Современные СУД – задачи и решения

Анна Бителева

Изменения, произошедшие за последние несколько лет на рынке видеоуслуг, неизбежно поменяли технологии защиты контента и отчасти сами задачи разработчиков систем условного доступа.

История угроз

С изменением технологий распространения видео менялся и характер пиратских угроз. Лет 15–20 назад атакам в основном подвергались приставки и смарт-карты. Данные с них либо клонировались, либо модифицировались таким образом, чтобы можно было декодировать передаваемую в потоке секретную информацию по упрощенной схеме. Это были дорогостоящие, технически сложные взломы, включающие в том числе неинвазивный мониторинг напряжений или электромагнитного излучения.

Но с распространением Интернета пиратские приемы упростились – злоумышленники ввели в обиход кардшаринг. Эта схема взлома использует слабость базовых систем защиты, основанных на применении технологии DVB Simulcrypt и стандартного алгоритма скремблирования (CSA).

В таких системах расшифрованное смарт-картой контрольное слово в открытом виде пересылалось в скремблер, расположенный в основном чипсете приставки. Это позволяло пиратам без особенных сложностей перехватывать его по дороге и через Интернет раздавать клиентам. Для противодействия кардшарингу разработчики СУД начали логически связывать смарт-карты с чипсетами приставок и шифровать канал передачи контрольного слова. Такая защита использует аппаратные элементы, и взломать ее достаточно сложно. Тем не менее решить проблему кардшаринга операторы могут, только заменив в сети все приставки без защиты канала передачи контрольного слова, а в крупных сетях этот процесс затянулся на годы.

Кроме того, сохранилась менее распространенная, но более опасная форма шаринга ключей – раздача сеансового ключа. Сеансовый ключ используется для кодирования последнего, дескремблирующего ключа и меняется довольно редко, например раз в месяц. Подписчики используют сеансовый ключ для расшифровки принимаемых в потоке контрольных слов, и далее, соответственно, самого контента.

Для извлечения сеансовых ключей требуется реверс-инжиниринг системы условного доступа. Это значительно более сложная задача, чем перехват контрольного слова, но сеансовые ключи и более ценная добыча для пиратов.

С защитой от классического шаринга новую жизнь получили и атаки путем неинвазивного мониторинга, тем более что соответствующие инструкции сейчас при желании можно найти в Интернете.

Однако это далеко не главные угрозы со стороны пиратского сообщества. Основная проблема сегодня – это незаконная раздача видео, принимаемого в основном на легальные устройства.

Пиратская раздача видео

С дальнейшим развитием Интернета и технологий раздачи видео по открытой сети задачи пиратов еще более упростились. Теперь нет необходимости рассылать ключи, можно просто принимать контент и доставлять его клиентам нелегальным образом. Первой формой такого пиратства стала пиринговая раздача файлов, обычно реализуемая в формате торрентов. Она до сих пор является основной формой пиратства для полноформатных фильмов и другого видеоконтента, передаваемого в файловом формате. При хорошей инфраструктуре некоторые популярные наименования сейчас уже можно смотреть в реальном времени.

Позже стали распространяться пиратские платформы со стримингом видео в реальном времени. Сначала видео принималось только на специально разработанные приложения, но сейчас для просмотра пиратского контента достаточно и стандартного устройства с вебраузером. В стриминговых форматах передаются разные услуги – от платных, с качественным контентом, до бесплатных сайтов, изобилующих рекламой и ссылками на вредоносное ПО.

В популяризацию пиратских услуг вносят свою лепту и программные медиаплееры, такие как Kodi. Это плагины, предлагающие электронные гиды с полупрофессиональными интерфейсами (look and feel). Они не привязаны к конкретным сервисам, легальным или пиратским, поэтому и отношение к ним двоякое. На продажи медиаплееров с предустановленным Kodi в некоторых странах наложен запрет, но плагин доступен для установки в плеер после его покупки. В этом отношении показательны санкции, недавно наложенные на Kodi в поисковой системе Google. Она не удаляет ссылки на плеер из поисковой базы, но исключила слово “Kodi” из автозаполнения в окне поиска.

