**МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ (ГУ)**
**Факультет радиотехники и кибернетики**

**Эссе по курсу «Защита информации»**

# Меры предотвращения атак на банковские системы электронных денег

*Подготовил студент 312 группы*
*Румянцев Л.А.*

Долгопрудный, 2007

**Введение**:

Для обеспечения целостности, достоверности и конфиденциальности критических данных следует использовать меры безопасности. Так же они защищают от несанкционированного дублирования или отмены транзакций. Здесь мы ознакомимся с различными видами мер безопасности, которые используются разработчиками систем электронных денег для того, чтобы оградить себя от следующих опасностей: дублирование оборудования, изменение или дублирование данных или кода, изменение сообщений, кража данных, отмена транзакций.

Меры безопасности могут быть сгруппированы непосредственно по действиям, которые они производят по отношению к опасности: предотвращают, детектируют или ограничивают. Основная задача мер, связанных с предотвращением опасности, - это гарантировать, что атака на компоненты системы будет предотвращена до того как выполнится несанкционированная транзакция. Детектирующие меры сигнализируют пользователя или оператора об атаке и помогают определить её источник. Ограничивающие меры не позволяют удавшимся поддельным транзакциям широко распространить своё влияние. Детектирующие и ограничивающие меры имеют огромное защитное значение, поэтому они важны не менее, чем предотвращающие. Но в рамках данного эссе мы рассмотрим лишь последние.

## Меры предотвращения

### *1. Физическая защита оборудования*

Оборудование, используемое в системах электронных денег, представляет собой первую ступень защиты от атак. В карточных системах, обработка, связанная с критическими данными, происходит в физически скрытых модулях, таких как смарт-карты, содержащие микропроцессорный чип. Со стороны банка таким оборудованием может тоже быть смарт-карта, а может быть терминал, обрабатывающий платежи. Очень сложные защитные механизмы карты включают в себя как логическую (программную) так и физическую (на уровне оборудования) защиту. Программный защитный код расположен в чипе так, чтобы его невозможно быть изменить или прочитать. Программная защита обеспечивает неприкосновенность критических данных, хранящихся на чипе, за исключением случаев, когда доступ производиться после предварительной аутентификации и соответствует протоколам доступа, включающим обычно стадию шифрования.

Хранение данных на смарт-карте имеет разные уровни защиты. Данные, которые не требуют изменения, хранят в ROM(read-only memory). Изменяемые, но чувствительные данные хранят в памяти EEPROM(electronically erasable programmable read-only memory). Их можно изменять внутренними функциями чипа.

Физическая защита создаётся вместе с оборудованием и представляет собой физические препятствия для оптического или электрического чтения данных или физического изменения содержимого чипа. Для карт очень важен размер проводов на микрочипе. Чем он меньше, тем труднее физически определить напряжения на них без специального дорогостоящего оборудования. Так же защита осуществляется с помощью изоляционной оболочки и расположения схем несколькими слоями, так чтобы невозможно было до них добраться, не повредив сам чип. Активная физическая защита может включать в себя датчики, определяющие необычно высокие уровни тепла, света или электрического напряжения. При обнаружении атаки эти датчики запрещают работу чипа, сигнализируя о попытке несанкционированного доступа. Другие методы обеспечивают бесполезность данных полученных в результате несанкционированного чтения с чипа. Например, компоненты располагают на чипе так, чтобы критические данные, такие как ключи шифрования, были равномерно разбросаны по всей площади чипа, и чтение с одного его участка предоставляло бы минимум информации.

Эти способы физической защиты с большой вероятностью не позволят одному нарушителю, даже наиболее способному, проанализировать работу чипа или совершить процедуру обратной инженерии. Но, если доступно большое количество работающих чипов, нарушитель может достичь успеха, совмещая данные атак на разные чипы, кроме того атаки можно повторять на одни и те же чипы. Такие атаки могут осуществить производители микрочипов или люди, занимающиеся обратной инженерией, на коммерческой основе.

В системах электронных денег, основанных на программном обеспечении, по определению не существует защиты продуктов пользователя или внешнего нарушителя от программ, используемых в самой системе. Обычно само программное обеспечение содержит механизмы позволяющие предотвратить несанкционированный доступ. Программному обеспечению обычно удаётся обнаружить лишь не самых опытных нарушителей, и его можно изменить, как и программы на обычном компьютере, используя широко доступные средства.

