УДК 621.396

Бельская А.А. к.т.н.,
Гуйда А.Г., ст. викл.,
Юхимчук Р.А.

ПОВЫШЕНИЕ БЕЗОПАСНОСТИ ОТ НЕЛЕГАЛЬНОЙ МАРШРУТИЗАЦИИ МЕЖДУНАРОДНОГО ТРАФИКА В GSM СЕТЯХ

Запропоновано алгоритм для боротьби з нелегальною маршрутизацією міжнародних дзвінків в мережах GSM, який ґрунтується на аналізі характеру поведінки абонентів

Предложен алгоритм для борьбы с нелегальной маршрутизацией международных звонков в сетях GSM, который основывается на анализе характера поведения абонентов

An algorithm is proposed to battle the with international call termination in GSM, which is based on an analysis of the behavior of users

Введение. Телекоммуникационные операторы по всему миру теряют значительные суммы от нелегальной маршрутизации международного трафика (Interconnection Bypass), в основном за счет увеличения использование VoIP-GSM шлюзов – часто называются SIM-BOX. GSM-VoIP шлюзы это телекоммуникационные устройства, которые разрешают совершать вызовы со стационарных или мобильных телефонов и направляются через VoIP непосредственно в соответствующие GSM-сети. Самые продвинутые GSM шлюзы могут использовать установки сотни мобильных SIM-карт и даже хранить SIM-карты при отсутствии их в шлюзе физически. GSM шлюзы часто устанавливаются в офисах для сокращения затрат на мобильные звонки сотрудников в пределах офиса - это законно в большинстве стран. Тем не менее, коммерческое предложение телекоммуникационных услуг, таких как предоставление международной связи через GSM-шлюзы без утверждения GSM оператора, является нелегальным.

Постановка задания. Системы по предотвращению мошенничества (FMS) стают все более популярными, и на это повлияли большие объемы нелегального международного трафика . В первое время GSM операторы использовали FMS для проведения сложного анализа CDR, чтобы найти необычные модели поведения абонентов для эффективного обнаружения незаконных международных звонков и блокировки мобильных SIM карт, которые замечены в такой незаконной активности.

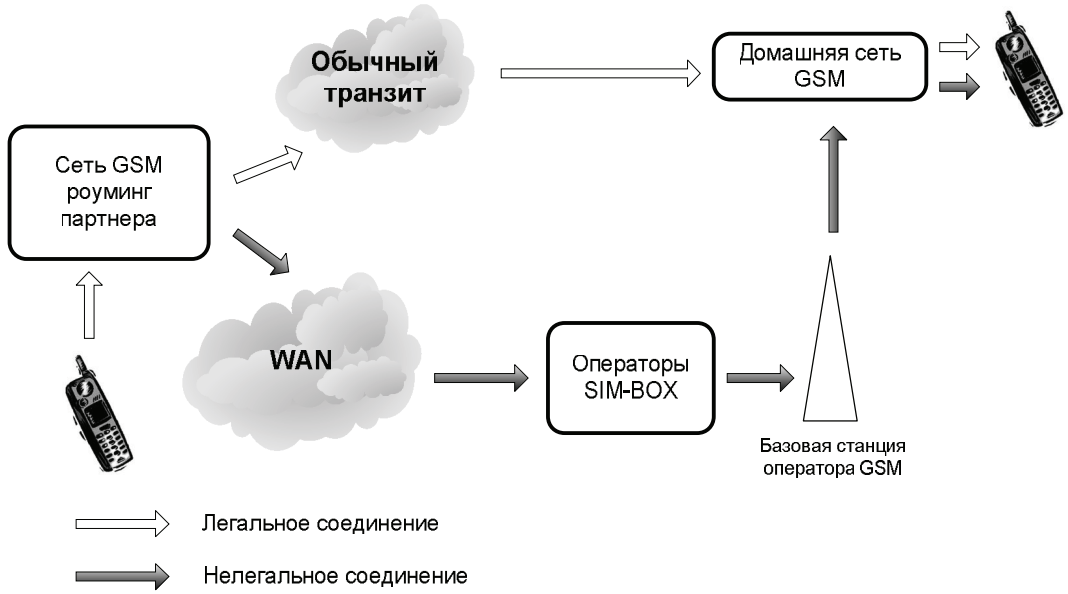

Рис.1 Схема легальной и нелегальной маршрутизации международных звонков

Хотя технологические достижения позволили GSM операторам лучше выявлять такой тип мошенничества и блокировать таких абонентов, проблема все еще остается нерешенной в связи с тем, что мошенники постоянно адаптироваться к новым мерам безопасности и учатся считывать методы обнаружения, которые приводят к их обнаружению на основе анализа шаблона поведения мобильных абонентов.В связи с этим требуется создать систему непрерывного мониторинга и анализа мошеннических действий абонентов, которые идентифицируются в результате тестовых звонков, и на основе этого анализировать CDR и идентифицировать мошеннические действия.

