sysБезопасность Bluetooth

Стандарт Bluetooth, атаки на соединения и защита от них.

[Содержание стандарта Bluetooth и смежных стандартов](#_329m6px9xv75)

[Аспекты безопасности](#_2ci2tgfx15d)

[Атаки на Bluetooth и защита от них](#_l149msbmewue)

[Утилиты для работы с Bluetooth](#_phc4lqal1f1l)

[Практика](#_c5d9qfauyv0k)

[Задача 1. Поднять протокол hci0](#_7qxsp0tzom87)

[Задача 2. Выполнить разведку пространства средствами hcitool](#_lpg2giocsgif)

Практическое [задание](#_3tfrjxxltv85)

[Дополнительные материалы](#_1pj11aaentb8)

[Используемая литература](#_uvp6qax5r1ok)

# Содержание стандарта Bluetooth и смежных стандартов

Чтобы понять принципы Bluetooth, необходимо изучить этот стандарт и понять его содержание. Чтобы найти уязвимости и уметь их использовать, нужно знать, какие вещи отсутствуют в стандарте. Ни один протокол или стандарт связи не содержит уязвимости по умолчанию — все они происходят от неполноты разработки, недальновидности программистов.

Стандарт Bluetooth можно [скачать с официального сайта Bluetooth](https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737).

## Аспекты безопасности

Мы будем работать на стороне хоста, поэтому стоит обратить особое внимание на параграф 5 главы 3 в части С стандарта Bluetooth — это «Аспекты безопасности». Там описаны алгоритмы аутентификации, принцип действия протоколов вплоть до форматов сигналов.

Несколько сюрпризов, которые готовит нам плотная работа с Bluetooth:

1. Спектр частот стандарта практически равен частотам Wi-Fi: около 2.4 ГГц. При снятии эфира мы неизбежно столкнемся с интерференцией сигналов.
2. Соседние несущие частоты отличаются на 1 Мгц, и их всего 78. Теоретически, снимая 78 каналов с эфира, можно получить что-то стоящее, но не стоит забывать про интерференцию.
3. 78 каналов предназначены вовсе не для многоканальной передачи, а для смены частот при передаче данных. Это дает помехоустойчивость и отчасти — взломостойкость: устройства при сопряжении передают друг другу карту смены частот.
4. Кроме частотной синхронизации используется временная. Разница во времени передается при сопряжении. Речь идет о базовых характеристиках импульсов.

Рассмотрим стек протоколов, которые использует Bluetooth.

**LMP** — Link Management Protocol — устанавливает радиосоединение между двумя устройствами и управляет им. Реализуется контроллером Bluetooth и является обязательным в стеке. Имеет приоритет выше других протоколов. Отвечает в том числе за аутентификацию.

**HCI** — Host/controller interface — определяет связь между стеком [хоста](https://ru.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82) (компьютера или мобильного устройства) и контроллером Bluetooth.

**L2CAP** — Logical Link Control and Adaptation Protocol — используется для мультиплексирования локальных соединений между двумя устройствами, использующими протоколы более высокого уровня. Позволяет фрагментировать и пересобирать пакеты, является обязательным в стеке.

**SDP** — Service Discovery Protocol — позволяет обнаруживать услуги, которые предоставляют другие устройства, и определять их параметры. Обязательный в стеке.

**RFCOMM** — Radio Frequency Communications — протокол замены кабеля. Создает виртуальный последовательный поток данных и эмулирует управляющие сигналы [RS-232](https://ru.wikipedia.org/wiki/RS-232).

**BNEP** — Bluetooth Network Encapsulation Protocol — используется для передачи данных из других стеков протоколов через канал L2CAP. Передает [IP-пакет](https://ru.wikipedia.org/wiki/IP-%D0%BF%D0%B0%D0%BA%D0%B5%D1%82)ы в профиле PAN.

**AVCTP** — Audio/Video Control Transport Protocol — используется в профиле Audio/Video Remote Control для передачи команд по каналу L2CAP.

**AVDTP** — Audio/Video Distribution Transport Protocol — используется в профиле Advanced Audio Distribution для передачи стереозвука по каналу L2CAP.

**TCS** — Telephony Control Protocol — Binary — протокол, определяющий сигналы управления вызовом. Это необходимо, чтобы устанавливать голосовые соединения и соединения для передачи данных между устройствами Bluetooth. Используется только в профиле Cordless Telephony.

Еще Bluetooth использует ряд заимствованных протоколов, в числе которых PPP, TCP/IP.

Разберем подробнее протокол **LMP**. Он утвержден стандартом RFC 4204 и опирается на другие стандарты серии: RFC 4201, RFC 4202 (MPLS). Перевод стандарта на русский язык можно [посмотреть на сайте protocols.ru](http://www.protocols.ru/WP/rfc4204/).

В нем описаны терминология, свойства и состояния каналов, сообщения и их значения. Там же разобраны вопросы безопасности и механизмы защиты.

Существует множество атак, с которыми могут столкнуться сессии LMP:

* использование фальшивых пакетов управления;
* изменение пакетов управления при передаче;
* повторное использование собранных пакетов управления;
* взлом (подбор) ключа с использованием криптографических средств. Если алгоритм хеширования или шифрования имеет известные уязвимости, можно узнать ключ, используя простые средства.

Защищаться от перечисленных методов атак следует на сетевом уровне, опираясь на стек протоколов IPSec (RFC 2401, RFC 2409, RFC 2402 и RFC 2406).

# Атаки на Bluetooth и защита от них

**BlueSnarf**

В этой атаке используется сервис **OPP** (OBEX Push Profile), который упрощает обмен «визитками» и прочими файлами. При нормальных обстоятельствах он работает вполне стабильно. Но чаще всего для доступа к этому сервису не требуется авторизация. Главная проблема в том, что если прошивка содержит уязвимость, атакующий может скачать любой файл командой GET. Например, файл **/telecom/pb.vcf**, в котором хранится телефонная книга устройства.

