Оптимизация системы обеспечения защиты доходов в посткарточную эпоху

Александр Гитин, *директор по продажам Verimatrix в России и странах СНГ*

Современные технологии доставки платного телевидения дают широкие возможности для привлечения абонентов и роста доходов операторов. Однако одновременно появляются и новые проблемы, связанные с обеспечением безопасности контента и доходов, которые необходимо решать для выполнения обязательств в отношении правообладателей контента. В этой статье рассматривается способ решения таких проблем и обсуждаются важные аспекты разработки стратегии обеспечения защиты доходов для операторов мультисервисных сетей. Также объясняется, как интеграция аппаратных и программных средств защиты может помочь в защите доходов, что актуально в эпоху TV Everywhere.

Обеспечение защиты доходов – краеугольный камень платного телевидения

Перед операторами платного ТВ стоит главная цель: монетизировать контент и защитить его и видеоуслуги от несанкционированного доступа – от пиратства. Особое внимание уделяется защите предоставляемых видеоуслуг от целого спектра угроз, таких как кража услуг, пиратство смарт-карт, клонирование устройств и т.д.

Методы, используемые для несанкционированного доступа к контенту и нелегального его использования различны. Острее всего проблема стоит, когда речь идет об услугах платного ТВ для сетей доставки контента на разные экраны, в отношении которых операторы должны заранее проработать целый комплекс вопросов по используемым технологиям и ведению бизнеса. В конечном счете, основная задача сводится к тому, чтобы выработать политику защиты и выбрать технические средства, которые позволят минимизировать расходы и при этом в долгосрочной перспективе будут удовлетворять постоянно изменяющимся требованиям к видеоуслугам (и обеспечению доходов). Выбор технологии обеспечения защиты имеет решающее значение для будущей конкурентоспособности оператора и его финансовых показателей.

Важные требования обеспечения безопасности

Гибкая и эффективная архитектура системы CAS/DRM является важнейшей движущей силой инновационных бизнес-моделей и, следовательно, определяет стратегический вектор развития. Выбор правильной технологии CAS/DRM смещает акцент с традиционной защиты контента для одной сети к более широкой концепции защиты доходов для мультисервисных сетей.

Необходимо также учитывать множество других факторов обеспечения доходов бизнеса, и в частности финансовых, таких как первоначальные затраты на приобретение (CAPEX), эксплуатационные расходы (OPEX), потери от сбоев функционирования системы защиты (текущая потеря доходов), затраты на модернизацию CAS/DRM в случаях хакерских атак, стоимость сертификации абонентской приставки (STB) и срок выполнения заказа по их поставкам, возможность широкого выбора среди поставщиков приставок (STB) и их ценовая доступность (конкуренция между производителями STB), возможность использования одной и той же CAS/DRM при доставке контента на экраны разных типов, И все это – без дополнительных неудобств для абонента. Нужно также проработать возможность лицензирования и продажи высококлассного контента (при использовании CAS/DRM и других технологий, одобренных правообладателями контента и студиями).

Требования правообладателей

Возможность предложить контент высокого класса имеет решающее значение для успеха в продвижении видеосервисов на платной основе. Для студий, правообладателей и поставщиков контента серьезной проблемой является угроза крупномасштабного пиратства, которое может нанести существенный финансовый ущерб. К тому же сегодня расходы на рекламу для HD-контента значительно выше, чем для SD-контента.

Правообладатели тщательно следят за соблюдением всех условий потребления лицензионного контента за счет использования одобренных технологий и правовых процессов. Они, как и операторы платного ТВ, ожидают, что разработчики систем CAS/DRM смогут решать постоянно изменяющиеся задачи по защите контента, используя набор технологий и инструментов, обеспечивающих полную безопасность доходов в течение всего периода времени от создания контента до его хранения, доставки и просмотра, в том числе и за пределами сети.

Выбор технологии защиты контента, которая пользуется доверием правообладателей, позволяет получить высококлассный контент и монетизировать его.

Использование интегрированного подхода

Одним из последних достижений в области обеспечения защиты контента в посткарточный период является интегрирование в чипсеты видеоприставок (STB), используемых для приема платного ТВ, специального программного обеспечения. В результате приставка на уровне SoCs способна эффективно защитить контент.

При интеграции на уровне ПО и аппаратных средств все особо важные с точки зрения безопасности функции чипсетов STB сосредоточены в аппаратном ядре, благодаря чему клонировать или копировать видеоприставку крайне сложно. Это, в свою очередь, позволяет создать серьезную защиту и предоставить

определенные архитектурные преимущества в построении решения.

Аппаратное ядро, защищающее от явных и скрытых атак, помогает достичь нового уровня защиты на чипсете STB, превосходящего большинство самых современных методов на смарт-картах. Благодаря этому интегрированный подход устраняет возможность хакерских атак, характерных для съемных аппаратных средств и компьютерных шин, связывающих данные аппаратные средства с STB.

