# ~~голубой зуб и его взлом~~охота за Голубым Зубом

крис касперски ака мыщъх, no-email

**голубой зуб наступает! поголовье bluetooth-устройств стремительно нарастает, обрушиваясь на рынок снежной лавной. реклама утверждает, что протокол передачи данных надежно защищен, но эта защита легко расстреливается снайперской винтовкой с расстояния в несколько километров. хакеры уже давно ломают голубые зубья и эта статья рассказывает как.**

**Рисунок 1 Джон Херинг (John Hering) – известный охотник за Голубым Зубом с ружьем BlueSniper, позволяющим сканировать и взламывать Голубые Зубья в радиусе нескольких километров. Первая версия этого ружья была представлена на хакерской конференции Defcon 2004**

## *введение*

Голубым зубом (BlueTooth) оснащаются сотовые телефоны, наладонники, нотебуки и многие другие мобильные устройства, что делает его заманчивым объектом для взлома. ~~в результате которого~~ Хакер может осуществлять несанкционированное подключение к устройству, перехватывать трафик, отслеживать перемещение жертвы в пространстве или устраивать полный DoS. Уже зафиксировано несколько случаев взлома влиятельных лиц и с каждым днем интенсивность хакеров все растет и растет. Разработчики Голубого Зуба делают морду тяпкой и сваливают всю ответственность на производителей оборудования, которые где-то что-то криво реализовали. Производители в свою очередь наезжают на пользователей, выбирающих предсказуемые PIN'ы, не выключающих Голубой Зуб после каждого сеанса передачи и т. д. Короче, виноватых не найдешь, а между тем количество BlueTooth устройств уже исчисляется сотнями миллионов (!) и все говорит о том, что несколько последующих лет пройдут под знаменем Голубого Зуба, реальных конкурентов которому пока не видно.

На Голубом Зубе собираются домашние и мелко корпоративные локальные сети, Голубой Зуб встраивается в клавиатуры, мыши, принтеры, часы и даже… системы управления

автомобилем. А вот это уже серьезно! Зверски спланированная операция может привести не только к утечке конфиденциальных данных, но и человеческим жертвам. Эта статья не призывает ничего ломать, я просто хотел показать насколько небезопасен Голубой Зуб, а доверять ему или нет — пусть каждый решает сам!