Причина массового распространения такого пиратства вполне понятна. Оно

легко реализуется технически, особенно с появлением облачных технологий, и обходится значительно дешевле прежних вариантов. И если результатами перехвата ключей или клонирования приставок можно пользоваться только в пределах сети, где совершен взлом, то нелегальное распространение контента может быть востребовано и далеко за ее пределами, фактически по всему миру. Таким образом, с точки зрения возврата инвестиций пиратская раздача видео явно интереснее всех видов взлома.

Опрос операторов, проведенный компанией Cartesian по заказу Verimatrix в рамках комплексного исследования, показал, что именно нелегальная ретрансляция сегодня более всего заботит операторов.

Для многих пользователей пиратских сервисов качество не является существенным фактором при выборе источника видео. Для них важнее легкий доступ, а также низкая цена или полная бесплатность услуги.

Проблема с нелегальными интернет-ретрансляциями заключается еще и в том, что пиратский характер сервиса не всегда очевиден для конечных пользователей. Причем в некоторых странах пользование такими сервисами может караться по закону.

Меры противодействия

Контент для ретрансляций пираты обычно получают с легальных авторизованных устройств. Для этого существует несколько способов.

Пираты могут:

• Перехватить контент в канале HDMI, используя HDCP-стриппер. Существуют устройства, умеющие снимать защищенный HDCP-контент с HDMI-выхода абонентской приставки и отправлять на компьютерные карты видеозахвата, заново кодирующие поток.

• Снять контент сервиса видео по запросу, полученного на ПК, путем захвата изображения на экране.

• Снять качественную копию с дисплея, например с помощью телевизионного камкодера.

HDCP 2.2, последняя версия стандарта, пока не взломана, но существуют способы понизить ее до взломанных версий и затем использовать HDCP-стриппер. По оценке бывшего вице-президента Verimatrix по маркетингу Стива Кристиана (Steve Christian), обход HDCP 2.2 — достаточно сложная процедура, что сокращает объемы пиратства, реализуемого таким способом.

Эффективных методов технологического противодействия двум другим способам пока не придумали. Единственный изобретенный вариант — наложение водяных знаков, некоего невидимого кода, в котором заложен номер авторизованного абонентского устройства, на который был принят нелегально распространяемый контент.

Необходимость защищать выход HDMI доверенным ПО, а сам премиальный контент — водяными знаками прописана в спецификации MovieLabs Specification for Enhanced Content Protection (MovieLabs — организация, созданная основными голливудскими студиями для решения разных задач, в том числе стандартизации, необходимой для работы студий). Распространение водяных знаков тормозится тем, что оно сопряжено с дополнительными расходами для операторов, которые им предложено нести, чтобы защитить бизнес студий, а они на это часто не готовы. Об этом говорили и руководитель отдела продуктового маркетинга Nagra Кристофер Шаутен

(Christopher Schouten), и вице-президент по маркетингу Viaccess-Orca Леонид Беркович, интервью с которым мы планируем опубликовать в одном из ближайших номеров «Теле-Спутника».

В то же время студии часто сами маркируют водяными знаками отдаваемые операторам копии фильмов. В случае утечки контента это помогает им определять, из какой сети она произошла.

Бескарточные системы

Удобство бескарточных систем очевидно. Они исключают расходы на изготовление, логистику и доставку карт, а также кардшаринг, если в сети используется только бескарточное решение. Однако до недавнего времени большинство операторов и самих разработчиков СУД не считали такие системы пригодными для защиты премиальных сервисов.

Тем не менее ситуация постепенно менялась, и в прошлом году разработчики СУД дружно признали, что бескарточные системы уже не уступают карточным по уровню безопасности. Хотя отношение к ним все-таки немного разнится. Кристофер Шаутен полагает, что карточные системы могут стать выбором крупных операторов, так как равный уровень безопасности не исключает того факта, что карты поменять легче, чем приставки. В то же время Стив Кристиан отдает предпочтение бескарточным системам. Он считает их более надежными, так как они допускают превентивные изменения алгоритмов защиты. Заметим, что большинство карт также имеют возможность апгрейда, но более поверхностного.

Поднять бескарточные системы на должный уровень безопасности позволило появление защищенных процессоров. Это может быть либо отдельный физический процессор, что, видимо, более надежно, либо виртуальный, выделенный из ресурсов основного.

