Безопасность в сетях GSM.

1.05.2003
Сергей А. Платоненков
ФРТК МФТИ

Обзор (Abstract)

Стандарты сетей GSM изначально разрабатывались с учетом необходимости защиты данных, передаваемых по радиоканалу, а так же обеспечения процедуры аутентификации. Принципы и алгоритмы обеспечения безопасности GSM Консорциум оставил в тайне и никогда их не публиковал. Тем не менее, некоторые алгоритмы и спецификации стали доступны широкой общественности, и в них были выявлены серьезные недостатки. Общая схема построена таким образом, что атаке могут подвергнуться многие части GSM сети, а не только конкретный телефон. Несмотря на то, что стандарты GSM разрабатывались для обеспечения защиты от несакционикованного доступа и прослушивания, схема безопасности оказалась неспособна это обеспечить

1. Введение

GSM – одна из первых систем цифровой сотовой связи, пришедших на смену аналоговым системам. GSM имеет более 100'000'000 пользователей и является наиболее популярной в мире. При ее разработке попытались решить проблемы стоявшие очень остро у аналоговых систем – подслушивание переговоров, возможность фальсифицировать данные, возможность выдавать себя за другого и делать звонки за чужой счет, т.е. проблемы аутентификации между MS и MSC и криптозащиты данных в радиоканале между MS и BTS.

Спецификации на сеть GSM были разработаны GSM Consortium в тайне, производителям оборудования, программных средств и операторам сетей были сообщены только минимально необходимые сведения. Спецификации никогда не публиковались и не обсуждались широкой общественностью. Консорциум полагался на «безопасность из-за неизвестности», т.е. что алгоритмы сложнее «сломать», если они не доступны публично. Однако известно, что стойкость криптосистемы зависит от стойкости ключа, и неизвестность самого алгоритма не является существенной помехой, и при анализе любой криптосистемы алгоритм можно считать известным. То, что алгоритмы были разработаны в тайне, наводит на мысль, что они не были сделаны очень стойкими, и, когда они все-таки стали известны общественности, так и оказалось.

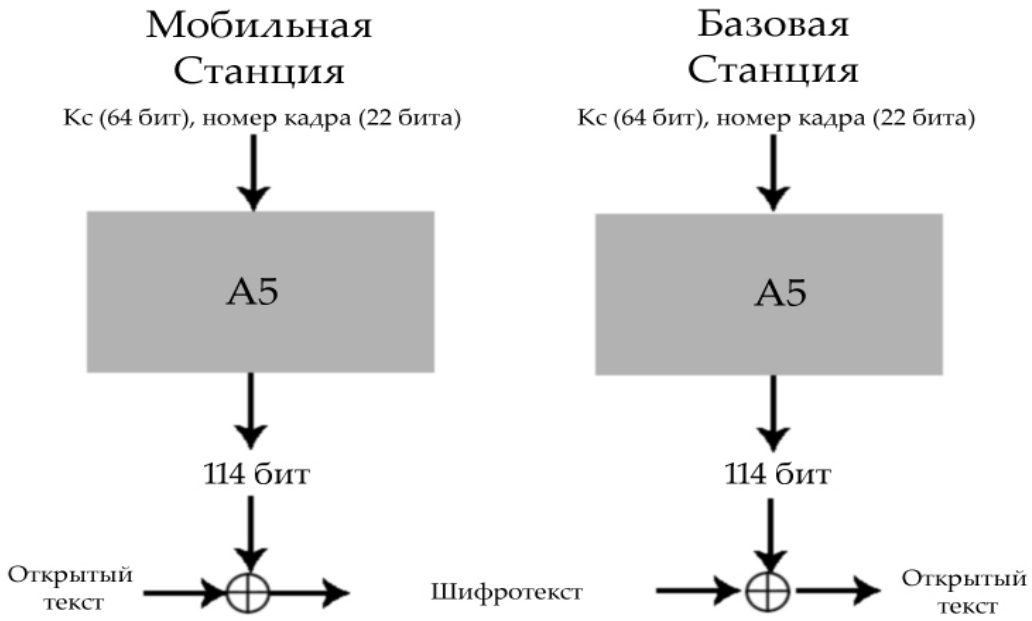
2. Общая схема криптозащиты GSM сетей

Криптозащита GSM сетей основывается на разделяемой между SIM и HLR секретной информации. Этой секретной информацией является Ki – секретный 128-битный ключ, который храниться в SIM и HLR, и используется для генерации 32-битного отзыва (SRES) на случайный пароль (RAND) в процедуре аутентификации, а также для выработки 64-битного сессионного ключа (Kc), который используется для шифрования данных в

радиоканале. При первом появлении MS в сети HLR предоставляет MSC пять троек, которые содержат случайный пароль (RAND), отзыв на этот пароль (SRES), сгенерированный при помощи секретного ключа (Ki), а так же сессионный ключ (Kc) , полученный из Ki. Каждая из троек используется только для одной сессии связи с MS и MSC. После 5 сессий MSC запрашивает у HLR новый набор из 5 троек.

