритмов. Проверка PIN осуществляется путем непосредственного сравнения введенного клиентом PIN со значениями, хранимыми в базе данных. Обычно база данных со значениями PIN клиентов шифруется методом прозрачного шифрования, чтобы повысить ее защищенность, не усложняя процесса сравнения. Алгоритмический способ

проверки PIN заключается в том, что введенный клиентом PIN преобразуют по определенному алгоритму с использованием секретного ключа и затем сравнивают со значением PIN, хранящимся в определенной форме на карте. Достоинства этого метода проверки:

отсутствие копии PIN на главном компьютере исключает его раскрытие персоналом банка;

отсутствие передачи PIN между банкоматом или POS-терминалом и главным компьютером банка исключает его перехват злоумышленником или навязывание результатов сравнения;

упрощение работы по созданию программного обеспечения системы, так как уже нет необходимости действий в реальном масштабе времени.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ СИСТЕМ POS

Системы POS (Point-Of-Sale), обеспечивающие расчеты продавца и покупателя в точке продажи, получили широкое распространение в развитых странах и, в частности, в США. Системы POS осуществляют проверку и обслуживание дебетовых и кредитных карт покупателя непосредственно в местах продажи товаров и услуг в рамках системы электронных платежей. POS-терминалы, входящие в эти системы, размещаются на различных предприятиях торговли - в супермаркетах, на автозаправочных станциях и т.п.

POS-терминалы предназначены для обработки транзакций при финансовых расчетах с использованием пластиковых карт с магнитной полосой и смарт-карт. Использование POS-терминалов позволяет автоматизировать операции по обслуживанию этих карт и существенно уменьшить время обслуживания. Возможности и комплектация POS-терминалов варьируются в широких пределах, однако типичный современный POS-терминал снабжен устройствами считывания как с карт с магнитной полосой, так и со смарт-карт; энергонезависимой памятью; портами для подключения PIN-клавиатуры (клавиатуры для набора клиентом PIN-кода); принтера; соединения с персональным компьютером или электронным кассовым аппаратом.

Обычно POS-терминал бывает также оснащен модемом с возможностью автодозвона. POS-терминал обладает "интеллектуальными" возможностями - его можно программировать. В качестве языков программирования используются язык ассемблера, а также диалекты языков Си и Бейсик. Все это позволяет проводить авторизацию карт с магнитной полосой в режиме реального времени (on-line) и использовать при работе со смарт-картами автономный режим (off-line) с накоплением протоколов транзакций. Эти протоколы транзакций передаются в процессинговый центр во время сеансов связи. Во время этих сеансов POS-терминал может также принимать и запоминать информацию, передаваемую ЭВМ процессингового центра. В основном это бывают стоп-листы.

Схема системы POS приведена на рис.4. Покупатель для оплаты покупки предъявляет свою дебетовую или кредитную карту и вводит значение PIN для подтверждения личности. Продавец, в свою очередь, вводит сумму денег, которую необходимо уплатить за покупку или услуги. Затем в банк-эквайер (банк продавца) направляется запрос на перевод денег. Банк-эквайер переадресует этот запрос в банк-эмитент для

проверки подлинности карты, предъявленной покупателем. Если эта карта подлинная и покупатель имеет право применять ее для оплаты продуктов и услуг, банк-эмитент переводит деньги в банк-эквайер на счет продавца. После перевода денег на счет продавца банк-эквайер посылает на POS-терминал извещение, в котором сообщает о завершении транзакции. После этого продавец выдает покупателю товар и извещение.

Следует обратить внимание на тот сложный путь, который должна проделать информация о покупке, прежде чем будет осуществлена транзакция. Во время прохождения этого пути возможны искажения и потеря сообщений.

Для защиты системы POS должны выполняться следующие требования:

Проверка PIN, введенного покупателем, должна производиться системой банка-эмитента. При пересылке по каналам связи значение PIN должно быть зашифровано.

Сообщения, содержащие запрос на перевод денег (или подтверждение о переводе), должны проверяться на подлинность для защиты от замены и внесения изменений при прохождении по линиям связи и обрабатывающим процессорам.

