Эссе по курсу «Защита информации»

Реализация безопасности передачи информации в стандарте сотовой связи CDMA 2000 1xRTT

Подготовил:
Васильев Николай, студент 915 группы

Введение.

Сотовая связь появилась в нашей жизни совсем недавно и за короткий срок успела превратиться из неслыханной роскоши в незаменимое средство связи, развиваясь буквально у нас на глазах. Аналоговым стандартам первого поколения 1G пришли на смену цифровые стандарты второго поколения 2G, которые вскоре эволюционировали в 2.5G, обеспечивающие более высокие скорости передачи данных . Не за горами уже и высокоскоростной 3G, позволяющий передавать даже потоковое видео, первые сети которого запущены в эксплуатацию в Японии.

Столь бурное развитие и огромная популярность отрасли особенно остро поставили перед разработчиками стандартов сотовой связи и оборудования вопросы надежной аутентификации пользователей и безопасности передачи информации. Безопасность была одним из главных аспектов сотовой телефонии с самого ее рождения как для операторов так и для абонентов. Причем, если операторов в большей мере беспокоила ее часть, связанная с предотвращение мошеннических операций таких как создание двойников мобильных телефонов или ложная аутентификация, то абонентов кроме этого очень интересовала безопасность передачи конфиденциальной информации. В 1996 году мошенничества, связанные с созданием двойников телефонов и другими способами, обошлись операторам в 750 миллионов долларов только в США.

В связи с тем что вся передаваемая информация в сотовой телефонии посылается через радиоканал, любой, обладающий соответствующим оборудованием, может прослушивать все телефонные разговоры, ведущиеся в зоне приема без опасения быть обнаруженным. При проектировке ранних систем сотовой телефонии обеспечению безопасности уделялось не так много внимания в связи с тем, что высокая цена необходимого для прослушивания оборудования делала его экономически нецелесообразным. Когда же подобные устройства стали широко распространенными и доступными по цене, проблему попытались решить с помощью создания соответствующей законодательной базы. Но введение правовых норм ситуации не изменило, и проектировщики систем для решения проблемы были вынуждены все в большей и большей степени обращаться за помощью к криптографии и, как оказалось, не зря. Криптографические методы являются одним из самых очевидных и эффективных способов предотвращения несанкционированного доступа к каналам связи и дублирования аппаратов, и вскоре они заслуженно нашли применение во всех последующих стандартах. В 1992 году рабочая группа TR-45 ассоциации промышленности средств связи (Telecommunications Industry Association – далее упоминающаяся как TIA) разработала TIA92 - стандарт интеграции криптографических технологий в системы сотовой телефонии следующих поколений, который был модернизирован с созданием TIA95. Стандарт TIA95 описывает четыре криптографических примитива для использования в системах цифровой сотовой связи Северной Америки:

1. CAVE – функция перемешивания, использующаяся в протоколах аутентификации запрос-ответ и для генерации ключей.

2. повторяющаяся XOR маска, налагающаяся на голосовые данные для обеспечения безопасности их передачи.

3. ORYX – потоковый шифр, предназначенный для использования в услугах беспроводного доступа к данным.

4. CMEA (Control Message Encryption Algorithm) – простой блоковый шифр, использующийся для шифрования служебных сообщений.

С появлением стандартов сотовой связи второго поколения (TDMA/CDMA-IS-41) операторы получили возможность улучшить безопасность своих сетей за счет использования более криптостойких алгоритмов шифрования и других средств. Что касается стандарта CDMA, то его шумоподобные сигналы делают подслушивание весьма затруднительным, благодаря использованию так называемого Long Code (псевдослучайной последовательности длины (2^{42} - 1)), используемой для кодирования голоса и передачи информации.

В этой статье обсуждается реализация в стандарте CDMA 2000 1xRTT - одного из семейства перспективных сейчас CDMA стандартов трех основных составляющих безопасности мобильной связи: аутентификации, защиты передаваемой информации и анонимности.

Безопасность в CDMA сетях.

Протоколы, обеспечивающие безопасность передачи информации в CDMA-IS-41 сетях, являются одними из лучших в индустрии. Кроме того сам CDMA стандарт по своему построению делает перехват сигнала и его расшифрование очень сложной и дорогостоящей задачей доступной, фактически, только государственным спецслужбам.

Криптографические протоколы стандарта CDMA основываются на 64-битном аутентификационном ключе (A-key) и серийном номере мобильного телефона – Electronic Serial Number (ESN). Для аутентификации абонента при регистрации мобильного телфона в сети а также последующей генерации вспомогательных подключей для обеспечения конфиденциальности передачи голосовых данных и кодированных сообщений используется случайное двоичное число RANDSSD, генерируемое аутентификационным центром реестра собственных абонентов (далее упоминающийся как HLR/AC - Home Location Register / Authentification Center). A-key запрограммирован в мобильном телефоне и хранится в аутентификационном центре сети.