Технологии защиты процессора отрабатывались годами, так как его защита требуется и в карточных системах. Процессор должен обеспечивать безопасную загрузку ПО приставки и безопасный апгрейд этого ПО, скремблирование содержимого памяти DRAM для защиты от перехвата. Вмешательство в эти процедуры может привести к взлому приставки. Процессор также отвечает за управление защитой HDMI-порта и наложение водяных знаков. И наконец, надо защищать от перехвата видео, циркулирующее по чипсету в открытом виде. Поэтому перенос в чипсет приставки функционала смарт-карт — не единственная причина для выделения в нем безопасной зоны. Скорее наоборот, перенос стал возможен после того, как технологии защиты чипсетов оказались на должном уровне.

Таким образом, сегодня в большинстве чипсетов выделяется безопасная среда исполнения (Trusted Execution Environment, TEE), в которой реализуются все секретные процессы. В рамках TEE формируется и безопасный видеотракт (Secure Video Path, SVP). Наличие в чипсете TEE и SVP — тоже требование спецификации Movie labs.

TEE обеспечивает взаимную изоляцию выполняемых в ней процессов и постоянную проверку собственной целостности во время обработки данных. А SVP изолирует от недоверенного ПО все манипуляции с незащищенным видео — его дешифровку, декодирование, наложение водяных знаков. Оно поступает в приставку в зашифрованном виде, и после декомпрессии в зашифрованном же виде передается на HDMI-выход.

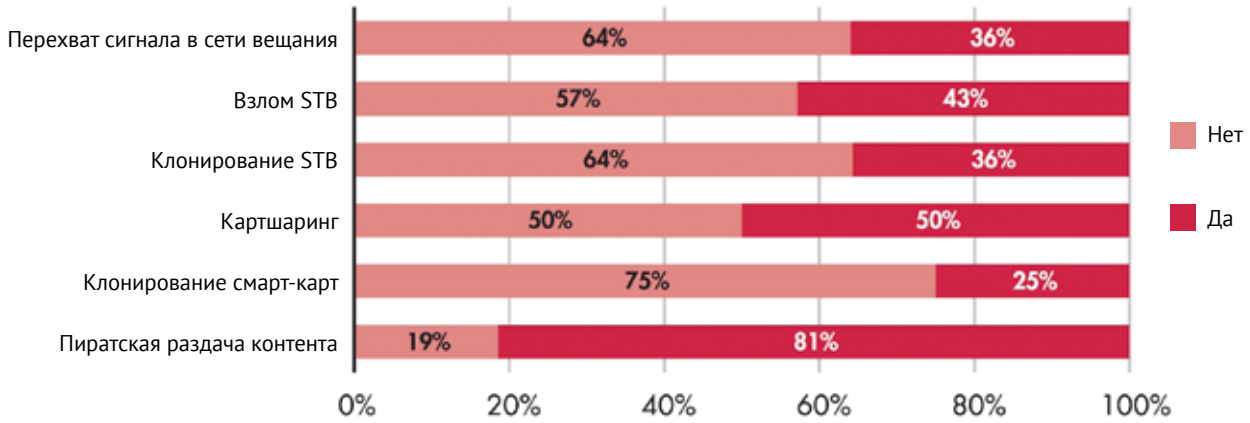
CAS vs DRM

Под CAS обычно понимают системы доступа, предназначенные для вещательных сетей без обратного канала и реализованные по стандарту DVB Simulcrypt. Они защищают передаваемый транспортный поток и не берут на себя функций управления воспроизведением.

DRM, в свою очередь, пришли из компьютерной сферы и традиционно используются для защиты контента в цифровой среде, то есть в IP-сетях. Они требуют обратного канала для запроса ключей и лицензий и управляют воспроизведением. Однако с распространением видеоуслуг в открытом Интернете DRM начали наращивать свою функциональность.

Руководитель отдела системной интеграции компании SmartLabs Артем Гелун описывает это следующим образом: «Современные DRM-системы, про которые в 99% случаев идет речь, объединили в себе возможности CAS в части криптографии, безопасности и надежности закрытия контента и функциональность DRM по ограничению распространения приобретенного контента после его расшифровки. Например, DRM может ограничить максимальное разрешение изображения, если не используется аппаратное шифрование на устройстве, запретить вывод HD-контента или вообще отображение любого контента на аналоговые

Какие виды угроз вызывают озабоченность операторов



Источник: отчет об исследовании Cartesian и Verimatrix «Будущее бескарточных систем безопасности», 2017 г.

