Воробьев Данил Сергеевич
студент
Койков Данил Сергеевич
студент
ФГБОУ ВО «Омский государственный
технический университет»
г. Омск, Омская область

ИСТОЧНИКИ УГРОЗ В GSM-СИСТЕМЕ

Аннотация*: в данной статье представлены источники угроз в сетях GSM и описаны методы борьбы с ними.*

Ключевые слова*: GSM, базовые станции, информационная безопасность.*

Многие эксперты в области систем связи пророчат о скором исчезновении системы GSM, но несмотря на это данная система продолжает существовать и активно развиваться.

Сотовая связь уже давно проникла в нашу жизнь, и колоссальные темпы роста и развития мобильных устройств являются этому подтверждение. Ежедневно миллионы людей в коммерческих и личных целях используют сети GSM. И более чем в 99% случаях всё проходит благополучно, однако забывать об источниках угроз в сотовых сетях не стоит.

Многие GSM компании, которые непосредственно имеют многолетний практический опыт, не понаслышке знают о том, как осуществляется перехват GSM сигнала, а также как злоумышленники могут дистанционно взломать SIM-карту (англ. Subscriber Identification Module – модуль идентификации абонента) и многое другое. Одной из основных задач таких компаний является защита конфиденциальности общения абонентов от несанкционированного вторжения.

Осуществление перехвата трафика и потока информации, идущие к абоненту, для злоумышленников давно уже не является серьёзной проблемой. Требуемое для данных операций оборудование может являться модифицированный мобильный телефон. Имитация сети является возможностью отправки

мошеннических данных и (или) сигнальных сообщений другому пользователю с целью их появления в подлинной сети. MITM (англ. Man-In-The-Middle – атака посредника, или атака «человек посередине») – это способность злоумышленника поставить себя между сетью и законным пользователем, чтобы подслушивать, изменять, удалять и подделывать сигнальные данные между двумя сторонами. Для этого требуется модифицированная BTS (Base Transceiver Station – базовая приемо-передающая станция) в сочетании с модифицированным мобильным телефоном. Подслушивание и имитация пользователя были единственными проблемами, известными в то время, когда была разработана защита 2G. Однако на сегодняшний день безопасность в сетях 3G и 4G направлены на защиту от всех проблем.

Основной мошеннической деятельностью является использование «слабых мест» для финансовой выгоды (свободный доступ к ресурсам, бесплатные междугородние звонки и т. д.). Любые атаки серьёзны и наносят ущерб сетевому оператору, атаки типа «отказ в обслуживании» безусловно являются самой серьёзной угрозой. Лицо, нацеленное против уязвимой организации, может парализовать трафик на больших площадях, в результате чего достаточно трудно оценить финансовые потери. Для того, чтобы атаковать сеть GSM, злоумышленник должен сначала иметь возможность вмешаться в прошивку телефона таким образом, чтобы атака была возможной. Это нетривиальная задача, которая требует обширных знаний о конкретной реализации мобильного устройства, встроенного кода и технических характеристик GSM. Злоумышленник также должен получить представление о топологии сети. Если целевой район является локальным, простой прогулки по городу достаточно, чтобы определить приблизительные места, где расположены базовые приемопередающие станции (BTS) и где будут работать вредоносные мобильные станции. Злоумышленник не обязательно должен присутствовать, поскольку мобильный телефон можно предварительно запрограммировать для запуска атаки, а городской пейзаж предоставляет множество мест, где можно спрятать такие маленькие устройства.

Одной из серьёзных ошибок в GSM системе является то, что сама сеть не аутентифицирует себя на телефоне и таким образом позволяет перехватывать данные во время сеанса связи абонента. Эта слабость была известна для проектировщиков GSM во время её конструкции, но было предположено, что строить ложные BTS будет дорого, и было бы трудно сделать атаки на них экономически эффективными. Однако на сегодняшний день существуют компании, производящие BTS в коротком диапазоне в следствии чего злоумышленник может просто купить её.

Ещё одной серьёзной уязвимостью GSM является отсутствие правильного идентификатора вызывающего абонента или отправителя. Другими словами, номер вызывающего абонента или номер отправителя SMS может быть подделан. Имитация АОН (Автоматический определитель номера) также является проблемой GSM. Самые популярные способы имитации АОН (Автоматический определитель номера) через использование PRI линии (Primary Rate Interface – стандартный интерфейс сети ISDN (англ. Integrated Services Digital Network – цифровая сеть с интеграцией служб)). Интерфейс первичной скорости – это интерфейс доступа к ISDN. Он был разработан для средств предприятий с цифровыми АТС для предоставления им доступа к коммутируемому телефонному аппарату. Линии PRI состоят из каналов B и D. Каналы B – это первичные данные или голосовые каналы связи, в то время как D-каналы предназначены для управления информацией. PRI линии уязвимы для подмены, поскольку голос отправляется через канал B, в то время как идентификатор вызывающего абонента отправляется через канал D. Другими словами, АОН в канале D является дополнительной информацией для передачи голоса в канале B и установки его фиктивного значения не нарушает трафик в голосовом канале. Этот факт обычно используется предприятиями для отображения одного основного номера телефона на все исходящие вызовы. Из-за высоких цен линии PRI были недоступны частным лицам, и он использовался главным образом предприятиями. Ситуация изменилась с ростом популярности Технология VoIP (англ. Voice over IP; IP-телефония – это вид телефонной связи, который обеспечивает передачу звукового сигнала по сети

Интернет или по другим IP-сетям). VoIP легко уязвим для подмены, поскольку голос отправляется через IP-пакет и установка ложного значения идентификатора вызывающего абонента не влияет на маршрутизацию IP-адресов.

В последствии анализа безопасности GSM можно видеть, что сеть не может обеспечить надежную защиту для своих пользователей. Разработчики GSM недооценили прогресс публичной криптографии, а компьютеры ускоряют прогресс, и в то же время они переоценили свою способность хранить технологии в тайне. Результаты GSM-сбоев в основном идут из комбинации алгоритмов проектирования в области безопасности. К счастью для большинства пользователей GSM, проблемы невелики. Серьезные угрозы, такие как прослушивание телефонных разговоров по-прежнему нелегко выполняется и более легкие атаки, такие как обход АОН не стали очень популярными среди мошенников, так что случайный пользователь телефона все еще может чувствовать относительно безопасно. Тем не менее, те, кто использует GSM для конфиденциальной информации, должны в первую очередь использовать специальные сотовые телефоны с собственной системой шифрования. На современном рынке предлагают множество решений, начиная с дорогих криптофоны для правительства или военных и заканчивая относительно дешевым шифрованием (программным обеспечением) для телефонов Symbian или Windows Mobile, чтобы каждый мог подобрать для себя то, что удовлетворит его потребности.

Список литературы

1. Источники угроз в системе GSM и защита от них [Электронный ресурс]. – Режим доступа: https://habr.com/company/tottoli_gsm/blog/269407/ (дата обращения: 05.12.2018).

2. Угрозы GSM [Электронный ресурс]. – Режим доступа: http://club.cnews.ru/blogs/entry/istochniki_ugroz_v_sisteme_gsm/ (дата обращения: 05.12.2018).

3. Безопасность сетей связи стандарта GSM [Электронный ресурс]. – Режим доступа: http://www.comprice.ru/articles/detail.php?ID=41090/ (дата обращения: 05.12.2018).