СПАЙДЕР–FMS

Система обнаружения мошенничества на сетях связи

Многие виды мошенничества основаны на «обмане» станционных средств, формирующих записи CDR, чтобы информация о произведенных вызовах регистрировалась некорректно или вовсе не регистрировалась.

Системы борьбы с мошенничеством, в основе которых лежит прин-цип обработки CDR, полученных от сетевых элементов, не способны обнаружить такие виды мошенничества, так как сетевое оборудование обычно регистрирует только те события, которые существенны для начисления платы.

Система **СПАЙДЕР-FMS**, работающая по принципу формирования CDR из межстанционных сообщений значительно эффективнее, так как фиксирует 100% сетевых событий.

Мошенничество или фрод в телекоммуникациях - это любая активность злоумышленника, направленная на извлечение прибыли путем использования уязвимостей в процессах предоставления или оплаты услуг сети связи.

В условиях высокой насыщенности рынка телекоммуникационных услуг эффективные инструменты, позволяющие снизить потери прибыли и предотвратить несанкционированное использование ресурсов, дают компании значительные конкурентные преимущества.

Основными задачами **СПАЙДЕР-FMS** являются:

- автоматический поиск и обнаружение различных типов мошенничества,
- пресечение новых попыток нелегального доступа лиц, однажды уличенных в мошенничестве,
- предоставление полной информации по источникам, типам и числу попыток совершения мошенничества в сети оператора.

Для решения этих задач система постоянно следит за ситуацией в сети, в режиме реального времени выявляет факты отклонения от нормы и информирует оператора о наличии таких фактов.

При работе в режиме реального времени в качестве основного источника информации для **СПАЙДЕР-FMS** используются данные, полученные пробниками системы мониторинга СПАЙДЕР по интерфейсам E1, STM1, Ethernet. Поддерживаются все цифровые протоколы сигнализации, которые применяются в сетях TDM, NGN, IMS, GSM/GPRS, CDMA.

При работе в режиме постпроцессинга в качестве входных данных могут использоваться записи о вызовах, получаемые:

- по интерфейсам от коммутационного оборудования,
- в виде файлов, собранных для биллинг-центра (системы Mediation),
- от других информационных систем (NRTRDE, TAP).

СПАЙДЕР-FMS собирает статистику о видах переносимого трафика по различным маршрутам, формируя информацию для системного аналитика. Встроенные в систему алгоритмы обработки собранных xDR (нейронные сети, графы решений, индуктивные и регрессионные методы и др.) способны с высокой вероятностью обнаруживать попытки краж и мошенничества, как в реальном времени, так и в режиме постобработки.

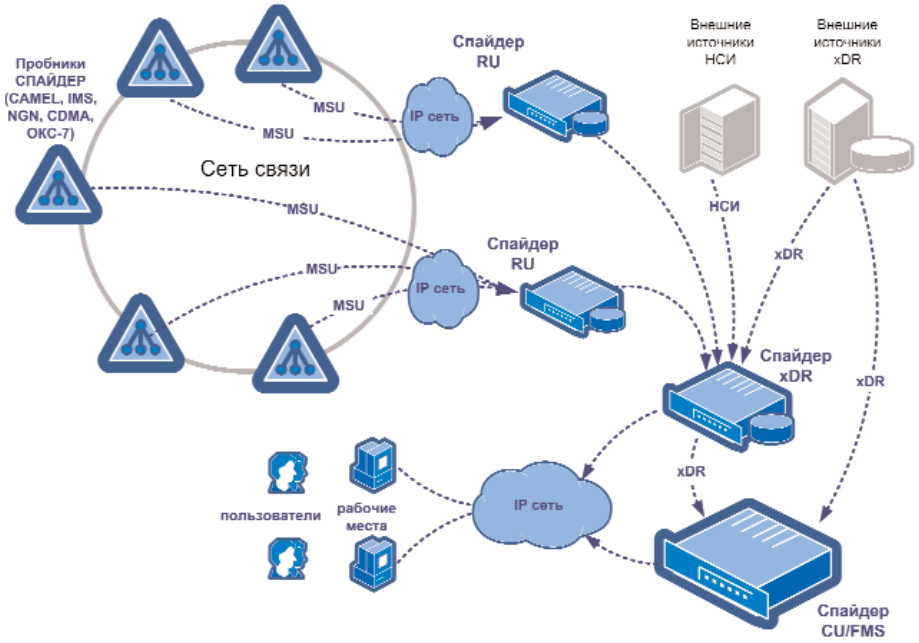
Архитектура системы СПАЙДЕР FMS

Входными данными для системы являются детализированные записи об оказанных услугах (xDR).