## 2. *Криптография*

Криптография – один из наиболее важных компонентов, предназначенных для предотвращения несанкционированных действий по отношению к электронным деньгам.

*Цели криптографии*.

Криптография представляет логическую защиту систем электронных денег, гарантируя конфиденциальность, аутентичность, и целостность оборудования, данных и связей, используемых в транзакциях. Существует множество различных криптографических методов, служащих для разных целей.

Шифрование используется для обеспечения конфиденциальности данных во время их передачи или хранения. Наиболее важными данными, которые подвергаются шифрованию, являются криптографические ключи. Другие данные, такие как величина платежей или серийные номера банковских карт, шифровать не обязательно.

Криптография так же используется для определения личности и допусков стороны участвующей в транзакции. Перед тем как отвечать на какие-либо запросы система выполняет криптографический тест, посылая данные, правильный ответ на которые сможет послать только устройство с корректными соответствующими ключами. Например, изменять критические данные на карте, такие как максимальный баланс на счете, могут лишь устройства, имеющие криптографические ключи соответствующие текущей системе. Так же для осуществления аутентификации используются цифровые подписи.

Криптография часто используется для проверки целостности сообщений между приборами в системе электронных денег, контролируя не было ли осуществлено изменение передаваемых данных. Для этого используются коды аутентификации сообщений. То есть, чтобы создать сообщение, которое будет принято адресатом, необходимо знание криптографических ключей. Также методы криптографии используют для защиты программного обеспечения, передаваемого через открытые сети.

*Типы и стойкость криптографии*

Криптографические методы работают в соответствии с математическими функциями, параметрами которых являются криптографические ключи. Существует множество криптографических алгоритмов. Обычно их разделяют на алгоритмы с симметричным и асимметричным (открытым) ключом. Алгоритмы с симметричным ключом используют один и тоже же ключ для шифрования и расшифрования. Примером симметричного алгоритма является DES(Data Encryption Standard), который был принят за стандарт во многих странах, в частности в сфере финансовой индустрии. Алгоритм DES можно значительно усилить, используя

шифрование triple-DES, где выполняются отдельно три операции шифрования и расшифрования с использованием ключа DES двойной длины.

Ассиметричные алгоритмы позволяют использовать комбинацию личного и общего ключа в процессе шифрования и дешифрования. Сообщение, закодированное общим ключом, может быть расшифровано лишь его личной парой. Общий ключ не требует скрытия по определению. Личный же ключ храниться в устройстве пользователя, ограничивая уязвимости системы. Алгоритмы построены так, что математически вывести личный ключ из общего практически невозможно. Один из наиболее известных ассиметричных алгоритмов - это RSA.

На системы, использующие криптографическую защиту можно осуществить атаку следующими способами: найти уязвимость в алгоритме, украсть секретный ключ или перебрать все возможные ключи(“brute-force attack”). Для данного криптографического алгоритма тем труднее осуществить полный перебор ключей, чем больше длина ключа. Но с другой стороны – чем длиннее ключ, тем больше времени тратится на работу с ним, что может оказать существенное влияние на общую производительность. Стойкость алгоритма обычно определяется математически и постоянно испытывается на тестах.

Для предотвращения атак, вторично посылающих предыдущие сообщения и наблюдающих за процессом обмена ключами, используется «активное» или «динамическое» шифрование, при котором чип карты создают цифровые подписи, или выполняют другие криптографические вычисления. Однако динамическая криптография требует большей производительности от микропроцессора (или крипто-процессора), что повышает стоимость приборов, может значительно увеличивать время транзакции, а так же повлиять на стабильность системы по отношению к пользователю. Таким образом, большинство существующих систем используют «пассивные» ассиметричные алгоритмы, с сохранением криптографических сертификатов на каждой карте, вместе с «динамическим» симметричным шифрованием, в котором уникальные ключи сессий создаются для каждой транзакции.

Системы, использующие криптографию, могут быть атакованы через уязвимости и их реализации. Например, если для генерации ключей система использует случайные данные, то эти данные должны быть случайными на самом деле. Иначе, исследование условий возникновения ключей может привести к значительному упрощению атаки на систему.