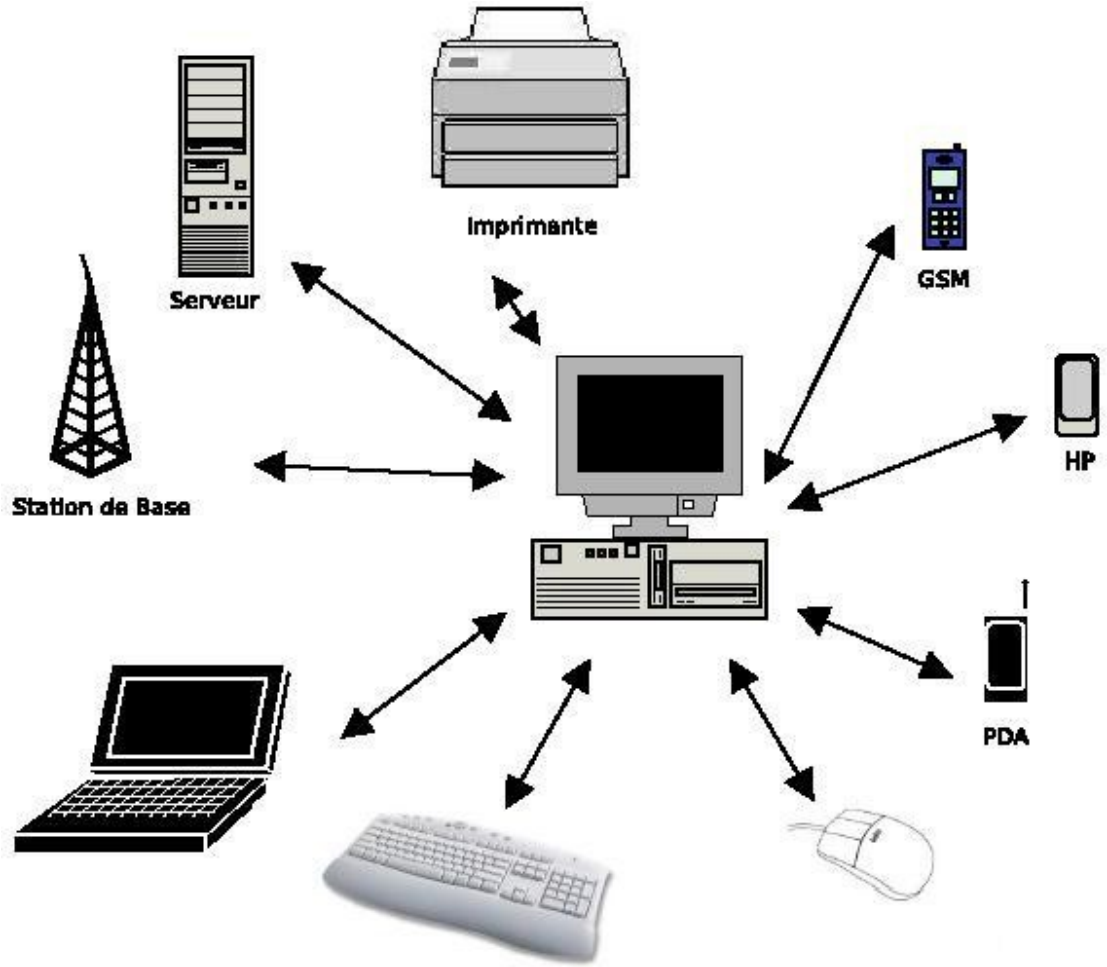


**Рисунок 2 вездесущий Голубой Зуб**

## >>> выноска: что в именем твоем

Общепринятая практика перевода BlueTooth "Голубым Зубом" выглядит довольно странной, если не сказать подозрительной. В качестве оправдания приводится король викингов Harald Blutend, якобы получивший свое прозвище из-за потемневшего переднего зуба и воссоединившего Данию и Норвегию. Дескать, произношение его имени созвучно с BlueTooth'ом, в честь которого он и был назван.

Легендарный хакер Юрий Харон предлагает свою версию перевода, которая мне кажется наиболее близкой к истине (если, конечно, допустить, что истина вообще есть). Blue – на жаргоне электронщиков означает "легкий", "простой", а tooth – "сцепка", "зацепление". Соединив все вместе, получаем: "Легкая сцепка", "Простая Связь". Логично?

## что такое голубой зуб

Голубой Зуб представляет собой устройство, работающее в диапазоне частот от 2.400 до 2.483,5 МГц (а вовсе не 2,4 МГц как думают некоторые!). На этой же частоте работают микроволновые печи, беспроводные сети стандарта 802.11b/g, радиотелефоны и многие другие устройства, агрессивно конфликтующие между собой. Для решения этой проблемы, Голубой Зуб использует специальный алгоритм скачкообразной перестройки частоты. Весь частотный диапазон "нарезается" на 79 каналов с шириной в 1 МГГц и каждые 625 мкс (1.600 раз в секунду) происходит смена канала, выбираемого по псевдослучайному принципу. Каждая такая

порция вещания ~~на определенной частоте~~ образует time-slot (тайм-слот) ~~в~~ для простоты называемый ***слотом***. Передаваемые данные разбиваются на пакеты по 2~~,~~745 бит, каждый из которых "размазывается" по нескольким ~~разбивается на несколько~~ тайм-слотам (до 5 слотов максимум).

Устройства взаимодействуют по схеме master-slave (хозяин-раб или ведомое и ведущее устройство). Один мастер может иметь до семи рабов, мастер вещает в четных слотах, а ~~каждый из~~ раб~~ов~~ — в нечетных.

Поддерживаются два типа связи: асинхронный (ACL — asynchronous connectionless) и синхронный (SCO — synchronous connection oriented). Синхронный режим преимущественно используется для передачи речи, асинхронный — для обмена данными.

Расчетная пропускная способность канала в асинхронном режиме составляет 1 Мбит/с, при этом заголовки и другая служебная информация "съедают" 20% трафика, оставляя нам ~820 Кбит/с, однако, на практике все зависит от условий связи и конструктивных особенностей конкретного передатчика. Ведомое и ведущее устройство могут иметь только один канал (link) асинхронной связи, организованный по схеме точка-точка (point-to-point) или работающий в широковещательном режиме (broadcast), причем, без разрешения хозяина раб не может переходить на асинхронный тип передачи.

В синхронный режиме связи мастер может поддерживать до тех каналов с одним, двумя или тремя ~~ведущими~~ ведомыми устройствами, с расчетной пропускной способностью каждого канала в 64 Кбит/с. Вещание ведется в слотах, назначаемых мастером. Слоты, не используемые в синхронном режиме, могут использоваться асинхронным.

Предельно допустимая мощность передатчика по спецификациям должна составлять 10 мВт, что обеспечивает устойчивую работу в радиусе 10 - 25 метров.

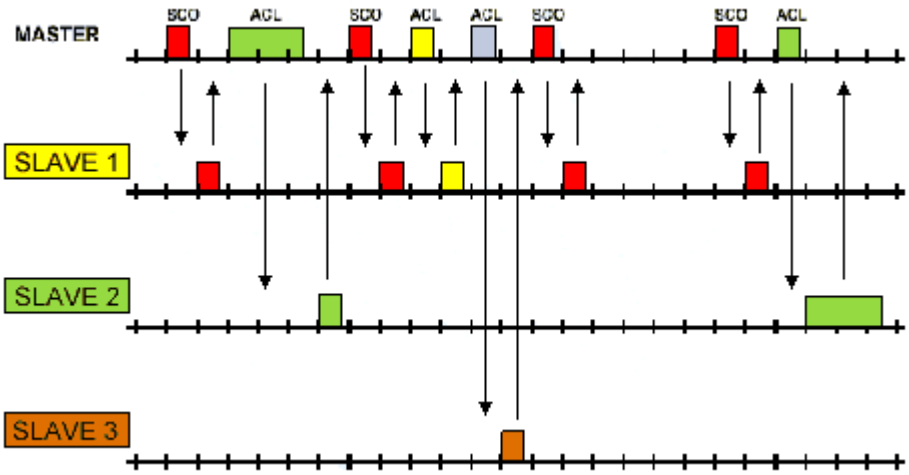


**Рисунок 3 схематичное изображение протокола передачи**

## *снайперская антенна*

Для охоты за Голубым Зубом необходимо увеличить радиус действия устройства хотя бы до сотни метров. Это легко! Достаточно разобрать адаптер, найти медную дорожку, изогнутую сексуальной буковой "П", и припаять к ней провод от внешней антенны на 2.4 ГГц, позаимствованн~~ую~~ой у WLAN-устройств.