Данные могут поступать из таких источников, как:

- подсистема **СПАЙДЕР-xDR**, формирующая записи на основе анализа сигнальной информации, поступающей от пробников системы мониторинга,
- внешние источники (например, коммутационное оборудование, системы сопряжения, предбиллинга, NRTRDE, TAP и т.д.).

В качестве дополнительных параметров, использующихся для создания фрод-критериев выступают данные об абонентах (профиль, регион регистрации, баланс и др.) а также другие источники нормативно-справочной информации (НСИ). Для их получения необходима интеграция АПК с системой биллинга и внешними справочниками.

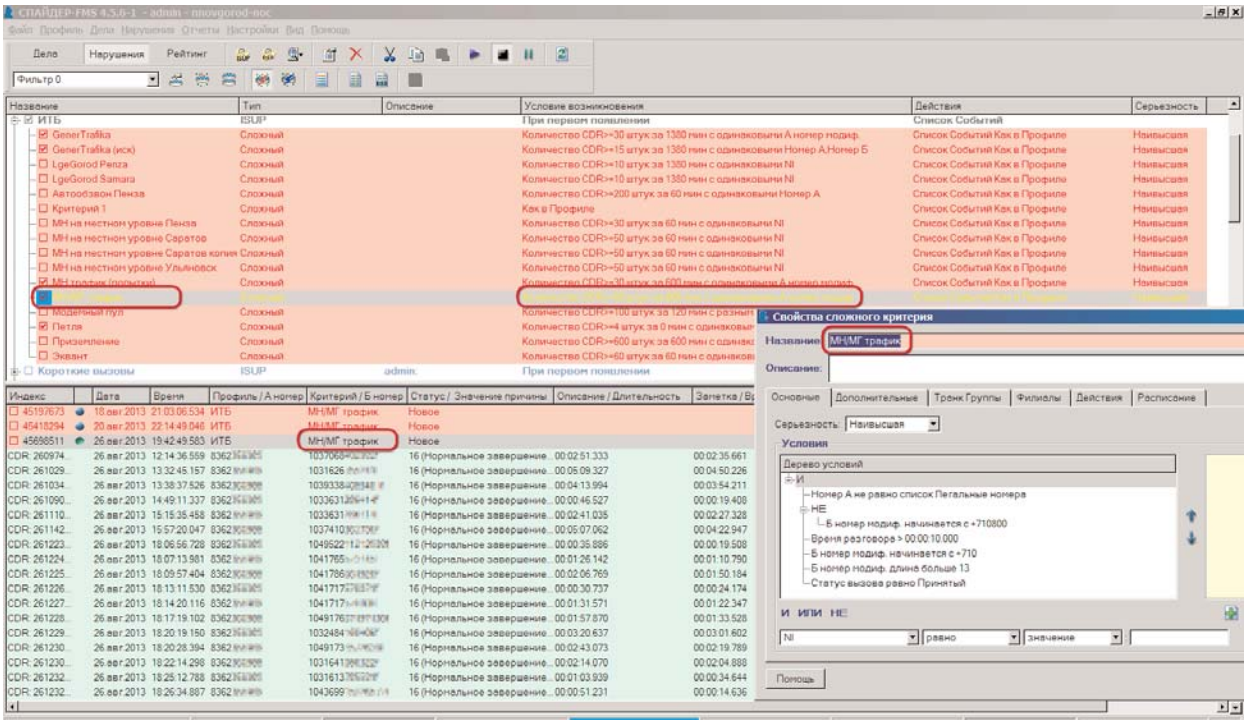


Преимущества использования пробников **СПАЙДЕР**:

- Работа системы в режиме Real Time. Задержки от момента прохождения вызова по сети и его анализом минимальны.
- Полнота данных. В CDR записи, формируемой пробом **СПАЙДЕР**, содержится максимально полная информация (более 40 значимых полей, а также исходные MSU), которые могут использоваться как при настройке критериев, так и давать исчерпывающую информацию при анализе трафика.
- Формирование независимого архива CDR и возможность его использования для функций верификации коммутаторов, мониторинга качества работы сети, формировании KPI KQI и др.

Пользователи работают с системой со своих рабочих мест, которые, обычно, организуются на имеющихся ПК под управлением ОС Windows, путем инсталляции специализированного клиентского ПО **СПАЙДЕР**.

Пример настройки фрод-критерия



Основные возможности СПАЙДЕР FMS

Проверяя входные данные на соответствие встроенным профилям поведения абонентов, система **СПАЙДЕР-FMS** выявляет аномалии в активности пользователей и заблаговременно информирует об этом оператора, формируя записи о нарушениях.

