А. В. Новицкий, Д. М. Михайлов, А. В. Стариковский, А. В. Зуйков

УЯЗВИМОСТИ СТАНДАРТА GSM И ПРОСЛУШИВАНИЕ ТЕЛЕФОННЫХ РАЗГОВОРОВ

С момента своего появления любые телекоммуникационные средства постоянно подвергаются атакам нескольких типов:

- перехват информации, когда устройство злоумышленника является пассивным приемником;
- подделка сообщений, когда это устройство является активным и отвечает вместо одного или нескольких участников обмена данными;
- DoS — Denial of Service — отказ в обслуживании.

Не является исключением и мобильный телефон. Наиболее распространенной атакой в данном случае — перехват: именно на нем изначально были сконцентрированы усилия взломщиков и именно в этой области ими были достигнуты самые значительные результаты (в отличие от средств защиты, которые годами не меняются и не адаптируются к новым методам прослушивания).

Перехват данных, передаваемых мобильным телефоном, в частности прослушивание разговоров абонентов, может происходить на различных этапах передачи сообщений.

— Информация, которую пользователь произносит при разговоре, может быть перехвачена злоумышленником с помощью прослушивающих устройств, направленных микрофонов и других технических средств.

— В телефон может быть внедрена вирусная программа, перехватывающая входящий и исходящий аудиопоток и либо передающая его с использованием сетевых возможностей телефона, либо сохраняющая разговор на мобильном устройстве для последующей отправки на персональный компьютер при подключении к нему телефона.

— Радиоканал, по которому передаются данные от телефона к базовой станции сотового оператора, может прослушиваться на достаточно большом (десятки метров) расстоянии от мобильного устройства.

— Затем данные передаются по проводным сетям, к которым также можно осуществить подключение.

После передачи голосового сообщения базовой станции, к которой подключен другой участник разговора, повторяется передача по радиоканалу, а затем по электрическим цепям внутри устройства в динамик.

Наиболее распространенные методики при атаке на мобильный телефон — его заражение вирусом или прослушивание радиоканала.

Вирусы для мобильных платформ являются относительно недавней проблемой и в ближайшем будущем могут стать реальным средством прослушивания разговоров, если разработчики безопасных решений не обратят внимания на проблемы мобильного сектора информационных устройств. Уже сейчас вирусы атакуют мобильные телефоны одним из следующих способов:

- с другого устройства посредством Bluetooth-соединения;
- через полученное MMS-сообщение;
- с персонального компьютера (через любое доступное соединение — Bluetooth, USB, Wi-Fi);
- при посещении web- или wap-сайтов.

Однако сегодня основным средством прослушивания является перехват радиоканала.

Сетевые анализаторы для радиоинтерфейсов появляются практически сразу с выходом стандарта на этот интерфейс, это произошло и с GSM.

Казалось бы, проблему легко решить, шифруя трафик, идущий по беспроводному каналу, что, собственно, и было реализовано. Но используемые шифры группы A5 поддаются взлому

либо в реальном времени, либо в течение суток, т. е. за период времени, когда информация еще не потеряет свою актуальность. Причем даже этот слабый механизм защиты может быть отключен, если на базовой станции введен так называемый полицейский режим.

Еще одной проблемой стандарта GSM является отсутствие механизмов аутентификации как «абонент — абонент», так и «абонент — базовая станция». Мобильный телефон просто подключается к сотовой станции с максимальным уровнем сигнала. Это позволяет злоумышленнику, обладающему собственной мобильной базовой станцией, приблизившись к телефонному аппарату таким образом, чтобы сила сигнала его станции была заведомо выше, чем сила сигнала «настоящих» базовых станций, вынудить телефон подключиться к нему. Такая технология получила название «виртуальная сота».

При ее использовании злоумышленник получает следующие возможности:

- прослушивать разговор в реальном времени;
- перехватывать SMS- и MMS-сообщения;
- перехватывать интернет-трафик через GPRS и EDGE, перенаправлять пользователя на собственные web-ресурсы;
- подключаться к телефонным разговорам;
- перенаправлять звонки и сообщения.

