А. В. Зуйков, Д. М. Михайлов, А. В. Стариковский, М. И. Фроимсон

ПРОСЛУШИВАНИЕ РАЗГОВОРОВ АБОНЕНТОВ МОБИЛЬНЫХ СЕТЕЙ

Глобальное распространение мобильных технологий связано с появлением все новых опасностей, угрожающих владельцам сотовых телефонов. Одним из важнейших аспектов информационной безопасности является обеспечение конфиденциальности передаваемых данных. К сожалению, существующие на сегодняшний день мобильные устройства не могут предоставить должного уровня защищенности данных.

Практически во всех существующих в настоящий момент мобильных телефонах передача голоса осуществляется с помощью стандарта GSM, встроенная защита которого, к сожалению, не безупречна. Основа системы безопасности GSM — три секретных алгоритма, которые сообщаются лишь поставщикам оборудования, операторам связи и т. д. A3 — алгоритм авторизации, защищающий телефон от клонирования, A8 — «сервисный» алгоритм, который генерирует криптоключ на основе выходных данных алгоритма A3, и, наконец, A5 — алгоритм шифрования оцифрованной речи для обеспечения конфиденциальности переговоров.

Существует несколько модификаций шифра A5, из которых наиболее распространены A5/1, используемый в США и странах Евросоюза, и A5/2, алгоритм с пониженной криптостойкостью, применяемый для шифрования связи в странах, не входящих в Евросоюз (в том числе и в России).

Рассмотрим подробнее функционирование шифра A5/1.

В GSM во время разговора от абонента к базовой станции и в обратном направлении передается последовательность кадров. Каждый кадр шифруется с помощью сессионного ключа K длиной 64 бита (общий ключ для всего разговора) и номера кадра Fn (известное число), которые используются для начальной инициализации генератора псевдослучайной последовательности. Биты с выхода генератора используют для операции XOR с передаваемым сообщением.

В A5/1 используются три регистра сдвига с линейной обратной связью с длинами 19, 22 и 23 бита, которые обозначаются как R1, R2 и R3 соответственно (рис. 1). Все три регистра являются регистрами сдвига

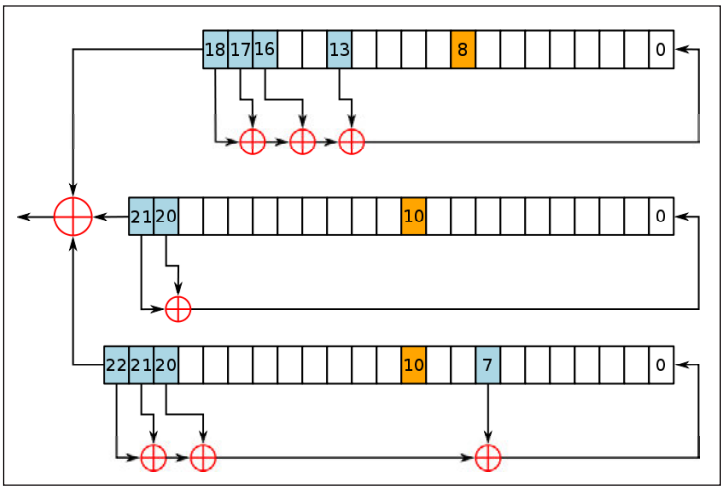

Рис. 1. Система регистров в алгоритме A5/1

максимального периода с периодами 2^19-1, 2^22-1, 2^23-1. Каждый такт вычисляется мажоритарная функция от битов синхронизации всех трех регистров, на основе которой выполняется управление тактированием.

Сеансовый ключ, используемый для начального заполнения генератора псевдослучайных последовательностей, вырабатывается с помощью алгоритмов A3 и A8 на основе ключа аутентификации пользователя (уникального номера, присваиваемого каждому абоненту в сети), а также случайного числа RAND, формируемого базовой станцией оператора в качестве запроса аутентификации.

Рассмотренные стандарты шифрования обладают уязвимостями, резко ослабляющими защиту, а именно:

- 10 бит сессионного ключа принудительно занулены;
- отсутствуют перекрестные связи между регистрами в A5/1 (кроме регистра управления сдвигами);
- количество шифруемой служебной информации, известной криптоаналитику, избыточно;
- свыше 40 % ключей приводит к минимальной длине периода генерируемой последовательности, а именно $\frac{3}{4}(2^{23}-1)$ [1, 2].

Из-за перечисленных конструктивных дефектов сложность полного перебора составляет не 2^64, а всего 2^40, что позволяет взломать алгоритм и вычислить сеансовый ключ связи за приемлемое время.

Несмотря на то что данный шифр позволяет защититься от прослушивания телефонных разговоров пользователя в реальном времени, остается угроза расшифровки записанных злоумышленником разговоров, что в случае особой важности передаваемой информации и ее актуальности в течение достаточно долгого времени является не менее опасным.

Таким образом, даже использование считающегося стойким к взлому алгоритма A5/1, не говоря уже о его ослабленных модификациях, не может гарантировать конфиденциальность переговоров абонентов.

Кроме того, при аутентификации телефона в сети сессионный ключ Kc не зависит от протокола шифрования, что позволяет злоумышленнику, обладающему необходимым оборудованием, прослушать зашифрованный разговор, не прибегая к взлому рассматриваемого шифра. Для этого он может перехватить трафик абонента, использующего A5/1, а затем с помощью ложной базовой станции инициировать соединение с атакуемым мобильным телефоном. Для установления связи понадобится случайное число, и злоумышленник может отправить число RAND, которое использовалось в перехваченном звонке. При этом сессионный ключ Kc будет таким же, как и в предыдущем случае. Если же теперь ложная базовая станция потребует от телефона шифрования в слабом режиме A5/2, который легко вскрывается, то атакующий сможет вычислить сессионный ключ и расшифровать интересующий его разговор, при этом пользователь даже не заметит факта подключения.

Таким образом, встроенные в GSM механизмы обеспечения безопасности голосовых данных не гарантируют защиту от их перехвата.

В качестве доверенного устройства для ведения конфиденциальных переговоров может выступать беспроводная Bluetooth-гарнитура, осуществляющая шифрование данных с помощью другого, более стойкого алгоритма и их передачу с использованием технологии CSD (Circuit Switched Data). При этом на телефон будет отправляться уже защищенная информация, что позволит предотвратить перехват данных на всех этапах их передачи. В данном случае телефон используется в качестве модема, через который осуществляется связь абонентов с помощью уже зашифрованных пакетов голосовых данных, что защищает передаваемую информацию от взлома даже при использовании виртуальных базовых станций.

В случае программной реализации шифрования голоса на телефоне разговор может быть перехвачен троянскими приложениями, установленными на нем. Отдельное устройство позволяет обеспечить доверенную среду обработки еще не защищенных данных.

Проводная же гарнитура не сможет перевести телефон в режим модема для использования CSD-канала и будет использовать шифрование аналогового сигнала (например, скремблирование), которое является заведомо уязвимым, создает задержку при восстановлении и помехи в исходном сигнале. Таким образом, только использование специально разработанной беспроводной гарнитуры позволит гарантировать безопасность мобильного телефона и конфиденциальность передаваемой информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Fast Software Encryption — Second International Workshop, December 1994. P. 154–170.
2. *Eli B., Dunkelman O.* Cryptanalysis of the A5/1 GSM Stream Cipher // Indocrypt 2000. P. 43–51.