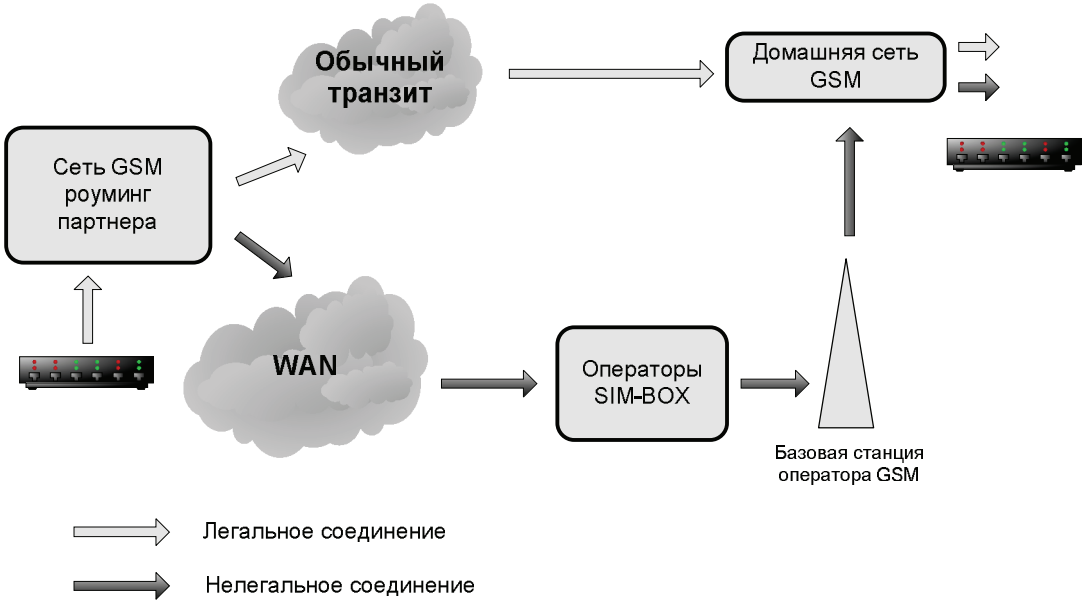

Рис.2 Схема тестовых звонков для идентификации нелегальных терминалов

Основные параметры поведения абонентов. Для создания шаблона характера поведения абонентов используются следующие параметры:

1. Отсутствие или низкая мобильность;
2. Много абонентов в одной соте с подозрительной активностью;
3. Необычное число ночных звонков на разные номера;
4. Отсутствие входящих звонков.

Ниже описаны более подробно несколько из выше перечисленных параметров поведения:

Отсутствие или низкая мобильность. VoIP-GSM шлюзы как правило устанавливаются в DATA-центрах с широкополосным подключением к Интернету. Таким образом, типичной характеристикой поведения SIM-карт, используемых для нелегальной маршрутизации трафика, будет очень низкая или отсутствие мобильности.

Эта характеристика используется для обнаружения GSM шлюзов и зависит отразмера соты GSM, но, как правило, такой SIM-модуль будет появляться только в нескольких соседних сотах, или будет исчезать и появляться в отдаленной соте реализации хэндовера между ними – это свидетельствует о том, что GSM шлюз был перенесен в другой DATA-центр. Эта характерность поведения мошенников является наиболее распространенной, так как ее избежание обходится довольно дорого.

Простейший метод, примененный мошенниками , во избежание этого шаблона поведения является так называемый "take SIMs for a ride".

Ежедневно, некоторые SIM-модули вынимают и помещают в VoIP-шлюз, который устанавливается на автомобиль, и его провозят через разные соты GSM. Таким способом SIM-карты помещают в различных местах и предотвращает базовую идентификацию стационарных SIM-карт с помощью FMS.

Однако, эта техника не является главным препятствием для оператора. Если используется такой способ борьбы с обнаружением модулей, так как GSM операторы могут настроить FMS путем проведения анализа не основанном на местах активации мобильных SIM карт, а на основании расположения SIM-карт во время совершения звонков. Хотя этот метод является очень эффективными в обнаружении GSM-шлюзов, маловероятно, чтобы остановить наиболее продвинутых мошенников, которые постоянно пытаются найти новые способы избежать обнаружения.Например, в одной стране, мошенники начали размещать GSMшлюзы в фургонах и работать из нескольких мест в течение дня, используя большие расстояния для подключение по Wi-Fi. Хотя это и не очень продвинутый способ избегания обнаружения, тем не менее, интересный метод. Наиболее продвинутые мошенники начали использовать «SIM Server technology».

