Ренат Низамов

Технологии борьбы с кардшарингом

С появлением первого платного телевизионного вещания началось развитие «систем условного доступа» (СУД), задачей которых является защита платных телевизионных каналов от несанкционированного просмотра. И, как вы уже догадались, раз есть защита, обязательно найдутся люди, которые захотят ее обойти, так называемые «пираты».

С ростом сложности защитных механизмов и технологий, предлагаемых разработчиками систем условного доступа, развивались и методы, которые пираты используют для обхода и взлома барьеров, заложенных в этих системах. Сегодняшнее поколение СУД базируется на решениях, демонстрирующих беспрецедентную взломоустойчивость и минимизирующих возможность эксплуатации слабых мест механизмов защиты. Так, например, наиболее известные СУД применяют сложную иерархическую комбинацию известных криптоалгоритмов и алгоритмов собственной разработки. С одной стороны, это говорит о проверенной временем криптостойкости систем, а с другой — о бессмысленности взлома методом полного перебора значений ключа, так как потенциальным злоумышленникам неизвестны детали собственных алгоритмов. В связи с этим профессиональные пираты концентрируют свои усилия на поиске путей обхода защитных барьеров, не требующих их взлома.

С переходом телевизионного вещания на цифровые форматы и, в частности, появлением и развитием стандарта DVB одним из самых распространенных методов обхода защиты контента стал так называемый «кардшаринг».

Кардшаринг (англ. card sharing — карта и общий доступ, дословно — общий доступ к карте) — метод, благодаря которому несколько независимых ресиверов могут получить доступ к просмотру платных каналов цифрового телевидения, используя одну карту доступа.

В современных системах платного телевидения формата DVB-контент шифруется с помощью стандартного алгоритма DVB-CSA, использующего принцип скремблирования с применением контрольных слов (CW).

Контрольное слово (CW: от англ. control — контроль и word — слово) — ключ относительно небольшой длины, но часто сменяемый и генерируемый случайным образом.

СУД шифрует CW криптографическими методами и совместно с сообщениями о правах доступа EMM передает их по открытому каналу на приемник абонента. Вследствие того, что на современном этапе развития техники смарт-карты не обладают вычислительной мощностью для непосредственного дескремблирования программ, эта функция выполняется чипом устройства дескремблирования, встроенного в приемник или модуль условного доступа (CAM), а смарт-карты занимаются расшифровкой CW. Таким образом, примерно раз в 10-15 секунд приемник отсылает смарт-карте ECM, запрашивая подтверждение прав доступа данного подписчика, и если права доступа подтверждаются, то смарт-карта в ответ отсылает CW.

DVB не стандартизирует схему безопасности этого обмена, оставляя детали реализации на усмотрение поставщиков системы условного доступа и приставок, что позволяет им гибко подойти к решению вопроса. И «пираты», используя специальные устройства, могут отлавливать раскодированные CW, поступающие на приемник. Таким образом, кардшаринг — это метод обхода защитных барьеров, основанный на перехвате диалога между смарт-картой и устройством дескремблирования.

Современная смарт-карта представляет собой мини-компьютер и готова обрабатывать любое переданное ей ECM-сообщение. И если раньше количество абонентов, обслуживаемых одной картой, ограничивалось производительностью

Рис. 1. Принцип дешифрации потока с помощью смарт–карты

процессора, встроенного в карту, то с развитием Интернета и локальных сетей данный вид пиратства стал более распространенным и убыточным для операторов платного телевидения. В принципе, обработка одного ECM-сигнала на канал позволяет обслуживать всех клиентов пиратской сети, настроенных на соответствующий канал. Поэтому кардшаринг может применяться и в значительно более широких масштабах.

Как уже было сказано, с развитием сетевых технологий кардшаринг стал серьезной проблемой для операторов платного телевидения, все больше производителей систем условного доступа стали искать пути решения этой проблемы. Один из способов борьбы с кардшарингом — ограничение распространения так называемых открытых приемников, которые позволяют устанавливать в свою операционную систему дополнительное программное обеспечение. Именно такими приемниками в большинстве случаев и пользуются пираты. Это возможно путем сопряжения приемника со смарт-картой, что не позволит просматривать контент оператора на приемниках других производителей. Недостатком данной технологии является то, что после сопряжения приемника с картой просмотр возможен только на данном приемнике, что не всегда удобно, если у вас дома их несколько.

Другим способом защиты от кардшаринга является частая замена контрольного слова, используемого для дескремблирования сигнала (раз в пять секунд). Но это налагает жесткие требования к производительности чипов дескремблера, так как скорость обработки информации должна быть в два-три раза выше, что приводит к удорожанию приемников в целом. Кроме того, данный способ не может полностью оградить операторов от кардшаринга. Уменьшение интервала смены CW вынудит пиратов приобрести более производительные серверы и обслуживать меньше клиентов, но саму проблему не решит.

Как мы уже показали, основным уязвимым местом при кардшаринге является протокол обмена между смарт-картой и устройством дескремблирования, так как именно в процессе передачи CW дескремблеру происходит его перехват. Поэтому все больше СУД предлагают новый подход к охране контента от кардшаринга, основанный на защищенном протоколе обмена между дескремблером и смарт-картой. Данный протокол подразумевает надежное шифрование данных обмена между смарт-картой и дескремблером при использовании современных средств безопасного обмена сессионными ключами с применением асимметричных алгоритмов. Так, при вставке смарт-карты в картоприемник дескремблера происходит ее инициализация, в процессе которой вырабатывается алгоритм; по нему впоследствии будут преобразовываться CW перед отправкой дескремблеру.

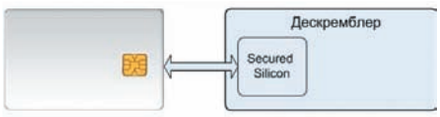

Рис. 3. Обмен сессионными ключами

Для исключения возможности перехвата и подмены информации во время процесса инициализации применяются специальные алгоритмы сертификации. А также для дополнительной защиты обмен сессионными ключами периодически повторяется.

Смарт-карта расшифровывает принятое в ECM-пакете контрольное слово, преобразует его по выработанному алгоритму и отправляет результат дескремблеру. Постпроцессинг контрольных слов осуществляется в защищённом от несанкционированного доступа сегменте основного чипа дескремблера, после чего в основном чипе происходит сам процесс дескремблирования.

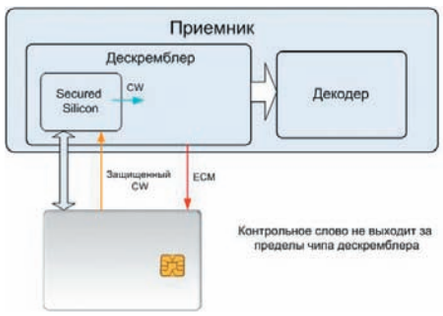

Рис. 4. Защита протокола обмена между картой и дескремблером

Поскольку открытые контрольные слова не выходят за пределы чипа дескремблера, пресекается возможность перехвата открытых контрольных слов злоумышленниками.

Защищенный протокол обмена между дескремблером и смарт-картой обладает несколькими положительными качествами. Он позволяет использовать стандартный интервал смены контрольных слов, тем самым не приводя к удорожанию приемников для абонентов. И, в отличие от сопряжения карты с приемником, данный протокол позволяет использовать карту в разных приемниках, так как сопряжение происходит всякий раз, когда вы ее вставляете в приемник, и не требует специальных команд от оператора.

Рис. 2. Принцип реализации кардшаринга