Самым уязвимым местом системы POS являются ее POS-терминалы. В отличие от банкоматов в этом случае изначально предполагается, что POS-терминал не защищен от внешних воздействий. Угрозы для POS-терминала связаны с возможностью раскрытия секретного ключа, который находится в POS-терминале и служит для шифрования информации, передаваемой этим терминалом в банк-эквайер. Угроза раскрытия ключа терминала достаточно реальна, так как эти терминалы устанавливаются в таких неохраняемых местах, как магазины, автозаправочные станции и пр. Потенциальные угрозы из-за раскрытия ключа получили такие названия.

"Обратное трассирование". Сущность этой угрозы состоит в том, что если злоумышленник получит ключ шифрования, то он может пытаться восстановить значения PIN, использованные в предыдущих транзакциях.

"Прямое трассирование". Сущность этой угрозы состоит в том, что если злоумышленник получит ключ шифрования, то он попытается восстановить значения PIN, которые будут использоваться в последующих транзакциях.

Для защиты от угроз обратного и прямого трассирования предложены три метода:

метод выведенного ключа;

метод Ключа транзакции;

метод открытых ключей.

Сущность первых двух методов состоит в том, что они обеспечивают модификацию ключа шифрования передаваемых данных для каждой транзакции. Метод выведенного ключа обеспечивает смену ключа при каждой транзакции независимо от ее содержания. Для генерации ключа шифрования используют однонаправленную функцию от текущего значения ключа и некоторой случайной величины. Процесс получения (вывода) ключа для шифрования очередной транзакции представляет собой известное "блуждание" по дереву. Вершиной дерева рис.5 является некоторое начальное значение ключа I. Чтобы получить ключ с номером S, число S представляют в двоичной форме. Затем при вычислении значения ключа учитывается структура двоичного представления числа S, начиная со старшего разряда. Если L-й двоичный раз-

ряд числа S равен 1, то к текущему значению ключа К применяется однонаправленная функция FL (K), где L - номер рассматриваемого двоичного разряда. В противном случае переходят к рассмотрению следующего разряда числа S, не применяя однонаправленной функции. Последняя реализована на основе алгоритма DES. Для получения достаточного быстродействия количество единиц в двоичном представлении числа S обычно ограничивается - их должно быть не более 10. Этот метод обеспечивает защиту только от угрозы "обратного трассирования".

Метод ключа транзакции позволяет шифровать информацию, передаваемую между POS-терминалами и банком-эквайером, на уникальном ключе, который может меняться от транзакции к транзакции. Для генерации нового ключа транзакции используются следующие составляющие:

* однонаправленная функция от значения предыдущего ключа;

* содержание транзакции;

* информация, полученная от карты.

При этом предполагается, что предыдущая транзакция завершилась успешно. Метод ключа транзакции обеспечивает защиту как от "обратного трассирования", так и от "прямого трассирования". Раскрытие одного ключа не дает возможности злоумышленнику вскрыть все предыдущие и все последующие транзакции. Недостатком данной схемы является сложность ее реализации. Метод открытых ключей позволяет надежно защититься от любых видов трассирования и обеспечить надежное шифрование передаваемой информации. В этом случае POS-терминал снабжается секретным ключом для расшифровки сообщений банка-эквайера. Этот ключ генерируется при инициализации терминала. После генерации секретного ключа терминал посылает связанный с ним открытый ключ на компьютер банка-эквайера. Обмен между участниками взаимодействия выполняется с помощью открытого ключа каждого из них. Подтверждение подлинности участников осуществляется специальным центром регистрации ключей с использованием своей пары открытого и закрытого ключей. Недостатком этого метода является его сравнительно малое быстродействие.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ ЧЕРЕЗ СЕТЬ INTERNET

Все большее значение приобретает электронная торговля. Число покупок по банковским картам будет расти по мере создания систем заказов в оперативном режиме Internet. Сегодня Internet может рассматриваться как огромный рынок, способный охватить практически все население планеты Земля.

Под термином "электронная торговля" понимают предоставление товаров и платных услуг через глобальные информационные сети. виды электронной коммерции:

продажа информации, например подписка на базы данных, функционирующие в режиме on-line.

электронный магазин, который представляет собой Web-site.

электронные банки.

