ИСПОЛЬЗОВАНИЕ GSM-ТЕСТЕРА ДЛЯ ПЕРЕХВАТА ЗВОНКОВ И СООБЩЕНИЙ С МОБИЛЬНЫХ ТЕЛЕФОНОВ

Елистратов К.В.[1], Янгулов И.П.[2]

[1]Елистратов Кирилл Владиславович - студент, ФГБОУ ВО «Пензенский государственный университет»

[2]Янгулов Игорь Петрович - студент, ФГБОУ ВО «Пензенский государственный университет»,

г. Пенза Российская Федерация

Аннотация: *в этой статье представляются как теоретические, так и практические основы перехвата мобильных телефонов с помощью GSM-тестера, и даются ценные рекомендации по безопасности связи.*

Ключевые слова: *GSM, GSM-тестер, перехват, IMSI-ловушка, безопасность, сотовая связь, мобильный телефон, GSM-ретранслятор.*

USING A GSM TESTER TO INTERCEPT CALLS AND MESSAGES FROM MOBILE PHONES

Elistratov K.V.[1], Yangulov I.P.[2]

[1]Elistratov Kirill Vladislavovich - student, «Penza state University»,

[2]Yangulov Igor Petrovich - student, «Penza state University»,

Penza, Russian Federation

Abstract: *this article presents both the theoretical and practical basics of intercepting mobile phones using a GSM tester, and provides valuable recommendations on communication security.*

Keywords: *GSM, GSM tester, interception, IMSI trap, security, cellular communication, mobile phone, GSM repeater.*

УДК 621.395

Перехват звонков по мобильным телефонам раньше был простым упражнением по радиосканированию еще в эпоху первых аналоговых систем. Цифровые системы, такие как GSM, оказались более безопасными, включающими шифрование, и трудноразрешимыми. Однако, как и в случае с любой другой технологией, научное сообщество вскоре начало теоретические

дискуссии о безопасности алгоритмов. Так как злоумышленникам удалось организовывать практические атаки. Существует множество работ, в которых обсуждаются крипто-атаки на сам стандарт GSM или на его всевозможные реализации различными поставщиками связи. Связь по мобильным телефонам GSM может быть легко перехвачена без проведения какого-либо криптоанализа с использованием поддельной базовой станции. Основным недостатком спецификации GSM в этом отношении является то, что в сети отсутствует возможность аутентификации пользователя. Пользователь должен пройти аутентификацию, чтобы получить доступ к сети. Во-вторых, шифрование не является обязательным, и при наличии алгоритма можно согласовать, если базовая станция не поддерживает шифрование, то мобильный телефон может перейти к вызову без него. Таким образом, поддельная базовая станция в непосредственной близости от пользователя без поддержки шифрования (или отключения) - это все, что необходимо для перехвата его связи тратим лицом.

Риски Перехвата

Необходимая настройка в идеале состоит из промышленной базовой станции, такой же, как и та, которая используются сетевыми операторами. Однако эту дорогостоящую установку можно легко заменить, используя какое-нибудь современное оборудование для тестирования GSM. Это оборудование обеспечивает всю необходимую сигнализацию для работы телефонной трубки, а также можно демодулировать голос из цифрового сигнала. Это устройство также может перехватывать IMSI (International Mobile Equipment Identity) SIM-карты пользователя (Subscriber Identity Module) карты и IMEI (International Mobile Equipment Identity) его телефона. В то же время они могут читать короткие сообщения (SMS), которые пытается отправить пользователь. Злоумышленник также может инициировать звонки или отправлять сообщения жертве, свободно выбирая любую личность вызывающего абонента, какую ему заблагорассудится.

Очень интересным фактом является то, что в телефон можно отправлять не только текстовые сообщения, но и конкретные двоичные команды. Такие сообщения обычно ограничены, и только для использования провайдером и

блокируются в случае, если простой пользователь попытается их отправить. С помощью этого оборудования и настроек, представленных в данной статье, эта проверка обходится, и теперь злоумышленник играет роль провайдера, и может отправлять такие сообщения.

Экспериментальная установка и инструменты

Инструменты, необходимые для проведения эксперимента, следующие:

1. GSM-тестер [1, 2], подобный тому, который показан на рис. 1
2. Антенна (GSM-тестеры обычно подключаются специальным кабелем непосредственно к антенне тестируемого телефона, но в нашем случае мы будем передавать на открытом воздухе с помощью антенны)
3. GSM-ретранслятор [4] (опционально, для увеличения эффективной дистанции перехвата)
4. Мобильный телефон с установленным или включенным программным обеспечением для мониторинга (подробнее описано ниже)
5. Второй мобильный телефон или стационарная линия для того, чтобы «направить» перехваченную связь через него. Этот телефон подключен к выходу аудиовыхода/аудиовхода демодулятора, как показано справа на рис. 1.

