Активная атака на шифры семейства A5.

Ибрагимов Адиль, группа 015.
Май 2004.

Вступление.

В наши дни уже никого не удивишь сотовым телефоном. Это средство связи прочно вошло в нашу повседневную жизнь, став предметом обихода. По мобильнику часто договариваются о встрече друзья, мило болтают влюблённые, ищут своих загулявшихся чад родители…. Но не только - по телефону часто ведутся деловые переговоры, в разговоре может ненароком проскочить информация, которая является коммерческой тайной. Насколько обоснована уверенность в конфиденциальности разговоров? Давайте поговорим о безопасности в сотовых сетях самого распространенного формата GSM.

Предварительно нужно сделать замечание, что безопасность в сотовых сетях можно разбить на три составляющие – идентификация, аутентификация и шифрование данных.

Идентификация нужна для проверки того, что тот человек, который в данный момент использует телефон, имеет право это делать. Обычно при включении телефона необходимо ввести специальный код, который знает владелец телефона и, может быть, несколько человек, которым позволено использовать этот телефон. Идентификация предназначена в первую очередь для защиты денег абонента на его счету в сотовой компании. В GSM отсутствует стандарт идентификации, её реализация зависит от конкретного производителя телефона и модели.

Аутентификация нужна для установления подлинности номера, с которого происходит звонок. Аутентификация происходит каждый раз при подключении абонента к системе сотовой связи. В стандарте GSM аутентификация происходит по алгоритму A3. Кроме того, имеется алгоритм A8 для генерации сеансового ключа. Алгоритмы A3 и A8 встроены в SIM-карту телефона и могут отличаться у разных сотовых операторов. Кратко алгоритм регистрации телефона в сети можно описать следующим образом. Телефон посылает базовой станции запрос на аутентификацию и получает в ответ случайное число RAND. Затем с помощью алгоритма A3 (однонаправленная ключевая хеш-функция) по значениям RAND и Ki (собственный индивидуальный ключ SIM-карты) формирует SRES (Signed RESult – подписанный результат). Базовая станция также вычисляет SRES (Ki берется из базы данных сотового оператора) и сравнивает его с полученным значением. В случае совпадения считается, что телефон идентифицировал себя и начинается подготовка к обмену информацией. Алгоритм A8 превращает часть выхода A3 в сеансовый ключ Kc для шифрования во время разговора.

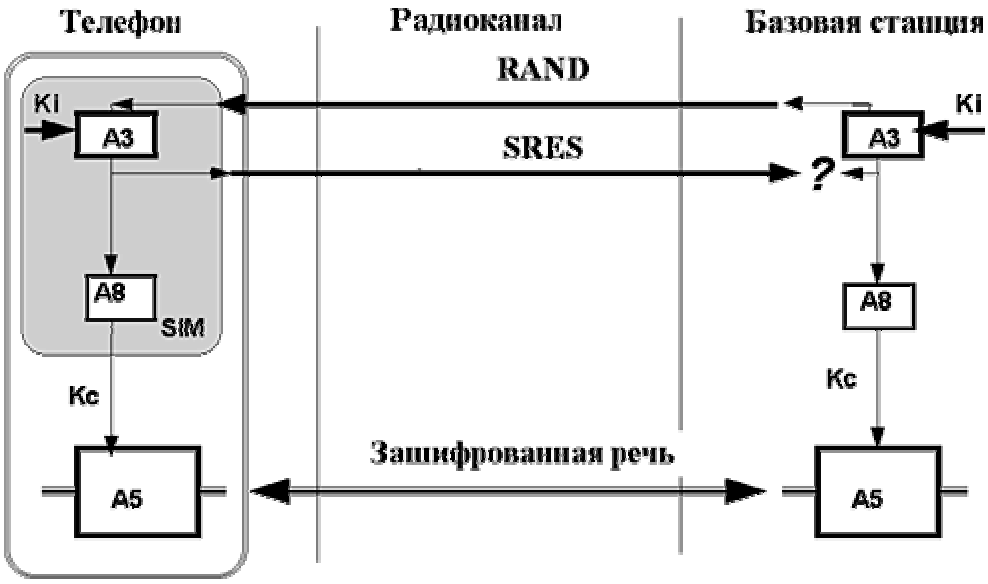

рис. 1. Схема идентификации в системе GSM.

