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

Применение криптографии в банковском деле

Студента 116 группы
Марданова Вадима

2005 г.

Применение криптографии в банковском деле

Проведение расчетов между субъектами банковской системы осуществляется юридическими, организационных, технологических, технических и информационных средствами. Под совокупностью этих средств понимается механизм, называемый платежной системой. Через платежную систему и выполняются обязательства, возникающие в результате экономической деятельности. Обычно в качестве субъектов платежной системы выделяют государство, коммерческие и общественные организации и предприятия и отдельных граждан. Между субъектами платежной системы происходят разного рода информационные отношения (получение, хранение, обработка, распространение и использование информации). В информационных процессах основными интересами субъектов информационных отношений (сокр. СИО) являются обеспечение своевременного доступа к необходимой им информации, конфиденциальности информации, достоверности информации, защиты от дезинформации, защиты информации от незаконного ее тиражирования и возможности осуществления контроля и управления процессами обработки и передачи информации. В целом СИО хотят обеспечить свою информационную безопасность, причем не любыми средствами, а в зависимости от величины ущерба, который в принципе им может быть нанесен. Для проведения анализа множество СИО с законными интересами дополняют еще одним субъектом информационных отношений, таким как "злоумышленник". Поэтому теперь остальным СИО необходимо обеспечивать информационную безопасность, поддерживая доступность, целостность и конфиденциальность информации. Заметим, что вред для СИО может быть нанесен через определенную информацию и носители информации, в том числе автоматизированные системы обработки. Для этого требуется также обеспечение безопасности систем обработки и передачи информации, но в конечном счете цель обеспечения информационной безопасности заключена в обеспечении законных прав СИО.

Мировая статистика случаев компьютерных преступлений в банковской сфере показывает, что около 70% - это воровство денеги услуг и около 20% - это воровство и подделка данных. Задача криптографии и применение криптографии в банковском деле устранение тех угроз, которые характерны для платежной системы. А это:

- несанкционированный доступ посторонних лиц, не принадлежащих к числу банковских служащих, и ознакомление с хранимой конфиденциальной информацией;
- ознакомление банковских служащих с информацией, к которой они не должны иметь доступа;
- несанкционированное копирование программ и данных;
- перехват и последующее раскрытие конфиденциальной информации, передаваемой по каналам связи;
- кража магнитных носителей, содержащих конфиденциальную информацию;
- кража распечатанных банковских документов;
- случайное или умышленное уничтожение информации;
- несанкционированная модификация банковскими служащими финансовых документов, отчетности и баз данных;
- фальсификация сообщений, передаваемых по каналам связи, в том числе и навязывание ранее переданного сообщения;
- отказ от авторства сообщения, переданного по каналам связи;
- отказ от факта получения информации;
- ошибки в работе обслуживающего персонала;
- разрушение файловой структуры из-за некорректной работы программ или аппаратных средств;
- разрушение информации, вызванное вирусными воздействиями;
- разрушение архивной банковской информации, хранящейся на магнитных носителях;
- кража оборудования;
- ошибки в программном обеспечении;

- сбои оборудования, в том числе и за счет отключения электропитания и других факторов, препятствующих работе оборудования.

У данных угроз могут быть разные вероятности появления, которые зависят от конкретных факторов в банке.

На сегодняшний день мы можем наблюдать некую скрытую борьбу между банками за сохранение ведущих позиций и привлечение новых клиентов, а это осуществимо только при условии предоставления большего количества услуг и сокращения времени обслуживания. А это в свою очередь достигается лишь при обеспечении необходимого уровня автоматизации всех банковских операций.

Но выше были назван список угроз, характерных для платежной системы, из которого напрашивается вывод, что применение вычислительной техники наряду с разрешением возникающих проблем приводит к появлению нетрадиционных для банка угроз. Эти новые угрозы связаны с подверженностью информации физическому искажению или уничтожению, возможностью случайной или умышленной модификации, а также опасностью несанкционированного получения информации лицами, для которых она не предназначена. Тем не менее, главная задача - задача защиты банковской информации и в том числе внедрение криптографических средств в банковском деле. И естественно, что уровень мероприятий по защите информации с помощью криптографических методов, как правило, немного отстает от темпов автоматизации и, в принципе, такое отставание может может повлечь к серьезным последствиям. И неразвитость рынка криптографической продукции - одна из основных причин этого отставания. Например, в России раньше нормативная база по этим вопросам закрепляла большие полномочия за ФАПСИ (Федеральное агентство правительственной связи и информации при Президенте РФ, занимавшейся лицензированием, сертификацией и т. д.), которая, как сообщается, прекратила свое существование после административной реформы. Необходимо также отличать банковскую информацию от военных и государственных секретов - традиционных объектов криптографической защиты. Поэтому требования к средствам криптографической защиты банковской информации должны быть «мягче».

