DOI 10.37882/2223–2966.2022.02.36

ОБНАРУЖЕНИЯ IMSI ЛОВУШЕК В СЕТЯХ СОТОВОЙ СВЯЗИ ПРИ ПРИМЕНЕНИИ АЛГОРИТМИЧЕСКОГО ПОДХОДА

DETECTION OF IMSI TRAPS IN CELLULAR COMMUNICATION NETWORKS USING AN ALGORITHMIC APPROACH

I. Khramtsov

Summary. Due to the low level of protection of mobile networks from man-in-the-middle attacks, where they are used from false base stations of the mobile network, protecting user privacy raises an urgent issue in providing protection against this type of threat. The material of this article discusses a method that uses the identification and detection of IMSL traps based on the infrastructure of the GSM network. The main advantage of using this method is that it will protect all users from the general coverage of the operator's network while saving users money and resources by not having to purchase additional equipment.

Keywords: False base station, GSM, IMSI trap, confidentiality; Information Security.

Храмцов Илья Александрович
Аспирант, Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева, г. Красноярск
ilia.khramcov@yandex.ru

Аннотация. В связи с низким уровнем защищенности сетей мобильной связи от атак типа «человек посередине», где они используются с ложных базовых станций мобильной сети, защита конфиденциальности пользователей ставит актуальный вопрос в обеспечении защиты от данного вида угроз. В материале данной статьи рассматривается метод, использующий идентификацию и обнаружение IMSL-ловушек, основанный на инфраструктуре сети GSM. Основное преимущество при использовании этого метода заключается в том, что он обеспечит защиту всех пользователей от общего покрытия сети оператора при экономии средств и ресурсов пользователей за счет отсутствия необходимости приобретения дополнительного оборудования.

Ключевые слова: ложная базовая станция, GSM, IMSI-ловушка, конфиденциальность, информационная безопасность.

До недавнего времени мобильные сети считались достаточно безопасными из-за строгой аутентификации, обеспечиваемой модулем идентификации абонента (SIM). Сейчас это доверие сильно подорвано из-за серии инцидентов, связанных с прослушиванием телефонных разговоров и прослушиванием телефонных разговоров. Высокопоставленные политики и простые граждане постоянно подвергаются слежке со стороны иностранных агентств и преступников. Для прослушивания можно использовать высокотехнологичное оборудование (Cellbrite 2 и др.) или ограничиться устройством на базе ПО с открытым исходным кодом и программным радиоприемником. Ловушка IMSI — это устройство, которое позволяет злоумышленнику перехватить личность абонента мобильной связи (IMSI), чтобы отслеживать местоположение пользователя, телефонные звонки или выдавать себя за законного абонента. Для защиты абонентов от этого типа угроз существует несколько приложений, которые устанавливаются на мобильный телефон и предупреждают о системах обнаружения прослушивания, которые позволяют операторам обнаруживать наличие IMSI-ловушек в их сети. Однако до сих пор в сеть GSM не интегрировано решение, позволяющее операторам мобильной связи определять точное местоположение IMSI-ловушки и защищать своих абонентов от атак. В данной статье представлен разработанный метод обнаружения IMSI — ловушек в произвольной соте, благодаря использованию информационных данных, полученных от нескольких базовых станций.

Методы обнаружения IMSI-ловушек

На сегодняшний день существующие методы обнаружения ловушек IMSI можно разделить на две категории: приложения для смартфонов и автономные системы обнаружения ловушек известных значений. Для максимальной производительности приложению необходим root-доступ к чипу, отвечающему за выбор базовой полосы частот. Этот чип отвечает за измерение уровня сигнала, передачу двоичных SMS-сообщений на SIM-карту и другие функции радиосвязи, поэтому необходимо получить доступ к конкретной информации о сети, такой как идентификатор обслуживающей соты (CID), код зоны местоположения (LAC) и сигнал. сильные стороны соседних соседей. Автономные системы обнаружения работают с использованием как программных приложений, так и специализированного оборудования, примерами таких систем являются GSMK Overwatch и Network Guard.

Таблица 1. Данные BTS.