После того как пользователь подтвердил свою личность введением кода, и телефон аутентифицировался в сети, пользователь может производить звонки и передавать информацию (голосовую или цифровые данные с помощью GPRS). Так как сигнал передается по радиоканалу и перехватить его не сложно (причем факт перехвата останется незамеченным для абонента), то для обеспечения конфиденциальности необходимо применять **шифрование данных**. Следует заметить, что в GSM данные шифруются только на «эфирном» участке передачи от телефона до базовой станции, далее они передаются по проводам в незашифрованном виде. В GSM для шифрования данных используется семейство протоколов A5. A5/0 – передача данных без шифрования. A5/1 – «сильная» версия шифра для «избранных» стран (США, страны Западной Европы и ещё несколько стран). A5/2 – ослабленная версия для всех остальных стран (в том числе и для России). A5/3 – модернизированная версия шифра A5/1, разработанная после компрометации шифров A5/1 и A5/2 с использованием алгоритма Касуми.

Шифры семейства A5.

Шифр A5/0.

В этой модификации шифра шифрование отсутствует. Разговор передаётся прямым текстом без шифрования. Соответственно разговор может быть прослушан при наличии у криптоаналитика простого сканера радиочастот соответствующего диапазона.

Шифр A5/1.

В GSM во время разговора посылается последовательность кадров каждые 4.6 мс. Каждый кадр состоит из 114-ти бит информации от Абонента к Базовой станции и 114-ти бит от Базовой станции к Абоненту. Каждый новый разговор может быть зашифрован новым сессионным ключом K. Для шифрования каждого кадра используется сессионный ключ K и номер кадра Fn (известное число), эти два числа служат для начальной инициализации генератора псевдослучайной последовательности. Биты с выхода генератора используют для операции XOR с передаваемым сообщением.

В A5/1 используется три регистра сдвига с линейной обратной связью с длинами 19, 22 и 23 бита, которые обозначаются как R1, R2 и R3 соответственно. Самый младший бит регистра называется нулевым битом. Обратная связь в регистре R1 осуществляют биты 13, 16, 17, 18; в R2 – 20, 21; в R3 – 7, 20, 21, 22. При сдвиге регистра значения битов обратной связи подвергается операции XOR и результат записывается в нулевой бит

сдвинутого регистра. Все три регистра являются регистрами сдвига максимального периода с периодами 2^{19}-1, 2^{22}-1, 2^{23}-1 соответственно. Управление сдвигом регистров происходит с помощью следующего мажоритарного правила: каждый регистр имеет один бит «синхронизации» (бит 8 для R1, бит 10 для R2 и бит 10 для R3). Каждый такт вычисляется мажоритарная функция от трёх битов синхронизации F(x,y,z)=x*y+x*z+y*z (* - логический AND, + - логический OR) и на данном такте сдвигаются только те регистры, в которых биты синхронизации совпадают с F.