В условиях уязвимости информации в автоматизированных комплексах необходимо принятие мер защиты. Однако имеются некоторые трудности. Во-первых, производителями средств защиты в основном предлагаются отдельные компоненты для решения частных задач, и потребителям приходится решать вопросы совместимости этих средств системы защиты. Во-вторых, для обеспечения надежной защиты требуется решение целого комплекса технических и организационных проблем и разработка соответствующей документации. В-третьих, видимо, квалифицированный злоумышленник в реальной сложной системе всегда может «обмануть» производителя средств защиты. Поэтому совершенствование защиты должно происходить постоянно в процессе накопления новых знаний.

Система защиты работает в три этапа: анализ риска, реализация политики безопасности и поддержка политики безопасности. Политика безопасности направлена на достижение конфиденциальности, целостности и готовности. В платежной системе высший приоритет следует отдать обеспечению готовности системы к обслуживанию, так как перерывы в ее функционировании приводят к значительным убыткам для всех ее участников. Следующее по значимости свойство платежной системы - обеспечение целостности информации. И третья по значимости цель защиты информации в платежной системе - обеспечение конфиденциальности, так как ее нарушение не ведет к прямым убыткам участников расчетов и, как правило, не носит катастрофических последствий, хотя и является необходимой для защиты участников платежной системы от промышленного шпионажа и криминальных структур.

Очень важный элемент для платежной системы - защита юридической значимости платежных документов для справедливого разрешения споров и определения виновных в нанесенном ущербе, т.к. имея юридическую защищенность, участники доверяют системе платежей. Это является аргументом в пользу того, что для платежной системы более приоритетными являются криптографические методы обеспечения подлинности и целостности платежных документов, а не методы обеспечения конфиденциальности.

Защита банковской информации при ее передаче по телеграфным и почтовым каналам связи осуществляется в основном организационными мерами с использованием криптографических средств. Этими средствами являются системы кодов подтверждения. В России в некоторых регионах, используется модемная связь для передачи информации, а в качестве средств защиты применяются средства шифрования и электронной цифровой подписи (ЭЦП) различных фирм-производителей криптопродуктов. Криптографические методы для защиты от несанкционированного доступа почти не применяются при обработке и хранении банковской информации, а также не реализована комплексная защита информации на всех этапах ее обработки, хранения и передачи.

Криптографическая защита платежной системы как информационно-телекоммуникационной системы должна удовлетворять некоторым стандартным требованиям: стойкие криптоалгоритмы, имитозащищенность, устойчивые к компрометациям ключевые системы и др. Также платежная система имеет ряд специфических особенностей, накладывающие дополнительные требования на средства криптографической защиты. Например, платежная система должна требовать надежность и оперативность перевода платежей между участниками расчетов. Например, в некоторых странах с развитой платежной системой требуется проводить платежи в течение суток. Еще один фактор, влияющий на криптографическую защиту платежной системы – то, что Центральный банк перед коммерческими банками и коммерческие банки перед своими клиентами несут ответственность за нарушение сроков и корректность проводки платежей. Необходимо также учесть то, что платежная система подвергается нападениям злоумышленников. В роли этих злоумышленников могут выступать как посторонние лица, так и сами пользователи платежной системы. Число участников платежной системы очень велико. Так, например, на сегодняшний момент участники платежной системы – это около 1400 расчетно-кассовых центров и более 3.5 тысяч коммерческих банков и их филиалов. Имеются и ряд других немало важных особенностей.

Считается, что для практических нужд платежной системы использование алгоритмов электронной цифровой подписи (ЭЦП) и шифрования достаточно. Эти алгоритмы обеспечивают стойкость в течение трех лет. Российские ГОСТы выполняют это требование со значительным запасом. Однако есть определенные трудности в обеспечении требуемой скорости реализации системы ЭЦП на гостированном алгоритме. Поэтому требуется разработка новых алгоритмов ЭЦП и шифрования, лучше учитывающих требования по сохранности банковской информации (3 года) и являющихся за счет этого значительно более скоростными при реализации.

Очень важная роль отдается организации ключевой системы при использовании криптосистем в банковских платежных системах. Высокие требования по надежности, оперативности и безотказности платежной системы в целом, ее подверженность постоянным нападениям со стороны злоумышленников (включая легальных пользователей), придание юридической значимости электронным платежным документам и другие особенности платежной системы существенно влияют на выбор ключевых систем. С учетом этого можно сформулировать следующие требования для ключевых систем. Какой должна быть ключевая система? Во-первых, компрометации не должны влиять на безопасную работу участников платежной системы с нескомпрометированными ключами, т.е. необходима устойчивость к компрометации ключей у любого числа корреспондентов сети. Во-вторых, в ключевой системе должна быть возможность быстрого восстановления при любом числе компрометаций, и она должна предусматривать как можно меньшее число ключей, подлежащих сохранности организационными мерами пользователей. И третье требование к ключевой системе – обеспечение носителями ключевой информации высокой степени защиты их от копирования.