Профиль представляет собой набор сложных или простых критериев, позволяющий создавать модель аномального поведения абонента (группы абонентов, пула номеров, и т.п.) во время одного вызова или в течение заданного интервала времени. Разные группы абонентов могут проверяться на соответствие разным профилям, в том числе и нескольким.

Каждый активный профиль должен всегда содержать не менее одного фрод- критерия, так как именно по критериям и происходит отбор xDR и обнаружение нарушений. Пользователь системы **СПАЙДЕР-FMS** может создавать собственные критерии и профили, по которым вызовы или транзакции будут считаться неправомочными. В качестве критериев допускается задавать последовательность цифр номера (префикс, постфикс, и т.д.), длительность отдельных фаз соединения, частоту вызовов, наличие переадресации или занятости вызываемого абонента, и множество иных параметров, которые характеризуют вызовы или транзакции, являющиеся фродом.

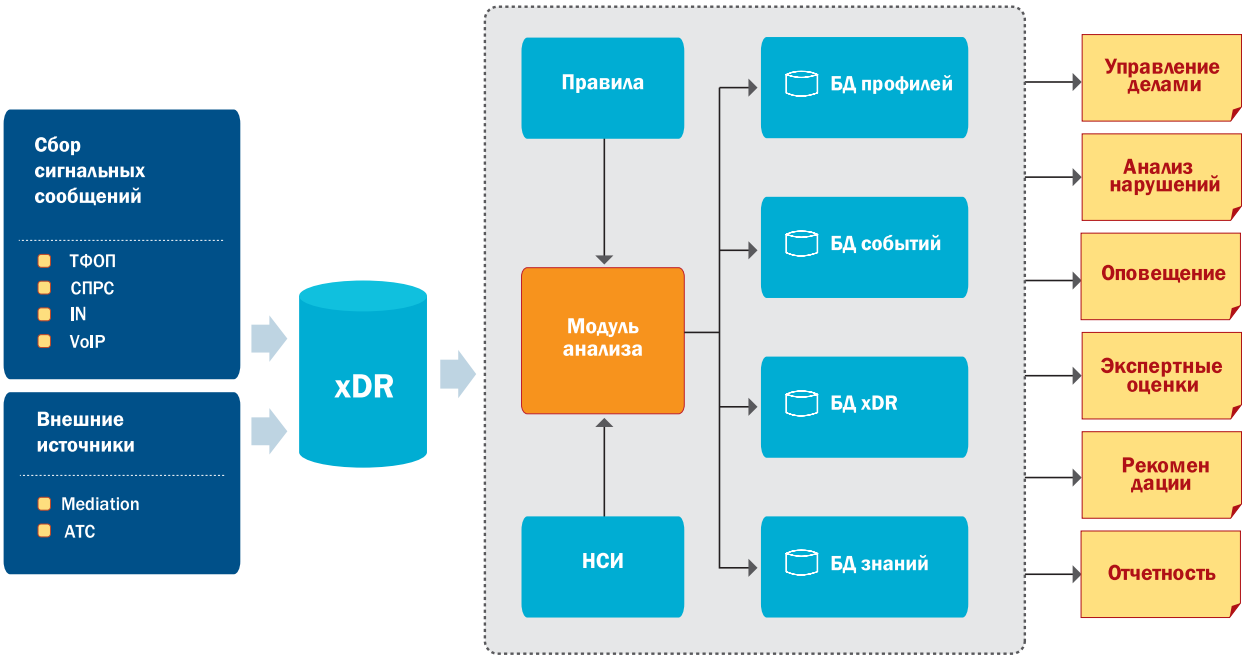
Применение правил анализа номеров A и B для всего объема трафика зачастую осложнено разным форматом представления номеров для вызовов, поступающих в различных точках присоединения. Для решения этой задачи в системе СПАЙДЕР используется модуль канонизации номеров, который позволяет анализировать номера абонентов во входящих xDR-записях и, при необходимости, осуществлять их модификацию (добавление или удаление префиксов, разделителей и т.п.).