Когда MS впервые появляется в области данного MSC, MSC посылает RAND из одной из троек, относящихся к данной MS. MS вырабатывает SRES при помощи A3 алгоритма, используя полученный RAND и Ki, хранящийся в SIM. MS отсылает SRES, и, если он совпадает с тем SRES, который содержится в данной тройке, то процедура аутентификации считается пройденной успешно.

Далее MS генерирует сессионный ключ Kc, при помощи алгоритма A8, используя уже полученный RAND и имеющийся Ki. Базовая станция (BTS), используемая для связи с данной MS, получает необходимый Kc у MSC. С этого момента радиоканал становится шифрованным.



Каждый кадр передаваемого по радиоканалу трафика кодируется своей 114-битной ключевой последовательностью. Эта последовательность генерируется при помощи алгоритма A5. Алгоритм A5 инициализируется сессионным ключом и номером передаваемого кадра, таким образом, для каждого кадра получается собственная последовательность. Это означает, что дешифрование одного звонка возможно только если аналитик знает Kc и номер кадра. Один и тот же Kc используется пока MSC не инициирует процедуру аутентификации заново, при этом будет сгенерирован новый Kc. На практике один и тот же Kc может использоваться несколько дней, т.к. аутентификация является необязательной процедурой в начале звонка и производится нечасто.

Надо так же отметить, что шифрованным в GSM сетях является только радиоканал, а между базовыми станциями данные передаются в открытом виде.

2.1. A3, Алгоритм аутентификации

Алгоритм аутентификации A3 используется для генерации отзыва SRES на случайный пароль RAND, получаемый от MSC. На входе A3 передаются RAND (128 бит) и Ki (128 бит), на выходе получают SRES (32 бита).

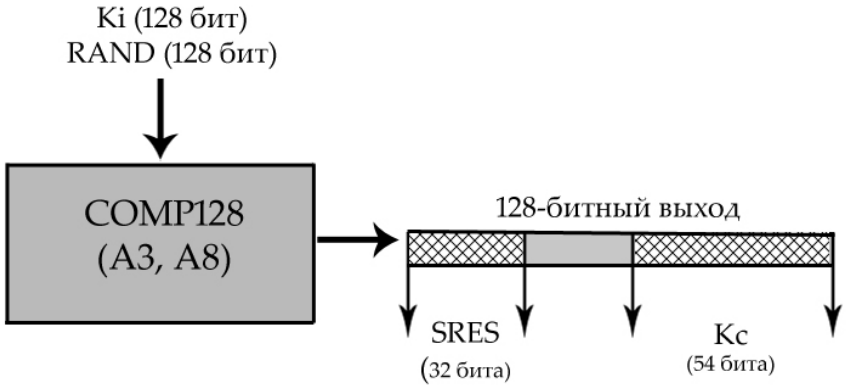
Практически все операторы GSM в мире используют алгоритм COMP128 в качестве A3 и A8 алгоритмов. COPM128 был утвержден GSM Consortium как опорный для A3 и A8. Есть пара операторов, которые используют другие, но тоже известные, алгоритмы.

На самом деле, COMP128 на выходе генерирует 128-битную строку, но как SRES используются только первые 32 бита.

2.2. A8, Алгоритм генерации сессионного ключа

Алгоритм A8 в GSM сетях используется для генерации сессионного ключа. На вход подают Ki и RAND, на выходе получают 64-битный Kc. BTS получает его от MSC, который в свою очередь получает от HLR. HLR способен генерировать Kc, т.к. знает RAND (который он же и генерирует) и секретный ключ Ki, который он получает при подключении пользователя и создании SIM карты. Новый сессионный ключ генерируется, в случае, если MSC инициирует процедуру аутентификации.

Как было сказано, COMP128 используется большинством GSM сетей в качестве A3 и A8. Таким образом COMP128 генерирует SRES и Kc за один проход. Для Kc используются последние 54 бита выходной последовательности COMP128,но алгоритм A5 требует 64-битного ключа. Его получают из уже сгенерированных 54 бит и 10 нулевых бит, которые приписывают в конец. Таким образом, ключ имеет эффективную длину 54 бита. Это сделано во всех реализациях A8, где используется COMP128, и, судя по всему, сделано умышленно.