выходы как наименее защищенные, или потребовать определенной версии HDCP для воспроизведения определенного фильма».

Что же касается CAS, то «они могут работать без обратного канала, а реализации с обратным каналом, как правило, сохраняют совместимость с ними, что позволяет один и тот же поток передавать как по спутнику, так и по IP-сетям; кроме того, они имеют ограниченную по сравнению с DRM функциональность».

Большинство крупных операторов сегодня работают в разных средах, поэтому им нужны и СУД, и DRM. Разработчики СУД удовлетворяют эту потребность по-разному. Компания Verimatrix, исходно предлагавшая систему DRM, дополнила ее стандартной CAS, а NagraVision, напротив, дополнила CAS собственной DRM. Обе DRM используются для защиты контента в приставках. А на планшетах, смартфонах и компьютерах контент защищается системами DRM, привязанными к платформе устройства. Widevine защищает контент на платформе Android, Fair Play — на платформе IoS, а Play Ready — на Microsoft. Таким образом, операторам приходится поддерживать несколько DRM, и все производители CAS предлагают зонтичные решения, упрощающие одновременное администрирование нескольких систем.

Widevine, используемая в приемниках на базе Android и встроенная в браузер Google Chrome, из-за крайней популярности этих продуктов обслуживает сегодня больше половины всех приемных устройств. Но в компании Google, видимо, хотят еще более закрепить доминирующее положение на рынке и планируют адаптировать DRM для применения в DVB-сетях. Для этого информацию о ключах и лицензиях, отправляемых DRM-сервером, нужно инкапсулировать в формат ECM- и EMM-сообщений, используемых в системах DVB Simulcrypt. Правда, чтобы создать СУД, конкурентную серьезным решениям, этого явно недостаточно. И захотят ли в Google вкладывать значительные средства в разработку для стагнирующего сектора — большой вопрос.

Заметим, что разработчики СУД не рассматривают платформу Android как пригодную для приема премиальных услуг. Вернее, не рассматривают лицензионную версию этой платформы. Причины тут две. Во-первых, лицензионная версия не допускает ограничений на использование сторонних приложений. А так как попадающие в магазин приложения не проходят сколько-нибудь серьезной проверки, на приемное устройство может попасть какое-то зловредное ПО. Например, предназначенное для вывода приемника из строя или для организации DDoS-атаки. Существуют также приложения, искажающие файлы в памяти гибридного устройства или стирающие ключи. Цель такого ПО не воровство контента, а вымогательство денег из операторов, чьи сети оказываются заблокированными.

Некоторые нарекания вызывает и сама безопасность Android-чипсетов. DRM Widevine предлагается в версиях с разными уровнями защищенности, и верхняя версия обеспечивает в чипсетах безопасный медиатракт. Однако лицензионный вариант Adroid не позволяет разработчикам СУД добавлять аппаратные схемы защиты в чипсеты. Поэтому для приставок они рекомендуют использовать нелицензионый вариант Android Open Source Project (AOSP), лишенный этих ограничений.

Виртуальные системы доступа

Важным трендом в скором будущем может стать появление виртуальных CAS и DRM. По принципу действия они аналогичны виртуальным SIM-картам. Они предполагают интеграцию в чипсет унифицированного аппаратного модуля, в который должен загружаться программный клиент конкретной CAS или DRM. Причем в один чипсет могут одновременно загружаться клиенты нескольких CAS и DRM. Сегодня параллельно продвигаются два таких проекта. Один — Embeded CI, его разработка инициирована группой, включающей операторов, вещателей, производителей приставок и других игроков рынка. Другой — совместное решение NagraVision и Broadcom, получившее название Nagra-On-Chip Security (NOCS). Какая из систем завоюет рынок, пока неизвестно, но то, что они появились почти одновременно, говорит о том, что идея витает в воздухе.

Изначально концепция CAS DVB Symilcrypt предполагала использование

приставок с одинаковой аппаратной реализацией со стандартным CSA-скремблером, различающимися только картами доступа. Но требования безопасности вынудили разработчиков СУД вводить аппаратные дополнения к стандартному «железу». Идея виртуальных СУД возвращает концепцию унифицированного «железа», но уже с новым уровнем безопасности.

