

StreamGuard — система условного доступа от Sumavision

В прошлых номерах журнала мы познакомили читателей с головным оборудованием для обработки цифровых ТВ-сигналов от компании Sumavision и, в первую очередь, с компактной головной станцией EMR. В этом материале мы рассмотрим другое решение от Sumavision — систему условного доступа StreamGuard.

В России StreamGuard до недавнего времени представлена не была и потому пока малоизвестна. Но в Китае она используется достаточно давно и, более того, последние годы держит устойчивое первенство по количеству обслуживаемых абонентов. Применяется в крупных кабельных сетях Китая, покрывающих целые провинции. Ею, в частности, закрыта сеть провинции Дзянси, покрывающая 14 городов с 3 млн подписчиков, а также сеть Внутренней Монголии, охватывающая 12 городов с тем же количеством подписчиков. Отметим, что в расчет берутся именно «цифровые» абоненты, который в этих сетях подавляющее большинство.

Система также получила распространение в региональных сетях мобильного телевидения, в частности, в крупнейшей региональной сети, развернутой в провинции Хунань. Эта сеть охватывает трехмиллионный административный центр и 14 более мелких городов. Популярность StreamGuard у операторов мобильного ТВ связана с тем, что она допускает оплату за определенное время просмотра — одну из наиболее актуальных для мобильного просмотра. К тому же она характеризуется низкой загрузкой транспортного канала служебными сообщениями.

Такие масштабы внедрения, возможно, являются лучшим подтверждением надежности, масштабируемости и высокой функциональности системы, возможности которой мы рассмотрим в этом материале.

Общая информация

StreamGuard — система, полностью соответствующая стандарту DVBSimulcrypt v.3 Open CAS. Поддержка DVBSimulcrypt имеет следующие практические следствия. Во-первых, система может работать не только со скремблерами и мультиплексорами производства Sumavision, но и с любым другим оборудованием, поддерживающим Simulcrypt. Во-вторых, она никак не связа-

на на алгоритм скремблирования, то есть может работать не только с CSA (3 DES), традиционным для DVB-сетей, но также и с более современными алгоритмами AES и RSA, равно как и с любыми другими, которые появятся в будущем. Эта возможность актуальна для IPTV-сетей, в которых обычно используются алгоритмы, отличные от CSA.

Кроме того, соответствие Simulcrypt допускает наложение на один поток нескольких вариантов условного доступа. Условия доступа могут формироваться как в рамках одной СУД, так и разными СУД. Эта особенность Simulcrypt'a допускает, в частности, сосуществование нескольких операторов в одной сети распространения. Каждый из них накладывает на поток свои условия доступа для его доставки своим абонентам. Но в России мультиоператорские сети пока не распространены, поэтому у нас эта возможность более актуальна для операторов, имеющих несколько периферийных сетей, в которых они хотят проводить различную тарифную политику. Simulcrypt-совместимая система позволяет сформировать для этих сетей единые физические ТВ-пакеты, но коммерчески предоставлять их на разных условиях. StreamGuard допускает наложение на каждый поток до 32 разных вариантов условий доступа.

Головная часть системы включает три сервера:

- Сервер шифрования (Encryption Server). Работает на базе ОС Windows 2003 Server и выполняет шифровку всех служебных данных, передаваемых абонентским устройствам.
- Сервер приложений (Application Server), на который устанавливаются различные служебные приложения, в частности, генераторы сообщений ECM и EMM, а также реализованы интерфейсы СУД с другими элементами ГС.
- Сервер с абонентской базой данных (Database Server) хранит информацию об абонентах и условиях их подписки. Реали-

зован на базе системы управления Oracle 11g. База данных может работать совместно с SMS от Sumavision ToView либо с системой другого производителя.

Система ToView, предлагаемая Sumavision совместно с CAS, обладает широким спектром возможностей. Она позволяет работать с информацией об абонентах — их лицевых счетах, условиях подписки, возможных скидках и кредитовании. Кроме того, она предоставляет развернутую систему складского учета приставок и карт, позволяет составлять аналитические отчеты о результатах сбыта за прошедшие периоды и формировать прогнозы доходов на будущее.

Эти программные серверы устанавливаются на специализированных аппаратных серверах, выполненных на базе IBM. В небольших сетях все три сервера можно реализовать на одном аппаратном сервере, а в более крупных рекомендуется использовать три отдельных. Вернее, шесть — для реализации горячего резервирования.

В состав StreamGuard входит также система дистанционного управления NetManager, ПО для программирования смарт-карт и несколько вспомогательных приложений.

