П. Е. Минин, А. С. Самойлов, А. А. Кузин

УЯЗВИМОСТИ КАНАЛА ДАННЫХ BLUETOOTH ДЛЯ ПРОСЛУШИВАНИЯ ЗЛОУМЫШЛЕННИКАМИ

Введение

Канал данных Bluetooth с его механизмами защиты не может гарантировать безопасности соединения, чем чаще всего пользуются злоумышленники для прослушивания телефонных переговоров. Подобная атака возможна, если жертва использует беспроводную Bluetooth-гарнитуру handsfree, которая становится все более популярна. Особенно часто пользуются гарнитурами водители автотранспорта ввиду вступившего в действие запрета на использование мобильного телефона за рулем. К сожалению, беспроводная гарнитура Bluetooth уязвима, так как с её помощью злоумышленники могут перехватывать и расшифровывать разговоры по мобильному телефону. Отметим, что прослушивание именно передаваемых по Bluetooth данных позволяет злоумышленникам отказаться от более дорогостоящих и сложных методов прослушивания сотовой связи, как, например, использование виртуальной соты.

Реализация атаки

Для реализации атаки взломщик прослушивает все сообщения обмена между двумя устройствами A и B, которые устанавливают соединение. Устройства A и B — это соответственно мобильный телефон и его гарнитура handsfree. Программы-снифферы для прослушивания Bluetooth-соединения в настоящее время достаточно широко распространены.

Прежде чем показать, как злоумышленник расшифровывает полученные данные, рассмотрим этапы прохождения аутентификации устройств:

- создание ключа инициализации (K_init);
- создание ключа связи (Kc);
- непосредственная аутентификация.

После того как будет выполнен третий шаг процесса аутентификации, устройства вырабатывают ключ для шифрования передачи данных.

Перед началом сеанса связи двух устройств Bluetooth в каждое устройство должен быть введен PIN-код. Если PIN-код устройства отсутствует, то такое устройство не может участвовать в обмене данными.

а) Создание ключа инициализации (K_init)

Ключ инициализации вырабатывается с помощью алгоритма шифрования E22. На вход алгоритма поступают следующие данные: адрес Bluetooth-устройства BD_ADDR, PIN-код и его длина, а также IN_RAND — случайно сгенерированное число длиной 128 бит. На выходе алгоритма получается 128-битовое слово — ключ инициализации.

Устройства, устанавливающие соединение, делятся на два типа: Master и Slave. Устройство типа Master передает случайное число IN_RAND устройству типа Slave в начале соединения в открытом виде. Если одно из устройств имеет фиксированный PIN-код, то значение BD_ADDR используется от того устройства, которое имеет нефиксированный PIN. Если же оба устройства имеют изменяемый PIN-код, то значение BD_ADDR предоставляет устройство, принимающее значение IN_RAND.

После получения ключа связи ключ инициализации (*K_init*) уничтожается.

б) Создание ключа связи (Kc)

После успешного создания ключа инициализации устройства переходят к выработке ключа связи. Ключ инициализации используется для обмена 128-битовыми словами LK_RANDA

и LK_RANDB. Каждое из устройств выбирает случайное 128-битовое слово, над которым выполняет побитно операцию XOR с ключом инициализации. Так как оба устройства знают ключ инициализации, то участникам доступны также значения LK_RANDA и LK_RANDB. После чего, используя алгоритм шифрования E21, каждое из устройств создает ключ связи [1].

Схема выработки ключа связи приведена на рис. 1.