Новые направления работы

Все крупные разработчики систем условного доступа не ограничиваются основным бизнесом и предлагают свои решения в смежных сферах. Долгое время на их стендах на различных выставках демонстрировались варианты абонентских middleware, по существу — пользовательских интерфейсов, иногда дополненных системой поиска и рекомендаций. Такие решения показывали NDS (Cisco), Nagravision, в свое время купившая Open TV, а также Irdeto. Однако в последнее время такие демонстрации со стендов исчезли. Леонид Беркович из Viaccess-Orca объясняет это тем, что операторы, развивающие интерактивные услуги, делают это на базе полномасштабных OTT/IPTV-платформ, для которых пользовательский интерфейс — лишь небольшая часть, привязанная к конкретной платформе. Поэтому такие интерфейсы уже не продвигаются их производителями, хотя и продолжают применяться в операторских сетях.

На сегодняшний день производители СУД считают для себя перспективными два направления.

Во-первых, это анализ данных, собираемых в сети оператора. Решения в этой области предлагают Viaccess-Orca, Nagravision и Verimatrix. По наблюдениям Стива Кристиана, операторов интересует информация трех категорий.

К первой относится группа вопросов о QoS: насколько хорошо рабо-

Новые решения для защиты контента

Беседовала Анна Бителева

На прошедшей в конце февраля 2018 года выставке CSTB мы встретились с директором по маркетингу продуктов Irdeto Джимом Филлипоффом. Накануне компания объявила о запуске нового решения — облачной CAS Irdeto Hosted CA. Это один из вариантов использования бескарточной системы Irdeto Cloaked CA. Новая модификация предполагает возможность использования операторами ресурсов системы, установленной у российских партнеров Irdeto. Облачные решения уже работают на нашем рынке и показали свою востребованность при грамотном маркетинге. Мы расспросили собеседника и о других направлениях работы компании.

Какие основные задачи стоят сейчас перед вашей компанией?

Irdeto работает в сфере защиты видеоконтента около 50 лет. В последнее время характер угроз со стороны пиратов постоянно меняется. И наша задача, как в шахматах, продумывать свои ходы на несколько шагов вперед. В этом часто помогают новые технологии. В частности, мы одни из первых начали внедрять бескарточную систему, сейчас это решение уже проверено на практике в сетях многих операторов.

Насколько высок интерес к бескарточной технологии защиты в СНГ и России?

На территории СНГ нашу бескарточную систему в общей сложности используют восемь сетей, в том числе три в Казахстане: эфирно-спутниковая сеть Kaztelradio, кабельная Alma TV и DTH-платформа Caspio HD. Бескарточная система также установлена у двух российских кабельных операторов и в эфирных сетях Украины, Белоруссии и Узбекистана.

И только что мы представили версию нашего бескарточного решения Irdeto Hosted CA, ориентированного на небольших кабельных операторов. Российские сети КТВ сейчас

тает распределительная сеть, есть ли ограничения по полосе пропускания или задержки в сетевых узлах, есть ли сбои в работе абонентских устройств?

Вторая группа вопросов касается статистики потребления. Операторов интересует, что смотрят их абоненты, как долго и на каких устройствах? Для оптимизации услуг важно понять предпочтения абонентов не только в плане контента, но и способа его потребления.

К третьей категории относятся вопросы относительно логики и эргономики интерфейса приставки или приложения. Например, сколько кликов обычно делает абонент, чтобы запустить услугу? Выбирает ли он прямой путь или обходной, с большим количеством кликов? Быстро ли он продвигается по этим пунктам? Эта статистика собирается в основном во время тестовых периодов и сейчас реже, чем раньше, интересует операторов. Видимо, правила формирования эргономичных интерфейсов уже отработаны.

