Смарт-карты :

обзор информационной безопасности смарт-карт.

Босак А. В.
915гр.
ФРТК МФТИ
2003 г.

1.Введение

Смарт-карта – интеллектуальное устройство, размера с кредитную карточку со встроенным интегральным чипом. В ней содержится не только устройство хранения информации, но и процессор, способный выполнять различные программы. Самодостаточность смарт карты делает её устойчивой к атакам, т.к. у неё отсутствует зависимость от уязвимых внешний устройств. Благодаря этим свойствам смарт-карты часто используются в приложениях , требующих высокого уровня конфиденциальности.

Например , смарт карты могут использоваться в качестве идентификатора владельца карты. Также такие устройства могут быть использованы в качестве медицинской карты из обладателя, хранящие историю болезней владельца. Кроме того, смарт-карты могут быть использованы, как кредитная или банковская карта, которая позволяет снимать и класть деньги на счёт. Все эти приложения требуют хранения дорогостоящей информации.

В ближайшем будущем, традиционные магнитные карточки будут заменены и интегрированные в одну многоцелевую карточку, которая известна под названием “электронный бумажник” в индустрии смарт карт. Смарт-карты становяться всё более и более важными в жизни человека. Они будут использоваться для хранения важной информации о владельце и, возможно , существенно более важной , чем информация на хранящаяся на магнитных карточках. Именно поэтому в настоящее время ведётся множество споров, по поводу безопасности хранения информации на смарт-картах. И , вероятно, споры по этому поводу будут продолжаться ещё долго.

В данном документе обсуждаются вопросы безопасности смарт-карт в трех различных аспектах. Сначала мы взглянем на физическую структура смарт-карты, и как эта структура помогает защитить информации в течении всего жизненного цикла смарт карты. Затем мы рассмотрим как информация защищается логикой хранения файлов на карте. В конце мы обсудим, каким образом обеспечивается секретность информации в программном обеспечении карты и сделаем заключения являются ли смарт-карты достаточно надёжными в плане секретности или нет. Также обсудим некоторые способы атак смарт-карт и их эффективность.

Физическая структура и “жизненный цикл”

В этом разделе обсуждается физическая структура смарт карты и различных её компонет.
Также рассматриваются фазы жизненного цикла смарт-карты , и исследуется как микроконтроллер смарт-карты безопасно хранит и передаёт информацию от изготовителя смарт-карты к приложению-получателю и далее владельцу. В результате мы определим способы защиты информации на карте.

Физическая структура смарт-карты определена Международной Организацией по Стандартизации(ISO) в стандартах 7810, 7816/1 и 7816/2. В общем она состоит из трёх элементов: пластиковая подложка, печатная плата и контактная площадка. На рис.1 показано физическая структура смарт-карты.

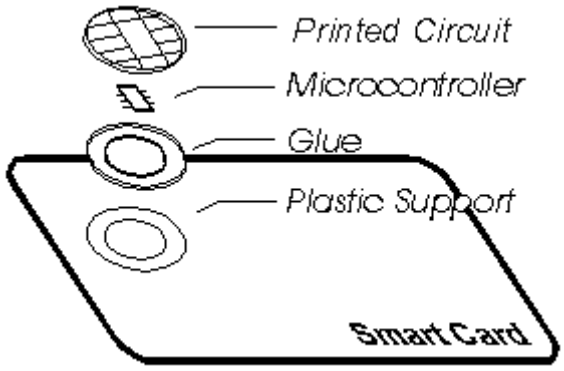

Рис. 1. Физическая структура смарт-карты.(Источник: Philips DX smart card reference manual, 1995)

Печатная плата соответствует стандарту ISO 7816\3 , который обеспечивает 5 контактов для питания и данных. Контакты герметично закреплены в специальном пазу в плате и соединены с логикой платы. Контакты также предохраняют чип от механических и электрических воздействий.

Возможности карты определяются её интегральным чипом. Обычно этот чип состоит из микропроцессора, ПЗУ ROM, нестатической RAM ОЗУ и электрически стираемой программируемой EEPROM, которая сохраняет своё состояние при выключенном питании. Чип сделан из кремния , что делает его достаточно хрупким . Поэтому для предотвращения его поломки при перегибании карты чип делают размеров в всего несколько миллиметров.