В следующих трех разделах мы рассмотрим систему с точки зрения ее защищенности, масштабируемости и функциональности. Сразу скажем, что эти три аспекта взаимосвязаны, поэтому деление будет довольно условным.

Защищенность

На ранних этапах защищенность системы оценивали в первую очередь по изоциренности ее криптоалгоритмов. На сегодняшний день прямой взлом этих алгоритмов — задача практически нереальная для сколько-нибудь серьезной системы. Вернее, практически нереально окупить траты на такой взлом, так как СУД поддерживают еще и комплекс контрмер, препятствующих коммерческому взлому системы.

В современных системах есть две более уязвимые мишени. Одна из них — головные серверы, с которых эти алгоритмы можно просто украсть, а вторая, и самая главная, — абонентское оборудование. В системе StreamGuard безопасности обоим сегментам уделено повышенное внимание.

ПО головных серверов устанавливаются производителем на специализированные серверы типа IBM с защищенным корпусом и замком сейфового типа. А безопасность системы на абонентской стороне в сильной мере определяется защищенностью смарт-карты и заложенными в нее функциями безопасности.

В StreamGuard используются карты известного мирового производителя IC, соответствующие максимальному из применяемых для смарт-карт уровню аппаратной защищенности AEL 5+. Аппаратные схемы защиты препятствуют типовым действиям, предпринимаемым хакерами для получения доступа к алгоритмам. Кроме того, карты поддерживают два механизма предотвращения шаринга, который сегодня является основной формой пиратства в крупных сетях. Первый заключается в привязке карты к MAC-адресу процессора приставки, так называемом паринге карты и приставки. Второй предусматривает шифровку диалога между картой и процессором асимметричными алгоритмами, причем формирование ключей завязано на сертификат карты. В результате осуществляется программная привязка карты к приставке. В процессе шифровки контрольное слово оказывается «подписанным» конкретной картой, что позволяет распознать карту, с которой ведется передача слова по шаринговой сети.

Карты также поддерживают ограничения по территории и времени использования.

Для возможности территориальных ограничений в приставки и карты вводятся коды территорий, на которых они работают, и оператор использует эти коды в качестве одного из критериев условного доступа. Временное ограничение заключается в том, что по истечении срока действия карты вся информация с нее стирается. Это исключает возможность применения старых карт для поиска лазейки в более новые.

Для двунаправленных сетей СУД дополнительно предусматривает периодическую отправку сообщений авторизации от карты головному серверу. Эти сообщения содержат цифровую подпись карты и являются еще одним средством контроля за ее легитимным применением. Кроме того, для интерактивных сетей предусмотрены механизмы борьбы с DoS-атаками.

Масштабируемость и надежность системы

Минимальная конфигурация системы StreamGuard рассчитана на 5 тыс. абонентов и пять транспортных потоков. Следующая конфигурация позволяет обслуживать до 200 тыс. абонентов и до 20 транспортных потоков. Для каждой из этих конфигураций возможно ее последующее наращивание с шагом в 5 тыс. абонентов и пять транспортных потоков. Максимальная конфигурация, поддерживаемая до 20 млн абонентов, сегодня в России могла бы быть актуальной только для крупных спутниковых сетей.

Остановимся на свойствах StreamGuard, которые делают ее работу надежной, удобной и пригодной для применения в крупных сетях.

Во-первых, в StreamGuard предусмотрена возможность стопроцентного горячего резервирования. Для этой цели все данные с основных серверов копируются на резервные в реальном масштабе времени. Полный резерв рекомендуется для любых систем.

Во-вторых, СУД имеет двухуровневую систему мониторинга и диагностики ошибок. Верхний уровень контролирует статусные состояния различных приложений, работающих в рамках системы. Он же принимает решение о переключении на резервные серверы. А нижний уровень контролирует все текущие операции сети и поддерживает ряд механизмов самовосстановления системы.

Здесь же следует сказать об особенностях StreamGuard в отношении авторизации. Во-первых, процесс авторизации одного абонента занимает всего 8 секунд, что существенно меньше, чем во многих других аналогичных системах. Во-вторых, StreamGuard поддерживает возможность групповой авторизации, что в случае массового подключения новых карт также резко ускоряет процесс и уменьшает количество служебных сообщений в канале. И, в-третьих, при авторизации в карту сразу заносится срок окончания подписки. Если по каким-либо причинам сигнал на отключение карты, посланный с ГС, до нее не дойдет, то карта отключится в срок самостоятельно.

StreamGuard также допускает возможность распределенной иерархической конфигурации с разнесением функций между центральной и периферийными станциями. На периферийную станцию при такой конфигурации выносятся скремблер и генераторы сообщений ЕСМ и ЕММ, вводящие эти сообщения в транспортный поток. А наиболее дорогие компоненты системы — криптосервер и сервер управления абонентской базой всей сети вместе с системой ее администрирования — остаются на центральной станции.

