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. +7 985 923-09-90, email: info@x-labs.ru

XLSIG-SMS

Техническое описание

Версия 1

05.11.2024

Оглавление

1. Общая информация

1.1. Описание системы XLSIG-SMS

XLSIG-SMS представляет собой платформу для активной интеграции с сетевыми элементами сети оператора связи и обработки сетевых событий для сервиса передачи коротких сообщений (SMS).

XLSIG-SMS защищает сеть оператора от различных мошеннических схем с использованием SMS-сообщений:

- обеспечивает полную защиту и контроль над всеми потоками данных сервиса передачи коротких сообщений;
- автоматически обнаруживает и блокирует спам во входящем трафике;
- оценивает и дополнительно фильтрует входящий трафик сообщений в режиме реального времени для последующей блокировки мошеннических сообщений P2P и A2P;
- выполняет построение аналитических профилей трафика для выявления моделей мошеннического поведения, с последующим созданием правил обработки сценариев мошенничества с помощью SMS;
- использует сетевые интерфейсы реального времени для просмотра, обнаружения и управления SMS-сообщениями.

Функциональные возможности:

- Интеграция с сетевыми элементами сети сервиса передачи коротких сообщений в сети оператора связи с использованием различных протоколов: MAP, SMPP, CAMEL, HTTP;
- Обработка (пропуск, блокировка, маршрутизация) поступающих событий от сетевых элементов в режиме реального времени с использованием заданных правил обработки;
- Обработка передаваемых коротких сообщений пользователей в зависимости от заданных правил;
- Выполнение активных запросов к сетевым элементам в сети оператора для обогащения сетевых событий дополнительной информацией.

XLSIG-SMS выполняет проверку и обработку поступающих SMS с помощью встроенного механизма rule engine, который позволяет создать для каждого типа SMS свою логику обработки, с помощью библиотеки правил. Обработка SMS осуществляется на основе параметров SMS и также на основе результатов активных запросов к внешним системам (HRL, листы нумерации и т.д.).

1.2. Предназначение системы

XLSIG-SMS – это решение для обеспечения защиты абонентов и сетей мобильной связи от мошеннического SMS-трафика, исходящего от SMPP-приложений, других сетей через интерфейсы SS7 и т.д. Данное решение для операторов позволяет монетизировать A2P SMS-трафик, бороться с SMS-мошенничеством и спамом.

Решение разработано в соответствии с документами:

- GSMA IR.70 – SMS SS7 Fraud

- GSMA SG.22 – SMS Firewall Best Practices and Policies
- 3GPP TR 23.840 – Study into routing of MT-SMs via the HPLMN
- GSMA FS.50

Определяемые виды мошенничества:

- Spamming Case
- Faking Case
- Spoofing Case
- Flooding Case
- DoS
- GT Scanning
- Open SMS-C case

1.3. Ключевые возможности XLSIG-SMS

Ключевые возможности продукта описаны в таблице ниже.

Таблица 1. Ключевые возможности XLSIG-SMS

Функционал	**Описание**
Контроль контента (Content Screening)	Функции фильтрации контента, такие как повторение похожего контента, поиск ключевых слов, поиск заданных фраз, проверка шаблона UDH (заголовок пользовательских данных), фишинговые атаки, вредоносное ПО и сайты с незаконными/хакерскими URL-адресами. Весь текст сообщения нормализуется, чтобы исправить любые искажения, допущенные спамером, перед обработкой функциями анализа контента (например, pr1ze — prize).
Контроль передаваемого объёма (Volumetric Peak Rate Screening)	Обнаружение больших объемов сообщений, исходящих от одного номера – ключевой индикатор СПАМа или серых A2P SMS.
Анализ сигнатур контента (Signature Analysis Engine)	Используется для определения различных типов сообщений, являющихся «спамом» и «не спамом» (также известно как «ham»). Обнаруживает типичные A2P SMS-сообщения на основе изучения контента. Анализирует все сообщения, проходящие через правила обработки, категоризация контента на «спам», «серые сообщения» и «ham».
Контроль A-номеров (Sender Number Screening)	Обеспечивает блокировку любых подозрительных отправителей на заданный период времени.
Информирование о подозрительной активности (Suspicious Event Notification)	При обнаружении подозрительных событий система незамедлительно информирует администратора и/или назначенного пользователя. В системе имеется методология обновления сигнатур и правил фильтрации в режиме реального времени.

Функционал	Описание
Возможность внедрения как облачной услуги для партнёров (Cloud Deployment Option)	Возможность предоставить облачную услугу для подключённых операторов-партнёров.

1.4. Защита периметра сети оператора

Ниже приведена схема защиты периметра сети оператора.

