Андрей Макашов
начальник Департамента внедрения и сопровождения ООО «СмартЛабс»

Различия систем условного доступа для IPTV- и DVB-сетей

Если рассматривать эти системы с точки зрения их основных функций, то принципиальных различий в них нет. Что же касается реализации смежных функций, то и те и другие должны иметь интерфейсы взаимодействия с системой управления услугами Middleware или непосредственно OSS/BSS.

В то же время DVB-совместимые системы имеют существенные ограничения по использованию абонентских устройств, так как должна быть реализована аппаратная поддержка смарт-карт или специализированных чипов. Данное ограничение сужает модельный ряд устройств и повышает их стоимость.

Системы условного доступа и технических средств защиты авторских прав (Conditional Access System/Digital Rights Management, CAS/DRM) можно разделить на два основных типа: карточные (с использованием смарт-карт для контроля доступа) и бескарточные. Карточные системы традиционно используются в системах кабельного и спутникового телевидения стандарта DVB, где отсутствие обратной связи с абонентским устройством не позволяет контролировать доступ к контенту. Единственным вариантом управления услугами для технологии DVB является использование смарт-карт или специализированных чипов, встроенных в абонентские приемники (Set Top Box – STB). При этом вся служебная информация (подписанные услуги, статус активации и т.д.) доставляется вместе с вещаемым потоком.

Для карточных систем технология шифрования и выдачи ключей описана достаточно хорошо, хотелось бы подробнее остановиться именно на бескарточных системах, наиболее широко используемых в IPTV.

Технология IPTV подразумевает наличие обратной связи, что позволяет сделать услуги интерактивными, обеспечить постоянный обмен данными между абонентскими устройствами и платформой предоставления услуг (Middleware). Нет необходимости использовать физические модули защиты, достаточно программных средств.

Бескарточные системы условного доступа разработаны с учетом специфики IPTV и имеют ряд неоспоримых преимуществ:

- Возможность быстрого обновления или даже замены системы в случае взлома.
- Отсутствие необходимости выпуска/перевыпуска дорогостоящих смарт-карт.
- Защита от клонирования.
- Удешевление абонентских устройств.

Андрей Макашов,
начальник Департамента внедрения
и сопровождения ООО «СмартЛабс»

- Возможность конвергентного предоставления услуг, когда абонент имеет доступ к услугам IPTV как с помощью специализированных STB, так и на персональных компьютерах и мобильных устройствах.

Шифрование широковещательного контента (телеканалы, радио) выполняется в онлайн-режиме в процессе вещания, шифрование видеофайлов для «видео по запросу» выполняется предварительно, на этапе подготовки контента к публикации. В системах условного доступа используются криптостойкие алгоритмы асимметричного шифрования, когда данные шифруются открытым ключом, а для их дешифрирования необходим закрытый ключ. Криптостойкость обеспечивается за счет того, что закрытый ключ трудно

(практически невозможно) вычислить по открытому ключу и шифрованным данным. Для повышения безопасности ключи периодически меняются (например, один раз в сутки).

Все бескарточные системы работают на основе ассиметричного шифрования. Версии CAS/DRM от различных разработчиков могут иметь особенности и отличаться деталями реализации.

Центральный сервер системы условного доступа случайным образом генерирует закрытый и открытый ключи.

Шифрование контента выполняется в два этапа. На первом контент шифруется симметричным ключом. Одновременно этот ключ шифруется с помощью открытого ключа системы условного доступа. Мультиплексер пакует поток ТВ-канала и зашифрованный симметричный ключ в один и добавляет зашифрованный идентификатор потока. Открытым ключом шифруется не полностью весь поток, а только симметричный ключ. Это делается для того, чтобы снизить вычислительную нагрузку на абонентском устройстве, так как ассиметричное шифрование является более простым.

По защищенному каналу авторизованная абонентская приставка периодически получает от центрального сервера системы условного доступа набор ключей для дешифрирования симметричных ключей потоков ТВ-каналов, на которые абонент имеет подписку. Ключи для дешифрования хранятся в защищенной области памяти на STB и действительны, как правило, в течение 24 часов.

Для того чтобы расшифровать контент для просмотра, абонентская приставка считывает идентификатор из потока, и если соответствующего ключа нет в кеше, по защищенному каналу посылает подписанный специальным сертификатом запрос закрытого ключа на центральный сервер системы. Центральный сервер посылает запрос в Middleware и проверяет, есть ли у данной приставки права на просмотр требуемого контента. Если Middleware подтверждает права, сервер возвращает ключ. Закрытый ключ используется для дешифрирования симметричного ключа, с помощью которого дешифруется поток ТВ-канала или видеофильм, а абонент видит трансляцию на экране ТВ.

> Важнейшим критерием, при выборе системы криптозащиты, является набор совместимыхс ней абонентских устройств и их стоимость для конечного пользователя

Возвращаясь к принципиальным отличиям систем защиты контента, хочу отметить, что одним из наиболее значимых критериев, при выборе решения оператором, является набор абонентских устройств, совместимых с системой криптозащиты, и их стоимость для конечного пользователя. О надежности систем от взлома может говорить только опыт эксплуатации, подтвержденный операторами и держателями контента.