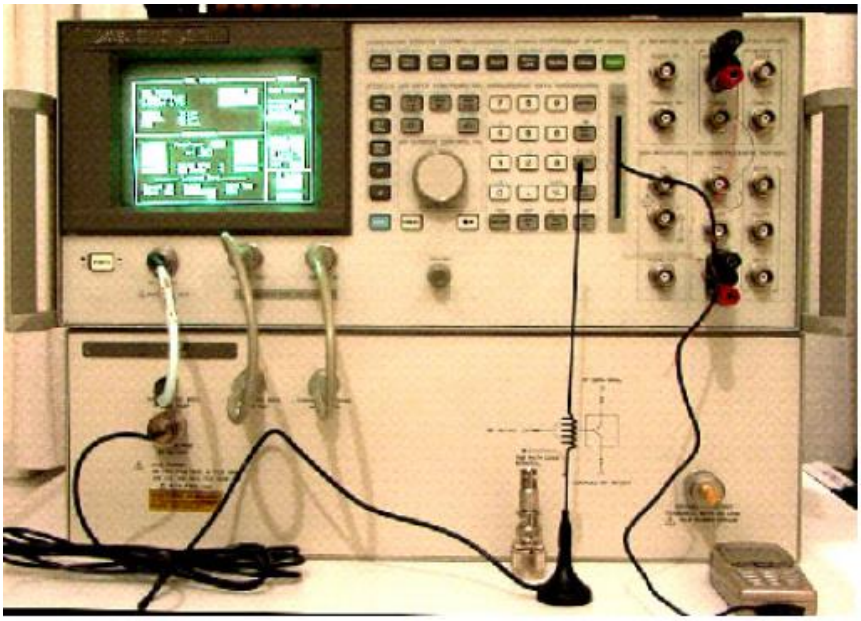

Рис. 1 Типичный GSM-тестер

ПК с последовательным портом IEEE488.2 или другим подключением позволит полностью автоматизировать процесс. В любом случае, детали подключения прямолинейны и не нуждаются в представлении здесь.

Теория и реализация

МСЭ-Т E.212 [5] определяет список кодов мобильных стран (MCC) для использования при идентификации мобильных станций в сетях беспроводной телефонной связи, в частности в сетях GSM и UMTS. Существуют также Коды мобильных сетей (MNC), которые еще больше разделяют операторов в данной стране. Таким образом, комбинация MCC/MNC универсально уникальна для каждого оператора. Эта информация находится в свободном доступе и даже может быть доступна через специальные меню в мобильных телефонах или других диагностических инструментах (Netmonitor).

Первым шагом в нашей демонстрации является установка в базовую станцию - GSM-тестер MCC и MNC оператора SIM-карты мобильного телефона для перехвата.

В таблице 1 показаны соответствующие позиции для России.

Таблица 1. MCC и MNC для России

MCC	Страна	MNC	Сотовый оператор
250	Россия	01	МТС
250	Россия	02	Билайн
250	Россия	06	Мегафон

Затем необходимо использовать режим Netmonitor (или инженерное меню), о котором упоминалось ранее, - это специальный режим (или приложение) в мобильных телефонах, используемый для измерения рабочих параметров и состояния работы сети и телефона [6]. При активации в старых телефонах обычно появляется новое дополнительное меню, содержащее огромное количество информации. Новые телефоны имеют приложения, которые могут быть установлены для той же цели. Следует отметить, что каждый

телефон имеет разные возможности в отношении Netmonitor и существуют разные методы активации.

Продолжая процесс, наиболее важной подсказкой, которую дает Netmonitor для нужд эксперимента, являются ARFCN (absolute RF channel numbers), в которые близлежащие базовые станции GSM BCCH передают данные. На рисунке 2 представлен экран телефона с приложением Netmonitor, предоставляющий информацию о BCCH (broadcast control channels) в непосредственной близости от телефона.

BCCH - это канал сигнализации, который передает информацию об идентификации, конфигурации и доступных функциях базовой станции. Мобильные телефоны непрерывно «прослушивают» этот широковещательный сигнал, чтобы иметь возможность общаться с сетью GSM. Этот канал также предоставляет список ARFCN (absolute radio-frequency channel number), используемых соседними BTS.

Рис. 2. Netmonitor, отображение соседних каналов

Рис. 3. Телефон жертвы подключен к поддельной базовой станции

Рис. 4. Подробные данные IMSI, IMEI и номера вызова жертвы, доступные для GSM- тестера

Итак, вторым шагом к запуску атаки было бы дать указание нашей поддельной базовой станции передавать данные по одному из этих радиочастотных каналов, эффективно маскируя законные сигналы и захватывая контроль над близлежащими мобильными телефонами.