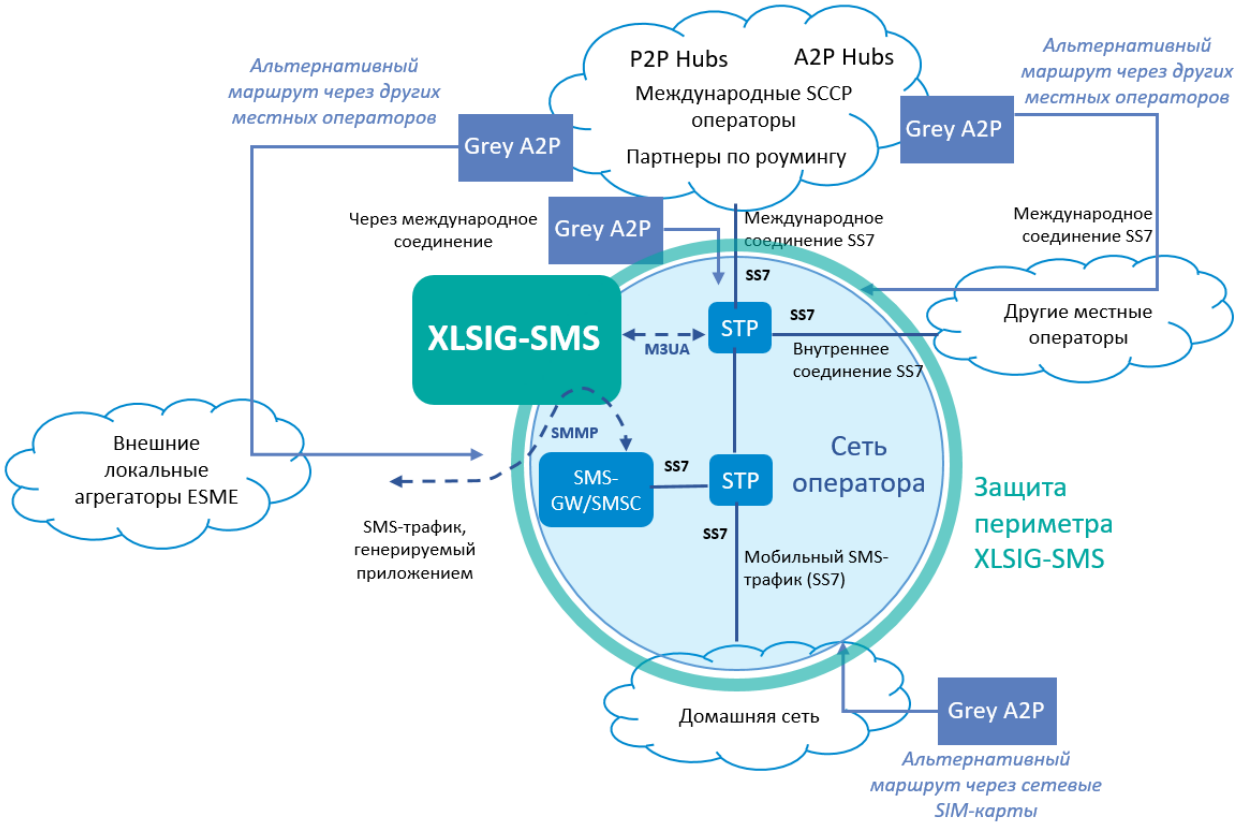

Рисунок 1. Защита периметра сети оператора

2. Области применения XLSIG-SMS

2.1. Противодействие мошенничеству

Таблица 2. Область применения: противодействие мошенничеству

Функционал	Описание
SMS HOME ROUTING	Для рассылки SMS через сторонние сети операторы вынуждены предоставлять идентификаторы абонентов и их местонахождение. Это небезопасно, так как открывает возможности для SS7-атак, таких как отслеживание местоположения абонента, перехват SMS и голосовых звонков.

Функционал	Описание
	Функция SMS Home routing позволяет операторам доставлять сообщения из сторонних сетей и не раскрывать при этом идентификаторы собственных абонентов.
SMS FLOODING	Рассылка огромного количества сообщений абоненту или другой системе. Это приводит к перегрузке сигнальной сети (SS7) и задержке доставки других сообщений. Система блокирует сообщения от определенного абонента, SMS-центра или GT отправителя после превышения порога MO- и MT-сообщений.
MT SMS FAKING	Использование удаленной системой идентификатора реального разрешенного SMS-центра, что не позволяет оператору домашней сети получить плату за терминацию трафика. Система блокирует сообщения в случае несовпадения GT отправителя с адресом SMSC.
MO SMS SPOOFING	Нелегальная рассылка сообщений путем эмуляции абонента, находящегося в роуминге, в результате которой абоненты получают счета за сообщения, которые не отправляли. Система блокирует отправку сообщений от имени абонента, если GT MSC в запросе отличается от GT MSC, который фактически обслуживает абонента.