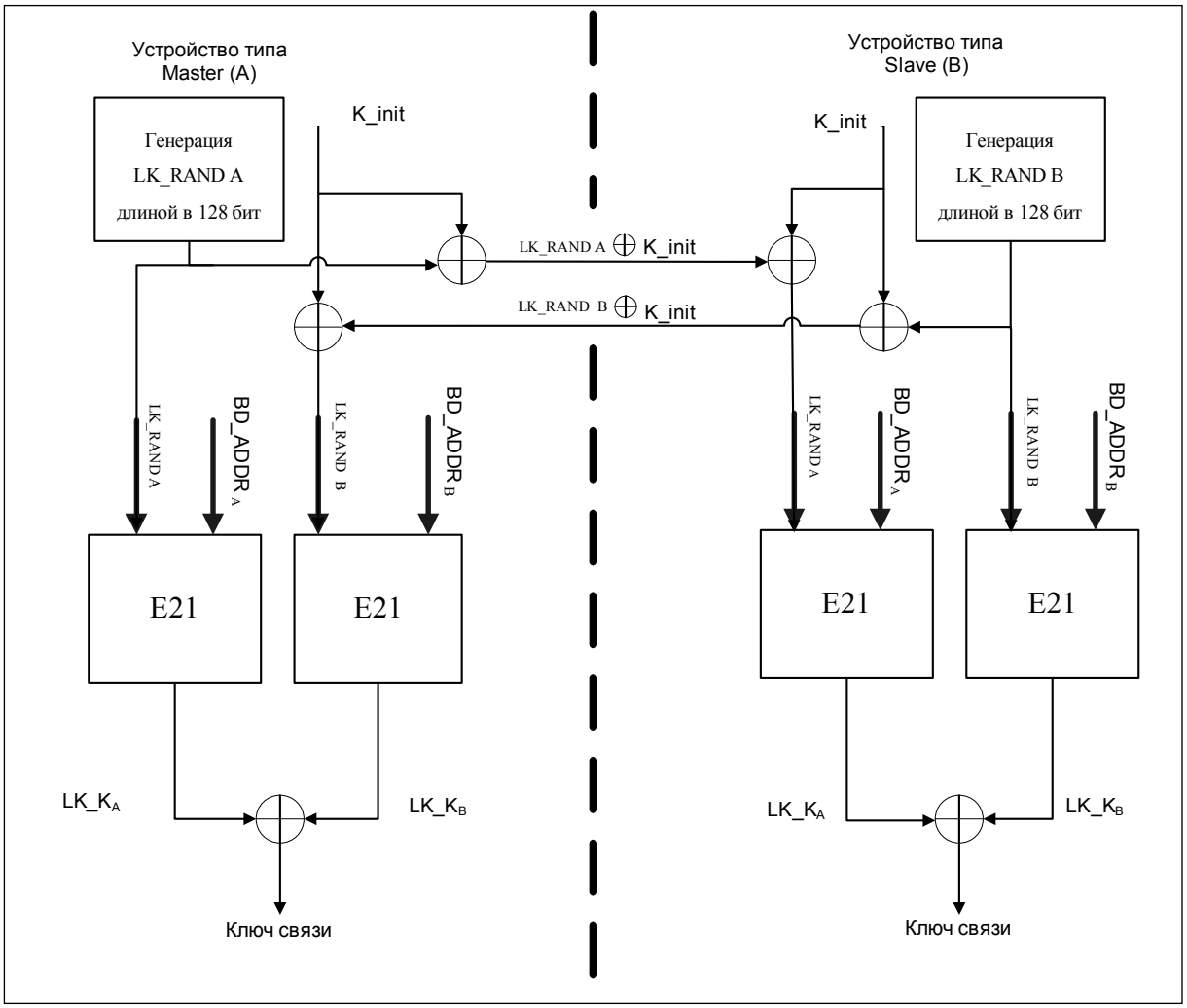

Рис. 1. Схема выработки ключа связи

На вход алгоритма E21 подаются следующие данные: BD_ADDR и случайное число LK_RAND.

Алгоритм используется дважды при создании ключа связи. В первом случае на него подается число LK_RANDA и BD_ADDR, а во втором – LK_RANDB и BD_ADDR. После получения результата от каждого шифрования по алгоритму E21 результаты складываются с использованием операции XOR.

в) Непосредственная аутентификация

После того как ключ инициализации сгенерирован, наступает этап непосредственной аутентификации. Одно из устройств (проверяющий) вырабатывает случайным образом и посылает в открытом виде 128-битовое слово AU_RANDA. Второе устройство (запрашивающий) вычисляет с помощью алгоритма E1 слово длиной в 32 бита, которое называется SRES.

Схема непосредственной аутентификации приведена на рис. 2.