Обмен данными между центральной и периферийной станциями осуществляется по защищенному VPN-соединению. Причем периферийные станции могут общаться только с центральной, но не между собой.

Открытые ТВ-потоки, поступающие на периферийную станцию, скремблируются, а используемое для этой цели контрольное слово отправляется на центральную станцию для кодирования. Оттуда оно возвращается периферийной станции в форме ЕСМ-сообщения. На центральной станции формируются также и ЕММ-сообщения для абонентов, приписанных к конкретной периферийной станции. Полученные периферийной станцией ЕММ и ЕСМ инкапсулируются в служебные таблицы шифруемых потоков и отправляются в сеть.

Такая схема позволяет оптимально использовать мощность центральной ГС, не очень сильно загружая при этом каналы VPN.

Если основная часть цифровых пакетов формируется на центральной станции, а на периферийной добавляются лишь несколько местных каналов, то общесетевые каналы шифруются на центральной станции, а местные — на периферийной, с применением иерархической схемы. Разумеется, и те, и другие будут открываться единой смарт-картой.

Иерархическая система допускает возможность лизинга ресурсов центральной ГС со стороны небольших операторов, которые не могут позволить себе приобрести полную систему.

Функциональные возможности системы

В этом разделе мы рассмотрим все функции StreamGuard, позволяющие оператору гибко выбирать бизнес-схемы введения цифрового ТВ и обогащать его различными дополнительными возможностями. Начнем с того, что StreamGuard поддерживает четыре варианта доступа к передаваемым программам:

- OPCC — постоянный доступ на срок договора с предварительной оплатой услуг;
- OPPV — предварительная оплата просмотра определенных программ в течение срока договора. Это в первую очередь актуально для высокорейтинговых передач, например трансляций матчей чемпионата мира по футболу;
- IPPV — оплата по факту просмотра программы. Стоимость программ, доступных для отдельной покупки, указывается оператором в EPG, из которого абонент может выбрать заинтересовавшее его наименование. Как только абонент начинает просмотр, указанная в EPG сумма снимается с его лицевого счета. Заказ на просмотр может быть оставлен на сайте оператора, отправлен в виде SMS-сообщения, а при наличии в сети обратного канала и подклю-

чения к нему абонентской приставки может быть отправлен прямо с пульта STB.

- IPRT — повременная плата. При этой схеме сумма, снимаемая с лицевого счета абонента, определяются фактическим временем просмотра платных программ. Причем оператор может задавать разную стоимость минуты просмотра для разного времени суток.

Система также позволяет управлять записью программы на жесткий диск. Отметка о разрешении заносится в таблицу EIT, а SreamGuard проверяет отметку и разрешает запись на жесткий диск в случае ее наличия. Это дает оператору возможность более дифференцированной тарификации.

СУД также поддерживает функцию мультипросмотра. Абоненту, имеющему дома несколько приставок или телевизоров с цифровым тюнером, дополнительно к основной карте может быть предоставлено несколько дочерних, продаваемых по льготным тарифам. Дочерние карты программно привязываются к основной и периодически получают от нее авторизацию. Это позволяет избежать злоупотреблений льготными картами. Периодичность авторизации задается оператором.

SreamGuard поддерживает множество вариантов адресации служебных сообщений. Во-первых, адресаты могут выбираться по одному из 40 признаков, таких как номер смарт-карты, код региона, просматриваемая в данный момент программа и другие. В смарт-картах SreamGuard под хранение возможных условий адресации зарезервировано 800 бит.

Система также имеет широкоэвещательный режим, предназначенный для передачи чрезвычайных сообщений. В этом режиме можно принудительным образом включить все приставки, настроив их на определенный канал. Кроме того, она поддерживает условное вещание, позволяющее при заданных условиях запрещать картам принимать определенные программы, даже если они были оплачены. Условия и программы определяются оператором. В системе также предусмотрена возможность возрастного контроля доступа к программам. Оператор вводит в таблицу EIT отметки о возрастном цензе каждой программы, а абоненты самостоятельно задают возрастной уровень для своих карт. В результате карты открывают только программы, соответствующие установленному или более низкому уровню. А доступ к функциям заказа и оплаты услуг закрыт PIN-кодом.

SreamGuard поддерживает два режима отправки текстовых сообщений от оператора к абоненту. В первом режиме, получившим название OSD, сообщение выводится в нижней части экрана и сохраняется там на время, заданное оператором. Кроме того он может запрограммировать определенное

количество повторов сообщения. Но после выполнения программы вывода сообщение стирается из памяти приставки.