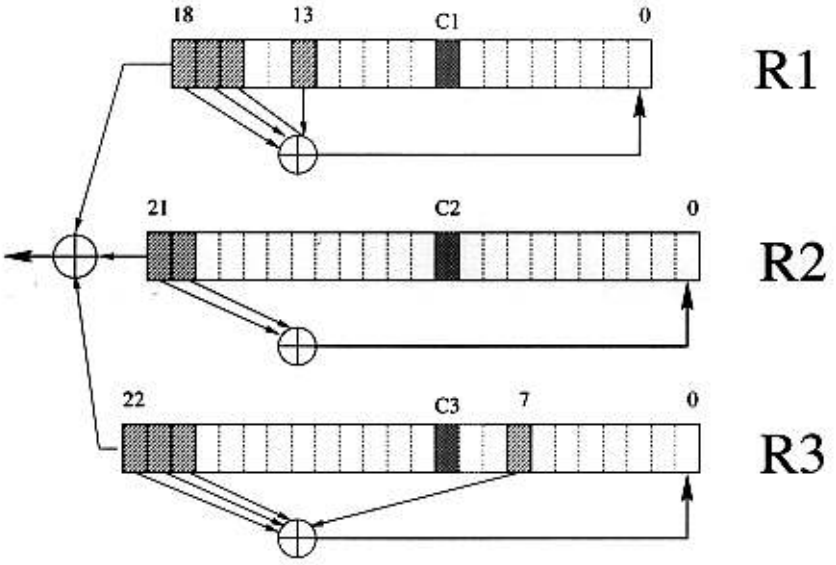

рис. 2 структура шифра A5/1.

Процесс генерации псевдослучайной последовательности из сессионного ключа K и счетчика кадров Fn состоит из четырёх шагов:

- В начале каждый из регистров равен нулю, затем производится 64 такта (причём без управления сдвигом). Во время этого шага на каждом такте каждый бит K (от младшего к старшему) XOR-ится с младшим битом каждого регистра.
- Производится ещё 22 такта (опять без управления сдвигом), причем младшие биты регистров XOR-ятся с битами Fn (от младшего к старшему). Состояние регистров в конце этого шага называется начальным состоянием кадра.
- Производится 100 тактов с управлением сдвигом, но без генерирования выходной псевдослучайной последовательности.
- Производится 228 тактов с управлением сдвигом и генерируются 228 бит выходной последовательности. На каждом такте генерируется один выходной бит как XOR старших битов трёх регистров.

Шифр A5/2.

Алгоритм A5/2 отличается то A5/1 более слабой системой шифрования, он специально создавался как экспортный вариант для стран, не входящих в Евросоюз. В A5/2 добавлен ещё один короткий регистр длиной 17 бит, который управляет движением бит в остальных трёх регистрах. Вагнеру и Голдбергу очень быстро удалось продемонстрировать, что в этих условиях для вскрытия системы достаточно лобовым перебором (сложность 2^{16}) отыскать заполнение управляющего регистра. Делается это всего по двум фреймам сеанса связи длиной по 114 бит (в системе GSM первые два фрейма шифрпоследовательности известны, поскольку шифруются одни нули). В атаке на A5/2 используются слабости в комбинирующей функции, которые позволяют по выходной последовательности получить информацию об отдельных входных

последовательностях узла усложнения. В этом случае говорят, что имеется корреляция между выходной последовательностью и одной из внутренних последовательностей. Вследствие такой корреляции отдельная внутренняя последовательность может быть проанализирована индивидуально вплоть до восстановления начального заполнения соответствующего регистра, затем внимание надо переключить на одну из других внутренних последовательностей. Подобным способом может быть восстановлен весь генератор - этот метод часто называют атака "разделяй-и-вскрывай". Причем первым из регистров надо выбрать тот, который проще чем остальные восстановить. Другими словами, вскрытие такого шифра осуществляется что называется "на лету", за 15 миллисекунд работы современного персонального компьютера.

Шифр A5/3.

Алгоритм A5/3 более стоек по сравнению с A5/1. Базой для A5/3 служит алгоритм Касуми, утвержденный 3GPP для использования в третьем поколении мобильных систем в качестве ядра для алгоритмов конфиденциальности и целостности информации. Касуми, в свою очередь, был получен из алгоритма MISTY, разработанного корпорацией Mitsubishi. В настоящее время считается, что данный поточный шифр обеспечивает требуемую криптостойкость.

Обзор известных атак на шифры A5.