При разработке программного обеспечения, интегрируемого в STB в сочетании с аппаратным ядром и защитой контрольного слова (CW), все важные для безопасности информационные данные не передаются через внешние или иные легкодоступные интерфейсы. Вместо этого CW доставляются внутри чипсета непосредственно к дешифраторам. При условии соблюдения всех требований к безопасности процессов дешифрования видео и декодирования защита от доступа с помощью CW значительно превосходит по надежности традиционные решения.

Кроме того, если процесс защиты управления ключами дешифрации полностью интегрирован с аппаратным ядром, у хакеров практически не остается никаких возможностей для отслеживания и изменения механизмов обеспечения безопасности устройства. Учитывая то, что сегодня на рынке видеоуслуг наблюдается рост количества используемых гибридных сетей (DVB/IP), важным является возможность предоставления подписки на видеоуслуги на уровне серверной части системы CAS/DRM. Такая комбинация серверной (CAS/DRM) и абонентской (STB) защиты обеспечивает надежную среду для проведения полной аутентификации устройств и всех сервисных сообщений (типа запросов – ответов), способных повысить защищенность системы CAS/DRM от несанкционированного доступа.

Преимущества использования программного обеспечения

Аппаратное ядро обеспечивает эффективную защиту на уровне микросхемы, а в сочетании с возможностями программного обеспечения формируется сквозная система высокоуровневого управления ключами защиты. Таким образом, аппаратное ядро является важным элементом системы CAS, а не заменой для нее.

Сегодня одна из наиболее явных тенденций в обеспечении защиты контента для сетей цифрового ТВ является применение бескарточных систем. Именно этот подход все чаще становится стандартным требованием операторов. Привлекательность такого метода заключается в полном использовании средств технического обеспечения на уровне чипсета STB с помощью подсистем безопасности CAS. Эта мощная комбинация обеспечивает экономическую эффективность, возможность обновлять ПО и гибко применять его в сочетании с самыми высокими уровнями защиты, заложенными в аппаратных средствах.

Подобно тому, как реализована в IP-сетях доставка видеоуслуг на основе STB с обновляемой на уровне ПО защитой контента, использование аппаратного ядра защиты в чипсете STB может решить ряд проблем, связанных с возможным доступом к CW и его распространением. В таких системах ПО защиты отвечает за прием запросов и выдачу ключей дешифрации, а также прием и хранение сервисных сообщений, синхронизацию дешифрования и управление пользовательским интерфейсом. Однако данное ПО не принимает участия в непосредственной обработке самих ключей дешифрования видео или расшифровывания медиапотоков. Кроме того, двусторонняя связь по IP в гибридных сетях DVB/IP добавляет возможность дополнительной аутентификации устройств, выявления и нейтрализации клонированных устройств.

Особенности решения Verimatrix

Verimatrix предлагает защиту контента и комплексное решение для предоставления видеоуслуг в мультисервисных сетях DVB, IPTV, OTT и гибридных. Платформа Video Content Authority System (VCAS) имеет следующие достоинства:

- высокую эффективность для абонентских устройств, работающих через IP-протокол;
- проверенную архитектуру на основе бескарточных технологий, а также (опционально) смарт-карт;
- единую шину для интеграции и сертификационных процессов для DVB, IPTV и OTT;
- возможность использования водяных знаков;
- широчайшую поддержку сторонними партнерами на аппаратном и программном уровнях.

Особенности решения Verimatrix:

- стирание границы между CA и DRM (единая система защиты и условного доступа для любых видов сетей);
- эффективное предоставление видеоуслуг независимо от используемых сетевых технологий;
- возможность проведения модернизации сетей без затрат на дополнительную интеграцию;
- возможность управления правами доступа для абонентов, имеющих разные экраны, на основании интеграции с внешними системами оператора.

Платформа Verimatrix VCAS является реализацией трехмерной стратегии безопасности цифрового ТВ, которая выходит за пределы классических подходов систем условного доступа (CA) для защиты услуг платного телевидения и помогает доставлять в защищенном виде видеоуслуги на любой экран, в любой сети и в любое время. VCAS предоставляет целый ряд функций для любого вида сетей (DVB,OTT, IPTV, Hybrid), построенных на единой платформе с возможностью расширения в зависимости от сегмента рынка. Данная платформа формирует единую систему защиты для всех видов сетей и абонентских устройств, поддерживающих различные видеоформаты и системы управления цифровыми правами (DRM), обеспечивая полную согласованность в управлении правами доступа в различных сетях оператора.

Заключение

Единая система обеспечения защиты контента платного телевидения является жизненно важным компонентом для операторов, стремящихся расширить спектр своих видеоуслуг, выполнить свои договорные обязательства по отношению к абонентам и правообладателям. Интеграция программных и аппаратных средств обеспечения безопасности позволяет сделать новый шаг в защите контента и доходов при использовании STB, что в свою очередь дает возможность предлагать абонентам и реализовывать новые видеоуслуги и внедрять новые бизнес-модели.