

Cracking BlueTooth for Phun and Profit

Brad (theNURSE) Smith,
RN,CISSP...

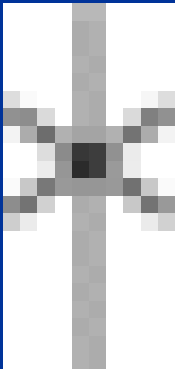
Director, National Cyber Defense Force
dir@NationalCyberDefenseForce.org

Agenda

- Basics of Bluetooth
 - Best chips for cracking, antennas, protocols, basic commands for Linux / Windows
- Review of programs used
 - Programs that could be used in a Assessment
- Securing Bluetooth
- Additional help resources

Why BT?

- *Blåtand* King Harald I of Denmark
- Name is binding rune on Haralds name
- Not really secure, wireless **serial port**
(Erickson)



OH, chipped my BTooth

- Not by price, by class

Class 1	100 mW (20dBm)	~100 meters
Class 2	2.5 mW (4dBm)	~10 meters
Class 3	1 mW (0dBm)	~1 meter

- External Antenna plugs
- Cambridge Silicon Radio (CSR) chipset



Low Level Protocols

- 2.4 – 2.4835 GHz, 79 bands, 1 mHz wide
- FHS - Hops 1600 X second
- “Discoverable” to Master device with data to start
- Piconet -> 255 slaves in Active, Sniff, Hold or Park
 - Park -> Still synchronized with Master




High Level Protocols

- LLC/Adaptation Protocol (L2CAP) -> **TCP**
 - LwCAP -> creation, sequencing, reassembles, QOS, Channel Identifiers (CI)
 - CI -> IRQ
- Radio Frequency Communication (rfcomm)
 - RSS-232 replacement, 60 emulated channels
- Service Discover Protocol (SDP)

Just Stinkin SERIAL cable!

- Just like old serial
 - Must set Memory location to match other device (IRQ 3, 02F8-02FF)
 - What is this?
 - To Audit, you **MUST** link to the CI (channel) and Memory address of TOE
 - 2 separate process, just like IRQ and MEM

Applications

- Dial-up Networking (DUN) 
- File Transfer Protocol (FTP) 
- Headset Profile (HSP)
- Object Push Profile (OPP) 
- Advanced Audio Distribution Profile (A2DP)

BTeeth in my Windows

- Best Win7
- PAN
- Server for piconet
 - DHCP
- Proximity Marketing 😊
 - Sales broadcast as you go by (buy)
 - “Hey stop in for 10% discount”



Bluetooth in Linux

- Make sure BT is plugged in/ light on
- Hciconfig scan
 - if no results, your toast
- Results, bring the BT up
- May not inject

```
root@bt:~# hciconfig scan
hci0:  Type: USB
      BD Address: 00:21:85:EA:C7:EF ACL MTU: 310:10 SCO MTU: 64:8
      DOWN
      RX bytes:1040 acl:0 sco:0 events:38 errors:0
      TX bytes:415 acl:0 sco:0 commands:38 errors:0

root@bt:~#
```

Default

```
root@bt:~# hciconfig -a hci0
hci0:  Type: USB
      BD Address: 00:21:85:EA:C7:EF ACL MTU: 310:10 SCO MTU: 64:8
      UP RUNNING
      RX bytes:2136 acl:0 sco:0 events:48 errors:0
      TX bytes:442 acl:0 sco:0 commands:48 errors:0
      Features: 0xff 0xff 0x8f 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: 'bt-0'
      Class: 0x0a010c
      Service Classes: Networking, Capturing
      Device Class: Computer, Laptop
      HCI Ver: 2.0 (0x3) HCI Rev: 0xc5c LMP Ver: 2.0 (0x3) LMP Subver: 0xc5c
      Manufacturer: Cambridge Silicon Radio (10)

root@bt:~# █
```

Concealment Commands

```
hciconfig -a or scan
```

```
hciconfig -a hci0 up or down
```

```
hciconfig -a hci0 class 0x500204
```

```
hciconfig -a hci0 lm accept, master;
```

```
hci.. -a hci0 lp rswitch,hold,sniff,park;
```

```
hciconfig -a hci0 auth enable
```

```
hciconfig -a hci0 encrypt enable
```

```
hciconfig -a hci0 name Resume
```

Reset

Ready to
go!

```
root@bt:~# hciconfig -a hci0
hci0:  Type: USB
      BD Address: 00:21:85:EA:C7:EF ACL MTU: 310:10 SCO MTU: 64:8
      UP RUNNING AUTH
      RX bytes:8139 acl:0 sco:0 events:143 errors:0
      TX bytes:2277 acl:0 sco:0 commands:143 errors:0
      Features: 0xff 0xff 0x8f 0xfe 0x9b 0xf9 0x00 0x80
      Packet type: DM1 DM3 DM5 DH1 DH3 DH5 HV1 HV2 HV3
      Link policy: RSWITCH HOLD SNIFF PARK
      Link mode: ACCEPT MASTER
      Name: 'Resume'
      Class: 0x500204
      Service Classes: Object Transfer, Telephony
      Device Class: Phone, Cellular
      HCI Ver: 2.0 (0x3) HCI Rev: 0xc5c LMP Ver: 2.0 (0x3) LMP Subver: 0xc5c
      Manufacturer: Cambridge Silicon Radio (10)

root@bt:~# █
```

