ООО «ИКС ЛАБЗ»
г. Москва, вн.тер.г. муниципальный округ Тверской,
ул. Новослободская, д. 24а, стр. 2, кв. 26

ОГРН 1237700394480
ИНН/КПП 9707001238/770701001

Тел. +7 (499) 709-39-95, email: info@x-labs.ru

XL Fraud

Описание решения

Версия 1

11.10.2023

1.XL Fraud – система выявления мошенничества в реальном времени

1.1.Ключевые функции

Узел XL Fraud обеспечивает обработку запросов, полученных по протоколам INAP или CAMEL с помощью SIGTRAN, либо с помощью SIP для сетей VoIP. Система анализирует каждый вызов перед установлением соединения, определяя необходимость его специальной обработки в случае совпадения с установленными сценариями мошенничества.

Помимо стандартных параметров INAP/CAMEL, для корректной обработки и предотвращения межоператорского фрода Системе, также требуется информация о присоединенном операторе, от которого получен вызов. Входящий оператор определяется с помощью служебного ключа, который должен однозначно определять либо конкретного оператора, либо конкретную транк-группу, принадлежащую оператору, в случае если для различных транк-групп применяются различные сценарии. Такой ключ также должен определять оператора и уровень присоединения оператора, от которого получен вызов.

1.2.Сценарии работы

1.2.1.Активный мониторинг

Система предотвращения мошенничества в режиме реального времени использует онлайн-интерфейс для активного отслеживания мошеннических вызовов и управления ими. На этапе установления соединения модуль контролирует доступные параметры сессии TDM (с использованием INAP/CAMEL) еще до установления связи. В случае обнаружения шаблона, ранее отмеченного в качестве фрода, система предлагает следующие возможности:

- Отклонение вызова;
- переадресация вызовов на специальную ветку маршрута или продукт (обычно в группу операторов более низкого качества, IVR и т.д.).

1.2.2.Создание сценариев

Логика выявления фрода основана на использовании сценариев. Каждый сценарий определяется с помощью одного или нескольких фильтров, которые применяются к каждому вызову, и в случае, если вызов удовлетворяет всем установленным фильтрам, выполняется соответствующее действие, определенное для данного сценария.

Весь анализ основывается на информации, которая получена из сообщений сигнализации CAMEL/INAP IDP и обычно включает следующие параметры:

- »Service key« (Оператор).
- Транк-группа и уровень присоединения (опционально – если служебный ключ определен на этом уровне).
- Вызывающий номер и дополнительный вызывающий номер.
- Вызываемый номер.
- Номер перенаправления.
- Тип адреса для вызывающего номера.

- Тип адреса для вызываемого номера.
- Тип адреса для перенаправляющего номера.
- Индикаторы вызова.
- »IMSI« (Идентификация мобильного абонента).
- »Bearer service« (Тип базовой услуги - голос, ...)
- Прочие параметры вызова, получаемые из сигнализации на этапе анализа.

Указанные параметры впоследствии обрабатываются с помощью фильтров, при этом доступны следующие возможности:

Проверка на соответствие шаблону номера

Сценарий позволяет проверить комбинации масок номеров A и B с помощью редактора шаблонов. Проверка может включать следующие параметры:

- Префиксы или части номеров.
- Длину номера.
- Отсутствие номера.
- Соответствие префиксов вызывающего и вызываемого номеров.

Проверка нумерации

Система включает в себя функцию привязки внутреннего оператора к одному или более операторам, определенным регулятором или во внутренней базе данных нумерации.

Проверка нумерации позволяет убедиться, что номер принадлежит именно тому оператору, который осуществляет вызов, либо, в более широком смысле – что данный номер в принципе присвоен и не является несуществующим или некорректным.

Проверка типа адреса

Среди прочих параметров Система также получает информацию о типе адреса для вызывающих, вызываемых или перенаправляющих номеров. Эти значения могут использоваться в конфигурации фильтров для специальной обработки номеров в зависимости от значений этого атрибута.

Проверка на присутствие в черном или белом списке

Административный Узел позволяет поддерживать несколько черных списков, которые определяются либо по критерию вхождения в список (черный список), либо по критерию не вхождения в список (белый список).

Черные списки могут использоваться в фильтрах при конфигурировании сценариев.

Прочие индикаторы вызовов

Система позволяет использовать дополнительные индикаторы, такие как индикатор переадресации вызова, при конфигурировании фильтров.

1.2.3.Функции активных проверок

В определенных случаях фрода для принятия решения о разрешении или блокировке вызова может понадобиться проверка дополнительной абонентской информации.

В рамках функционала системы предлагаются следующие типы проверок:

Интеграция с независимыми поставщиками
Система позволяет интегрироваться с независимыми поставщиками т.н. активной прозвонки на уровне окс-7 (триггерования вызовов) с целью сделать прозвонку незаметной для мошенников и позволить получить повышенную эффективность.

Проверка HLR

Выполнение операции SS7 MAP ATI или SRI4SM для вызывающего абонента позволяет анализировать последний зарегистрированный VLR и затем определить, находится ли абонент в настоящее время в домашней сети или в роуминге.

Callback (обратный вызов)

Вызов вызывающего абонента на этапе установления вызова, с целью определения, занят ли номер. В этом случае требуется обеспечить дополнительную транк-группу SIP для каждого сервера XL Fraud.

