Александр Гитин, Verimatrix, директор по продажам в Восточной Европе

Безопасность доставки видео в OTT-среде

Сегодня вряд ли кто-нибудь возразит против того факта, что предложения видеоуслуг через Интернет серьезно подрывают бизнес платного телевидения. И хотя операторы минимизировали процесс «обрезания кабелей», вносящий главную лепту в снижение объемов подписки на платные ТВ-услуги, но игнорировать мощный потенциал OTT-доставки невозможно. Во избежание оттока абонентов в открытый Интернет операторы платного телевидения все чаще добавляют OTT-услуги в собственное комплексное предложение, изобретая варианты их монетизации в своей сети. Но на этапе внедрения OTT стоимость и сложность поддержки инфраструктуры услуг резко повышаются. И один из факторов здесь — необходимость обеспечить безопасность доставки услуг на разные устройства.

Распространение доставки интернет-видео на планшеты и смартфоны привело к доминированию приема видеоуслуг с помощью приложений, заменяющих в этом плане браузеры. Операторы также переняли модель с приложениями, позволяющую им эффективно управлять поиском контента, доступом к нему и его защитой. Даже развитие технологии HTML 5, кажется, не спасает браузерные интерфейсы от перспективы их превращения в арену битв конкурирующих технологий, что усложняет, а не упрощает предоставление услуг. Наиболее агрессивен в этом отношении Google, внедряющий свои технологии в устройства на базе Android, в первую очередь браузер Chrome и сервис Youtube, конкурирующий с аналогичными услугами операторов.

По мере формирования привычки пользования OTT-услугами на разных устройствах, у абонентов появляется и набор требований, ассоциирующихся с понятием качественного сервиса. Среди этих требований доступ к услугам на разных устройствах без дополнительного введения пароля и логина, а также автоматический перенос закладок, предпочтений и прочих атрибутов абонентского профиля.

В чем нуждаются операторы

Так как на рынке давно используется целый спектр DRM, операторы нуждаются в единой системе администрирования прав, предоставляющей общий интерфейс для работы с разными DRM и изолированной от их технологических особенностей. Единая система администрирования должна уметь «читать» бизнес-правила, сформулированные стандартным образом, и последовательно их реализовывать, обеспечивая их правильную техническую интерпретацию в каждом приемном устройстве. Чтобы убедить правообладателей в надежности систем безопасности, предназначенных для интернет-среды, в них должны включаться инструменты безопасности, применяемые в администрируемых DVB- и IPTV-сетях, в сочетании с дополнительным функционалом, разработанным специально для OTT.

Такие системы, в частности, должны обеспечивать оптимизацию защиты для адаптивного стриминга, полную проверку прав доступа к запрашиваемой услуге до отправки устройствам ключей и поддержку гибких, изменяемых бизнес-схем, в том числе обновлением лицензий.

При этом механизмы надежной защиты не должны снижать удобство пользования услугой (user experience) и противоречить ожиданиям пользователя в отношении прав и ограничений, формируемых у него при подписке на услугу. Одновременно при OTT-доставке на несколько экранов добавляется требование единообразия схем потребления услуги с разных устройств. Если пользователь сталкивается с тем, что ограничения доступа к услугам на разных устройствах выглядят по-разному, причем разница связана не с бизнес-правилами, а с особенностями технологической реализации, то это снижает впечатление от пользования услугой и, соответственно, ее ценность для абонента. Это типичная проблема систем безопасности, добавляемых в процессе разработки системы. На самом деле об этом нужно думать еще на стадии составления техзадания для пользовательского интерфейса.

Аутсорсинг администрирования мульти-DRM

Передача администрирования системы мульти-DRM на аутсорсинг позволяет оператору получить эту услугу в виде «черного ящика» и сконцентрироваться на своем основном бизнесе. Она также обеспечивает профессиональную поддержку системы, в том числе своевременный апгрейд по мере появления новых технологий безопасности. Такую систему в формате «черного ящика» Verimatrix предлагает как часть платформы VCAS под брендом MultiRights™. Система MultiRights™ обеспечивает единообразие реализации бизнес-правил применительно к различным DRM, работающим на устройствах разного типа.

Она автоматически распознает тип DRM подключенного устройства, выявляет требуемый характер отклика на запросы, а также определяет, какие ключи нужно использовать и какой тип криптографии нужен для их шифровки.

Попытки создать единую, пригодную для всех устройств бесплатную DRM успеха не имели, и многие устройства исторически используют старые типы DRM. Это имеет свои плюсы, по крайней мере всю систему безопасности разом взломать невозможно. Поэтому системы администрирования мульти-DRM еще долго сохранят свою актуальность. Более того, по мере дальнейшего распространения OTT-услуг будет расти и потребность операторов в таких решениях.