Рассмотрим, как данные алгоритмы были скомпрометированы различными атаками:

- Скомпрометирована длина ключа. Длина ключа составляет 64 бит, 10 из которых принудительно занулены, что ослабляет систему на три порядка.
- Скомпрометирован сильный алгоритм шифрования A5/1. Из-за конструктивных дефектов сложность полного перебора составляет не 2^64, а всего 2^40 (то есть ослабление системы на 6 порядков). Кроме того, ослабляет систему независимость трёх регистров: для каждого регистра значение бит других регистров влияет только на управление смещением, но не на содержание самого регистра. В [2] отмечается тот факт, что добавление перекрестных обратных связей между регистрами и взаимное их влияние на записываемые в младшие разряды значения увеличивает стойкость системы к взлому не уменьшая при этом статистические свойства генератора псевдослучайной последовательности.
- Скомпрометирован слабый алгоритм шифрования A5/2. Этот алгоритм изначально создавался слабым, но в результате он оказался настолько слабым, что для его вскрытия достаточно знать 2 кадра по 114 бит.
- Обнаружены серьёзные недостатки в структуре дополнительных алгоритмов стандарта. В частности код коррекции ошибок прибавляется к сообщению до шифрования, что приводит к лишней избыточности и позволяет сильно упростить процесс вскрытия шифра.

Активная атака на A5.

Все выше перечисленные атаки – пассивные. Недавно в GSM была обнаружена серьёзная слабость, которая позволяет успешно проводить активные атаки на протоколы семейства A5. Эта уязвимость была обнаружена и описана группой израильских криптографов в составе: Элад Баркан, Эли Бихам и Натан Келлер. Уязвимость состоит в следующем: при аутентификации телефона в сети сессионный ключ Kc не зависит от протокола шифрования. Пусть мы перехватили телефонный звонок, который был зашифрован A5/1 или даже более сильным A5/3, и хотим узнать содержание этого разговора. Для этого мы проводим активную атаку на телефон – включаем рядом с телефоном ложную базовую станцию и посылаем на телефон вызов. Для установления

соединения потребуется случайное число, и мы вышлем телефону число RAND, которое использовалось в том звонке, который мы хотим расшифровать. При этом сессионный ключ Kc будет такой же, как и в предыдущем случае. Если же теперь потребовать от телефона шифрования в слабом режиме A5/2, который легко вскрывается, то можно легко узнать сессионный ключ и расшифровать интересующий нас разговор. Мы можем успеть выполнить все операции до того, как телефон зазвонит, поэтому пользователь даже не узнает, что его телефон куда-то подключался. Эта серьёзнейшая брешь в системе требует пересмотра всей структуры безопасности в GSM.

Можно ли исправить эту уязвимость программными патчами? Специалисты утверждают, что в некоторых случаях это возможно – в некоторых телефонах имеется полный программный доступ к протоколам GSM. Можно сделать программу, которая при каждом вызове будет определять, не использовалось ли данное значение RAND ранее. Другой способ решения этой проблемы – отказаться от использования A5/2. В пользу этого приводят следующий довод: A5/2 достаточно слаб и если злоумышленник имеет сканер радиочастот, то он легко может взломать протокол на обычном персональном компьютере.

Из всего вышесказанного можно сделать несколько выводов:

- Стандарт, стойкость которого основана на том, что злоумышленник не знает внутренней структуры системы, не может быть очень надёжной, так как рано или поздно такая информация появится в публичном доступе.

- Слабость системы определяется самой слабой её частью – разработав умышленно ослабленный шифр A5/2, разработчики GSM в результате поставили под удар всю систему.

- Новые стандарты должны разрабатываться при участии мирового научного сообщества. Как говорится «одна голова хорошо, а две лучше».

Литература:

1. Elad Barkan, Eli Biham, Nathan Keller, «Instant ciphertext-only cryptanalysis of GSM encrypted communication», http://cryptome.org/gsm-crack-bbk.pdf

2. Alex Biryukov, Adi Shamir, David Wagner «Real Time Cryptanalysis of A5/1 on a PC», http://cryptome.org/a51-bsw.htm, April 2000.

3. M. Briceno, I. Goldberg, D. Wagner, «A pedagogical implementation of A5/1», http://www.scard.org/, May 1999.

4. Материалы сайта http://www.gsm-security.net/