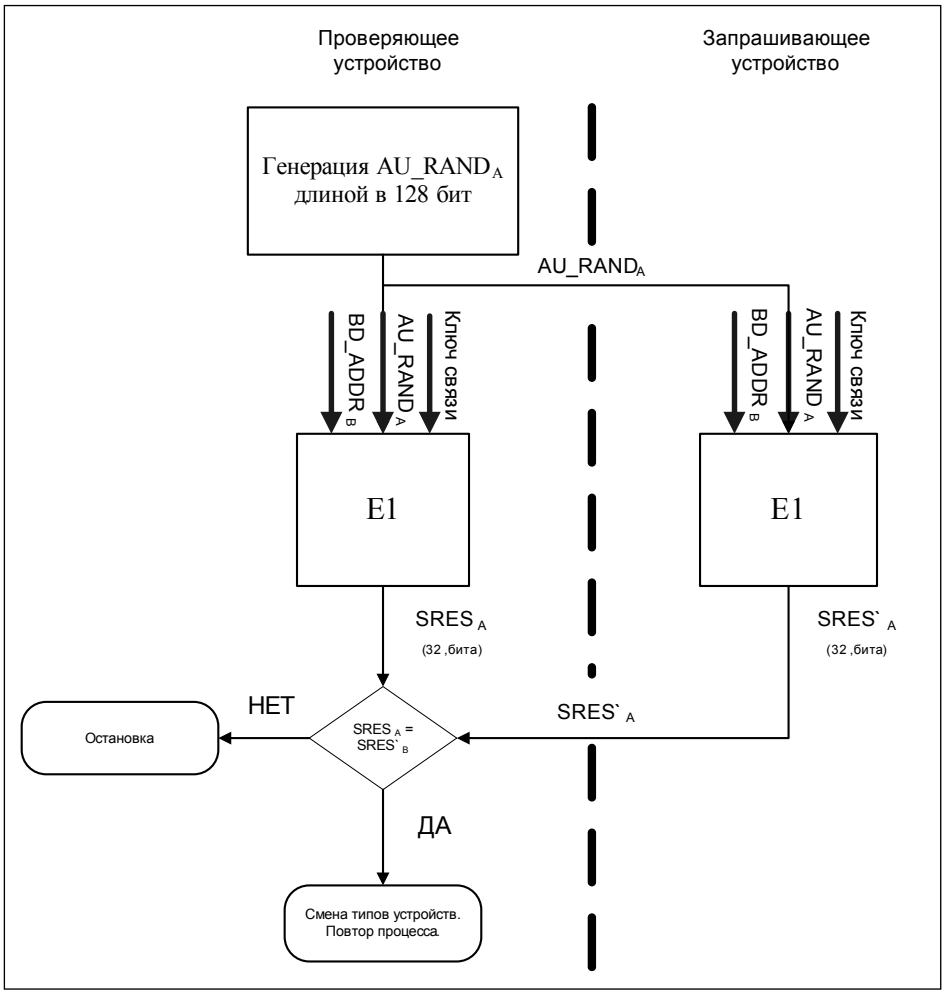

Рис. 2. Схема непосредственной аутентификации

Запрашивающий отправляет сгенерированное слово SRES как ответ на запрос. Проверяющий в это время также вычисляет SRES и сравнивает его с поступившим значением. На вход алгоритма E1 при вычислении SRES подаются следующие данные: AU_RANDA, ключи связи, адрес Bluetooth-устройства BD_ADDRB.

Таким образом, в процессе разговора каждый пакет данных преобразовывается на основе определенного алгоритма с использованием ключа. Ключ же генерируется на основе вводимого PIN-кода. Если он будет взломан, то восстановить содержание каждого пакета будет несложно, поэтому самым важным моментом данной атаки является именно взлом PIN-кода.

Злоумышленник при прослушивании передаваемых данных между гарнитурой и мобильным телефоном получает сообщения, представленные в таблице 1.

Таблица 1. Список перехватываемых злоумышленником сообщений

№	Источник	Приемник	Данные	Длина данных	Пояснение
1	A	B	IN_RAND	128 бит	Открытый текст
2	A	B	LK_RANDA	128 бит	После операции XOR с ключом инициализации
3	B	A	LK_RANDB	128 бит	После операции XOR с ключом инициализации

4	A	B	AU_RANDA	128 бит	Открытый текст
5	B	A	SRES	128 бит	Открытый текст
6	B	A	AU_RANDB	128 бит	Открытый текст
7	A	B	SRES	128 бит	Открытый текст

После того как соответствующие значения, приведенные в таблице, перехвачены, взломщик переходит к определению PIN-кода, предварительно пронумеровав все его возможные значения. Так как атакующий знает значения IN_RAND и BD_ADDR, то он запускает процедуру кодирования E22 с предполагаемым значением PIN-кода и получает возможное значение ключа инициализации [2].

Этот PIN-код используется для раскодирования второго и третьего сообщений, которые содержат достаточно информации для того, чтобы атакующий мог найти предполагаемый ключ сеанса связи. Данные в последних четырех сообщениях теперь могут быть использованы злоумышленником для проверки верности предположения значения PIN.

Взломщик поступает следующим образом. Используя ключ связи и перехваченное сообщение со значением AU_RANDA, он определяет значение SRES и сравнивает его с сообщением номер пять. Эта операция выполняется до тех пор, пока не будет обнаружен правильный PIN-код.

Имея компьютер с вычислительной мощностью, аналогичной Pentium III 450MHz, злоумышленник определяет четырехзначный PIN-код за время не более 0,8 секунды [2].

Таким образом, из приведенных данных становится очевидным, что использование существующих моделей Bluetooth-гарнитур не обеспечивает конфиденциальности разговоров.

Решение проблемы может заключаться во введении дополнительного шифрования трафика по CSD (Circuit Switched Data) между мобильным телефоном и гарнитурой, что даст возможность предотвратить перехват ключа сеанса связи. Разработка гарнитуры, осуществляющей шифрование канала передачи данных, позволит защитить пользовательскую информацию от перечисленных атак.

СПИСОК ЛИТЕРАТУРЫ:

1. *Hermelin M. and Nyberg K.* Correlation properties of the Bluetooth combiner generator // Information Security and Cryptology, LNCS 1787. Springer-Verlag, 1999. P. 17–29.
2. *Krause M.* BDD-based cryptanalysis of keystream generators // Advances in Cryptology - EUROCRYPT'02, LNCS 1462 / L. Knudsen (ed.). Springer-Verlag, 2002. P. 222–237.