Как видно на рис. 3, через несколько мгновений после срабатывания GSM - тестера телефон «жертвы» подключается к нашей поддельной базовой станции в соответствии с процедурами стандартов GSM [7, 8, 9]. А именно, GSM-тестер передает в канале 84 (который был уже выбран мобильным телефоном до «вторжения», как показано на рис. 2). Полученный сигнал от GSM-тестера перекрывает законный сигнал, так как наш передатчик находится намного ближе, чем антенна базовой станции сетевого провайдера. Также интересно отметить, что в определенной настройке мы проинструктировали BCCH из GSM-тестера не выдавать какие-либо другие BCCH (следовательно, остальные соседние каналы заполнены 00).

После этого каждая попытка вызова, исходящая с мобильного телефона, будет регистрироваться нашим оборудованием. На рис. 4 мы видим, среди

прочего, что IMSI, IMEI и номер, который пытается набрать пользователь, декодируются. Нужно просто набрать запрошенный номер (444444 в нашем примере) по телефону «жертвы», используя второй телефон, который фактически наберет вызов, направляя сообщение, как в классической концепции человека в середине атаки.

Решение проблемы

Инженеры GSM предположили, что отсутствие шифрования, в будущем приведет к тому, что телефон находится под возможным перехватом, следовательно, об этом необходимо сообщить пользователю. Это можно было бы достичь с помощью специального индикатора (рис. 5).

Рис. 5. Индикатор (отсутствие) шифрования

Как мы видим, очевидно, потребовалось много времени, чтобы эта обязательная функция появилась, и даже сейчас не все производители используют ее. Большинство производителей телефонов реализуют этот механизм с помощью значка или загадочного символа, значение которого пользователь должен сам понять (например, восклицательный знак или разблокированная панель). Что еще хуже, сами пользователи (более 80% из них) совершенно не знают о существовании этого показателя [10].

Таким образом, мы рассмотрели и продемонстрировали в этой статье, что злоумышленник с ограниченным знанием деталей GSM может легко перехватить связь близлежащих сотовых телефонов (голос и sms). Кроме того,

он может инициировать телефонные звонки и короткие сообщения, выбирая любую личность по своему усмотрению, эффективно маскируясь. Основная проблема - отсутствие сетевой аутентификации, которая вытекает из самого стандарта. Проблема с уведомлениями, которая так часто реализуется, может быть легко улучшена, чтобы предупреждать пользователей, когда такое происходит нападение. Мы надеемся, что в дальнейшем, исходя из исследований текущих телефонов на рынке, производители сделают основой упор на то, чтобы перейти к более совершенным телефонам и графическим пользовательским интерфейсам, которые, даже если и не будут полностью безопасными, по крайней мере, будут достаточно информативными при атаке [11].

Список литературы

1. Руководство пользователя набора GSM-тестов Agilent Technologies 8922 M/C. Agilent 08922-90211
2. Руководство пользователя по Тестированию Цифрового Радиоприемника Racal 6103B. Racal Instruments Ltd
3. Особенности радиоперехвата сообщений APCO P25 в России, Дмитрий Сергеевич Сильнов Кафедра информационных систем и технологий, Национальный исследовательский ядерный университет "МИФИ" (Московский инженерно-физический институт), Москва, Россия (Июнь 2016)
4. Qixiang Electron Science & Technology Co. Ltd.: AnyTone AT-400 GSM. Повторитель руководство пользователя, Китай (2006)
5. МСЭ-Т E.212: МЕЖДУНАРОДНЫЙ СОЮЗ ЭЛЕКТРОСВЯЗИ (Май 2008 года)
6. Страница Марцина В Интернете. [Электронный ресурс] – URL: http://www.mwiacek.com/ (Дата обращения: 1 ноября 2008 года).
7. Цифровая Система Сотовой связи (Фаза 2): Интерфейс Мобильной Радиосвязи Спецификация уровня 3 (GSM 04.08). Док. ETS 300 557 (1997)
8. Цифровая Система Сотовой Связи (Фаза 2+): Канал Радиоподсистемы Управление (GSM 05.08 v. 8.5.0 выпуска 1999 года). Док. ETSI TS 100 911 v. 8.5.0 (2000 -10) (1999)
9. Цифровая система сотовой связи (Фаза 2+): Функции, связанные с Мобильная станция (MC) в режиме ожидания и в режиме группового приема, (GSM 03.22 v. 8.3.0 Выпуск 1999 года). Док. ETSI TS 100 930 v. 8.3.0, (2000-01) (1999)

10. Андрулидакис И., Кандус Г.: Уровень осведомленности пользователей и практика в области безопасности мобильных телефонов, количественный опрос в 10 странах и 17 университетах (в процессе представления, 2010)
11. Андрулидакис, И., Кандус, Г.: Графические интерфейсы мобильных телефонов против атак "человек посередине" (или история криптографического бита OFM) (в процессе представления, 2011)