Более того, физическая пропускная способность интерфейса обмена информации между картой и картоприёмным устройством ограничена 9600 бит.сек. Коммуникационный канал двунаправленный соответствующий стандарту ISO 7816/3 . Весь процесс обмена данными происходит под управлением центрального контроллера смарт-карты. Команды и входная информация посылается чипу, который , затем , отвечает словом состояния и выходной информацией. Обмен данными происходит в полудуплексном режиме, что означает невозможность одновременной передачи информации между картой и считывающим(записывающим) устройством. Этот протокол поддерживает запрет передачи информации на скоростях больших допустимой.(предотвращая тем самым возможность проведения одного из классов атак)

В общем , размер , толщина и гибкость смарт карты разработаны для защиты карты от физических повреждений. Однако, это также ограничивает функциональные способности карты , как-то ёмкость памяти, мощность процессора и других ресурсов, которые могут быть размещены на карте. В результате для функционирования смарт-карта почти всегда необходимы дополнительные внешние устройства. Например, для обеспечения ввода и вывода информации, источник питания и т.д. Эти ограничения в некоторых услових делают смарт карту уязвимой .

Жизненный цикл Смарт Карты.

В каждой смарт карте есть операционная система, которая может содержать идентификационный номер, тип, серийный номер, информацию о профилях и т.д. Более важно то , что системная часть может содержать различные секретные ключи, такие как ключ производителя или фабричный ключ, и персонализирующий ключ. Вся эта информация должна держаться в секрете и быть недоступна для общего пользования.

Следовательно, от момента изготовления до , сначала фирмы пользователя, затем владельца карты, “жизнь” смарт карты разделена на различные фазы. Соответственно ограничения на передачу информации и доступ к ней изменяется на различных фазах жизненного цикла карты. Существует 5 основных фаз жизненного цикла смарт-карты.

Фаза изготовления.

Эта фаза проводиться производетелем чипов. Кремниевый чип создается и тестируется. Фабричный ключ (ФК) добавляется для защиты чипа от мошеничества и его модификации до тех пор, пока чип не попадает в пластиковый корпус. Фабричный ключ является уникальным и включает в себя информацию о производителе чипа. Другая производственная и служебная информация записывается на чипа в конце этой фазы. Теперь чип готов к отправке к изготовителю смарт-карт , но уже под защитой фабричного ключа(ФК).

Пре-персонализирующая фаза.

Эта фаза проводиться поставщиком карт. В этой фазе , чип будет закреплён в пластиковый корпус на котором может быть напечатан логотип поставщика смарт-карт. Связь между чипом и печатной контактной платой также осуществляется на этой стадии и всё устройство в целом подлежит тестированию. Для повышения секретности и для обеспечения конфиденциальной доставки карт конечным пользователям, фабричный ключ заменяется на персонализирующий ключ(ПК). После этого на карту записывается специальный ключ $V_{PER,}$ который недопускает возможности модификации ПК. Кроме того, инструкции модификации физической памяти отключаются и доступ к памяти карты может осуществлятся только использую логическую адресацию. Эти меры позволяют запретить изменение системной информации , хранящейся на карте.

Фаза персонализации.

Эта фаза осуществляется в тесном взаимодействии с конечным пользователем. На этой стадии завершается создание логической структуры данных. Данные и программы записываются на карту. Информация о владельце карты, PIN и деблокирующий PIN коды также записываются на карту. Далее специльный блокирующий ключ V_{UTIL} записывается в память карты для обозначения того, что карта используется.

Фаза использования.

Это фаза обычного использования карты её владельцем. Система приложений, логический доступ к файлам , и другие возможности карты активированы. Доступ к информации на карте ограничен политикой безопасности , установленной приложениями.

Фаза анулирования карты.

Существуют два пути попадания карты в эту фазу. Один из них – инициированный приложением, которое записывает ключ недействительности карты в специальный файл. Все операции включая запись и обновление будут запрещены операционной системой. Останется возможность только для чтения. Другой путь для помещения карты в эту фазу , это блокирование PIN и деблокирующего PIN, тогда будут запрещены все операции , включая чтение.

Угрозы безопасности Смарт-карт.

Введение

Смарт-карты являются в некотором роде камнем преткновения в мире компьютерной безопасности. Они предназначены прежде всего для контроля доступа к секретной информации, электронной коммерции, аутентификации, конфиденциальности и т.д. Однако, довольно мало работ посвящено анализу информационной безопасности смарт-карт и тому особому окружению , в котором работают смарт-карты.
Далее мы обсудим модель безопасности системы смарт-карт, независимо от их приложений. Рассмотрим фундаментальные свойства смарт карт, процессора памяти включённых в состав карты, не углубляясь в проблемы взаимодействия с внешним миром и покажем, как эти свойства делают системы основанные на смарт-картах небезопасными , в сравнении с обычными системами основанными на самодостаточном компьютере. Простым примером является человек, владелец карты, чей компьютер находится под чьим либо контролем. Это необычная ситуация для типичного компьютера, и вполне обычная для для смарт-карт. Мы покажем, что для многих приложений использование смарт-карты конфиденциально означает понимание того, смарт-карта не является надёжной вычислительной платформой, а лишь банк данных с ограниченными вычислительными способностями.