Временное подключение к IVR

Эта функция позволяет подключить вызов к ресурсу IVR до его подключения к вызываемому абоненту.

Проверка state-сервера
Данная функция позволяет в режиме реального времени проверять текущее состояние вызывающего или вызываемого абонента в агрегированных данных, либо в сторонних системах.

Для использования функций активных проверок необходимо сконфигурировать соответствующие права для XL Fraud в сигнальной сети, либо выделить дополнительные ресурсы. При использовании активных проверок продолжительность установления соединения увеличивается на время, необходимое для выполнения соответствующих операций. С учетом этого, данная функциональность должна использоваться только для потенциально проблемных вызовов. Однако в некоторых случаях данные функции представляют собой единственный способ выявления фрода и, таким образом, являются очень эффективными.

Детальный и точный список активных проверок определен и разрабатывается на этапе внедрения системы.

1.2.4.Действия, определяемые в сценариях

Если вызов не соответствует ни одному из определенных сценариев, в процесс установления соединения не вносится никаких изменений.

В рамках каждого сценария доступны следующие действия:

- Продолжить вызов без изменений.
- Перенаправить вызов на специальный префикс (вызываемый номер дополняется специальным префиксом).
- Завершить вызов с определенным кодом завершения.
- Завершить вызов со случайным кодом завершения из списка.
- Вызов устанавливается, но его максимальная длительность ограничивается.

- Вызов устанавливается, но значение его максимальной длительности ограничивается случайным образом.

Все указанные действия могут быть применены ко всем вызовам или к определенному проценту вызовов. В последнем случае определенный процент вызовов в случайном порядке обрабатывается в соответствии с определенным в сценарии действием, а к остальным никакие действия не применяются.

1.2.5. Типовые сценарии

Пользователь может создать множество различных сценариев. Примеры типовых сценариев перечислены ниже:

- "Серая" терминация входящих вызовов:
  - Международный трафик направляется по маршрутам, где разрешен только внутренний межоператорский трафик.
  - Международный трафик маскируется под внутренний и направляется по маршрутам, где разрешен только внутренний межоператорский трафик.
  - Вызовы с отсутствующим или некорректным вызывающим номером.
  - Вызовы с номеров, включенных в тот или иной заблокированный интервал.
- Вызовы, при которых вызывающий или вызываемый номер находятся в черных списках.
- Исходящие вызовы на дорогие направления:
  - Схема обратных вызовов ("wangiri").
  - Взломанный PBX.
- Маршрутизация фрода абонентов, находящихся во внутреннем роуминге:

  Фрод, потенциально создаваемый абонентом, находящимся во внутреннем роуминге, выявляется с помощью механизма XL Fraud, для этого необходима возможность передачи в XL Fraud соответствующих триггеров, относящихся к вызовам таких абонентов.

  Вызовы, покидающие сеть, должны в любом случае направляться в XL Fraud с использованием имеющейся конфигурации триггеров, однако для вызовов, терминируемых в мобильной сети , возможны следующие варианты:
  - Создание триггеров NCSI с помощью фильтра, устанавливаемого для вызывающего номера (нумерация не соответствует международному префиксу РФ).
  - Создание прокси для триггеров роуминга OCSI CAMEL (если большинство абонентов используют роуминг CAMEL).

Детальный и точный список типовых сценариев, а также типов маршрутизации вызовов через XL Fraud определяется и разрабатывается на этапе внедрения Системы.

1.2.6. Модуль управления

Модуль управления является веб-приложением, которое с одной стороны позволяет управлять правилами предотвращения фрода (включая в себя подготовку и запуск сценариев с соответствующими фильтрами и действиями), а с другой – осуществлять полное управление операторами и списками номеров (обеспечивая, таким образом, необходимые входящие данные для управления правилами и сценариями фрода).

Модуль также обеспечивает возможность наблюдения за работой Системы, включая отслеживание состояния системы, мониторинг работы серверов и активные сценарии за последние 20 минут. Это помогает пользователю следить за поведением Системы, контролировать новые сценарии и выявлять потенциальные проблемы до того, как данные попадут в отчетность для детального анализа.

Права пользователя могут включать в себя либо только возможность мониторинга (доступ "только для чтения"), либо предоставлять доступ к функциям редактирования правил или их активации.

Детальный и точный список распределения прав пользователей будет определен и разработан Поставщиком и согласован Покупателем на этапе проектирования Системы.

1.2.7.Отчетность и витрины данных

Модуль отчетности предоставляет возможность создания специальных отчетов по данным, полученным с серверов реального времени. Данные собираются и обрабатываются в режиме близком к реальному времени (обычно с задержкой в 15 минут) для возможности получения актуальной информации, на основании которой можно принять обоснованное решение, уже через несколько минут после возникновения специфических событий.

В дополнение к специальным отчетам система позволяет создавать витрины данных, где можно просматривать набор отчетов.

Пользователь также может устанавливать пороговые значения для отчетов. В случае превышения установленных порогов система может периодически рассылать по электронной почте оповещения пользователям или группам пользователей.

Отчеты и витрины данных можно сделать общими, то есть, сделать их доступными для других пользователей.

Детальный и точный список стандартных предустановленных отчетов определяется и разрабатывается на этапе внедрения.