BTS	ARFCN	BSI	сообщения от других BTS	Позиция об изменения в отчете
1	70	29	2,3,4	1–3
2	60	28	1,3,4,5	1–3
3	65	27	1,2,4,5	1–3
4	55	26	1,2,3	1–3
5	75	29	2,3	2,4
Ловушка IMSI	75	29	-	-

Механика работы «IMSI-ловушек»

Простейшие варианты ловушек IMSI часто работают только в режиме аутентификации. В этом режиме ловушка IMSI создает поддельную ячейку, часто подделывая настоящую, для получения международного идентификатора мобильного абонента (IMSI) и международного идентификатора мобильного оборудования (IMEI). Более сложные версии ловушек IMSI способны выполнять активные атаки «человек посередине» (MPM), которые могут перехватывать вызовы, манипулировать данными и манипулировать службой коротких сообщений (SMS). В этом режиме IMSI перехватывает перенаправленный трафик от MS обратно в реальную сеть, позволяя злоумышленнику оставаться незамеченным.

Обнаружение спуфинга с помощью ловушек IMSI возможно путем сбора и анализа отчетов, отправляемых мобильными устройствами. После отключения мобильного устройства жертвы от IMSI-ловушки эта ловушка становится одной из ближайших поддельных BTS с сильным сигналом к соседним MS. Если телефон подключился к ловушке IMSI, которая была настроена с другим LAC, чем соседние мобильные устройства, MS выполнит процедуру обновления местоположения, после чего подключится к подлинной сети. В результате MS отправит отчет, включающий 6 ближайших BTS, обратно в сеть оператора сразу после подключения к исходной BTS. Проверяя идентификацию соседа вместе с позицией в отчете о соседстве по базе данных зарегистрированных BTS, мы можем искать несоответствия, которые указывают на наличие поддельной BTS или ловушки IMSI. Чтобы мобильная станция (MS) могла постоянно подключаться к наиболее подходящей соте, как с точки зрения качества канала, так и сетевых ресурсов, MS измеряет мощность и качество сигнала RX нисходящей линии связи от своей обслуживающей и соседних BTS. Отчеты об этих измерениях затем отправляются обратно в сеть. В это время MS находится в активном состоянии и может выполнять обновление местоположения, устанавливать вызов или выполнять активный вызов, выделять TCH или канал данных на радиоинтерфейсе по целому ряду причин, таких как отправка или прием пакетных данных или SMS.

Рассмотрение механики метода обнаружения сетевой IMSI-ловушки

Чтобы продемонстрировать осуществимость предлагаемого метода обнаружения, приведем модель построенной на методе предложенной механики.

Он состоит из физической сети GSM, ловушки IMSI и двух мобильных телефонов. В ходе эксперимента полная сеть GSM была построена с использованием OpenBTS с открытым исходным кодом, установленного на персональном компьютере под управлением Linux Mint 17.3 и подключенного через USB3.0 с использованием USRP (Universal Software Radio Peripheral) B200.

Ловушка IMSI будет построенна с использованием OpenBTS, установленного на персональном компьютере под управлением Linux Mint 17.3 и подключенного через гигабитное соединение Ethemet к USRP (Universal Software Radio Peripheral) N200. Простое веб-приложение также использовалось для обнаружения ловушек IMSI путем перекрестной проверки соседней BTS в списке.

Поскольку тестовая сеть GSM состоит только из одной соты, нам нужно создать сценарий для фактической BTS, где сота имеет несколько соседей.

В процессе предложенного метода нужно будет выполнить:

- Сформировать отчет, с показаниями измерения соседних BTS, и проанализировать пару ARFCN/BSIC в списке возможных соседних BTS. Если BTS, к которой запрашивается соединение, находится в списке, проверить, отражено ли ее местоположение в отчете и имеет ли она самый сильный сигнал. Если идентифицированной BTS нет в списке, запустить отправку сигнал тревоги на другие BTS.
- Найти в базе данных идентификатор BTS (ARFCN/BSIC позиция BTS. Если BTS нет в базе, то выявлена ловушка IMSI. Далее передать информацию о найденной ловушки на другие BTS и так же сообщить ее статус: активна ли ловушка или нет, используется для роуминга и т.д.
- Рассчитать расстояние до шести ближайших BTS в используемой базе данных Используя расстояние и дополнительный ближайший сосед BTS в базе данных. Главная задача в том, чтобы понять, действительно ли следует использовать сообщаемую соседнюю BTS, и имеет ли она самый сильный сигнал. Если предположить, что мобильный телефон «поймал» ловушку IMSI, то последняя должна обеспечить наиболее сильный сигнал наилучшего качества.