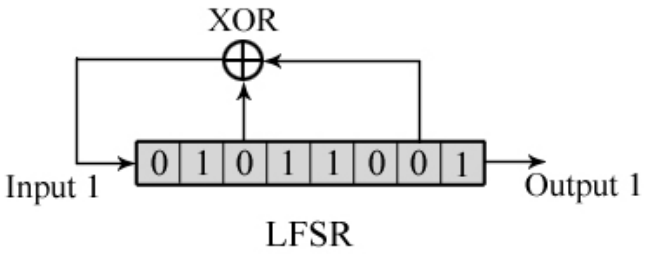


Алгоритмы A3 и A8 «зашиты» в SIM карте. Это позволяет оператору сотовой связи самому решить, какие именно алгоритмы будут использоваться в его сетях в качестве A3 и A8, и не зависеть от производителей оборудования и других операторов. При этом проблем с аутентификацией в «гостевых» сетях не возникает, т.к. местная сеть получает уже готовые RAND, SRES и Kc от HLR «домашней» сети, которой, в свою очередь, известны Ki и конкретные реализации A3 и A8.

2.3. A5, Алгоритм шифрование радиоканала

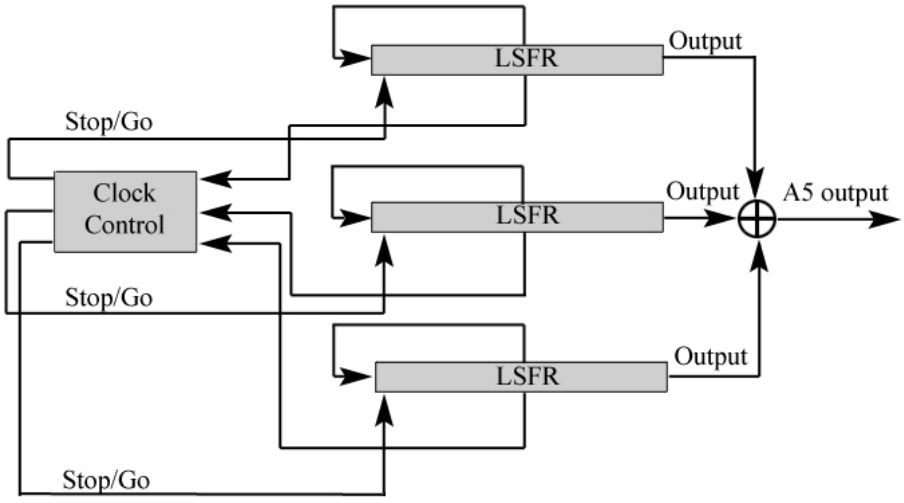
Алгоритм A5, применяемый для шифрования данных передаваемых по радиоканалу, является потоковым алгоритмом шифрования. Схема шифрования инициализируется сессионным ключом Kc и номером передаваемого кадра. Один и тот же сессионный ключ используется на протяжении всего звонка, но номера кадра кадров меняются, таким образом, перед передачей очередного кадра схема инициализируется заново, и для каждого кадра генерируется своя уникальная ключевая последовательность.

Основным элементом схемы шифрования алгоритма A5 является линейный регистр сдвига с обратной связью (Linear Feedback Shift Register – LFSR). Как видно на схеме, LSFR представляет собой регистр сдвига, в котором значение вытесняемого бита зависит от предыдущих состояний и определяется конфигурацией обратных связей.



При удачном выборе конфигурации обратных связей, LSFR может генерировать псевдослучайную последовательность, функция автокорреляции и спектральная плотность которой позволяет использовать ее в качестве псевдошума.

Схема алгоритма A5 используемого в европейских странах содержит 3 LSFR различной длинны (19, 22, 23 бита), суммарной длинной в 64 бита. Для получения очередного бита ключевой последовательности, выходы всех регистров складываются по модулю 2. Все 3 регистра имеют управление сдвигом, т.е. можно запретить сдвиг по очередному сигналу тактового генератора. Управление сдвигом происходит по среднему биту. Сдвиг происходит, если значение среднего бита регистра совпадает с преобладающим значением средних битов всех 3 регистров. К примеру, если значения средних битов 0 0 1, то сдвиг будет произведен только у 1 и 2 регистров, а если 1 0 1, то у 1 и 3. Таким образом по крайней мере 2 из 3 регистров сдвигаются на каждом шаге.