CDMA использует стандартизованный алгоритм шифрования CAVE (Cellular Authentification and Voice Encryption) для генерации 128 битного подключа SSD (Shared Secret Data). A-key, ESN и генерируемое сетью случайное число RANDSSD подаются на вход CAVE генерирующего SSD. SSD состоит из двух частей: SSD_A, используемой для создание аутентификационной цифровой подписи, и SSD_B , используемой при генерации ключей для шифрования голосовых данных и служебных сообщений. SSD может быть передан гостевой сети при роуминге абонента для обеспечения локальной аутентификации. Новый SSD может быть сгенерирован при возвращении абонента в домашнюю сеть или смене гостевой сети в роуминге.

Аутентификация.

Как было уже сказано, для аутентификации абонента в CDMA сети используется вспомогательный ключ SSD_A генерируемый CAVE алгоритмом из A-key, ESN и RANDSSD. Сеть генерирует и рассылает открыто по эфиру случайное число RAND*, мобильные устройства, регистрирующиеся в сети, используют его как входные данные для CAVE алгоритма, генерирующего 18-битную аутентификационную цифровую подпись (AUTH_SIGNATURE), и посылает его на базовую станцию. Эта цифровая подпись сверяется в

центре коммутации (далее упоминается как MSC - Mobile services Switching Center) с подписью генерируемой самим MSC для проверки легитимности абонента. Число RAND* может быть как одним и тем же для всех пользователей, так и генерироваться каждый раз новое (использование конкретного метода определяется оператором). Первый случай обеспечивает очень быструю аутентификацию.

И мобильный телефон и сеть ведут 6-битные счетчики вызовов, что обеспечивает возможность детектирования работающих двойников: для этого достаточно лишь контролировать соответствие значений счетчиков на телефоне и в MSC.

Секретный ключ A-key является перепрограммируемым, в случае его изменения информация на мобильном телефоне и в HLR/AC должна быть синхронизирована. A-key может быть перепрошит несколькими способами: на заводе, дилером в точке продаж, абонентом через интерфейс телефона, а также с помощью OTASP (over the air service provisionig). OTASP передачи используют 512 битный алгоритм согласования ключей Diffie-Hellman'a, гарантирующий достаточную безопасность. OTASP обеспечивает легкий способ смены A-key мобильного телефона на случай появления в сети двойника мобильного телефона. Изменение A-key автоматически повлечет за собой отключение услуг двойнику мобильного телефона и повторное включение услуг легитимному абоненту. Таким образом, как можно было заметить, секретность A-key является важнейшей компонентой безопасности CDMA системы.

Безопасность передачи голосовых данных, информации и служебных сообщений.

Мобильный телефон использует вспомогательный подключ SSD_B и CAVE алгоритм для генерации Private Long Code Mask (унаследованную от TDMA сетей), 64-битного подключа CMEA (Cellular Message Encryption Algorithm) key и 32-битного DATA-key. Private Long Code Mask используется как мобильным телефоном, так и сетью для изменения характеристик Long Code Mask. Этот модифицированный Long Code используется для шифрования голосовых данных, что повышает секретность их передачи.

Private Long Code Mask не шифрует информацию, она просто заменяет известные величины, используемые в кодировке CDMA сигнала секретными величинами, известными только мобильному телефону и сети. Таким образом подслушивание разговоров без знания Private Long Code Mask является чрезвычайно сложной задачей.

Более того, мобильный телефон и сеть используют CMEA и улучшенный CMEA (E_CMEA) алгоритмы для шифрования и дешифрования служебных сообщений при передаче их по эфиру. Отдельный DATA-key и алгоритм шифрования ORYX используется мобильным телефоном и сетью для шифрования и дешифрования потока информации по каналу связи CDMA. Рисунок 1 иллюстрирует механизмы аутентификации и шифрования в CDMA сети.