SIM Server – это решение, которое реализует удаленный доступ центральному хранилищу и управление любым количеством SIM-модулей, которые могут использоваться удаленно в шлюзах или другом оборудовании GSM через SIM адаптеры подключенные в LAN (Local Area Network). Это позволяет удаленно менять местоположение виртуально переключая SIM-модуля.

Много абонентов в одной соте с подозрительной активностью. Главные операторы, которые используют шлюзы GSM обычно вставляют сотни SIM-карт в большие шлюзы VoIP, которые могут быть одновременно активизированы и введены в эксплуатацию. Большое количество SIM –карт, которые используются в одной соте могут свидетельствовать о использование шлюза GSM. Тем не менее, расположение и нагрузка должны также быть учтены. Например, большое количество абонентов расположенных за пределами города это очень необычный шаблон, что указывает на возможное мошеннического использования. Кроме того, SIM-карты, которые используются для нелегальной маршрутизации международного трафика будут часто появляться на той же или соседних сотах, таким образом, при положительном обнаружении нескольких случаев незаконных звонков в одной соте, другие, менее подозрительные SIM-карты в той же соте могут автоматически классифицируются как мошенничество, хотя они и имею меньше фродстерских признаков. В целях предотвращения такого значительного необычного увеличение SIM-модулей на одну соту, мошенники пытаются найти крупные соты и разместить GSM шлюзы, где возможно спрятать любое количество SIM-карт. В связи с требованием использования несколько SIM-карт в одном месте, довольно трудно найти большие свободные соты, которые могут обрабатывать большие объемы трафика, делая это основным препятствием для такого типа операторов. По желанию мошенники также можете отключить SIM-карты когда они не используются и активировать их всякий раз, когда нет больше SIM-карты, которые могут обрабатывать звонок. В общем, очень трудно для мошенников избежать территориальной близости SIM-карт, для них это является даже сложнее чем отсутствие мобильности, что делает этот характер поведения особенно полезным в идентификации GSM шлюзов.

Большое количество вызовов на различные номера. Использование нелегальной маршрутизации международного трафика также характеризуется высоким количество голосовых вызовов на различные номера телефонов, так как VoIP шлюзы как правило, обслуживают большое количество пользователей, которые звонят на разные номера. Тем не менее, применение этого шаблона бывает неоправданным, как GSM шлюзы могут легально использоваться в PABX

рекрутинговых компаний и могут часто ошибочно классифицироваться как мошенничество.

Необычное число ночных звонков на разные номера. Для офисного сотрудника является весьма необычным часто звонить на разные номера ночью. Таким образом, наличие частых ночных звонков на различные номера еще одна необычная модель, которая может указывать на SIM-боксы. В сочетании с характерным высоким числом различных направлений голосовых звонков, он может дать очень хорошие результаты. Мошенникам также трудно избежать этого шаблона. Международные VoIP услуги удовлетворяют большое количество пользователей, которые звонят на различные телефоны. Очень необычно для «честного» пользователя постоянно звонить на различные мобильные номера, что и делает эту характеристику полезной в обнаружении SIM-боксов. Распространенный метод противодействия обнаружению по FMS является внедрение автоматических SIM-отображений в зависимости от времени суток, и маршрутизировать ночные звонки через отдельные SIM-карты. Такие функции маршрутизации, как правило обеспечиваются SIM-серверным решением и иногда поддерживаются более продвинутым оборудованием GSM. Подавляющее большинство мобильных пользователей сети часто используют как SMS так и голосовые услуг, а значит, отсутствие SMS также является характеристикой SIM-бокса. В теории мошенники могут отправлять случайные SMS, например, информировать абонентов о продолжительности звонков или совершать рассылки SMS в рекламных целях. Тем не менее, это редко наблюдается в реальных сетях. Таким образом, использование голосового трафика абонентами остается очень ценной характеристикой в обнаружении шлюзов.

В моей работе была создана модель пуассоновского потока в виде CDR (Call Detail Record), а также поток, которому присущий характер поведения абонентов, использующих нелегальные терминалы (рефайл). С помощью запросов к БД определяется количество блокировок «честных» абонентов, при каждом последующем изменении характера поведения терминалов нелегальной маршрутизации. Таким образом, определен запрос, результатом которого является допустимое количество «честных» абонентов при любом изменении поведения абонентов. При помощи процедурного расширения SQL – PL/SQL анализируется трафик абонентов «рефайла», создается на его основе шаблон характера поведения абонентов и по этому нему ищутся соответствия в Call Detail Records. Для создания БД, а также ее заполнения будем использовать средства Oracle, а также Gedis Studio для генерации CDR.

