СОВРЕМЕННЫЕ СРЕДСТВА ЗАЩИТЫ ВИДЕОКОНТЕНТА В СЕТИ ИНТЕРНЕТ

Автор: Куканов Антон
Федеральное государственное бюджетное образовательное учреждение высшего образования МТУ «МИРЭА», 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: kukanton@ya.ru

В настоящее время количество людей, активно использующих сеть Интернет в качестве основного источника получения информации, неуклонно растет. При этом доля онлайн видеозрителей уже существенно превышает долю телезрителей. Такая популярность сети Интернет и онлайн видео в частности, разумеется, не может не привлекать хакеров. Поэтому проблема цифрового пиратства в области медиа сегодня актуальна как никогда. В связи с этим правообладателям и распространителям контента приходится использовать технические средства защиты авторских прав (сокращенно ТСЗАП или DRM), принцип работы и критерии выбора которых я попытался описать в своей статье. При этом отдельное внимание было уделено ключевым особенностям основных существующих DRM систем и области их применения.

Ключевые слова: DRM, ТСЗАП, видеоконтент, видео, защита, Интернет-вещание, потоковый сервис, стриминг, streaming, Live TV, Video on Demand, VoD, DRM решения, Adobe Primetime, Google Widevine, Microsoft PlayReady, Marlin, HTML 5

MODERN VIDEO PROTECTION ON THE INTERNET

Kukanov A.A.
Federal State Educational Institution of Higher Education MTU «MIREA», 119454, Russia, Moscow, Vernadscogo avenue, 78 e-mail: kukanton@ya.ru

A lot of people use Internet nowadays. Moreover, they employ it as a main source of information. The share of online video viewers has already significantly exceeded the share of TV viewers. However, such popularity of network has one disadvantage. A lot of hackers do their affairs in media sphere. The problem of digital piracy is very important. Thereby rights holders and distributers have to use Digital Rights Management (abbreviated to DRM). The principle of operation and selection criteria I described in my article. Special attention was paid to the key features of main existing DRM systems and their applications.

Key words: DRM, video content, video, security, Internet broadcasts, streaming service, streaming, streaming, Live TV, Video on Demand, VoD, DRM solutions, Adobe Primetime, Google Widevine, Microsoft PlayReady, Marlin, HTML 5.

Введение. В настоящее время количество людей, активно использующих сеть Интернет в качестве основного источника получения информации, неуклонно растет. При этом доля онлайн видеозрителей уже существенно превышает долю телезрителей. И это вполне объяснимо. В отличии от телевидения в Интернете мы сами выбираем что и когда смотреть. При этом

спектр доступного видеоконтента очень широк. Будь-то видеоподкасты или видеоблоги, создаваемые пользователями-любителями, или профессиональные репортажи новостных агентств, записи телевизионных программ, полнометражные фильмы и сериалы. И если простых авторов-видеоблогеров не очень волнует вопрос защиты авторских прав, то для студий и творческих объединений, для которых производство видео является основной деятельностью и источником дохода, этот вопрос весьма насущный. Для монетизации контента в Интернете, правообладатели адаптируют различные бизнес-модели начиная от создания видео на деньги из рекламного бюджета и заканчивая подписками и разовыми платами за просмотр. Однако, чтобы защитить свой видеоконтент и доходы от него владельцы и дистрибьюторы медиапродукции вынуждены противостоять хакерам, которые успешно обходят их бизнес-модели и нарушают авторские права.

Актуальность. Проблема пиратства в области видеоконтента сегодня актуальна как никогда. Например, хакеры могут попытаться обойти оплату в модели с монетизацией каждого просмотра. Или же, легально купив право на одноразовый просмотр, незаконно распространять видеопродукцию среди неограниченного количества пользователей при помощи файлообменников или P2P (peer-to-peer) протокола. Хуже того, могут найтись и те, кто попытается получать прибыль от пиратского контента, или станет показывать защищенное авторским правом онлайн-видео со своей собственной рекламой или брендингом, разумеется, без каких либо разрешений со стороны правообладателей и финансовых отчислений.