От компьютера к смарт-карте.
Лучший способ понять угрозы , которые возникают при использовании смарт-карты это начать с угроз обычному персональному компьютеру. Мы полагаем, что самый важный аспект безопасности смарт-карт, как участвующего в протоколе обмена устройства, это особые свойства, отличающие смарт-карту от других вычислительных устройств. Начав с персонального компьютера и урезая его соответствующие характеристики, дабы прийти к смарт карте мы увидим как изменяется безопасность использования системы. Каждая итерация добавляет новые возможности для атаки.
Например, рассмотрим случай , в котором владелец карты не контролирует информацию , которая на ней записана.
Это приведет к возможности атаки на информацию , хранящуюся на карте человеком, который позаимствовал карту. Это атак , конечно невозможна, если такого предположения не вводить. Наша модель персонального компьютера состоит из центрального процессора, устройства хранения информации, устройств ввода-вывода и источника питания. В нормальном компьютере все эти компоненты соединены в один блок. Этой модели в общем достаточно для рассмотрения основных угроз безопасности.
Начнём постепенно уменьшать наш компьютер до размера смарт-карты.
Порты ввода-вывода заменяются низкоскоростным последовательным портом. Система , к которой присоединяется карточка имеет ограниченные возможности атаки, так как карта предназначена в основном для взаимодействия с компьютером владельца карты, или , возможно, иногда к чужому компьютеру для обмена информацией. Продолжая , уберём из компьютера клавиатуру , и предположим, что ввод информации осуществляется через клавиатуру , подключенную к карте. Оевидно, что эта клавиатура может записать PIN код и информацию о карте для последующей атаки. В конце концов убираем экран. Теперь возможность просмотра информации возможна только через внешне подключенное устройство.

Одними из важнейших характеристик смарт-карты, выгодно отличающих её от ПК являются её малый размер и невозможность взаимодействия с внешним миром без дополнительных внешних же устройств. Это в основном и определяет доверительную модель в которой смарт-карты должны функционировать.

Функциональность смарт-карты ограничена и в других аспектах. Владелец смарт-карты не должен иметь доступа к программному обеспечению карты. Это должно быть верно даже для многофункциональных карт.
В следующей секции мы обсудим разведвления отличительных особенностей ,описанных выше вместе с другими, обычными для систем со смарт-картами. Наши модели часть включают в себя 5 или 6 участников. Мы проанализируем как участники могут атаковать друг-друга. Мы также исследуем мотивации , заставляющие атакующих причинять различный вред , что становится возможным когда роли разделяются.

Моделирование доверительного окружения смарт-карты.
Существует множество ролей, потенциально вовлеченных в системы с использованием смарт карт. Обчно их минимум 5 или 6, это владелец карты, терминал, владелец информации, запращивающая карту сторона, изготовитель смарт-карты, изготовитель программного обеспечения.
Владелец смарт-карты это сторона, которая постоянно владеет картой. Карта находиться в его бумажнике, и он решает , использовать ее или нет. В этом случае смарт карта может быть использована как электронный бумажник. Он может контролировать информацию на карте, в зависимости от системы, однако крайне нежелательно , если он имеет доступ к протоколам, и приложениям на карте, или к внутренней электронике карты. Заметьте, контраст с персональным компьютером, где владелец имеет полный доступ к информации и hardware.