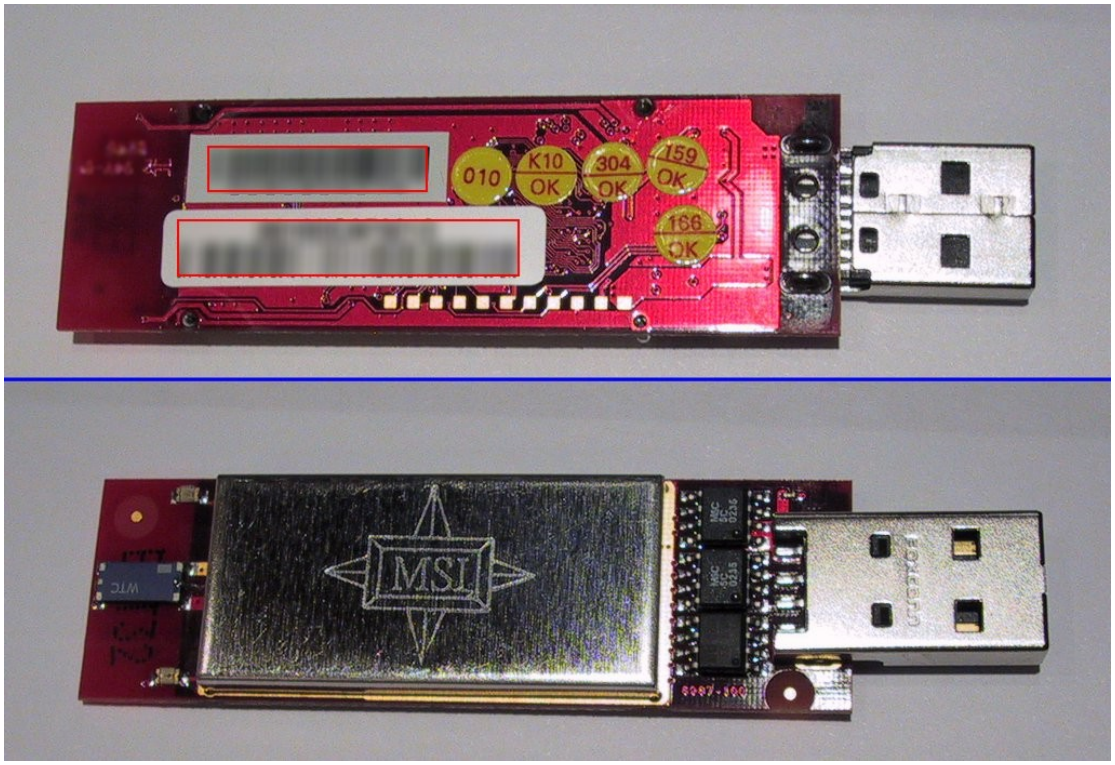


**Рисунок 4 адаптер Голубого Зуба**

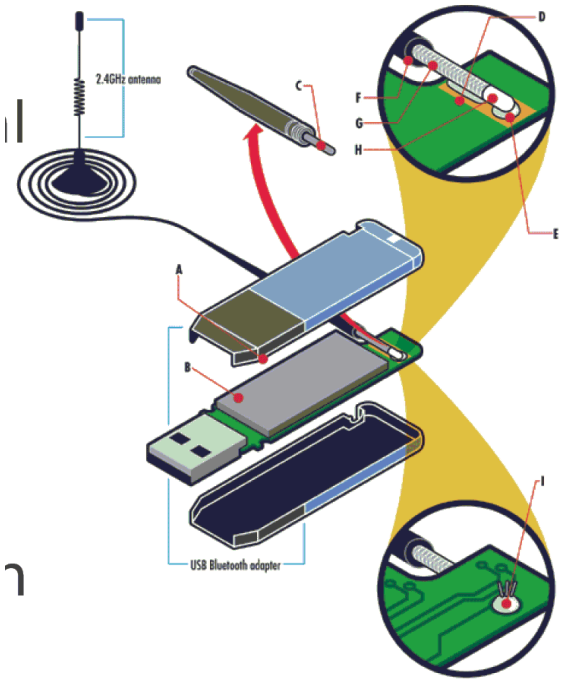


**Рисунок 5 подключение внешней антенны**

Однако, для серьезной атаки дистанция в сотню метров явно недостаточна и настоящие охотники обзаводятся узконаправленными антеннами типа randome или parabolic. Ими торгуют многие компании, например, HyperLink ~~Tech~~Technology или MAXRAD. Оформить заказ можно ~~и~~ по Интернету. Хорошая антенна стоит в пределах полусотни долларов плюс пересылка и растаможка.

**Рисунок 6 внешний вид антенны HG2415Y типа Randome от ~~HYPERLINK TECH~~ HyperLink Technology**

Наибольшей популярностью пользуется модель HG2415Y от ~~HYPERLINK TECH~~ HyperLink Technology с коэффициентом усиления 14 dB и подходящей диаграммой направленности. Компактные габариты (462 x 76 мм) позволяют уложить антенну в спортивную сумку или рюкзак, скрывающий ее от посторонних глаз и не привлекающий внимания посторонних.