Эти и другие подобные угрозы вынуждают правообладателей искать всевозможные средства и методы защиты своей медиапродукции, чтобы минимизировать финансовые потери, наносимые пиратством. И на помощь им приходят DRM (Digital Rights Management) системы - технические средства защиты авторских прав (ТСЗАП), при выборе которых следует помнить о нахождении правильного баланса между удобством пользователей и защитой контента. На рынке существует немало решений, призванных помочь владельцам платной медиапродукции, однако идеального средства защиты, к сожалению, нет.

Технологии онлайн-доставки и особенности защиты видеоконтента

Для начала необходимо разобраться, как видеоконтент попадает к потребителям. В зависимости от этого могут использоваться различные средства его защиты.

Упрощенная схема современной видео-платформы для Интернет-вещания включает в себя подготовку видео (перекодирование), его защиту и распределение по устройствам конечного пользователя (Рисунок 1). Как правило, сначала исходное видео попадает в систему перекодирования, которая адаптирует его для просмотра на различных устройствах конечного пользователя с учетом необходимого битрейта. А затем подготовленный контент уже доставляется зрителям.

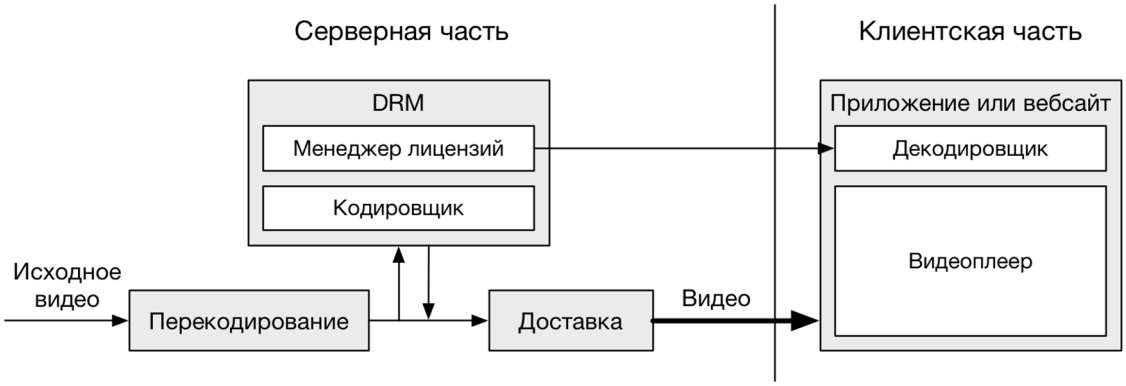

Рис. 1 - Упрощенная схема видео-платформы для Интернет-вещания

В настоящее время наиболее популярными методами онлайн-доставки видеоконтента являются:

- скачивание видеофайла для просмотра в специальной программе;
- скачивание файла по фрагментам, склеивание фрагментов воедино в видео-плеере и просмотр видео в процессе загрузки;
- потоковая передача видеоконтента в режиме онлайн с использованием специальных протоколов (RTSP, RTMP, MPEG2-TS).

Если видео нуждается в защите, то до доставки пользователям оно должно быть зашифровано с помощью DRM решения. В этом случае при воспроизведении плеер обнаружит зашифрованные данные и запросит от менеджера лицензий проверку подлинности и ключ расшифровки.

Почти все DRM решения построены на унифицированной архитектуре и состоят из двух частей: серверной и клиентской. Серверная часть также имеет два модуля: кодировщик, который зашифровывает исходное видео, и менеджер лицензий, который выдает пользователям лицензии на воспроизведение контента. Большинство DRM систем используют стандарт AES-128 для шифрования контента. А сервер лицензий впоследствии принимает решения о выдаче ключа дешифровки видео в соответствии с установленными правилами распределения контента.