Защититься можно, установив авторизацию для OPP и не принимая неизвестных подключений.

**BlueBug**

Этот вид атаки открывает доступ к выполнению AT-команд на телефоне. Это может привести к тому, что злоумышленник сможет читать и отправлять смс, работать с телефонной книгой. Возможности атаки почти не ограничены.

Чтобы защититься, надо установить свежую прошивку модуля Bluetooth на телефоне и отклонять неизвестные подключения.

**BlueDump**

Эта атака основана на методе подмены BT-MAC адреса, чтобы получить доверие к обладателю настоящего MAC. Если злоумышленник знает MAC-адреса двух спаренных устройств, ему достаточно дождаться выхода одного из них из зоны действия, присвоить себе его MAC и инициировать повторную аутентификацию с оставшимся устройством. Это становится возможным из-за того, что одно из устройств может забыть ключ соединения, которым шифруется передача данных, и запросить его повторную генерацию.

На данный момент защиты не существует. Но не зная адрес доверенного устройства, злоумышленник не сможет атаковать: перебрать все возможные адреса за короткое время невозможно.

# Утилиты для работы с Bluetooth

**Hcitool** — c помощью этой утилиты можно:

* показать локальные устройства;
* запросить удаленные устройства;
* для каждого обнаруженного можно вывести адрес устройства Bluetooth, разность показаний часов, класс, название, версию и поддерживаемые возможности;
* запустить процесс периодического допроса, подтвердить произвольную команду HCI на локальном устройстве;
* вывести соединения в активном диапазоне частот;
* создать в диапазоне частот подключение (по умолчанию допустимы пакеты всех типов), выступая в роли ведущего или подчиненного устройства;
* разорвать радиоподключение с удаленным устройством;
* поменять роль удаленного устройства на роль ведущего (master) или подчиненного (slave);
* изменить типы пакетов устройства;
* показать информацию о качестве канала и мощности принимаемого или переданного сигнала для соединения с устройством;
* отобразить карту каналов (перестройки частот) для соединения;
* запросить аутентификацию у устройства;
* включить или выключить шифрование;
* изменить канальный ключ у подключения.

**Bluelog** — предназначена для исследований и мониторинга трафика. Подразумевается, что он должен запускаться на длительное время в одном месте, чтобы определять, как много обнаруживаемых Bluetooth-устройств в окрестностях. Так как Bluelog запускается «без присмотра», она не имеет пользовательского интерфейса и не требует действий пользователя после запуска. Она обладает полностью настраиваемым форматом лог-файла. Может вести лог в **syslog** для централизованной регистрации сетевой активности.

**Blueranger** — определяет мощность сигнала до устройства, используя **l2ping** и простой алгоритм оценки. Чем мощнее сигнал, тем ближе устройство.

**Bluesnaffer** — позволяет удаленно смотреть телефонный справочник, журналы вызовов.

**Btscanner** — утилита, которая извлекает максимум информации об устройстве без подключения к нему.

**Redfang** — позволяет сканировать адресные пространства и находить устройства, пребывающие в скрытом режиме.

**Spooftooph** — утилита для автоматической подмены (спуфинга) или клонирования имен, класса и адреса Bluetooth-устройств. Клонирование этой информации позволяет устройству скрываться из вида. Программы по сканированию Bluetooth отобразят только одно устройство, если в диапазоне в режиме обнаружения доступны несколько с аналогичной информацией — особенно это касается одинакового адреса.

# Практика

## Задача 1. Поднять протокол hci0

**hci0** — интерфейс bluetooth-адаптера. Прежде чем его включить, необходимо пробросить адаптер в виртуальную машину. Чтобы это сделать, необходим внешний адаптер — со встроенным можно работать только в хостовой системе:



Затем от имени **root** выполнить команды:

|  |
| --- |
| systemctl enable bluetooth.servicesystemctl start bluetooth.servicehciconfig hci0 start |

## Задача 2. Выполнить разведку пространства средствами hcitool

Выполнить разведку пространства командами:

|  |
| --- |
| hcitool scanhcitool inq |

Найти информацию о классах обнаруженных устройств.

# Практическое задание

1. Изучить утилиты для работы с bluetooth. Отчет — скриншоты с результатами исследований.
2. Отключить режим обнаружения на смартфоне, попытаться найти его с помощью Redfang. Отчет — скриншоты с результатами исследований.
3. \* Разобрать дамп hci-соединения. Указать, к какому устройству осуществлялся доступ, увенчался ли он успехом, назвать имя устройства, класс и смещение времени. Отчет должен содержать информацию об адресе, имени, смещении во времени и наличии доступа за время дампа.

<https://drive.google.com/open?id=1_XjbChRUdY06R6ZNXmNUpvJmi9UGUa5q> — ссылка на файл дампа.

# Дополнительные материалы

1. [Стандарт Bluetooth](https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737).
2. [Стандарт протокола LMP](http://www.protocols.ru/WP/rfc4204/).
3. [Описание уязвимостей](https://ru.wikipedia.org/wiki/BlueBorne).
4. [Построение связей в MPLS — для продвинутых](http://www.faqs.org/rfcs/rfc4201.html).

# Используемая литература

Для подготовки данного методического пособия были использованы следующие ресурсы:

1. [Man-page Bluelog](https://kali.tools/?p=2470).
2. [Man-page Spooftooph](https://kali.tools/?p=2479).
3. [Стандарт протокола LMP.](http://www.protocols.ru/WP/rfc4204/)
4. [Стандарт Bluetooth](https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=229737).