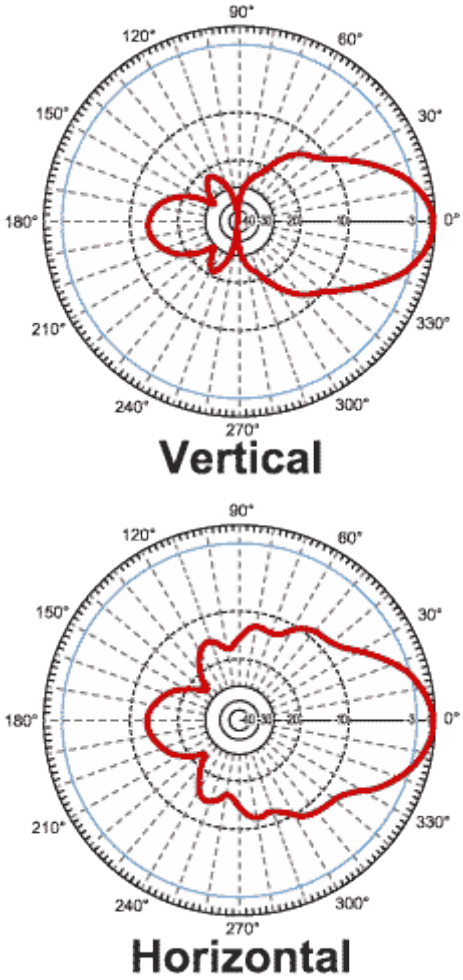


**Рисунок 7 диаграмма направленности антенны HG2415Y**

Для удобства "прицеливания" (а попасть в Голубой Зуб при такой диаграмме направленности не так-то легко!~~достаточно трудно~~), многие хакеры насаживают антенну на

фотографический штатив, приделывают к ней приклад и оптический прицел, в результате чего получается самое настоящее радио-ружье с поражающим действием в один километр.

**Рисунок 8 антенна HG2415Y, превращенная в снайперское радио-ружье**

**Рисунок 9 еще одно радио-ружье**

Из параболических антенн хотелось бы порекомендовать HG2424G все от той же ~~HYPERLINK TECH~~ HyperLink Technology. Коэффициент усиления в 24 dB выше всяких похвал. Острая диаграмма направленности бьет Голубой Зуб за несколько километров, однако неуклюжие габариты (100 x 60 см) существенно затрудняют ее транспортировку, а чрезмерная узконаправленность создает проблемы прицеливания, особенно актуальные при слежении за быстродвижущейся жертвой, так что во многих случаях HG2415Y все же оказывается предпочтительнее.

**Рисунок 10 внешний вид параболической антенны HG2415Y от ~~HYPERLINK TECH~~ HyperLink Technology**

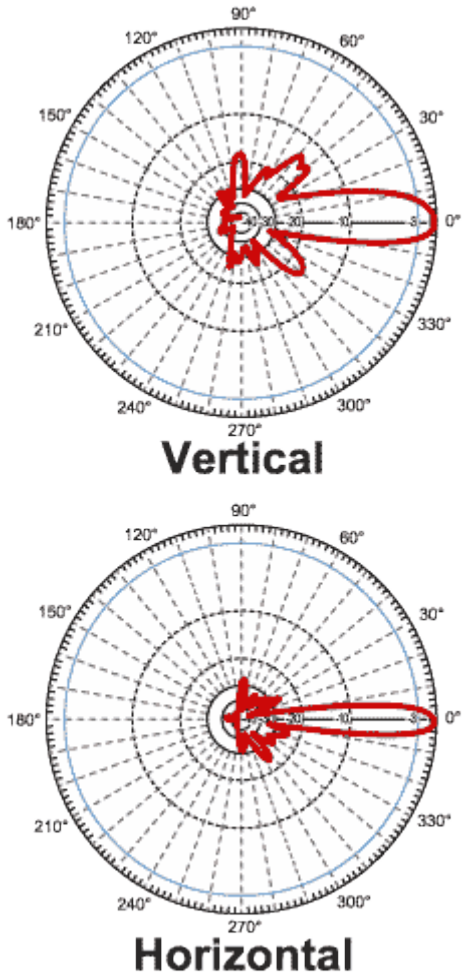


**Рисунок 11 диаграмма направленности антенны HG2415Y**

Полутораметровая параболическая антенна HG2430D с усилением в 30 dB обойдется уже в 300 долларов. Стоит ли она того? Для охоты с балкона на стационарные мишени (например, правительственное здание) несомненно — да, а вот для полевой охоты она слишком громоздка и неудобна.

## >>> врезка: полезные ссылки по антенному вопросу

- MAXRAD:
  - американская компания, выпускающая антенны и торгующая ими через Интернет: http://www.maxrad.com/cgi/press.cgi;
- ~~HYPERLINK TECH~~ HyperLink Technology:
  - еще одна американская компания, у которой можно купить антенну: http://www.hyperlinktech.com/web/antennas_2400_out_directional.php;
- Собираем ружьё Bluetooth: охота за "синими зубами":
  - познавательная статья по превращению антенны типа HG2415Y в снайперское ружье (на русском языке): http://www.thg.ru/network/20050316/print.html;

## авторизация и аутентификация

Голубой Зуб поддерживает несколько режимов секретности: Security Mode 1 (nonsecure — открытый), Security Mode 2 (Service-level enforced security — секретность уровня сервиса) и Security Mode 3 (Link-level enforced security — секретность уровня канала).