Второе направление — это Интернет вещей. IoT включает самые разные сегменты, требующие разного уровня защиты, и разработчики СУД надеются, что их компетенции окажутся востребованными в данной индустрии. Это для них очень важное направление, так как в отличие от вещательного рынка, сферу IoT никак нельзя назвать стагнирующей. В какой мере они впишутся в новую отрасль, во многом зависит от того, каким образом туда впишутся их партнеры — производители чипсетов и поставщики облачных серверов. Компания Irdeto уже нашла свое место в сегменте защиты автомобилей. Verimatrix и Nagra на прошлогодней выставке IBC еще не раскрывали своих переговоров, но готовились к вступлению на этот рынок. Их оптимизм основан на том, что сфера IoT очень широка и там должно найтись место всем. ■

массово переходят на DVB, и это решение адресовано тем, кто не готов нести значительные расходы на покупку и поддержку собственной системы условного доступа. Сервисная модель оплаты за использование CAS исключает большие первоначальные инвестиции. В дальнейшем, по мере роста доходов от бизнеса, оператор может приобрести собственную систему условного доступа без замены абонентского оборудования. В качестве приемных устройств мы предлагаем и CAM-модули, которые пользуются в России особенным спросом, и приставки. Сама система установлена в дата-центре и управляется нашими российскими партнерами, а оператор управляет своими абонентами через Интернет, используя портал.

Но оператор, видимо, должен иметь собственный скремблер?

Обычно на головных станциях скремблер есть, но если его нет, то оператор может получать от наших партнеров уже скремблированный контент. Все зависит от конкретной конфигурации. Уже появился первый клиент этой услуги — «Телеком МПК», кабельный оператор из Дубны.

Большинство разработчиков традиционных систем условного доступа до последнего времени позиционировали свои бескарточные решения как не предназначенные для крупных сетей, тем более с премиальным контентом. Irdeto уже давно позиционирует свое решение как равноценное карточным по уровню безопасности. Какие технологии позволили компании добиться паритета?

Сейчас это обеспечивается решением FlexiCore, которое компания запустила в 2015 году.

Это какое-то криптографическое ПО, эмулирующее защищенную область в открытой области чипсета?

В целом да, но чипсет должен соответствовать определенным требованиям. Это встроенный в чипсет процессор безопасности, который может быть аппаратно выполнен в виде отдельного процессора или быть виртуальным, деля ресурсы основного.

Можно ли его изменять дистанционно или меняется только надстройка, накладываемая на эмулируемую область?

Сам процессор прошивается на заводе, поменять его дистанционно нельзя, но он позволяет изменять все, что стоит над ним, и увеличивает гибкость и надежность решения.

В связи с распространением пиратских ретрансляций усилился интерес к водяным знакам. Какие категории клиентов Irdeto заказывают наложение водяных знаков?

Чаще всего — голливудские студии. Они накладывают водяные знаки на копии фильмов, передаваемые операторам платного ТВ. Это позволяет им отдавать свой контент для показа в ранних окнах, в которых как раз и формируется основной доход от телепоказов. Иногда наложение водяных знаков заказывают телеком-операторы или спортивные лиги — наше решение допускает быструю расшифровку, поэтому годится для защиты спортивных трансляций в режиме реального времени.

Есть ли у Irdeto еще какие-то решения, разработанные в ответ на появление UHD?

Мы видим спрос на прием видеоформата 4K на платформе Android. Эта платформа дает оператору готовое решение с множеством сервисов, ему остается лишь сделать свои приложения для приемников. К тому же интерфейс Android знаком и привычен пользователям. Поэтому Irdeto серьезно работает над интеграцией клиента безопасности в новые Android-чипсеты с поддержкой 4K.

Однако у лицензируемой версии Android есть и недостатки. Нельзя ограничить пользование библиотекой, абонент может установить любое приложение, в том числе пиратское или от конкурентов. Возможности защиты чипсета тоже ограничены — в сертифицированные чипсеты Android не допускается внедрение собственных кодов от разработчика системы безопасности.

Да, ограничения есть и устраивают они не всех, но есть определенные категории операторов, для которых такая модель приемлема. В первую очередь, она нравится сотовым операторам, которые строят свои телевизионные платформы.

Какие еще перспективные направления работы для компании вы видите?

У нас появилось новое подразделение для работы в автомобильной индустрии. Сейчас на автомобилях как минимум реализуется дистанционное информирование о местоположении и состоянии его датчиков. А дистанционное вмешательство в работу современных беспилотников может быть опасно для жизни пассажиров. Поэтому ожидаем расширения этого сектора нашей работы. ■