Если ловушка IMSI все еще активна и MS не перемещается при подключении к новой BTS, то сообщаемая соседняя BTS, скорее всего, будет самым сильным соседом, т.е. первой позицией в отчете. Если ловушка IMSI имитирует BTS, расположенную на определенном расстоянии, с несколькими соседними BTS, расхождение между ожидаемым и сообщенным положением будет заметно на шаге 5. 5 будет заметно расхождение между ожидаемой и сообщенной позицией.

Чтобы случайные пользователи не попали в нашу тестовую сеть, открытая регистрация была отключена, и были приняты только два тестовых телефона. Из-за ограничений в OpenBTS в список BA можно передавать только реальных соседей. Это означает, что BA в данном эксперименте состоит только из одного ARFCN — сконфигурированного соседа GSM (ловушка IMSI).

В обычных коммерческих сетях GSM этот VA может содержать до 32 ARFCN. 3, со значениями конфигурации, описанными в табл. 1 список БА должен содержать как минимум следующие ARFCN: 55, 60, 65, 70 и 75. В результате примера IMSI-ловушкой были захвачены два тестовых телефона. После отключения, от которой и последующего подключения к BTS1 результаты измерений отправлялись с мобильной станции (МС) обратно в сеть и отображались в веб-приложении. Поскольку BTS1 не ожидает получения отчетов об измерениях от BTS, был отправлен аварийный сигнал. Кроме того, мы можем видеть, что в этом районе есть четыре ближайших BTS и что BTS5 не считается самым сильным соседом при нормальных обстоятельствах. Расчетное расстояние между BTS1 и заявленной поддельной BTS (BTS5) составляет 2,4 км +\- 1100 метров.

В реальной сети на это решение будут влиять другие параметры, такие как географические характеристики, мощность передачи и помехи. Этот эксперимент был проведен для того, чтобы показать оптимальный сценарий предлагаемого метода IMSI-ловушка может обмануть ближайшую БПС и тем самым попытаться избежать этого обнаружения. Однако, поскольку этот метод обнаружения применяется к каждой BTS в сети оператора, вероятность того, что мобильная станция (MS), пойманная ловушкой IMSI, подключится к BTS, которая не ожидает, что обнаруженная ловушка IMSI будет ее соседом, будет увеличиваться. Веб-приложение предназначено только для демонстрации инструмента и не реализует полный метод, описанный выше, поскольку шаги четвертый и пятый в эксперименте являются наглядными.

Заключение

В приведенном материале был описан метод обнаружения IMSI-ловушек на основании использовании существующих оперативных данных мобильной сети, которые используются в управлении роумингом мобильной станции (MS). Также используются отчеты об измерениях, отправленные мобильной станций (MS) на базовые станции, которые содержат сведения об обслуживающей и соседних сотах, для обнаружения присутствия IMSI-ловушек.

Возможность и удобство использования предлагаемого метода обнаружения демонстрируется простой концепцией, построенной с использованием программного обеспечения для мобильной связи. При проведении дальнейших исследований необходимо расширить доказательство концепции, используя шесть сот и большее количество мобильной станции (MS), для увеличения количества отчетов об измерениях, в следствии, улучшения возможности обнаружения данной угрозы. Тем не менее окончательная проверка будет заключаться том, чтобы протестировать решение реальной мобильной сети и обнаружить встроенный улавливатель IMSI, в моменте, когда происходит захват сотовой мобильные станции.

ЛИТЕРАТУРА

1. А.Н. Степутин, А.Д. Николаев. Мобильная связь на пути 6G (1 Том) 384с.
2. В.И. Данилов. Сети и стандарты мобильной связи // СПбГУТ 2015 100с.
3. Кормильцев Н.В., Уваров А.Д., Корнилов Г.С., Перухин М.Ю. Оптимизация процесса аутентификации для защиты конфиденциальных данных пользователей при подключении к сети LTE / Вестник технологического университета. 2018, т. 21, в.3, с. 134–139
4. Сети мобильной связи LTE технологии и архитектура / В.О. Тихвинский С.В, Тереньев А.Б. Юрчук // Эко-Трендз 2010 390с.

Журнал «Современная наука: актуальные проблемы теории и практики»

г. Красноярск