DRM решения обычно используют алгоритмы асимметричного шифрования, в этом случае контент шифруется с помощью мастер-ключа, но пользователи должны применить свои ключи уникальной сессии. В случае потокового вещания в режиме реального времени ключ, как правило, изменяется по истечению заранее определенного времени. Если же необходимо зашифровать так называемые «видео по запросу» (Video on Demand (VoD)), то в этом случае используются различные ключи для различных видеофайлов, при этом лицензии могут кэшироваться, то есть храниться на локальном компьютере определенное время или до достижения заданного количества просмотров.

Тем самым можно выделить следующие основные принципы обеспечения защиты видеоконтента:

- прохождение аутентификации пользователем перед просмотром;

- срок доступности видео для просмотра, как с момента покупки, так и с начала воспроизведения;
- проверка подлинности пользовательского приложения;
- защита аналоговых и цифровых выходов;
- кэширование лицензий, позволяющее просматривать видеоконтент на протяжении определенного времени офлайн.

Для доступа к защищенному контенту со стороны пользователя используется комплекс программных средств, который взаимодействует с сервером лицензий и декодирует видео перед воспроизведением. Кроме того, он может обеспечивать защиту аналоговых и цифровых выходов, обнаруживать хакерские атаки, а также проверять все технические и логические ограничения, установленные на видеоконтент и конкретных пользователей.

При этом метод доставки контента потребителям совершенно не зависит от способа его защиты и определяется в первую очередь бизнес-моделью, выбранной производителем или дистрибьютором медиапродукции. Таким образом защищенное видео может доставляться как при помощи потокового вещания, так и обычного скачивания.

DRM решения

В настоящее время на рынке представлено немало DRM решений. Каждое из них имеет свои сильные и слабые стороны. При этом ситуация усугубляется высокой степенью сегментации рынка устройств: потребители могут просматривать видео как на компьютерах под управлением различных операционных систем через разнообразные браузеры, так и на мобильных устройствах, а также телевизорах или телевизионных приставках. В связи с этим создание универсальной технологии чрезвычайно затруднено.

Особой популярностью в настоящее время пользуется просмотр видео через браузер, что заставило консорциум W3C разработать спецификации Encrypted Media Extensions (EME) для защиты видеоконтента. Они обеспечивают канал связи между веб-браузерами и программным обеспечением DRM. Это позволяет использовать HTML5 для воспроизведения защищенного DRM контента (такого как потоковое видео), без привлечения сторонних плагинов, например, таких как Adobe Flash.

Что же касается мобильных устройств, то у них поддержка DRM систем в браузерах отсутствует, в связи с чем, обеспечить доставку медиаконтента и его защиту можно только при помощи создания специальных приложений, которые будут распространяться через App Store на iOS и Google Play на Android.

Наиболее популярными DRM системами являются Adobe Primetime, Google Widevine, Microsoft PlayReady и другие.

DRM-приложение Adobe Primetime считается одним из ведущих решений в области защиты видео, в виду широкой распространенности Flash-плеера в браузерах. Транслируемый контент «на лету» шифруется Flash Media сервером, при этом исходные файлы не нуждается в шифровании (в отличии от DRM системы от Microsoft - PlayReady, о которой речь пойдет чуть позже). При передачи данных используется специальный протокол: или RTMPE (Real-Time

Media Protocol Encrypted), или RTMPS (Real-Time Media Protocol over SSL). Первый из них использует 128-битное шифрование, чтобы предотвратить перехват потокового видео в сети Интернет или сторонними приложениями. А протокол RTMPS в свою очередь использует промышленный стандарт SSL, который обеспечивает TCP/IP-соединения и защищает все передаваемые через них данные. Выдача лицензий на воспроизведение видео выполняется серверами лицензий.