Владельцы подписи должны производить генерацию ключей ЭЦП, а регистрация, учет и рассылка открытых компонент ключей ЭЦП производятся централизованно администраторами безопасности на региональном и межрегиональном уровнях с обеспечением невозможности их фальсификации и подмены. Разработчики системы управления ключами (поддержание баз открытых ключей, замена ключей при нештатных ситуациях и т.п.) должны в максимальной

степени автоматизировать ее и минимизировать число конечных пользователей в процессах управления ключами.

Выбор и построение системы криптозащиты должен также учитывать, до какой степени снижается производительность платежной системы и каковы дополнительные ограничения накладываются на технические средства и программное обеспечение. Поэтому эффективной системой защиты называют такую систему, которая не приводит к ощутимым трудностям в работе банка. В случае возникновения конфликтов необходимо иметь механизмы их справедливого разрешения, а, значит, криптографические системы должны иметь проработанные технологии разрешения конфликтных ситуаций, включая процедуры создания третейских судов, описание порядка разрешения споров с их помощью, требования к предоставляемой архивной информации для разрешения споров и требования к техническим средствам, используемым при разрешении споров.

Многие аспекты криптографической защиты банковской информации на сегодняшний день регламентированы международными стандартами. Это осуществляется Техническим комитетом ТК68 Международной организации стандартов (МОС/ТК68) "Банковское дело и соответствующие финансовые операции". Здесь непосредственная разработка стандартов по защите банковской информации осуществляется двумя подкомитетами: МОС/ТК68/ПК2 - "Операции, процедуры и безопасность" и МОС/ТК68/ПК6- "Карточки для финансовых операций, операции и соответствующие носители информации". МОС/ТК68/ПК2 занимается безналичными электронными расчетами при так называемых оптовых финансовых операциях, т.е. операциях по расчетам между финансовыми учреждениями и организациями и обслуживаемыми ими субъектами экономической деятельности. А МОС/ТК68/ПК6 занимается безналичными электронными расчетами в розничной торговле (а это использование наличных денег на потребительском рынке товаров и услуг населению. Собственно ТК68, так же, как и другие подкомитеты, занятые стандартизацией конкретных приложений, не занимается разработкой методов и средств криптографической защиты, а занимается разработкой стандартов по "встраиванию" стандартных механизмов защиты в банковские процедуры и технологии электронного обмена.

Стандартизация общих методов и средств защиты информации в информационных технологиях в рамках МОС возложена на специализированный подкомитет ПК27, который был создан в 1989 г. в рамках Объединенного технического комитета Международной организации по стандартизации и Международной электротехнической комиссии МОС/МЭКОТК1 "Информационные технологии". Международные стандарты, разработанные в рамках ПК27, определяют общие универсальные механизмы обеспечения безопасности в открытых системах. Здесь рассмотрены вопросы организации и управления, но без их привязки к конкретным приложениям.

Выше было сказано о криптографических схемах (таких как криптосистемы, схемы электронной подписи и т. п.) универсального назначения. По отношению к ним защита банковской информации - всего лишь одна из возможных областей применения. Но в в теории по криптографии есть два направления исследований, разрабатываемых специально и исключительно для банковских приложений. Это *криптографическое обеспечение банковских карточек* и *банковские криптографические протоколы*.

Банковские карточки называют также интеллектуальными карточками.

Пластиковая банковская карточка - это пластина размеров 85.6 мм на 53.9 мм. Она изготовлена из пластмассы, устойчивой к механическим и термическим воздействиям. Одна из основных функций пластиковой карточки - обеспечение идентификации использующего ее лица как субъекта платежной системы. Ввиду этого на нее наносятся логотипы банка-эмитента и платежной системы, обслуживающей карточку, имя держателя карточки, номер его счета, срок действия карточки и т.п. Еще на карточке может быть фотография держателя и его подпись. Алфавитно-цифровые данные - имя, номер счета и др. - могут быть нанесены рельефным шрифтом. Поэтому при ручной обработке принимаемых к оплате карточек быстро перенести данные на чек с помощью специального устройства, импринтера, осуществляющего

"прокатывание" карточки (в точности так же, как получается второй экземпляр при использовании копировальной бумаги).