В mode 1 все системы защиты выключены, не используется ни аутентификация, ни шифрование, а само BlueTooth устройство работает в широковещательном режиме (он же "неразборчивый" — promiscuous), что делает возможным построение снифферов из доступных компонентов.

В mode 2 сразу же после установки соединения начинается процесс аутентификации, осуществляемый по L2CAP-протоколу (Logical Link Control and Adaptation Protocol — Протокол Управления Логическим Каналов и Адаптации) и выполняемый Менеджером Безопасности (Security Manager), находящимся на канальном уровне и взаимодействующим с протоколами верхних уровней. Это позволяет выборочно ограничивать доступ к устройству, например, все могут просматривать данные, но не все изменять их.

В mode 3 аутентификация происходит перед установкой соединения на канальном уровне, за счет чего все "левые" устройства будет отшиты еще на этапе подключения. Поддерживается "прозрачное" шифрование трафика, выполняемое без участия протоколов верхнего уровня, что обеспечивает максимальный уровень безопасности и комфорта, однако, даже в этом случае степень защиты относительно невелика и устройство может быть легко взломано.

Фундаментом безопасности является схема генерации ключей. Ключи генерируются на основе PIN-кодов. PIN-код представляет собой персональный идентификационный номер от 1 до 16 байт длинной, назначаемый владельцем устройства, и хранимый в энергонезависимой памяти. Большинство мобильныхх~~й~~ устройств используют 4х-значный (32-битный) PIN-код, по умолчанию выставленный в ноль. Некоторые устройства отказываются работать с нулевым PIN'ом, вынуждая пользователей изменять его на "1234" или что-то в этом роде. Но ломать такие PIN'ы неинтересно. Это все равно, что расстреливать кабана, привязанного к дереву.

На основе PIN-кода генерируется 128-битный Link Key, вычисляемый по E2 алгоритму. В свою очередь, на основе Link Key'я генерируется 128-битный Encryption Key, вычисляемый по алгоритму E3. Link Key используется для аутентификации, а Encryption Key – для шифрования трафика.

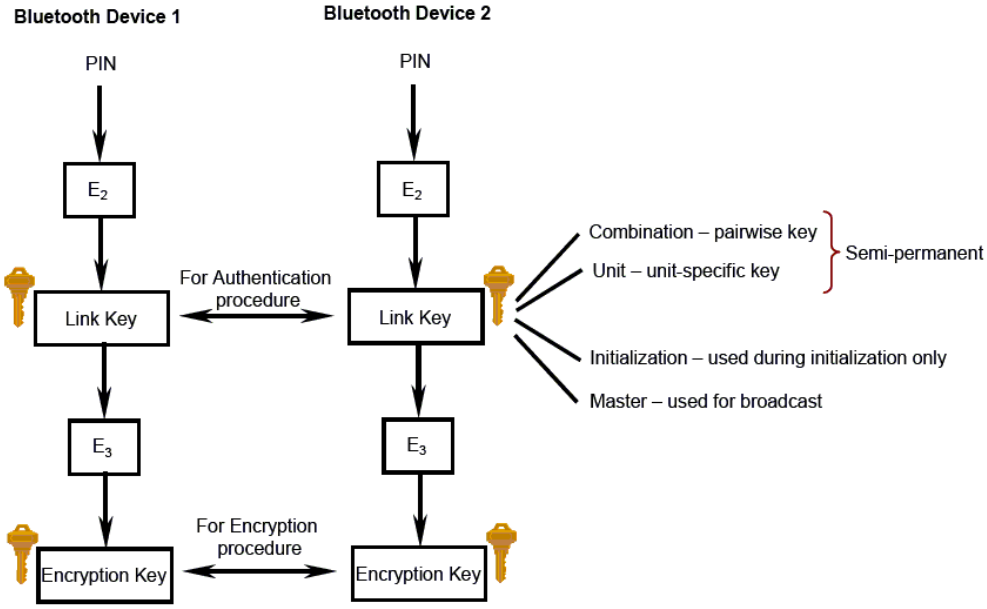


Figure 4-6. Bluetooth Key Generation from PIN

**Рисунок 12 генерация секретных ключей на основе PIN-кода**

Аутентификация осуществляется по классической схеме запрос — отклик, такой же древней как сам компьютерный мир (регистрация пользователя в UNIX и Windows NT построена на тех же принципах).

---

**Первый шаг:** Инициатор соединения (claimant~~transmitter~~) посылает заинтересованному устройству (verifier) свой уникальный 48-битный аппаратный адрес (BD_ADDR), в каком-то смысле похожий на обычный MAC-адрес, зашитый в каждой сетевой карте;

**Второй шаг:** Verifier передает ~~transmitter~~claimant'у 128-битную привязку (challenge), генерируемую случайным образом, и обозначаемую как AU_RAND;

**Третий шаг**: на основе BD_ADDR, Link Key и challenge Verifier генерирует секретную шифропоследовательность (SRES), тоже самое делает и ~~transmitter~~claimant;

**Четвертый шаг**: полученную шифропоследовательность ~~transmitter~~ claimant передает Verifier'у;

**Пятый шаг**: Verifier сравнивает вычисленную им SRES с откликом ~~transmitter~~claimant'а и если они совпадают, устанавливает соединение.