Владелец информации – сторона , которая контролирует информацию , хранящуюся на карте. В случаях использования карты, как механизма хранения электронных сертификатов, владелец карты является также и владельцем информации Однако, если карта- карта электронной наличности, то лицо, предоставляющее наличность является владельцем информации, - это создаёт возможность для атаки.
Терминал- устрйоство , которое взаимодействует со смарт-картой для обеспечения ее взаимодействия с внешним миром. Терминал контроллирует весь ввод-вывод смарт-карты: клавиатура, с которой данные поступают на карту, экран, на котором информация, содержащаяся на карте отображается. Если карта –телефонная карта, то терминал – провайдер телефонной связи, если карта- карта идентификации в сетях АТМ- то терминалом служит провайдер АТМ. Если карта – карта для оплаты спутникового телевидения, то терминал – компьютерная приставка к спутниковому телевидению.
Вышеуказанные примеры, АТМ карты , или карты оплаты спутникового ТВ показывают, что так же как и сама карта , терминалы могут быть разделены на несколько ролей. В случае АТМ, использование терминалов и сетей другого банка является обычным делом, что означает некоторое недоверие к терминалу. В случае спутникового ТВ , терминал вообще может быть атакован в теплоте и уюте домашней обстановки! ☺

Поставщик смарт-карт - это сторона , которая поставляет смарт карты ☺ Эта сторона контроллирует операционную систему смарт-карты , и любую информацию , которая изначально записывается на смарт –карту. Если это карта для оплаты телефона – поставщик – телефонная компания. Если карта – идентификационная карта служащего – поставщик – работодатель. Иногда поставщик просто предоставляет карту и исчезает из системы. В других случаях он сопровождает карту на протяжении всего жизненного цикла.
В некоторых многофункциональных картах поставщик не может контролировать приложения , выполняющиеся на карте, или может контроллировать только работу операционной системы. В других картах поставщик может контроллировать всё программное обеспечение на карте.

С точки зрения анализа безопасности часто удобно рассматривать поставщика карт, изготовителя и разработчика ПО одним лицом, однако в жизни так редко случается.
Далее, производитель карты – сторона , которая производит смарт-карты. Заметим, что это некторое упрощение: производитель может и не иметь собственных производственных мощностей для изготовления чипов, а заказывать изготовление некторых блоков у сторонних производителей, или, например , использовать для производства инструментальные средства сторонних производителей, такие как VHDL компиляторы.
Производитель ПО – сторона , которая изготовляет программное обеспечение , которое затем распологается на смарт-карте. Это опять же некоторое допущение, так как возможно производитель

ПО использовал множество сторонних разработчиков,средств разработки, утилит, компиляторов и т.д.

Примеры разделения прав в системах со смарт-картами.
Далее следуют примеры систем, базирующихся на использовании смарт карт для обозначения , какие стороны контролируют какие аспекты системы. Этот список не является исчерпывающим, однако отражает некоторые ключевые характеристики таких систем.

Карта Электронной наличности. (Digital Stored Value Card)
Это карты, для замены наличности. Mondex и VisaCash являются примерами таких систем. Владелец карты- покупатель. Владелец терминала – продавец. Владелец данных и поставщик карты – финансовый институт поддерживающий систему.
Карта цифровых чеков.Digital Check Card- то же самое, только владелец карты является и владельцем информации на ней.

Телефонная Карта предварительной оплаты .
Это специльно устроенная карта хранения информации. Владелец карты – покупатель. Владелец терминала , данных, и поставщик карты – телефонная компания.
Кредитная Телефонная карта. Account-based Phone Card.
В этой системе смарт карты не содержат баланс счёта, а просто номер счета , который является просто указателем на строчку в базе данных. Владелец карты и данных – покупатель, владелец терминала и поставщик карты – телефонная компания.
Ключ доступа.
В этих приложениях смарт карта содержит ключ, который используется для аутентификации. В случае корпоративного использования владелец карты – служащий, а владелец информации, терминала, поставщик карты – корпорация. В случае многоцелевого ключа, владелец карты и владелец информации могут быть одним и тем же лицом.

Модель угроз безопасности смарт-карт.

Атака, проще говоря, это попытка одной или нескольких сторон сжульничать. Мы рассмотрим 2 класса атакующих: являющиеся частями системы, и сторонние атакующие. Атакой участников может быть попытка взлома владельцем карты терминала, или попытка обмана владельца карты поставщиком .Внешние атаки могут быть проведены кем-либо, кто украл карту : временный владелец, который украл карту у легального пользователя, или подменил программу терминала, или сам терминал. Внешние атаки схожи с атаками на протоколы обычных ПК.

Мотивация
Мотивы атак распадаются на несколько больших категорий. Первое и наиболее очевидное – финансовые мощенничества, включаю кражу денег со счёта, или незаконное использование различных сервисов, таких как телефон или спутниковое ТВ. Так же существует класс атак только косвенно направленных на смарт карты, в них взлом карты не является конечной целью, а только способом доступа к другому компьютеру, или контроллирующему устройству. Существуют атаки на конфиденциальность, когда атакующий хочет получить доступ к большему количеству информации, чем предусмотрено протоколом. Так же существует класс атак, которые направлены скорее на получение авторитета в обществе, нежели на некоторую материальную выгоду.