Виртуальная сота является одним из самых мощных средств атаки на мобильные телефоны, в то время как механизмы защиты от ее использования не предусмотрены ни стандартами GSM, ни встроенными средствами мобильных устройств.

Рассмотрим подробнее возможные признаки, по которым можно обнаружить факт прослушивания устройства с помощью виртуальной соты [1].

— Устройство переключилось на новую соту при высоком уровне сигнала предыдущей. Факт изменения можно зафиксировать с помощью идентификатора базовой станции, уникального для каждой вышки.

— Телефон часто переключается между двумя сотами. Это может означать «конкуренцию» между настоящей базовой станцией и виртуальной сотой.

— Устройство длительное время подключено к одной и той же соте. Этот факт однозначно говорит о подключении к виртуальной соте, если телефон перемещается. Для регистрации перемещения можно использовать GPS-модуль.

— Аппарат подключен к одной соте, в то время как идентификаторы сот с более слабым сигналом (которые также регистрируются большинством современных телефонов) меняются. Этот факт аналогичен предыдущему, однако не требует использования GPS-модуля для проверки.

— Идентификатора вышки, к которой подключен телефон, нет в базе станций данного оператора или ее координаты не совпадают с положением телефона (такие базы, как правило, открыты и доступны).

Разумеется, все это лишь косвенные признаки, однако создание более совершенных механизмов должно начинаться с пересмотра стандартов связи GSM.

Иногда для получения нужной информации достаточно просто ответить на телефонный звонок вместо того человека, которому он предназначается. Это становится возможным из-за уязвимости стандарта GSM, а конкретно — его управляющего (или сигнального) протокола SS7 (известного также как ОКС-7 в России и CCSS-7 в США), который был разработан для определенной закрытой системы и поэтому функции аутентификации не были реализованы должным образом [2]. Конвергенция телефонных сетей общего пользования, Интернета и беспроводных сетей значительно увеличила уровень потенциальных рисков безопасности систем на базе SS7. Этот протокол позволяет устройству злоумышленника представиться базовой станции

любым телефонным номером и получать все входящие звонки и сообщения, предназначенные этому абоненту.

Все перечисленные уязвимости являются прямым следствием недостатков GSM, и их фундаментальное решение требует переработки самого стандарта. В то же время обеспечивать безопасность мобильных устройств необходимо уже сегодня. Некоторые задачи можно решить на уровне программного обеспечения мобильного телефона:

- защита от вирусов — антивирусные системы, контроль над действиями приложений на уровне ядра;
- защита от хакерских атак — сетевые экраны;
- обнаружение подключения к виртуальной соте — приложения, реализующие описанные алгоритмы определения виртуальной соты;
- системы безопасной мобильной связи — устройства, использующие телефон как модем и реализующие свои функции шифрования и аутентификации поверх встроенных в аппарат.

Поскольку мобильный телефон как вычислительная платформа все же далеко отстоит по производительности от персональных компьютеров, внедрение первых трех средств как отдельных программных продуктов может быть проблематичным. Имеет смысл реализовать их как составную часть мобильной операционной системы. На данный момент на рынке отсутствуют подобные «доверенные» отечественные операционные системы.

Создание такой системы становится все более актуальным с каждым днем, так как роль мобильного телефона в повседневной деятельности человека постоянно возрастает, равно как и объем конфиденциальных данных, которые проходят через него в различной форме, будь то речь, фотографии или документы, в то время как уровень безопасности, обеспечиваемый стандартами связи, только падает за счет обнаружения все новых уязвимостей и создания новых видов оборудования для взлома.

СПИСОК ЛИТЕРАТУРЫ:

1. *Lambert M.* OpenBTS / Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow (Ed.). Betascript publishing, Düsseldorf 2011.
2. *Travis R.* Signaling System 7. 5th ed. The McGraw-Hill Companies, New-York, 2006.