Описание
системы безопасности сервисов Albix MAX

Настоящий документ содержит описание ключевых функций защиты СМС-обменников линейки Albix MAX от действий мошенников и иных сопутствующих обменному сервису рисков.

~~Данное описание является документом для служебного пользования и предназначается только для специалистов компаний агрегаторов смс-трафика, для принятия решения о сотрудничестве с нами, и выработке совместных мер защиты.~~

~~Данный документ не должен передаваться третьим лицам в любом виде, или использоваться иным образом.~~

Настоящий документ состоит из двух частей:

- Описание функций защиты;
- Анализ угроз и методы противодействия им.

1. Описание функций защиты

1.1. Диалог с пользователем

Взаимодействие с пользователем система осуществляет в диалоговом режиме. При этом решение о дальнейших возможных действиях пользователя принимаются на стороне сервера, на основании предыдущей истории взаимодействия с ним.

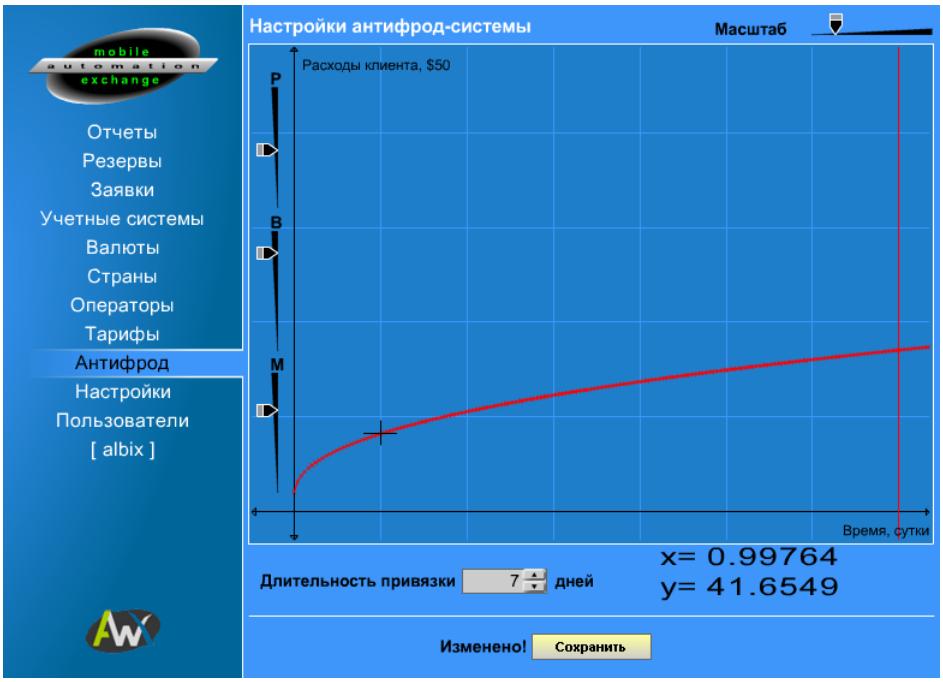
Это исключает возможность несанкционированного обхода защитных функций на ранних этапах диалога, путем манипуляций с данными, отправляемыми на сервер.

1.2. Долгосрочное лимитирование

В отличие от широко применяемой схемы лимитирования, введением одного или нескольких порогов расходования средств со счета телефона в единицу времени, в нашей системе используется технология долгосрочного лимитирования.

Ее суть заключается в том, что мы задаем непрерывную кривую, описывающую норму расхода на длительный промежуток времени (на месяц).

На следующем рисунке видна страница панели управления Albix MAX, отвечающая за настройку этой функции:



Красная кривая на графике – и есть предельно допустимый расход средств пользователем, от текущего момента времени (слева) в прошлое (справа). Идентификация пользователей производится скрыто, и осуществляется по нескольким параметрам.

История расхода средств всегда просматривается на глубину в один месяц от текущего момента времени. Практика показывает, что такой глубины анализа истории достаточно.

Такой подход делает бессмысленными периодические малые атаки на систему, которые легко проходят стандартную защиту, так как период этих атак становится чрезвычайно большим (более месяца).

1.3. Привязка реквизитов

На выше приведенном рисунке также можно увидеть параметр «Длительность привязки» и соответствующую ему вертикальную красную линию на графике.

Данный параметр позволяет установить условие, по которому на ранее использованный номер счета получателя выплаты можно осуществить перевод только с того же самого номера телефона, что был использован в последний раз.

Длительность привязки, соответственно, задает, сколько дней с момента последнего использования номера счета хранится его ассоциация с номером телефона.

Данная мера дополняет комплексную идентификацию и направлена против использования мошенниками большого количества номеров счетов и телефонов.

1.4. Двойная проверка на превышение лимитов

Проверка на превышение лимита расходования средств пользователем выполняется дважды:

- При фильтрации доступных пользователю тарифов;
- При обработке входящего смс-запроса.

Первая проверка позволяет не предлагать пользователю тарифы, использование которых привело бы к превышению им лимита расходования средств.