Табл.1 Пример CDR

MSISDN	DURATION	CELL_ID	CALL_TYPE	B_NUMBER	CALL_DATE	CALL_TIME
601234583	554	CELL_ID-2	VOICE_OUT	601234607	9/22/2011	22:54:00
601234645	884	CELL_ID-2	VOICE_OUT	601234603	9/22/2011	12:15:00
601234633	387	CELL_ID-3	VOICE_IN	601234658	9/22/2011	13:30:00
601234605	840	CELL_ID-7	VOICE_IN	601234637	9/22/2011	12:41:00
601234635	664	CELL_ID-2	VOICE_IN	601234611	9/22/2011	17:06:00
601234603	0	CELL_ID-1	SMS_IN	601234649	9/22/2011	12:15:00
601234606	0	CELL_ID-2	SMS_IN	601234593	9/22/2011	13:30:00
601234592	888	CELL_ID-5	VOICE_OUT	601234659	9/22/2011	13:00:00
601234569	779	CELL_ID-7	VOICE_IN	601234612	9/22/2011	22:54:00
601234613	1114	CELL_ID-7	VOICE_IN	601234613	9/22/2011	12:41:00
601234601	104	CELL_ID-4	VOICE_IN	601234631	9/22/2011	13:00:00
601234646	0	CELL_ID-4	SMS_IN	601234579	9/22/2011	14:36:00
601234639	0	CELL_ID-4	SMS_IN	601234585	9/22/2011	14:00:00
601234643	0	CELL_ID-1	SMS_IN	601234581	9/22/2011	12:15:00
601234626	205	CELL_ID-1	VOICE_OUT	601234632	9/22/2011	12:41:00
601234606	65	CELL_ID-6	VOICE_OUT	601234574	9/22/2011	14:00:00
601234664	0	CELL_ID-1	SMS_IN	601234621	9/22/2011	13:30:00
601234580	0	CELL_ID-5	SMS_IN	601234590	9/22/2011	17:06:00
601234612	351	CELL_ID-3	VOICE_OUT	601234647	9/22/2011	22:54:00
601234587	729	CELL_ID-1	VOICE_OUT	601234568	9/22/2011	13:30:00
601234635	702	CELL_ID-1	VOICE_OUT	601234594	9/22/2011	14:36:00
601234653	478	CELL_ID-4	VOICE_IN	601234614	9/22/2011	17:06:00
601234645	1138	CELL_ID-4	VOICE_IN	601234641	9/22/2011	12:41:00
601234586	687	CELL_ID-1	VOICE_IN	601234579	9/22/2011	12:41:00
601234582	0	CELL_ID-7	SMS_IN	601234657	9/22/2011	12:41:00

Табл.2 Пример детализации звонков абонента

MSISDN	DURATION	CELL_ID	CALL_TYPE	B_NUMBER	CALL_DATE	CALL_TIME
601234574	11	CELL_ID-5	VOICE_IN	601234567	9/22/2011	22:54:00
601234574	56	CELL_ID-4	VOICE_OUT	601234659	9/22/2011	17:06:00
601234574	0	CELL_ID-6	SMS_IN	601234583	9/22/2011	14:36:00
601234574	1068	CELL_ID-1	VOICE_IN	601234618	9/22/2011	14:00:00
601234574	126	CELL_ID-4	VOICE_OUT	601234656	9/22/2011	13:30:00
601234574	983	CELL_ID-2	VOICE_IN	601234567	9/22/2011	13:00:00
601234574	0	CELL_ID-1	SMS_IN	601234581	9/22/2011	12:41:00
601234574	980	CELL_ID-7	VOICE_IN	601234571	9/22/2011	12:15:00

Выводы. Комбинация тестовых звонков и определение характера поведения абонентов является оптимальным способом для борьбы с нелегальной маршрутизацией международного трафика. Мошенники адаптируются к новым видам шаблонов, поэтому нужно непрерывно считывать их модель поведения и генерировать новые шаблоны.

При этом нужно минимизировать количество блокировок «честных» абонентов. Предложенный алгоритм позволяет реализовать мониторинг такого типа. На данном этапе ведется разработка процедуры для считывания параметров поведения мошенников.

Использованные источники информации:

1. Nokia Siemens Networks “Battling illegal call operations with Fraud Management Systems”
2. Christopher Allen “Oracle PL/SQL 101”