Классы атак.
Из-за большого числа лиц, вовлеченных в любую систему со смарт-картами возникает большое число различных классов атак. Наша цель структурировать эти классы по функциональности. А именно, мы рассмотрим атак участников системы друг на друга. Большинство этих атак невозможны в обычных компьютерных системах, так как они будут в окружении традиционных ограничений компьютерной безопасности. Однако эти атаки будут иметь место в мире смарт-карт.
Атаки терминала против владельца карты или владельца информации.
Этот тип атак понять проще всего. В момент, когда владелец карты вставляет свою карту в терминал, он доверяет терминалу передать информацию карте или от карты точно. Например, если пользователь захочет снять со счёта 1$, он доверяет терминалу, и в результате операции будет действительно снято счёта 1$, и информация об операции верно отобразиться на экране терминала. Возможность мошенничества с использованием модифицированного ПО терминала, или подобных изменений весьма велика. Причем такой тип жульничества крайне трудно обнаруживаем пользователем в контексте единственного терминала.

Защитные механизмы в большинстве систем со смарт-картами построены в основном на факте , что терминал имеет доступ к карте в течение малого промежутка времени. ПО на карте может ограничить возможности для нанесения ущерба поддельным терминалом. Например, для карт электронной наличности можно запретить переводить со счёта более 1$ за транзакцию. И запретить проводить более 1 транзакции в минуту. Однако эти механизмы не срабатывают, если у пользователя есть собственный терминал с неограниченным доступом к карте. Таким образом , реальные механизмы защиты не могут ничего поделать с обменом информацией между картой и терминалом. И карта и терминала ,как конечные вычислительные системы должны быть "подозрительны" по отношению к своему партнёру.

Атаки владельца карты против терминала.

Более тонкая атака владельцем карты терминала. Это использование взломанных или модифицированных карт, со специальным ПО. В хороших протоколах существует защита от данного типа атак, например усложняя физические аспекты доступа к содержимому карты , и целостность информации на карте может быть проверена терминалом. (например голограммы на Visa и MasterCard картах). Заметим, что цифровая подпись ПО не эффективна, так как поддельная карточка может обманывать о своем сертификате ПО, и не существует способа проверить это, т.к. нельзя проникнуть внутрь карты. Защита от этого типа атак требует запрета на изменение информации внутри карты её владельцем.

Во многих смарт картах для коммерческих систем, информация записанная на карте должна быть защищена от владельца карты. В некоторых случаях владелец вообще не должен знать эту информацию. Создавая карту доступа, например, нужно исключить возможность попадания секретного ключа в руки пользователя. Знание этого ключа может позволить пользователю создать ещё один такой же. Знание ключя в карте электронной наличности может позволить владельцу смарт-карты смошенничать. В других случаях владелец карты может знать значение, но не может его изменять.

Атаки владельца карты против владельца информации.

Во многих смарт-картах, на которых базируется функционирование коммерческих систем, информация, хранящаяся на карте должна быть защищена от проникновения владельца карты. В некоторых случаях , владелец карты не должен вовсе иметь доступ к информации на карте. Например , карты для доступа в здания или помещения могут иметь некоторый секретный ключ. Знание этого ключа владельцем карты недопустимо – т.к. он может дублировать карты. Знание секретного ключа карты электронной комерции может позволить владельцу карты провести незаконные транзакции. В других случая владелец карты может знать значение ключа на карте, но не должен иметь возможность изменить это значение. Изменение информации , хранящейся на карте может позволить владельцу карты наносить ущерб владельцу сервиса .

Существуют две важные характеристики таких атак , одна из них - функционирование карты как защитщённого периметра, предназначенного для сокрытия информации внутри карты от владельца карты. В этом контексте карта должна быть достаточно интеллектуальной и физически закрытой , для того , чтобы обнаруживать и предотвращать атаки не имея существенного влияния на своё окружение.

Вторым важным фактором является свобода владельца карты пользоваться ей сколь угодно долго, использовать для проведения атаки своей лаборатории, имеет возможность неограничено разрушать и уничтожать карты в процессе исследования их работы.

Известно множество способов проведения таких атак. Среди них инженерный анализ, уничтожение защитных систем карты, анализ ошибок, косвенные методы: анализ напряжений и временных диаграмм. Такие атаки довольно эффективны, особенно в случае с картами оплаты спутникового ТВ, и сим-карт сотовых телефонов.