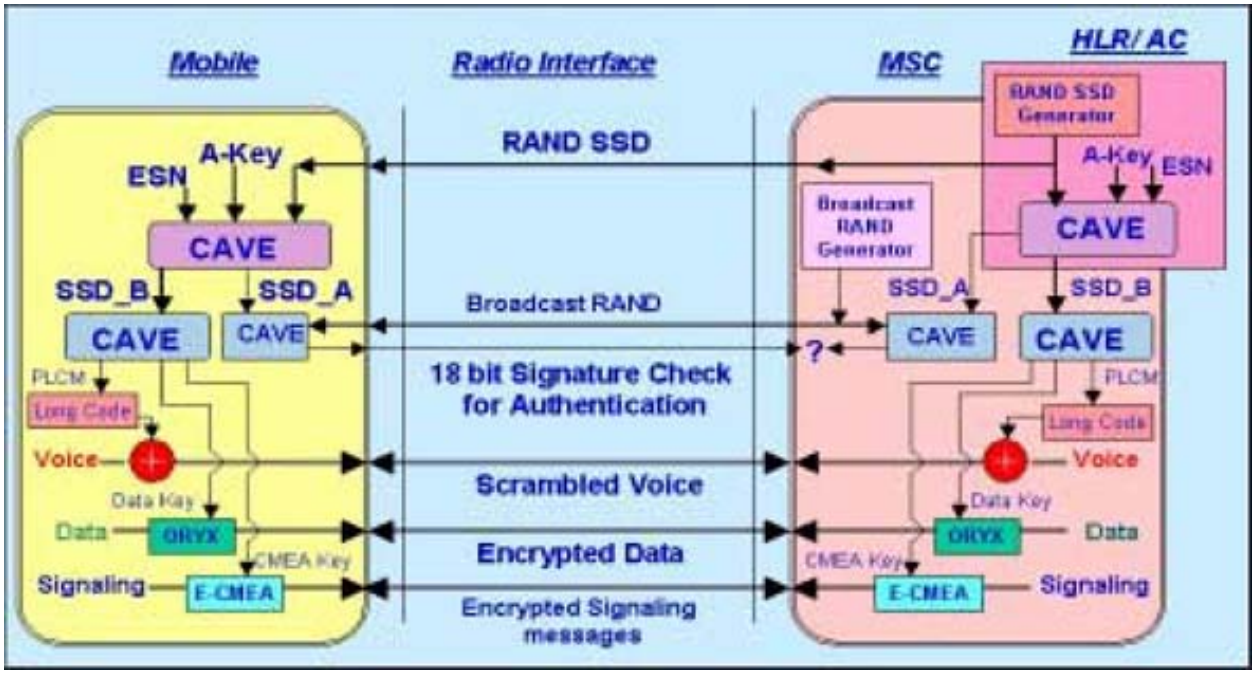

Рисунок 1.

Анонимность.

CDMA сеть поддерживает назначение мобильному телефону временного идентификатора мобильного абонента TMSI (Temporary Mobile Station Identifier) для его представления в процессе передачи информации по эфиру между мобильным телефоном и сетью. Эта функция еще более затрудняет сопоставление передаваемых данных конкретному абоненту.

3G CDMA 2000: Что дальше?

В сотовых стандартах третьего поколения (3G) используются еще более криптоустойчивые протоколы обеспечения безопасности системы, включающие использование 128-битного секретного и аутентификационного ключей. В сетях третьего поколения стандарта CDMA 2000 для хэширования и проверки достоверности используется Secure Hashing Algorithm-1 (SHA-1), для шифрования сообщений – Advanced Encryption Standard (AES Rijndael). Также для всех следующих версий после CDMA 2000 Release C будет использоваться AKA (Authentification and Key Agreement) протокол для аутентификации и согласования ключей. AKA протокол вместе с алгоритмом Kasumi будет использоваться и в WCDMA-MAP сетях для шифрования и проверки достоверности сообщений.

Заключение.

В настоящее время оборудование стандарта CDMA является самым новым и самым дорогим, но в то же время самым надежным и самым защищенным. Технологические решения и стойкие криптографические протоколы, нашедшие применение в этом стандарте, обеспечивают высокий уровень конфиденциальности сетей, построенных на его основе. Подслушать из эфира разговор можно, но стоимость и сложность оборудования способного на такое значительно выше чем для других стандартов. Причем дело усугубляется тем, что при незначительном удалении от БС мощность излучаемая телефоном крайне низка, поэтому подслушивающий должен находится в непосредственной близости от объекта наблюдения, а при значительном удалении от БС вообще не понятно через какую БС работает телефон. Сообщение, появившееся в новостной ленте сайта ixbt.com, о развертывании сети стандарта CDMA 2000 1xRTT поверх старых сетей оператора МСС является лишь подтверждением достоинств этого стандарта.

Список сокращений:

AC (AuC)	Authentication Center
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
CAVE	Cellular Authentication and Voice Encryption
CDMA	Code Division Multiple Access
CMEA	Cellular Message Encryption Algorithm
ESN	Electronic Serial Number
HLR	Home Location Register
IDC	International Data Corporation
IS	Interim Standard
MAP	Mobile Applications Part
MSC	Mobile Switching Center
OTASP	Over The Air Service Provisioning
RAND	RANDom challenge
SHA-1	Secure Hash Algorithm -1
SSD	Shared Secret Data
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Station Identifier