3. Функциональность

3.1. Соответствие отраслевым стандартам

XLSIG-SMS полностью соответствует рекомендациям и стандартам GSMA и 3GPP:

- GSMA IR.70 – SMS SS7 Fraud;
- GSMA SG.22 – SMS Firewall Best Practices and Policies;
- 3GPP TR 23.840 – Study into routing of MT-SMs via the HPLMN.

Система поддерживает базовые протоколы обмена сообщениями:

- SS7 over IP в соответствии со стандартом рабочей группы SIGTRAN IETF;
- SMPP.

3.2. Базовый функционал

XLSIG-SMS реализует контроль прохождения входящих SMS в режиме реального времени и основан на обработке SMS сообщений и связанных управляющий сигнальных запросов, полученных через MAP (SIGTRAN) и/или SMPP. Система анализирует каждый MT SMS, для определения необходимости их обработки в соответствии с предопределёнными сценариями.

Система поддерживает следующие режимы работы:

- Прокси-режим: перехват SMS-трафика в режиме реального времени с активным реагированием на случаи мошенничества;
- Отказ с настраиваемым кодом причины;
- Тихое отбрасывание (silent discard);

- Сброс/отбрасывание с положительным подтверждением.

В системе реализованы следующие функции:

- Взаимодействие с коммутационным оборудованием оператора связи (MAP, SIGTRAN, SMPP);
- Выявление и блокирование различных видов SMS-мошенничества на основе настраиваемых сценариев.

Обнаружение мошеннических SMS-сообщений:

- Логика обнаружения мошеннических SMS-сообщений основана на настраиваемых сценариях;
- Каждый сценарий определяется с помощью одного или нескольких фильтров, которые выполняются для каждого SMS (в режиме реального времени), а в случае соответствия сообщения всем определенным фильтрам, выполняется соответствующее действие, определенное для такого сценария.

При создании фильтров могут использоваться следующие параметры:

- Calling global title/ Called global title;
- IMSI;
- Вызывающий номер / Вызываемый номер и другие значимые SMS атрибуты;

Имеются следующие опции сверки текста сообщения по ключевым словам:

- Анализ/проверка незашифрованного текста на наличие ключевых слов;
- Хеширование содержимого слов и сопоставление с ключевыми словами хэша;
- Анализ регулярности повторений с помощью незашифрованного текста или хэша слов.

После применения сценариев система может выполнять следующие действия над обрабатываемыми сообщениями:

- Частичная фильтрация СМС-сообщений;
- Блокировка SMS-сообщений;
- Доставка SMS-сообщений.

Настраиваемые правила обработки при срабатывании сценария:

- Если SMS-сообщение не соответствует ни одному из определенных сценариев оно не обрабатывается, при этом SMS доставляется без каких-либо изменений.

Все действия могут быть применены как для всех SMS-сообщений или для определенного процента сообщений. В последнем случае определенная часть сообщений обрабатывается в случайном порядке в соответствии с определенным сценарием действий, а к остальным сообщениям не применяется никакое действие.

В рамках каждого сценария можно использовать следующие действия:

- Продолжить доставку SMS без каких-либо изменений;
- Отклонить / блокировать SMS (сообщение заблокировано / отклонено, и информация об отказе сообщается отправителю);
- Молча отклонить / блокировать SMS (сообщение заблокировано / отклонено, и информация об отказе не отправляется);
- Отклонить / блокировать SMS с поддельным отчетом «сообщение отправлено» (сообщение заблокировано / отклонено, но ложная информация об успешно отправленном сообщении отправляется отправителю).

3.3. Логическая архитектура системы

Система состоит из следующих модулей:

- SMPP Proxy: предоставляет интерфейс для подключения внешних приложений по протоколу SMPP, осуществляет проверки на уровне протокола SMPP;
- Ядро системы (Rule-Processing engine, Real-time analytics, Active Check – это запросы к HLR и т.д.) – отвечает за проверку коротких сообщений, находящихся в процессе доставки, управляет выгрузкой CDR-файлов;
- Протокольный уровень, обеспечивает взаимодействие с коммутационным оборудованием по SIGTRAN, осуществляет проверки на уровне соответствующих протоколов;
- Text Analyzer, обеспечивает комплексный анализ текста короткого сообщения.

3.4. Инфраструктура системы

XLSIG-SMS представляет собой программно-аппаратный комплекс, в состав которого входят:

1. Серверное оборудование: система функционирует на серверах с x86 - архитектурой или в виртуальных средах различных платформ виртуализации;
2. Системное программное обеспечение:
    - Операционная среда серверов или виртуальных машин: AstraLinux, Dedian.