Основные методы защиты информации

Традиционный и проверенный способ электронной торговли, который ведет свое начало от обычной торговли по каталогам, представляет собой оплату товаров и услуг кредитной карточкой по телефону. В этом случае покупатель заказывает на Web-сервере список товаров, которые он хотел бы купить, и потом сообщает по телефону номер своей кредитной карточки продавцу коммерческой фирмы. Затем происходит обычная авторизация карты, а списание денег со счета покупателя производится лишь в момент отправки товара по почте или с курьером.

Для того чтобы покупатель - владелец кредитной карточки мог без опасений расплатиться за покупку через сеть, необходимо иметь более надежный, отработанный механизм защиты передачи электронных платежей. Такой принципиально новый подход заключается в немедленной авторизации и шифровании финансовой Информации в сети Internet с использованием схем SSL и SET.

Протокол SSL (Secure Socket Layer) предполагает шифрование информации на канальном уровне.

Протокол "Безопасные электронные транзакции" SET (Secure Electronic Transactions), разработанный компаниями Visa и MasterCard, предполагает шифрование исключительно финансовой информации.

Особенности функционирования протокола SET

Для того чтобы обеспечить полную безопасность и конфиденциальность совершения сделок, протокол SET должен гарантировать непременное соблюдение следующих условий.

1. Абсолютная конфиденциальность информации. Владельцы карточек должны быть уверены в том, что их платежная информация надежно защищена и доступна только указанному адресату. Это является непременным условием развития электронной торговли.

2. Полная сохранность данных. Участники электронной торговли должны быть уверены в том, что при передаче от отправителя к адресату содержание сообщения останется неизменным." Сообщения, отправляемые владельцами карточек коммерсантам, содержат информацию о заказах, персональные данные и платежные инструкции. Если в процессе передачи изменится хотя бы один из компонентов, то данная транзакция не будет обработана надлежащим образом. Поэтому во избежание ошибок протокол SET должен обеспечить средства, гарантирующие сохранность и неизменность отправляемых сообщений. Одним из таких средств является использование цифровых подписей.

3. Аутентификация (установление подлинности) счета владельца карточки. Использование цифровых подписей и сертификатов владельца карточки гарантирует аутентификацию счета владельца карточки и подтверждение того, что владелец карточки является законным пользователем данного номера счета.

4. Владелец карточки должен быть уверен, что коммерсант действительно имеет право проводить финансовые операции с финансовым учреждением. Использование цифровых подписей и сертификатов коммерсанта гарантирует владельцу карточки, что можно безопасно вести электронную торговлю.

Участники системы расчетов и криптографические средства защиты транзакций. Протокол SET изменяет способ взаимодействия участников системы расчетов. В данном случае электронная транзакция начинается с владельца карточки, а не с коммерсанта или эквайера.

Коммерсант предлагает товар для продажи или предоставляет услуги за плату. Протокол SET позволяет коммерсанту предлагать электронные взаимодействия, которые могут безопасно использовать владельцы карточек.

Эквайером (получателем) является финансовое учреждение, которое открывает счет коммерсанту и обрабатывает авторизации и платежи по кредитным карточкам. Эквайера обрабатывает сообщения о платежах, переведенных коммерсанту посредством платежного межсетевого интерфейса. При этом протокол SET гарантирует, что при взаимодействиях, которые осуществляет владелец карточки с коммерсантом, информация о счете кредитной карточки будет оставаться конфиденциальной.

Системы кредитных карт утвердились в значительной степени в качестве платежного средства для приобретения товаров непосредственно у продавца. Основное отличие использования кредитных карт в сети Internet заключается в том, что в соответствии со стандартом SET для защиты транзакций электронной торговли используются процедуры шифрования и цифровой подписи.

Сеть Internet рассчитана на одновременную работу миллионов пользователей, поэтому в коммерческих Internet-приложениях невозможно использовать только симметричные криптосистемы с секретными ключами. В связи с этим применяются также асимметричные криптосистемы с открытыми ключами. Шифрование с использованием открытых ключей предполагает, что у коммерсанта и покупателя имеются по два ключа - один открытый, который может быть известен третьим лицам, а другой - частный (секретный), известный только получателю информации

Правила SET предусматривают первоначальное шифрование сообщения с использованием случайным образом сгенерированного симметричного ключа, который, в свою очередь, шифруется открытым ключом получателя сообщения. В результате образуется так называемый электронный конверт. Получатель сообщения расшифровывает электронный конверт с помощью своего частного (секретного) ключа, чтобы получить симметричный ключ отправителя. Далее симметричный ключ отправителя используется для расшифрования присланного сообщения.