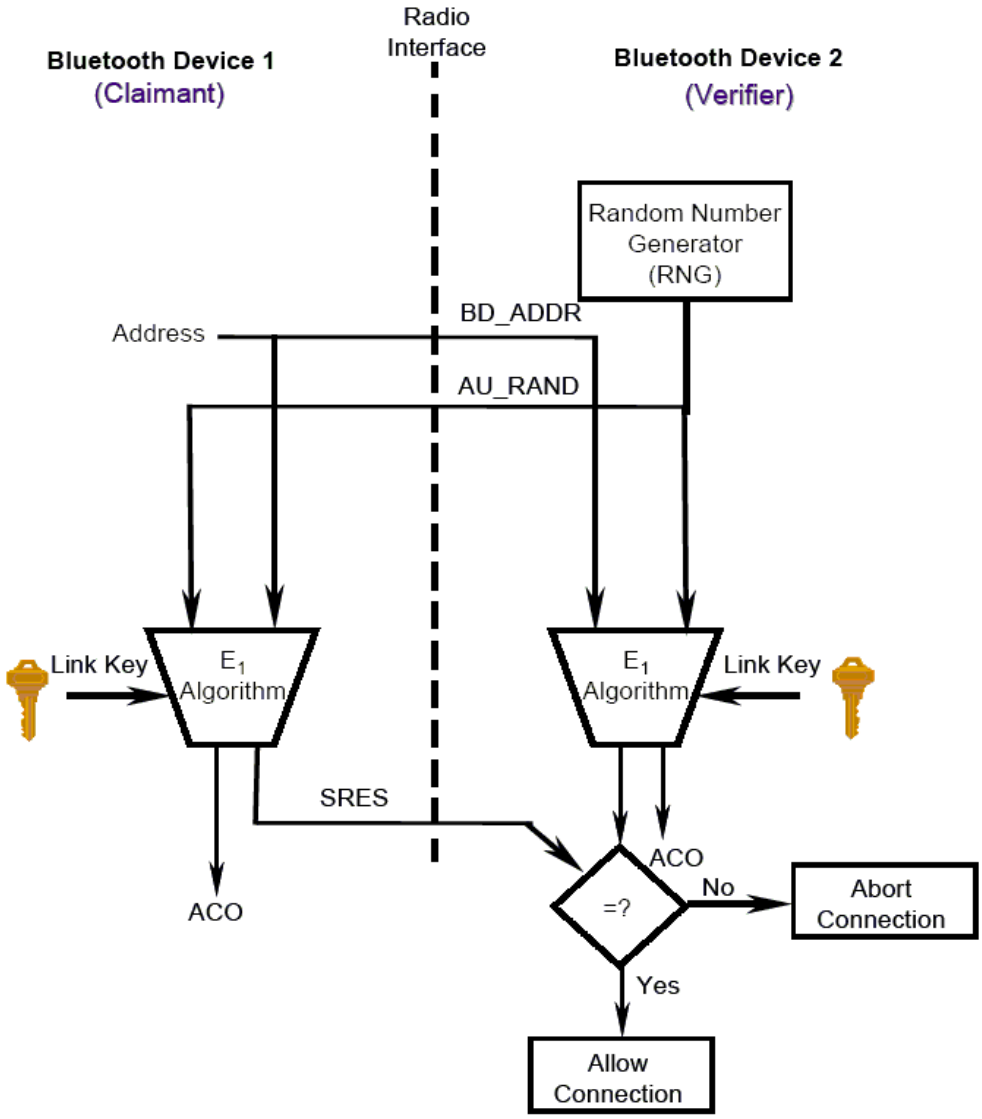


Figure 4-7. Bluetooth Authentication

**Рисунок 13 процесс аутентификации**

Таким образом, в открытом виде PIN-код не передается и поэтому не может быть перехвачен! Однако, он может быть подобран. В самом деле, мы можем перехватить BD_ADDR, AU_RAND и SRES, после чего нам остается всего лишь подобрать такой Link Key, который бы при заданных BD_ADDR и AU_RAND ~~давал бы~~выдавал идентичный SRES. Даже если используется 128-битный PIN, полный перебор на Pentium-4 занимает всего лишь несколько часов, а 4х-символный PIN взламывается практически мгновенно!

## >>> врезка: ссылки по алгоритмам шифрования

- Wireless Network Security
  - шикарное руководство по безопасности беспроводных сетей с подробным описанием протоколов аутентификации и шифрования (на английском языке): http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf;
- Bluetooth Security
  - хорошая статья с описанием протоколов аутентификации и шифрования (на английском языке): http://www.niksula.cs.hut.fi/~jiitv/bluesec.html;
- Bluetooth Security — Protocol, Attacks and Applications
  - презентация в Power Point с обзоров ключевых особенностей криптографических алгоритмов, используемых Голубым Зубом для аутентификации и шифрования (на английском языке): www.item.ntnu.no/fag/ttm4705/kollokvie_presentasjoner_2004/bluetooth_security.ppt;

## методы атаки

Три наиболее распространённых типа атаки на Голубой Зуб — это Bluetracking, Bluesnarfing, и Bluebugging.

Атаки типа Bluetracking основаны на том, что адрес устройства BD_ADDR передается в сеть в незашифрованном виде и может быть легко перехвачен и декодирован. Хакер может определить производителя устройства, модель и ее происхождение. Группа хакеров, рассредоточенных по городу и вооруженных антеннами типа randome, без труда отслеживает перемещение жертвы со вместе вытекающими последствиями.

