АНАЛИЗ СТОЙКОСТИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ В GSM СЕТЯХ

А. Н. Моксяков, Е. П. Погодин

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Необходимо признать, что жизнь в современном мире невозможна без использования продуктов технического прогресса. Автомобили, компьютеры, сотовые телефоны и многое другое все – это все то, без чего не представляется настоящее и без чего не видеться будущее, поэтому безопасности продукта используемого миллионами людей уделяется особое внимание.

Цель данной исследовательской работы – рассмотрение стойкости криптографических алгоритмов в GSM сетях, на основе которых построена конфиденциальность разговора по мобильному телефону.

Безопасность в GSM сети организованна с помощью трех криптографических алгоритмов: A3 – алгоритм аутентификации абонента, используется в большинстве сетей; A5 – поточный алгоритм шифрования речи, имеет несколько спецификаций в зависимости от географического расположения абонента; A8 – алгоритм выработки сессионного ключа, который участвует в алгоритм шифрования речи.

Модель безопасности и алгоритмы шифрования разрабатывались в тайне и никогда не были опубликованы. Со временем некоторые алгоритмы и спецификации стали доступны. Алгоритмы изучили, и были найдены критические ошибки. Таким образом, при более детальном рассмотрении стандарта GSM видно, что его модель безопасности не совсем эффективна. Из возможных атак на GSM сеть следует выделить несколько самых популярных:

1. Лобовая атака A5 в реальном времени невозможна, так как требует относительно больших аппаратных мощностей и составляет 250 часов для Pentium III с тактовой частотой в 600 МГц.

2. «Разделяй и властвуй» основана на известной атаке открытого текста. Атакующий пытается определить начальные состояния регистров сдвига из известной последовательности гаммы. Атакующий должен знать 64 последовательные бита гаммы, которые можно извлечь, если атакующий знает какой-либо текст шифра и соответствующий открытый текст. Это в большой степени зависит от формата GSM кадров, посылаемых туда и обратно. Кадры GSM содержат большое количество постоянной информации, например, заголовки кадров. Требуемые 64 бита не всегда могут быть получены, но 32 или 48 бит, иногда и больше, обычно известны. Атакующему необходим только сегмент из 64 битов открытого текста.

3. Доступ к сигнальной сети оператора позволяет слушать все передачи, так как за пределами базовой станции в сети оператора трафик передается открытым текстом.

4. Извлечение ключа из SIM карты в эфире основана на следующем. Требуется, чтобы мобильный телефон откликалась на каждый вызов сети GSM. Если мощность законного сигнала базовой станции превышена нестандартной базовой станцией злоумышленника, злоумышленник может бомбардировать вызовами мобильный телефон и реконструировать секретный ключ по откликам. Мобильный телефон должен быть доступен злоумышленнику в эфире все время, необходимое для атаки. Неизвестно, сколько времени продлится атака в эфире предположительно от 8 до 13 часов.

5. Существует вероятность взлома алгоритма A8, так как кто-либо может без особых усилий взломать алгоритм генерации ключа A8 и извлечь секретный ключ, K*i*, основанный на случайном вызове, RAND, сеансовом ключе, Kc, и отклике SRES (предполагается, что один и тот же алгоритм используется в A3 и A8, как в случае с COMP128). Например, злоумышленник может найти RAND, который производит в результате K*i* (самый легкий пример). Все три переменные относительно просто найти. RAND и SRES отсылаются по эфиру открытым текстом. Сеансовый ключ Kc можно относительно легко при наличии достаточного количества времени вычесть из зашифрованных кадров и известного открытого текста. Уязвимость такого рода в алгоритме генерации ключа, конечно, разрушит всю систему безопасности GSM и даст Консорциуму GSM повод для размышления, когда они будут изобретать свои следующие алгоритмы безопасности.

6. Извлечение ключа из SIM самая дерзкая атака из всех, так как если скомпрометировать секретный ключ K_i, то появляется возможность прослушивать звонки абонентов и переадресовывать счета за звонки на счет других абонентов.

Из представленных атак нас заинтересовала последняя, ввиду наличия подходящего оборудования и небольшого накопленного опыта по прошлым работам. Как было сказано чуть ранее, атака основана на извлечение идентификационного ключа, который хранится в памяти SIM карты и к которому исключен прямой доступ. K_i необходим для выработки сессионного ключа и ответа подтверждающего результат либо подписанные отклики. Самым важным звеном в цепочке защиты является алгоритм A5.

В этом алгоритме каждому символу открытого текста соответствует символ шифротекста. Текст не делится на блоки (как в блочном шифровании) и не изменяется в размере. Для упрощения аппарат-

ной реализации и, следовательно, увеличения быстродействия используются только простейшие операции: сложение по модулю 2 (XOR) и сдвиг реестра.

Формирование выходной последовательности происходит путём сложения потока исходного текста с генерируемой последовательностью (гаммой). Особенность операции XOR заключается в том, что применённая чётное число раз, она приводит к начальному значению. Отсюда, декодирование сообщения происходит путём сложения шифротекста с известной последовательностью.

Таким образом, безопасность системы полностью зависит от свойств последовательности. В идеальном случае каждый бит гаммы – это независимая случайная величина, и сама последовательность является случайной. Такая схема была изобретена Вернамом в 1917 году и названа в его честь. Как доказал Клод Шеннон в 1949 году, это обеспечивает абсолютную криптостойкость. Но использование случайной последовательности означает передачу по защищённому каналу сообщения равного по объёму открытому тексту, что значительно усложняет задачу и практически нигде не используется.

В реальных системах создаётся ключ заданного размера, который без труда передаётся по закрытому каналу. Последовательность генерируется на его основе и является псевдослучайной. Большой класс поточных шифров (в том числе A5) составляют шифры, генератор псевдослучайной последовательности которой основан на регистрах сдвига с линейной обратной связью.

Алгоритм A5 был подвергнут корреляционному анализу, который позволяет узнать ключ путем использования информации о заполнении трех или четырех регистров сдвига. Со своей стороны мы прорабатываем этот вариант и работаем над симулятором SIM карты на основе PIC процессора, что в дальнейшем при положительных результатах при вычислении K_i позволит копировать SIM карты.

Литература

1. Haverinen H., Salowey J. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) and Subscriber Identity Modules (EAP-SIM), 1994.

2. Anderson, Ross A5 – The GSM Encryption Algorithm, 1996.

3. Шнайнер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке СИ. М: ТРИУМФ, 2003.