Во втором режиме, TV mail, сообщение сохраняется в памяти до тех пор, пока подписчик не удалит его сам. При поступлении такого сообщения на экране появляется надпись New Email, приглашающая абонента оторвать и прочитать сообщение. В интерактивных сетях добавляется поддержка видео по требованию; возможно как предварительное шифрование контента для хранения его на сервере в закрытом виде, так и шифрование в реальном времени.

Для двунаправленных сетей в системе имеются инструменты для сбора информации о просмотрах и формирования рейтингов на базе этой статистики.

Абонентские приставки

Важнейшим критерием выбора системы доступа является ассортимент абонентских приемников с ее поддержкой. Ввиду широкой распространенности SreamGuard в Китае, приемники с встроенной СУД выпускают более 35 местных производителей. Компания «Сатпро» предлагает несколько русифицированных моделей под своей маркой. Они заказываются у производителя, рекомендованного Sumavision. Линейка включает базовый приемник SD MPEG-2, приемники среднего класса SD MPEG-2 на базе современного процессора STI 520 и верхнюю модель с поддержкой ТВЧ и H.264, оснащенную самыми разнообразными интерфейсами. В принципе, набор интерфейсов во всех моделях определяется заказчиком. Приемники любого класса можно заказывать с портами Ethernet (RG-45) и USB. Первый предназначен для подключения приемника к параллельной сети передачи данных, а второй — для подключения внешнего жесткого диска.

Все возможности CAS, такие как заказ IPPV-просмотра, поиск программ NVoD, получение информации по балансу счета и кредиту, управление письмами TV Mail, составление списка заданий для видеозаписи, также заложены в меню всех приемников. Но оператор имеет возможность оставить видимыми только те опции, которые реализованы в его сети.

В данный момент русифицированные приемники поставляют только компания «Сатпро», но из-за обилия альтернативных предложений на китайском рынке опасаться появления поставщика-монополиста в данном случае не стоит. К тому же для SreamGuard выпускаются и внешние CAM-модули производства компании SMiT. Предлагаются бытовой и профессиональный варианты, последний открывает до 24 PID'ов. Это позволяет использовать для приема закрытых SreamGuard каналов цифровые телевизоры и широкий спектр приемников с CI-интерфейсом.

Следующие важные факторы оценки системы — степень ее подготовленности для местного рынка и уровень сервисной поддержки.

Цены и послепродажная поддержка

В минимальной комплектации оператор должен приобрести один специализированный сервер стоимостью 11,5 тыс. долларов. На него устанавливаются все программные серверы для базового варианта СУД, обслуживающего до 5 тыс. абонентов. Этот базовый вариант обойдется еще в 7000 долларов. Он уже включает все функции CAS, ни одна из них не требует дополнительных лицензий. Смарт-карты IC со всем заложенным в них функционалом обойдутся оператору по 7,5 долларов на штуку. Никаких ежегодных выплат за пользование системой не предусмотрено.

Стартовые выплаты за SreamGuard несколько выше, чем в самых бюджетных вариантах Simulcrypt-совместимых систем. Это в первую очередь обусловлено немалой стоимостью защищенного сервера, который должен быть подготовлен производителем и доставлен из Китая. Но это неизбежная плата за отсутствие слабых звеньев в цепи передачи шифрованного сигнала от ГС до абонента. С другой стороны, стоимость SreamGuard значительно ниже, чем у систем схожего со SreamGuard класса по уровню функциональности, защищенности и масштабируемости. А отсутствие ежегодных выплат и лицензий на дополнительные функции делают систему еще более привлекательным объектом для инвестиций.

Инсталляция системы выполняется бесплатно, надо оплатить только проезд и проживание инсталляторов. Возможно двухнедельное обучение двух сотрудников оператора в Пекине и трехдневное обучение еще двух сотрудников дистанционным образом. Последующая поддержка может проводиться с выездом на место или по Интернету. Дистанционная помощь при неисправностях предоставляется круглосуточно. В некоторых случаях специалисты компании дистанционно подключаются к системе и устраняют проблему самостоятельно. Для разрешения особо сложных проблем в Sumavision применяется метод их моделирования на собственном оборудовании в Пекине. При инсталляции комплексных решений от Sumavision обеспечивается совместная поддержка для СУД и цифровой головной станции. Вся послепродажная поддержка оказывается сотрудниками Sumavision на английском языке.

Что же касается самой системы, то она полностью русифицирована и сейчас находится в процессе сертификации по системе CCC.

Информация предоставлена компанией «Сатпро»