Серия нашумевших атак типа Bluesnarfing все еще овеяна ореолом загадочности. Под изумленные взгляды окружающих хакеры вытягивают с сотовых телефон~~ах~~ов записные книжки, содержимое адресной книги, архив SMS-сообщений и другую приватную информацию. Черт возьми, как?! Хакеры улыбаются, но не отвечают. Разработчики Голубого Зуба подтверждают возможность атаки (http://www.bluetooth.com/help/security.asp), но технически~~х~~ детал~~ей~~и не разглашают. Еще бы! Во многих мобильных устройствах служба обмена объектами (Object Exchange — OBEX) работает в non-secure режиме, не требуя никакой аутентификации! Этим, в частности, грешат сотовые телефоны от Nokia, Ericsson и Sony Ericsson (в особенности модели T68, T68i, R520m, T610 и Z1010), ~~и~~ Nokia (модели 6310, 6310i, 8910 и 8910i)~~.~~ и ~~Телефоны~~ Motorola (V80, V5xx, V6xx and E398)~~менее уязвимы (OBEX протокол не требует авторизации, но обладает ограниченными возможностями)~~, а Siemens всегда работает в защищенном режиме.

Атаки типа Bluebugging (так же называемые Blue Bug) представляют собой разновидность Bluesnarfing-атак, но теперь вместо обмена объектов происходит засылка AT-команд по все тому же OBEX-протоколу. AT-команды это обыкновенные коммуникационные команды, знакомые любому модемщику. С их помощью можно отправлять SMS-сообщения, совершать голосовые звонки за счет жертвы и даже выходить в Интернет по WAP/GPRS протоколам. И все это безо всякой аутентификации! Короче, Blue Bug это серьезно, так что владельцам неблагонадежных сотовых телефонов лучше ~~всего~~ всегда держать Голубой Зуб выключенным.

Наконец, даже полностью защищенные телефоны типа того же Siemens'a могут быть взломаны лобовым перебором. Как уже отмечалось, 4х-значный PIN вскрывается за несколько секунд и даже если в будущих моделях производители увеличат длину PIN-кода до 16-~~символов~~байт, это не остановит взломщиков, ~~и~~но сильно напряжет пользователей. Такой PIN запомнит далеко не каждый, а это значит, что повсеместно будут использоваться осмысленные "словарные" номера, существенно упрощающие их перебор.

Всего же существует более двух десятков типов атак, которые было бы слишком утомительно описывать здесь. Тот кто хочет узнать больше, может обратиться к замечательной книге "Wireless Network Security" и другим подобным документам.

## >>> врезка: ссылки по теме взлома

- Bluetooth Security Preliminary Study
  - обзор основных атак на Голубой Зуб (на английском языке): http://student.vub.ac.be/~sijansse/2e%20lic/BT/Voorstudie/PreliminaryStudy.pdf;
- Wireless Security

- перечень уязвимостей Голубого Зуба, подтвержденный его создателями: http://www.bluetooth.com/help/security.asp;

- Hardware Hacker
  - замечательное пособие для хакеров-железячников (на английском языке): http://www.grandideastudio.com/files/books/hpyn2e_chapter14.pdf;

## *чем ломать*

Хачить Голубой Зуб лучше всего под Линухом, открытая архитектура которого позволяет использовать уже готовые компоненты и содержит кучу полезных утилит, которые можно использовать для сканирования или Bluesnarfing атаки. Например, hciconfig, запущенную с ключом "-ifconfig" или hcitool со следующими ключами: Scan — просканировать периметр и распечатать список обнаруженных BlueTooth устройств; Name — возвратить имя удаленного устройства, Cmd — управление локальным Голубым Зубом по HCI-интерфейсу, Cc — создать подключение. Подробное разъяснение всех команд содержится в man'e.

```
# hciconfig -a
hci0:   Type: USB
        BD Address: 00:02:5B:A1:88:52 ACL MTU: 384:8  SCO MTU: 64:8
        UP RUNNING PSCAN ISCAN
        RX bytes:9765 acl:321 sco:0 events:425 errors:0
        TX bytes:8518 acl:222 sco:0 commands:75 errors:0
        Features: 0xff 0xff 0x8b 0xfe 0x9b 0xf9 0x00 0x80
        Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
        Link policy: RSWITCH HOLD SNIFF PARK
        Link mode: SLAVE ACCEPT
        Name: 'Casira BC3-MM'
        Class: 0x1e0100
        Service Classes: Networking, Rendering, Capturing, Object Transfer
        Device Class: Computer, Uncategorized
        HCI Ver: 1.2 (0x2) HCI Rev: 0x529 LMP Ver: 1.2 (0x2) LMP Subver: 0x529
        Manufacturer: Cambridge Silicon Radio (10)

# hcitool scan
Scanning ...
        00:04:0E:21:06:FD       AVM BlueFRITZ! AP-DSL
        00:01:EC:3A:45:86       HBH-10
        00:04:76:63:72:4D       Aficio AP600N
        00:A0:57:AD:22:0F       ELSA Vianect Blue ISDN
        00:E0:03:04:6D:36       Nokia 6210
        00:80:37:06:78:92       Ericsson T39m
        00:06:C6:C4:08:27       Anycom LAN Access Point
```