Атаки владельца карты против поставщика услуг.

Существует множество типов финансовых атак, которые, как кажется направлены на поставщика услуг и сервисов, однако это является заблуждением. Фактически, атаки направлены на целостность и аутентичность (достоверность) данных и программ , записанных на карте.

Такие атаки становятся возможными вследствие решения поставщика использовать карты в системе, где владелец карты должен хранить информацию о поставщике или других сторонах . Например в случае оплаты телефона, если телефон использует систему, основанную на счетах клиента, и где карта хранит очень длинный номер счета , непосредственно используемый телефонной компанией, то неизбежны атаки связанные с угадываением номеров счетов и других махинациях с номерами.

Системы такого типа могут быть существенно защищены добавлением аутентификации с запросом и подтверждением, или механизмом цепочки обратных хэшей для пересылки стойких паролей.

Этот способ может иметь отличный эффект также в системах использующих смарт карты для связывания с бэк офисом , как надёжная система аутентификации , стойкая к взлому. Если поставщик смарт карты решает хранить биты , которые авторизуют использование системы на карте , не нужно удивляться , если эти биты будут атакованы. Эти биты могут быть как аутентификационные номера счетов, так и пароли, зашитые в карту. Причём работа таких систем базируется на сомнительном предположении, что защитный периметр карты стойкий достаточно для данного применения карты, ключ не может быть просто извлечен и протокол подтверждения информации на карте достаточно надежен.

Атаки владельцем карты против производителя ПО.
Обычно, в системах , где карта используется с предположительно враждебной стороной, существует предположение, что новое ПО не будет загружаться на карту. Это вызвано наличием фазой "предиспользования" с множеством односторонних преобразований , проводимых производителем карты для того , чтобы удостоверится в безопасности ПО. Эти рассуждения основаны на предположении, что производитель карт и производитель ПО существенно разделены. Однако атакующая сторона часто показывает необыкновенную способность получать необходимое оборудование , часто бесплатно, для проведения атак.

Атаки владельцем терминала против поставщика услуг.
В некоторых системах , таких как телефонные карты предварительной оплаты, владелец терминалов и поставщик услуг – одно лицо. В более открытых системах, таких как Mondex , владелец терминала – продавец, поставщик услуг – Mondex. Это разделение позволяет предположить существование следующих новых типов атак.
Терминал контроллирует все взаимодействие между картой и поставщиком услуг. В таких системах, терминал всегда имеет возможность фальсифицировать записи, отказываться проводить транзакции и т.д. Терминал также может пропустить некоторые шаги транзакции, чтобы упростить взлом системы, или затруднить доступ к системе.
Эти атаки не связаны со "смарт-картовой сущностью" системы, а являются простыми атаками против связи между владельцем терминала и поставщиком услуг. В некоторых системах предпринималась попытка уменьшить угрозу таких атак созданием защищенного соединения между картой и поставщиком через терминал. Многие системы используют мониторинг процесса для уменьшения эффективности таких атак.

Модель защитной системы фокусируется на проектировании системы с безопасной архитектурой в целом. Добавляя аспекты безопасности к системы после фазы проектирования оказывается весьма сложным, дорогим и ненадёжным. Поэтому, мы предлагаем модель, в которой аккуратный дизайн с самого начала исключает необходимость сложных и дорогих попыток построить надёжную и безопасную систему на поздних фазах. Редукционистская модель не только упрощает просесс проектирования и реализации, но и уменьшает возможность некорректной работы системы на заключительной стадии.
Другой гранью прозрачной защиты является желание избежать усложнения систем и риска применения многозадачных смарт-карт. Отказ от использования мультизадачных смарт карт во первых уменьшает количество сторон, вовлеченных в процесс, и практически исключает возможность кросс-задачных атак.

Вывод.
Мы показали, что расщепление периметра безопасности является достаточно сложной задачей. В особенности, если пользователь носит с собой компьютер с разрешения владельца информации, он, конечно, может решить воспользоваться этой информацией , что является весьма рискованной ситуацией для владельца данных. Мы так же показали, что недостаток карт , заключающийся в невозможности самостоятельно "общаться" делает их весьма уязвимыми для терминалов. Эти уязвимости являются частью систем со смарт-картами, и бороться с которыми очень нелегко.
Мы так же подчеркнули несколько фундаментальных средств защиты смарт карт, которые оперируют на уровне проектирования системы, предлагая дизайнерам и системным интеграторам н