Регистры инициализируются сессионным ключом Кс и номером кадра. Сначала бит за битом загружается 64-битный Кс. После чего, последние значащие биты ключа в каждом регистре складываются по модулю 2. При отключенном управлении сдвигом, производят сдвиг и загружают еще раз 64 бита Кс. Далее , загружают 22 бита номера кадра, но уже при включенном управлении сдвигом. После того, как регистры были таким образом инициализированы, производят 100 шагов и полученную последовательность отбрасывают. Следующие 228 бит составляют выходную ключевую последовательность,

первые 114 бит которой используют для шифрования кадра от MS к BTS, а остальные 114 обратно от BTS к MS. Для шифрования следующего кадра, схема инициализируется заново, и процесс повторяется.

Кроме этой схемы алгоритма A5, были также разработаны и другие. Основная причина в том, что данную схему посчитали слишком стойкой для поставок на Ближний Восток, в страны восточной Европы и Россию. «Оригинальный» A5 был переименован в A5/1. Другие алгоритмы стали обозначать A5/x. A5/0 предполагает вообще отсутствие шифрования, A5/2 – более слабый чем A5/1 (имеет стойкость 2^{16} против 2^{54}). О других вариантах A5 достоверных сведений нет, как, впрочем, и подтверждения того, что они успешно применяются.

3. Возможные атаки

Как и в любой системе шифрования, в системе безопасности GSM наибольший интерес представляет её стойкость к дешифрованию, особенно, если, по крайней мере, один из алгоритмов уже «взломан».

Перехват и дешифрование данных передаваемых по радиоканалу в реальном времени на данный момент пока еще представляется затруднительным, но существующие виды атак позволяют производить дешифрование за приемлемое время и без значительных затрат.

3.1. Атака A5 прямым перебором

Стойкость алгоритма A5 при атаке «грубой силой» – 2^{54} (последние 10 бит Кс - нули), и прослушивание в реальном времени не представляется возможным при разумных затратах. Можно только записать звонок и дешифровать его позже.

Если мы имеем чип класса Pentium III, который содержит примерно 20 миллионов транзисторов, а для реализации одного набора LSFR схемы шифрования алгоритма A5 требуется 2000, то в одном чипе можно организовать примерно 10000 реализаций A5. При тактовой частоте 600 МГц, и если каждая реализация A5 выдает 1 бит за такт, и необходимо сгенерировать 100+114+114 бит, можно проверять 2 миллиона ключей в секунду. Пространство ключей в 2^{54} требует для перебора 900000 секунд или приблизительно 250 часов при одном чипе. Атака может быть оптимизирована отбрасыванием целых классов ключей после первого «плохого» бита ключевой последовательности. Задача легко распараллеливается, чем можно сильно сократить время дешифрования.

3.2. Атака A5 на основе известного открытого текста

Атака на основе известного открытого текста позволяет уменьшить стойкость алгоритма A5 до 2^{45}. Целью криптоаналитика является определение начального состояния всех LSFR по известной ключевой последовательности. Аналитик должен для этого знать 64 бита ключевой последовательности, которые можно получить, зная шифротекст и соответствующий ему открытый текст. Эту информацию можно извлечь из GSM кадров, которые содержат много постоянной, известной информации, например заголовки кадров. Требуемые 64 бита не всегда могут быть получены, но 32 или 48 бит обычно становятся известны.

3.3. Другие виды атак

В шифрованном виде информация передается только по радиоканалу, а по сети SS7 используемой операторами GSM звонки и служебная информация передаются в

открытом виде. Таким образом, получив доступ к сети оператора злоумышленник может не только прослушивать текущие звонки, но и получает возможность доступа к HLR, где хранятся Ki абонентов, к счастью HLR обычно более серьезно защищен.

Наиболее желаемой информацией является конечно же Ki, который храниться в SIM карте и HLR. Имея компьютер, SmartCard reader, саму SIM карту и соответствующее программное обеспечение можно клонировать SIM карту, это займет около 8 часов, скорость определяется в основном скоростью работы SIM карты. Существует так же теоретическая возможность получения Ki без физического доступа к SIM карте, но это сопряжено с некоторыми трудностями: необходимо иметь специальное оборудование, а так же достаточно долго находиться недалеко от взламываемого телефона.

Заключение

Система защиты сетей GSM имеет серьезные недостатки на многих уровнях защиты, т.к. имеет бреши в различных частях сети оператора GSM. Саму схему нельзя признать удачной. Даже если применять стойкие алгоритмы шифрования, вся система все равно не защищена от различных «социальных» сценариев, например если злоумышленник работает в компании-операторе.

Остается надеяться, что в следующем поколении цифровых сетей связи все это будет исправлено, а пока если вы хотите надежной защиты от прослушивания – применяйте дополнительное шифрование. ☺