Целостность информации и аутентификации участников транзакции гарантируется использованием электронной цифровой подписи.

Протокол SET вводит новое применение цифровых подписей, а именно использование двойных цифровых подписей. В рамках протокола SET двойные цифровые подписи используются для связи заказа, отправленного коммерсанту, с платежными инструкциями, содержащими информацию о счете и отправленными банку.

Например, покупатель Боб хочет направить коммерсанту Алисе предложение купить единицу товара и авторизацию своему банку на перечисление денег, если Алиса примет его предложение. В то же время Боб не хочет, чтобы в банке прочитали условия его предложения, равно как и не хочет, чтобы Алиса прочитала его информацию о счете. Кроме того, Боб хочет связать свое предложение с перечислением так, чтобы деньги были перечислены только в том случае, если Алиса примет его предложение.

Все вышесказанное Боб может выполнить посредством Цифровой подписи под обоими сообщениями с помощью одной операции подписывания, которая создает двойную цифровую подпись. Двойная цифровая подпись создается путем формирования дайджеста обоих сообщений, связывания двух сообщений вместе, вычисления дайджеста итога предыдущих операций и шифрования этого дайджеста личным операции подписывания, которая создает двойную цифровую подпись. Двойная цифровая подпись создается путем формирования дайджеста обоих сообщений, связывания двух сообщений вместе, вычисления дайджеста итога предыдущих операций и шифрования этого ключом для подписи автора. Автор обязан включить также дайджест другого сообщения, с тем, чтобы получатель проверил двойную подпись.

Получатель любого из этих сообщений может проверить его подлинность, генерируя дайджест из своей копии сообщения, связывая его с дайджестом другого сообщения (в порядке, предусмотренном отправителем) и вычисляя дайджест для полученного итога. Если вновь образованный дайджест соответствует расшифрованной двойной подписи, то получатель может доверять подлинности сообщения.

Если Алиса принимает предложение Боба, она может отправить сообщение банку, указав на свое согласие и включив дайджест сообщения с предложением Боба. Банк может проверить подлинность авторизации Боба на перечисление и дайджеста сообщения с предложением Боба, предоставленного Алисой, чтобы подтвердить двойную подпись. Таким образом, банк может проверить подлинность предложения на основании двойной подписи, но банк не сможет прочитать условия предложения.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы была написана программа по генерации персонального идентификационного номера из номера счета клиента. Данная программа может генерировать PIN длиной 4,8 и 12 десятичных цифр.

В будущем, надеюсь, продолжить изучение электронных платежных систем и более подробно ознакомится с алгоритмами цифровой подписи

СПИСОК СОКРАЩЕНИЙ

COS (Cards Operation System) - операционная система карты

DES (Data Encryption Standart) - старый американский стандарт шифрования, заменен в 2002 году стандартом AES

ISO (International Organization for Standardization) - международная организация по стандартизации

PIN-код (Personal Identification Number) - персональный идентификационный номер

POS-терминалы (Point-Of-Sale) - оплата в точке продажи

SET (Secure Electronic Transactions) - протокол "Безопасные электронные транзакции"

SSL (Secure Socket Layer) - протокол защиты транзакций в интернете

НСПК - национальная система платежных карт "Российская платежная карта"

ОЗУ - оперативное запоминающее устройство

ПЗУ - постоянное запоминающее устройство

ЦП - центральный процессор
ЭВМ - электронная вычислительная машина
ЭСППЗУ - электрически стираемое программируемое ПЗУ

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Романец Ю.В. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин. - 2-е изд. исп. - М.: Изд-во “Радио и связь”, 2001. - 376с.

2. Деднев М.А. Защита информации в банковском деле и электронном бизнесе / М.А. Деднев Д.В. Дыльнов, М.А. Иванов. - М.: Изд-во “ОЦ КУДИЦ-ОБРАЗ”, 2004. - 512с.

3. Воронков Б.Н. Криптографические методы защиты информации / Б.Н. Воронков. - Воронеж: Издательско-полиграфический центр Воронежского Государственного университета, 2008. - 58с.