DRM решение от Google - Widevine - сочетает в себе немалое количество принятых индустрией стандартов, таких как «Dynamic Adaptive Streaming over HTTP (DASH)», «Common Encryption (CENC)», «Encrypted Media Extensions (EME)» для обеспечения надежной защиты видеоконтента. Widevine широко используется в телевизионных приставках и телевизорах (например, в Smart TV), в мобильных устройствах, а также для защиты Blue Ray дисков, и имеет поддержку HTML5.

Еще одна заслуживающая внимания DRM система - Microsoft PlayReady. Она поддерживается большим количеством платформ и устройств, включая настольную и мобильную операционные системы Windows, ОС Linux, iOS и Android, а так же HTML5, игровые приставки и умные телевизоры, Blu-Ray и DVD-плееры. PlayReady поддерживает все типы контента и различные пользовательские сценарии для VoD и Live TV, в том числе подписку, прокат и отдельные покупки. Это позволяет использовать DRM систему от Microsoft таким известным американским провайдерам онлайн-видео как HBO и Netflix. Однако стоит отметить, что портированием PlayReady на устройства потребителей занимается не Microsoft, а другие компании, в чем и кроется одна из основных проблем этой DRM системы — невозможность приобрести решение сразу на все устройства, а необходимость платить за каждую оболочку отдельно.

Стоит также отметить и менее распространенную DRM систему Marlin, созданную на базе открытых стандартов. Marlin позволяет устройствам пользователей импортировать контент из разнообразных независимых сервисов и обеспечивать пиринговые взаимодействия. Marlin используется для защиты контента компанией Sony в PlayStation Network и британским сервисом YouView.

Выводы

Одним из наиболее важных вопросов при выборе DRM решений является спектр поддерживаемых платформ и пользовательских устройств. Например, Adobe Primetime предлагает удобные инструменты для защиты видеоконтента, которые не требуют установки дополнительных плагинов, так как Flash Player уже установлен на огромном количестве устройств. Ведь необходимость установки дополнительных плагинов может отпугнуть потенциальных покупателей платного контента из-за низкого уровня компьютерной грамотности или банального нежелания устанавливать что-либо на свой компьютер. Кроме того, существует большое сообщество разработчиков, использующих технологию Adobe, что также является преимуществом этой

DRM системы. Однако, стоит отметить, что сама платформа Adobe Flash в настоящее время теряет свою популярность, в виду отсутствия поддержки мобильных операционных систем (поддержка Android была прекращена в 2013 году) и конкуренции со стороны HTML5, продвигаемой Apple.

Не уступают Adobe Primetime и решения Widevine и PlayReady, основными преимуществами которых являются поддержка огромного количества устройств, в том числе мобильных, и интеграция с вышеупомянутыми спецификациями HTML5 EME.

Все описанные решения DRM являются масштабируемыми, потребляют примерно одни и те же ресурсы и используют единые алгоритмы шифрования. В связи с этим при выборе DRM решений следует в первую очередь опираться на список поддерживаемых пользовательских устройств и кодеков, цену, удобство использования, бизнес-модели и технологии доставки видеоконтента.

Справочная информация

1. Denis Bulichenko, «Online Video Services and DRM Technology», DENIVIP Media, 01.12.2011.

2. Digital rights management [Электронный ресурс] URL: https://www.adobe.com/ru/solutions/primetime/digital-rights-management.html (дата обращения 20.05.2016).

3. Adobe Access [Электронный ресурс] URL: https://www.adobe.com/support/adobeaccess/pdfs/server/AdobeAccess_4_Overview.pdf (дата обращения 20.05.2016).

4. Widevine DRM [Электронный ресурс] URL: https://www.widevine.com/wv_drm.html (дата обращения 20.05.2016).

5. PlayReady Product Suite [Электронный ресурс] URL: https://www.microsoft.com/playready/features/ (дата обращения 20.05.2016).

6. Marlin DRM [Электронный ресурс] URL: http://www.marlin-community.com/technology (дата обращения 20.05.2016).