Если доступных пользователю тарифов в настоящий момент нет, то диалог прерывается и инструкция на отправку смс не отображается. Что позволяет заблокировать саму отправку смс-запрос. А, значит, позволяет избежать и возможных конфликтов с ОСС, как для самого обменного сервиса, так и для смс-агрегатора.

Вторая проверка – контрольная. Сведения о номере телефона поступают не от пользователя, а от агрегатора, и потому обладают более высокой достоверностью. На основании чего выплата по заявке может быть приостановлена или отменена.

1.5. Динамический код в теле исходящего смс-запроса

На представленном ниже рисунке приведен клиентский интерфейс Albix MAX, на этапе диалога, соответствующем инструкции по отправке смс-запроса:

Для каждой новой заявки генерируется случайный четырехзначный цифровой код, действительный только для этой заявки, входящий в состав текста смс-запроса, который должен отправить пользователь. На рисунке выше это число 2476.

До момента отображения инструкции этот код не существует в системе, поэтому только пользователь, дошедший до данного этапа диалога, знает его и может отправить корректный смс-запрос.

Соответственно, если система не допустит пользователя к инструкции на отправку смс, то предсказать корректный текст запроса практически нереально. И отправлять платный смс-запрос в таких условиях абсолютно бессмысленно.

Это позволяет избавиться от значительной части проблемного трафика и делает практически невозможным мошенничество, путем обмана третьей стороны по поводу целей и условий отправки ею смс-запроса («фишинг»).

1.6. Динамический код в ответном смс-сообщении

При формировании заявки также генерируется случайный четырехзначный цифровой ответный код, который отправляется пользователю в ответном смс-сообщении. Пользователь должен ввести его в соответствующее поле диалога с системой. На приведенном выше рисунке в этом поле введено число 1234.

Не зная это число, невозможно корректно завершить диалог с системой, так чтобы заявка не была аннулирована или не отнесена к «подозрительным» (в зависимости от настроек системы).

Эта мера также направлена против «фишинга» и возможного мошенничества с некоторыми реализациями МТ-тарификации.

1.7. Ограничение по времени на отправку смс и ввод ответного кода

В правом нижнем углу на приведенном выше рисунке виден таймер, показывающий остаток времени на текущую операцию. По его истечении диалог автоматически завершается по варианту «таймаут», с соответствующими вытекающими для заявки последствиями: отмена, отказ или холд (в зависимости от настроек системы и факта поступления соответствующего смс-запроса).

Эта мера делает окончательно бессмысленным «фишинг», так как на нахождение жертвы мошеннику остается совсем мало времени, и делать ему это придется лично и вручную.

1.8. Выявление и холд подозрительного трафика

В системе есть понятие «подозрительного трафика», к которому относятся заявки, в ходе оформления которых не было выявлено явных признаков мошенничества или грубых нарушений пользовательских соглашений, но были замечены особенности, которые могут свидетельствовать о возможном мошенничестве или проблемности.

Такой статус заявки означает, что администрации обменника требуется обратить на нее особое внимание, прежде чем будет принято окончательное решение.

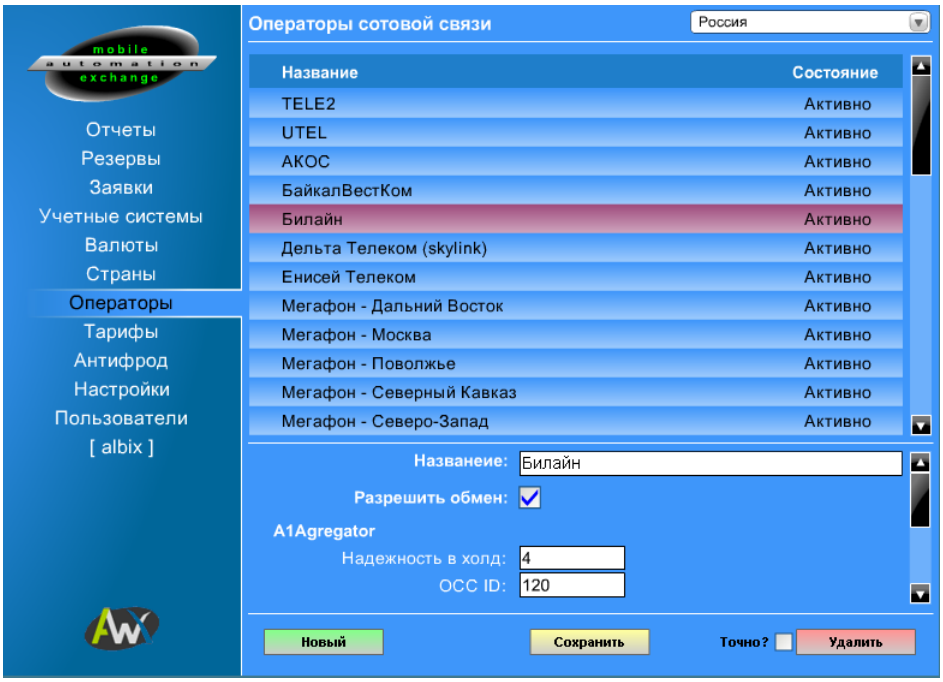
То есть, такие заявки обрабатываются по альтернативному регламенту, как правило означающему выплату средств по факту их поступления от агрегатора (если в ходе рассмотрения заявки администрацией не будет принято иное решение).