**Рисунок 14 сканирование BlueTooth устройств утилитой hcitool**

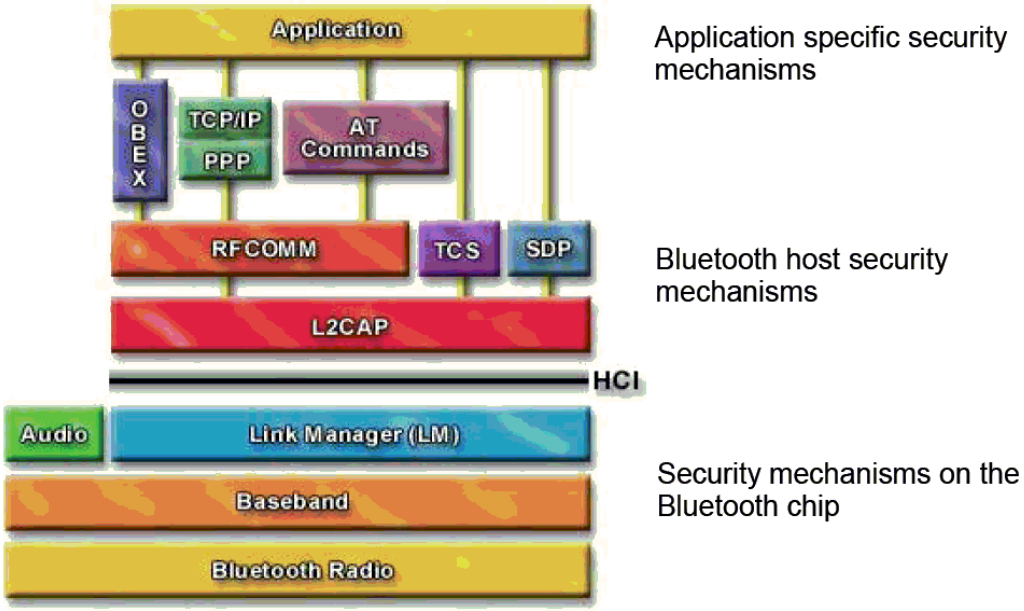


**Рисунок 15 стек протоколов Голубого Зуба**

До HCI-интерфейса можно дотянуться через Ioctl-коды или опции сокетов. Команды, отвечающие за это имеют характерный префикс HCI. К их числу принадлежат HCI_Create_New_Unit_Key, HCI_Read_Pin_Type, HCI_Read_Authentication_Enable, HCI_Read_Encryption_Mode, HCI_Change_Local_Link_Key, HCI_Master_Link_Key и многие другие.

## >>> выноска: ссылки по программированию Голубого Зуба

- Bluetooth and Linux
  - большой сборник HOW-TO по программированию Голубого Зуба под Линухом (на английском языке): http://www.holtmann.org/linux/bluetooth;

## >>> врезка: ошибка переполнения в WIDCOMM

Создатели Голубого Зуба предлагают готовое программное обеспечение для его поддержки, ~~так называемое~~ распространяемое под торговой маркой WIDCOMM (Wireless Internet and Data/Voice Communications — Беспроводной Интернет и Коммуникации для передачи Голоса и Данных), что избавляет производителей оборудования от необходимости реализовывать весь стек протоколов самостоятельно. Программисты старой школы (к которым принадлежит и Юрий Харон) хорошо знают истинную цену решений из "пробирки". Обжегшись на чужих ошибках пару раз, они не доверяют никакому коду, кроме своего собственного. И ведь не зря!

В августе 2004 года в WIDCOMM'е было обнаружено тривиальное переполнение буфера, позволяющее захват~~ить~~ывать управление устройством простой посылкой специально подготовленного пакета. Никакой PIN для этого подбирать не нужно~~адо~~!.

Уязвимость затрагивает BTStackServer версии 1.3.2.7, 1.4.1.03 и 1.4.2.10, ~~которые используется~~ используемые в Windows 98, Windows XP, Windows CE и др-угих системах. Кроме этого, WIDCOMM используется многими компаниями: Logitech, Samsung, Sony, Texas Instruments, Compaq, Dell… полный перечень включает в себя более трех десятков наименований. Все BlueTooth устройства, производимые этими компаниями, находятся под угрозой и в любой момент могут быть атакованы. Для популярного наладонника HP IPAQ 5450 даже написан специальный эксплоит! В некоторых случаях, проблема решается установкой всех заплаток или сменой прошивки, некоторые же устройства остаются открытыми до сих пор.

Подробности можно найти здесь: http://www.pentest.co.uk/documents/ptl-2004-03.html

## *заключение*

Взлом Голубого Зуба это не фантастика! Это реальность, доступная каждому из нас! Есть такой вид радиоспорта — охота на Лис. В укромном месте закладывается передатчик (лиса), который пытаются запеленговать вооруженные приемниками радиолюбители. Кто первый его обнаружит — тот и победил. По аналогии с этим, дистанционный взлом Голубого Зуба был прозван Охотой на Кур — беззащитный пользователей, трепещущих под снайперским радиоружьем словно желторотые птенцы.

Это азартно и интересно. Это захватывает и не отпускает. Подстрелив свою первую дичь, хочется стрелять еще и еще. Здесь и долгое сидение в засаде, и предварительная техническая подготовка, и тщательно отлаженная экипировка, которая ни за что не подведет и конечно же чувство справедливого восторга хищника, набрасывающегося на ничего не подозревающую добычу.