*Работа с ключами и их хранение*

Работа с ключами включает в себя различные типы криптографических ключей, их взаимоотношения, создание, использование, распространение, хранение и срок действия. Меры в этой области являются критичными для всего продукта в целом. Ущерб, нанесенный системе из-за утечки ключа, может быть ограничен уменьшением сферы действия этого ключа. Многие системы, например, используют различные ключи для различных операций: загрузки, покупки, вложения. Отдельные карты могут иметь индивидуальные ключи, выводимые из главного ключа. Крайне критичные операции загрузки, которые позволяют увеличивать баланс на карте, обычно хранятся только у производящей стороны и могут содержать ключи повышенной длины. Многие системы электронных денег вводят возможность быстрой замены криптографических ключей или алгоритмов. Время действия критических ключей обычно мало и составляет порядка нескольких месяцев.

Все системы электронных денег имеют дело с криптографическими ключами, которые следует хранить в тайне, избегая несанкционированного получения, изменения, дублирования или удаления данных. В системах, основанных на смарт-картах, существует множество мер, охраняющих ключи, хранящиеся внутри оборудования и передающиеся между устройствами. В системах, основанных на программном обеспечении, в частности тех, где есть дос-

туп в открытые сети, хранение криптографических ключей является труднейшей задачей, так как в безопасности оборудования пользователя невозможно быть уверенным.

### *3. Авторизация онлайн*

В системах, основанных на смарт-картах, авторизация онлайн необходима только в случае, когда устройство получает дебет с банковского счета. Такая авторизация необходима для того, чтобы гарантировать, что держатель карты имеет доступ к деньгам, на счету. В таких транзакциях от пользователя обычно требуется Личный Идентификационный Номер(PIN). Процедура оплаты между продавцом и покупателем обычно происходит таким же образом. Централизованная система со стороны покупателя проверяет журнал продавца, на наличие лишь одной транзакции. В некоторых, основанных на картах системах, терминал продавца может потребовать процедуры онлайн авторизации для транзакции покупки. Это может происходить случайным образом, или быть основано на параметрах карты или транзакции.

Обычно онлайн авторизация считается необходимой для всех транзакций систем электронных денег. Для того, чтобы обнаружить нарушителя, копирующего отдельные электронные сообщения и посылающего их несколько раз подряд, центр авторизации обязан проверять каждую транзакцию последовательно на основе информации об операциях, которые уже были выполнены. Эти средства не помогут предотвратить нарушения, однако, с их помощью его можно обнаружить. С помощью усложненных криптографических методов возможно определить в какой именно инстанции произошло нарушение.

## **4.** *Другие меры*

Системы электронных денег могут предоставлять дополнительные уровни защиты против взлома, требуя от отдельных устройств выполнения дополнительных проверок по время транзакций. Это может включать в себя, например, проверку сроков действия, количества транзакций осуществленных устройством, баланс на устройстве (в сравнении с его максимальным значением) и сам максимальный баланс.

Системы электронных денег также включают в себя меры по предотвращению неавторизованного увеличения баланса с помощью прерывания транзакций. Протоколы сообщений построены таким образом, что транзакция завершается только в случае, если все сообщения определённые для этой транзакции, удачно доставлены. Незаконченные передачи, например, вследствие выключения питания, могут привести только к сохранению счетов на одном устройстве, не к передаче счетов на контр-устройство. Журнал незавершенных транзакций обычно храниться в устройстве для исследования пользователем или системным оператором.

Наконец, очень важно осуществлять административный контроль над системой. Такие задачи, как производство карт, работа с криптографическими ключами и персонализация карт являются объектом строгого контроля, и разнесены как географически, так и административно. При этом увеличивается количество человек, которым необходимо объединиться для сбора необходимого количества информации, позволяющей обходить защиту системы. Терминалы, в частности, позволяющие загружать балансы, располагают под специальным контролем. Процессы в них можно удалённо наблюдать, что и делает центральный оператор. Так же важной частью безопасности является контролирование оборудования продавца, так как оно может иметь повышенную максимальную сумму на счете и служить заманчивой целью для нарушителя. Административные меры также важны в предотвращении неправомерных действий со стороны самой системы или её сотрудников.

*Литература:*

**1. SECURITY OF ELECTRONIC MONEY Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries. Basle. August 1996**
**2. ECB • Electronic money system security objectives • May 2003**
**3. EUROPEAN BANKING STANDARD: THE INTEROPERABLE FINANCIAL SECTOR : ELECTRONIC PURSE, June 1999**
**4. Aston University : Smart Card Standards and Electronic Purse, May 1997**