Криптографическая часть банковской карточки может включать в себя наряду с специфическими для банков компонентами криптоалгоритмы, реализующие схемы аутентификации, электронной подписи и т.п. Новое поколение пластиковых карточек отличается от всех предшествующих тем, что появились развитые возможности для реализации средств защиты информации. Сейчас интеллектуальные карточки становятся основным платежным средством. Имеющиеся в интеллектуальных карточках вычислительные возможности становятся все более эффективными в реализации сложных криптографических схем. Хотя проблема компромисса между эффективностью реализации и стойкостью криптографических схем остается достаточно острой для банковских систем, использующих интеллектуальные карточки.

Еще одно направление, разработанное для банковских приложений - это *банковские криптографические протоколы*. Их задача - обеспечить безопасность систем электронных платежей. Цифровая подпись является одним из элементов криптографического протокола - способа обмена информацией, при котором стороны своих целей достигают, а противник не достигает. Цели сторон - целостность, конфиденциальность. Именно надежность криптографических алгоритмов обеспечивает достижение упомянутых целей. Понятно, что если взломать шифр или подделать ЭЦП можно при небольших затратах за небольшое время, то говорить о достижении целей не приходится. Параметры стандартов криптографических преобразований, длины ключей выбираются таким образом, что их взлом (помимо похищения ключа) невозможен в течение десятков лет. Что касается злоумышленников, то их успехи возможны только при использовании "слабых" или нестандартных криптопротоколов. Надежные криптопротоколы (и соответствующие шифрсредства) известны и используются многими странами более 50 лет для защиты дипломатической, военной и др. переписки. Вопреки распространенным заблуждениям криптографическая стойкость таких систем может сохраняться еще в течение десятков лет. Для взлома такой системы потенциальный злоумышленник должен будет решить классические задачи из некоторых разделов математики, что маловероятно.

Автоматизированные системы банковских расчетов также называют системами электронных платежей, хотя представляют собой системы безналичного расчета с использованием современных средств связи. Сейчас в системах электронных платежей бумажные деньги полностью заменяются электронными деньгами, используемые клиентами для платежей при расчетах с банком или между собой. Еще одна особенность систем электронных платежей является обеспечение неотслеживаемости действий клиентов. Зарубежные специалисты объяснили необходимость обеспечения неотслеживаемости на примерах подобных следующему: кредитные карточки полностью идентифицируют их владельцев при каждом платеже. И если владелец кредитной карточки использует ее для покупки билетов на автобусы, то транспортная компания «знает» обо всех его поездках. Конечно же, это не серьезная угроза, но если рассматривать переводов крупных сумм и участие организованной преступности очевидно. Поэтому разработчики осознают необходимость обезопасить автоматизированные банковские системы от действий злоумышленников. Некоторые противники неотслеживаемости говорят, что неотслеживаемость не нужна, т.к. если клиент не доверяет банку, то он никогда не положит в этот банк свои деньги. Но дело в том, что клиент не доверяет персоналу, работающему в банке и третьим лицам, которые могут перехватывать информацию в каналах связи. С другой стороны, всякий банк, который заботится о неотслеживаемости платежей, повышает доверие клиентов к себе.

Индивидуальным платежным средством в системах электронных платежей является электронный бумажник клиента. Электронный бумажник - это карманный вычислитель со встроенным в него защищенным модулем. Бумажник выдается клиенту и используется в системах электронных платежей как. Электронные бумажники, с одной стороны, обеспечивают неотслеживаемость действий клиента, а с другой - безопасность банка и высокую

эффективность системы электронных платежей. Привычный кошелек превращается в портативное электронное устройство для оплаты покупок как в традиционных магазинах, так и в онлайне. Многие компании преследуют именно такую цель. С помощью электронного бумажника покупатели могут выбирать необходимую им кредитную карту и передавать информацию о карточке на терминал, который заносит информацию о покупке в электронный бумажник. Внешне бумажник напоминает обычное кожаное портмоне с карманами, но со встроенным экраном и клавиатурой.

Таков общий взгляд на применение криптографии в банковском деле.

Литература:

1. **Криптография в банковском деле.** М. И. Анохин, Н. П. Варновский, В. М. Сидельников, В. В. Ященко - М.: МИФИ. 1997. 274с. (http://www.cryptography.ru/db/msg.html?mid=1169307&uri=node189.html)
2. **Электронные бумажники на подходе** (http://www.revkom.ru/info/?id=1919)
3. **Криптографический протокол** (www.enigma.by/crypt4.html)
4. http://www.ibusiness.ru/offline/2003/238/25105/
5. **Пластиковая карточка как платежный инструмент (основные понятия)** (www.citforum.ru/marketing/articles/art_8.shtml)
6. **Основы криптографии.** Учебное пособие. А.П.Алферов и др.