Применение общих правил, описывающих нарушения, к большим объемам данных порождает появление большого количества ложных записей о нарушениях. Для минимизации количества ложных нарушений и выделения из их числа наиболее вероятных случаев фрода в системе применяются следующие методы:

- Использование информации из внешних источников данных, которые могут представлять собой независимые информационные системы (Система биллинга, CRM) так и отдельные локальные справочники (например, справочники абонентской информации, черные и белые списки и т.д.)
- Применение технологии CASE-Management, которая заключается в группировке нарушений, имеющих одинаковые значения определенных полей, (например, номер A, или номер B). Нарушения группируются в Дела, в которых отображается количество зафиксированных нарушений, поле группировки и т.д. Данная методика позволяет выделить источники и типы трафика, с наибольшим объемом нарушений. Таким образом, осуществляется приоритезация обработки нарушений, а также анализируется история по источнику трафика. Существует возможность закрепить Дело за любым пользователем, который будет им заниматься.

Система **СПАЙДЕР-FMS** может работать как в режиме online, так и в режиме offline (работа с архивами). В режиме online собираются все нарушения, подходящие под заданные пользователем критерии, с момента их активации. Режим offline позволяет проверить на соответствие критерию архив данных (например, за прошедший месяц).

По факту регистрации записи о выявленном нарушении система может выполнять различные действия, например: отправка e-mail или sms, генерация SNMP и другие действия.



Основные угрозы, выявляемые СПАЙДЕР FMS

Злонамеренная активность, угрожающая бизнесу оператора	
Атаки типа brute-force с перебором паролей	Подбор паролей может осуществиться успешно, если подбираемый пароль недостаточно надежен. В этом случае клиент оператора становится жертвой, которая за короткий период генерирует существенный трафик с потреблением основных услуг, критичных для бизнеса оператора.
Несанкционированный доступ к услугам сети	Если оператор не может обеспечить правильное выполнение процессов по активации услуг или их тарификации, клиенты получают возможность нелегального использования или перепродажи услуг без соответствующей оплаты.
Нежелательные входящие вызовы (SPAM, реклама)	В случае, когда абонент получает слишком много рекламных сообщений, он переходит к другому оператору связи.
Мошенничество в роуминге	Использование услуг сетей подвижной связи в роуминге в кредит с намеренением впоследствии избежать оплаты этих услуг, помимо потерь доходов, приводит к некомпенсированным выплатам роуминг-партнерам.
Нелегальные узлы услуг	Абонент несанкционированно предоставляет какие-либо услуги. Например, перепродает абонентам внешних операторов вызовы на направления повышенной стоимости или какие-либо другие услуги.
Вирусная активность	В случае инфицирования "умных" абонентских терминалов, преимущественно использующихся на сетях с сигнализацией SIP, вредоносное ПО потребляет услуги внешнего провайдера.
PRS вызовы на ТфОП	Вызовы повышенной стоимости, за которые оператор расплачивается с контент-провайдером до получения оплаты со стороны абонента. В случае взлома абонента счет может быть оспорен, что приведет к прямым убыткам оператора.
Взлом абонентов	Взлом корпоративных клиентов оператора, как правило, приводит к тому, что на счету клиента вырастает задолженность, которую абонент отказывается оплачивать, а оператор вынужден ее списывать, чтобы не потерять клиента.
Различные ошибки установления сессий	Ошибки при обмене сигнальной информацией могут служить индикатором потенциальных проблем на стороне клиента: невозможности установления сессии с технической точки зрения и с точки зрения потенциального взлома клиентского терминала.
Взлом УПАТС	Взлом станций корпоративных клиентов позволяет проводить перепродажу услуг, предоставляемых клиентам без их ведома.
Приземление трафика в сеть, операторские шлюзы	Различный ввод трафика в сеть оператора в обход узлов интерконнекта, из-за чего невозможна корректная тарификация подобного трафика
Атаки с переопределением получателя (Man In The Middle)	Выявление системой попыток таких атак предотвращает неправильное списание средств со счета клиента за услуги, которыми данный клиент не пользовался.
Атаки типа DoS/DDoS	
DDoS на сервера регистрации	Блокирует процесс регистрации абонентского терминала, приводит недоступности услуг входящей и исходящей связи для абонента, регистрация которого задерживается.
DDoS на абонентские шлюзы, терминальные устройства	Блокирует работу группы абонентов или конкретного абонента. Как правило, преследует своей целью блокирование бизнес-активности клиентов оператора, что негативно влияет как на бизнес оператора, так и на бизнес клиента.
DDoS атаки на IMS подсистемы	Приводит к потере доступа абонентов к основным или всем услугам сети. Характеризуется тем, что не требует больших технических ресурсов для осуществления. Используется возможность цепных реакций в IMS, потенциально приводящих к отказу основных подсистем при атаке со стороны даже небольшого числа устройств.

тел/факс: +7 (812) 333 36 37
e-mail: sales@seventest.ru
http://www.seventest.ru