1.9. Учет оценок надежности абонента от агрегатора

Некоторые агрегаторы смс-трафика имеют свою систему оценки платежеспособности абонентов сотовой связи, смс-запросы которых проходят через их систему, и предоставляют эти сведения при вызове обработчика партнера. Например, компания A1Агрегатор передает на обработчик партнера параметр «надежность номера», выраженную по десятибалльной шкале.

Albix MAX использует эти сведения для выявления подозрительного, или даже блокировки явно проблемного трафика.

Система допускает тонкую настройку своей реакции на такого рода дополнительные сведения, включая возможность индивидуальных настроек для разных операторов связи:



Также активно используются другие, часто передаваемые по техническим протоколам данные, такие как идентификатор оператора сотовой связи, контроль которых необходим для установления соответствия заявленных пользователем данных действительности.

Мы готовы разработать индивидуальные алгоритмы защиты, оптимизированные для эффективного взаимодействия с системами безопасности агрегаторов смс-трафика.

2. Анализ угроз и методы противодействия им

Логика любой защиты всегда сводится к повышению накладных расходов атакующего до такого уровня, чтобы результат успешной атаки имел для него меньшую ценность, чем потраченные на нее ресурсы.

Рассмотрим основные виды атак и меры борьбы с ними, реализованные в Albix MAX.

2.1. Хищение средств с корпоративных телефонов

Пожалуй, это наиболее опасная угроза, так как в случае обнаружения хищения почти наверняка будет иметь место возврат средств на крупную сумму. То есть, у оператора связи будут проблемы. А значит и у агрегаторов с партнерами тоже.

Так как полные данные о всех сериях корпоративных телефонов нам не доступны, то абсолютной технической защиты тут предложить нельзя. За то отлично работает простая логика!

Не давая украсть слишком много, мы не только снижаем шанс на возникновение проблемы с откатом, но и ограничиваем объем этого возможного отката.

Для этих целей отлично подходит наша схема долгосрочного лимитирования, которая как раз и позволяет ограничить общий объем возможного хищения на протяженном отрезке времени.

2.2. Массовое использование бонусов с новых sim-карт

Такой вариант однозначно не нравится операторам сотовой связи, так как они теряют значительные средства. Что опять приводит к проблемам у агрегаторов и партнеров.

Усложнить жизнь злоумышленнику в таком случае поможет наша комплексная идентификация и привязка номера счета получателя к телефону.

Плюс еще динамические коды и реализация Albix MAX на флеше, что исключает автоматизацию процесса перебора.

То есть процесс становится ручным, сложным и нудным. Мало кто вытерпит это достаточно долго, чтобы успеть сгенерировать заметный трафик. А раз явление минимизировано до пренебрежимо малых масштабов, то и проблем нет.

2.3. Фишинг (социальная инженерия)

Речь идет об инициации под ложным предлогом отправки платного смс-запроса, соответствующего инструкции смс-обменника, третьими лицами, не подозревающими о его реальной стоимости и назначении. В результате чего мошенник предполагает получить выплаты за эти смс-запросы.

Как уже отмечалось в первой части данного документа, против этого явления в нашей системе предусмотрен целый комплекс мер, включающих комплексную идентификацию, динамические коды в тексте смс-запроса и ответном сообщении. А также ограничение по времени на отправку корректного смс-запроса и ввод ответного кода.

2.4. Загон sim-карты «в минус»

Сливание бонусов с новых sim-карт также иногда приводит к уводу баланса ее лицевого счета «в минус», вследствие временного лага биллинговой системы некоторых ОСС. Что часто становится причиной невыплаты ОСС агрегатору всего объема потраченных с данной сим-карты средств. То есть, проблемой для агрегатора и партнера.

Предотвратить это явление можно, обеспечив достаточный для срабатывания биллинговой системы ОСС промежуток времени между посылаемыми пользователями смс-запросами.

Обеспечить это нам снова поможет наша схема долгосрочного лимитирования, но на этот раз внимание нужно обратить на поведение кривой нормы расхода у самого начала координат (то есть, на недавний от текущего момента отрезок времени).

Непрерывный и плавный рост нормы расхода, фильтрация доступных пользователю тарифов, уникальность кодов в смс-запросе и подтверждения позволяют надежно обеспечить необходимую нам задержку.

А раз пользователь физически не может отправить подряд несколько корректных запросов, которые были бы оплачены обменником, то масштабы этого явления будут минимальны. А попытки отправить смс сверх баланса счета телефона, с навязанной нами задержкой, приведут к их блокировке на уровне успевшего сработать биллинга ОСС.

Мы готовы рассмотреть и обсудить другие типы угроз, объяснить логику работы нашей системы в различных условиях и, если понадобится, внести в нее изменения, чтобы обеспечить надежную защиту интересов всех участников процесса.