Успешное внедрение OTT-сервисов на неоператорских устройствах

Родриго Фернандес, *директор Irdeto по маркетингу*

Никаких признаков ослабевания темпов роста спроса на OTT-услуги не наблюдается. Это происходит потому, что у потребителей становится все больше устройств, и они хотят иметь доступ к контенту на всех этих устройствах. Поэтому для операторов ключевым фактором завоевания предпочтения клиентов становится поддержка OTT-сервиса на максимально возможном числе экранов. Тем не менее сам по себе процесс доставки OTT-контента на данный момент не слишком прост. Дело в том, что отраслевые игроки сами усложнили этот процесс, поскольку одни и те же вещи на разных устройствах обеспечиваются разными конкурирующими технологиями. В результате мир OTT-услуг был и остается весьма фрагментированным, и операторам становится все сложнее ориентироваться на этой пересеченной местности в стремлении удовлетворить все более взыскательные запросы клиентов.

Однако сейчас, похоже, ход игры начинает меняться, и в отрасли предпринимаются шаги к упрощению безопасной доставки OTT-услуг. Такие факторы, как активное внедрение технологии MPEG-DASH в 2015 году и массированный переход операторов на CBC-шифрование, упростили процесс развертывания и расширения OTT-предложений в соответствии с ожиданиями потребителей. Эти ожидания включают индивидуализацию просмотра, расширение спектра контента, повышение удобства просмотра и оптимальное соотношение цены и качества. При всем этом операторы должны быть уверены, что у них есть правильная стратегия безопасности, позволяющая им доставлять высоконенный контент на неоператорские устройства и гарантировать успех своим OTT-сервисам.

Упрощение развертывания OTT

Фрагментированность DRM-технологий ранее представляла огромную проблему для операторов, планирующих развертывать OTT-сервисы. Для охвата наиболее распространенных браузеров и устройств операторы должны уметь поддерживать несколько систем DRM. Несмотря на то что поддержка нескольких DRM может сбивать с толку, к счастью, это не особенно затратно. Однако реальная проблема фрагментированности DRM-технологий заключается в том, что все они поддерживают различные медиаконтейнеры, а наличие нескольких медиаконтейнеров на каждую единицу видеоконтента в несколько раз повышает затраты на пакетирование, хранение и доставку видеофайлов.

В 2015 году в практику вещания была введена технология MPEG-DASH, которая стала первым шагом к существенной экономии средств во фрагментированном мире OTT. Это технология потокового вещания, основанная на открытом стандарте и не зависящая ни от используемого кодека, ни от типа DRM. MPEG-DASH позволяет операторам использовать единый формат потокового видео на всех устройствах как для широковещательных, так и для OTT-сервисов. Даже компания Apple добавила в свой протокол HLS поддержку DASH-совместимых видеоконтейнеров CMAF. Это означает, что на устройствах iOS теперь можно использовать один и тот же формат видеоконтента (хотя и с применением разных манифест-файлов).

Применение CMAF и MPEG-DASH объединило формат видеофайлов OTT на различных устройствах, но актуальность проблемы шифрования для операторов платного телевидения сохранилась. Проблема заключается в том, что

выбор технологий шифрования обширен: Apple отдает предпочтение технологии AES 128 Cyber Block Chaining (CBC) для FairPlay DRM, а все остальные выбирают другую. Поэтому для передачи высокоценного контента через OTT операторы должны зашифровать файл двумя разными способами, позволяющими покрыть все основные DRM, а это удваивает затраты на CDN-сети.

К счастью для операторов, в данном направлении ситуация сейчас также меняется: начиная с 2016 года Google Widevine и Adobe Primetime начали поддерживать CBC, а на выставке NAB 2017 компания Microsoft объявила о поддержке CBC к концу 2017 года. Это не означает, что проблемы исчезнут немедленно, поскольку устаревшие устройства необходимо поддерживать, как и прежде, до окончания срока их службы. Но хорошо уже то, что новые технологии делают путь к росту охвата аудитории OTT-сервисами менее тернистым.

Решение проблемы раннего показа на неоператорских устройствах

Наличие вышеупомянутых разработок для OTT, безусловно, хорошая новость для операторов. Однако с повышением требований к безопасности при внедрении новых технологий, таких, например, как 4K UHD, и смещением предпочтений потребителей в сторону просмотра контента на неоператорских устройствах, вызовы на этом не заканчиваются. Новые требования к защите высокоценного контента повышают стоимость его доставки на неоператорские устройства. Многие из этих требований ожидаемо поддерживаются на уровне операторских устройств, но это подняло планку и для OTT-сервисов на неоператорских устройствах. А значит, на них должен обеспечиваться тот же уровень безопасности.

Спецификация Enhanced Content Protection (ECP) от MovieLabs определяет для операторов новый стандарт требований для получения прав на трансляцию premium-контента. Спектр этих требований широк: от обеспечения обновляемости защиты в системах CA и DRM до блокировки потребительских устройств, комплексных ответных мер по борьбе с пиратством и поддержки цифровых водяных знаков. На выполнение этих требований может уйти немало времени и финансов, особенно, если у операторов нет опытных партнеров по безопасности. Многие операторы платного ТВ быстро приходят к выводу, что единственный способ получить UHD-контент или ранние релизы контента для неоператорских устройств заключается в использовании только оригинальных для данного класса устройств DRM. Соответственно, чтобы получить требуемое покрытие всего спектра устройств, необходима стратегия защиты контента на базе нескольких DRM.

Быстрая эволюция рынка OTT привела к объединению высоких требований к безопасности. Это означает, что операторам пришло время сделать шаг назад и пересмотреть свою стратегию защиты контента в контексте собственной дорожной карты предоставления услуг, задавшись ключевым вопросом: насколько эта стратегия целесообразна и отвечает ли она будущим тенденциям? Некоторые операторы могут быть не готовы к изменениям или изо всех сил им сопротивляться, но это ошибка. В последние годы варианты стратегии защиты контента претерпели существенные изменения, и если операторы хотят продолжать доставлять потребителям контент и развивать пользующиеся все большим спросом возможности его просмотра на различных видах устройств, то им стоит обратить внимание на эффективную защиту контента как ключевой фактор. Правильная стратегия безопасности, внедренная при помощи правильно выбранного партнера, может помочь операторам успешно внедрить OTT-сервис, который станет двигателем их развития на высококонкурентном рынке.

реклама

РЕШЕНИЕ «IRDETO HOSTED CA»

БЫСТРОЕ И ЭКОНОМИЧЕСКИ ЭФФЕКТИВНОЕ ВНЕДРЕНИЕ СИСТЕМЫ УСЛОВНОГО ДОСТУПА МИРОВОГО КЛАССА ДЛЯ ЦИФРОВОГО КАБЕЛЬНОГО ТВ

irdeto
Building a Secure Future.™