BT Scanning Methodology

Step	Tool	Task
Live Systems	BTscan hcitool scan	Live BT in area
Open ports (CI)	L2ping sdptool browse	Find open Channels (ports)
Banners /service	Sdptool browse TOE	Services for exploit TOE

Vulnerable services	BTbugger bluesnarfer	Find services to exploit
Prepare Proxies	Bccmd sdptool	Match Mem / CI (channel) of TOE
Attack	Bluebugger Bluesnarfer	Profit: phone book, messages, contacts,

Bluescan

Hora: 05:49:33

Dispositivo: 00:21:85:EC:00:70

Nombre: theNURSEnetbook

Fabricante: TOSHIBA

Servicios activos: Audio Source Audio Sink COM7 A/V Remote
Network Service File Transfer Service Object Push Service

Canales activos: 1 2 3 4 5 6

Hora: 05:49:34

Dispositivo: 00:90:4B:20:8C:57

Nombre: BRAD

Fabricante:

Servicios activos:

Canales activos:

Hora: 05:49:40

Dispositivo: 00:23:AA:E0:66:01

Nombre: CHIPHONE

Fabricante:

Servicios activos:

Canales activos:

Hora: 05:49:41

Dispositivo: 00:21:85:EC:00:70

Nombre: theNURSEnetbook

l2Ping

SDPTool

```
root@bt: /pentest/bluetooth/blueprint - Shell - Konsole
Session Edit View Bookmarks Settings Help
root@bt: /pentest/bluetooth/blueprint# l2ping 00:21:85:EC:00:70
Ping: 00:21:85:EC:00:70 from 00:21:85:EA:C7:EF (data size 44) ...
44 bytes from 00:21:85:EC:00:70 id 0 time 65.68ms
44 bytes from 00:21:85:EC:00:70 id 1 time 38.75ms
44 bytes from 00:21:85:EC:00:70 id 2 time 38.74ms
44 bytes from 00:21:85:EC:00:70 id 3 time 38.76ms
44 bytes from 00:21:85:EC:00:70 id 4 time 34.91ms
44 bytes from 00:21:85:EC:00:70 id 5 time 36.91ms
c44 bytes from 00:21:85:EC:00:70 id 6 time 34.90ms
44 bytes from 00:21:85:EC:00:70 id 7 time 28.75ms
^C8 sent, 8 received, 0% loss
root@bt: /pentest/bluetooth/blueprint# sdptool browse
Inquiring ...
Failed to connect to SDP server on 00:23:AA:E0:66:01: Operation al
Browsing 00:21:85:EC:00:70 ...
Service Name: Audio Source
Service Provider: TOSHIBA CORPORATION
Service RecHandle: 0x101f0
Service Class ID List:
  "Audio Source" (0x110a)
Protocol Descriptor List:
  "L2CAP" (0x0100)
    PSM: 25
  "AVDTP" (0x0019)
    uint16: 0x102
Language Base Attr List:
  code_IS0639: 0x656e
```

hcitool

```
root@bt:~# hcitool info 00:21:85:EC:00:70
Requesting information ...
  BD Address: 00:21:85:EC:00:70
  Device Name: theNURSEnetbook
  LMP Version: 2.1 (0x4) LMP Subversion: 0x12e7
  Manufacturer: Cambridge Silicon Radio (10)
  Features page 0: 0xff 0xff 0x8f 0xfe 0x9b 0xff 0x59 0x83
    <3-slot packets> <5-slot packets> <encryption> <slot offset>
    <timing accuracy> <role switch> <hold mode> <sniff mode>
    <park state> <RSSI> <channel quality> <SCO link> <HV2 packets>
    <HV3 packets> <u-law log> <A-law log> <CVSD> <paging scheme>
    <power control> <transparent SCO> <broadcast encrypt>
    <EDR ACL 2 Mbps> <EDR ACL 3 Mbps> <enhanced iscan>
    <interlaced iscan> <interlaced pscan> <inquiry with RSSI>
    <extended SCO> <EV4 packets> <EV5 packets> <AFH cap. slave>
    <AFH class. slave> <3-slot EDR ACL> <5-slot EDR ACL>
    <sniff subrating> <pause encryption> <AFH cap. master>
    <AFH class. master> <EDR eSCO 2 Mbps> <EDR eSCO 3 Mbps>
    <3-slot EDR eSCO> <extended inquiry> <simple pairing>
    <encapsulated PDU> <non-flush flag> <LST0> <inquiry TX power>
    <extended features>
  Features page 1: 0x01 0x00 0x00 0x00 0x00 0x00 0x00 0x00
```

BTScanner

Session Edit View Bookmarks Settings Help

Time	Address	Clk off	Class	Name
2010/09/01 05:38:05	00:03:7A:D1:DD:ED	0x3329	0x1c010c	(unknown)
2010/09/01 05:49:39	00:90:4B:20:8C:57	0x2c30	0x020104	BRAD
2010/09/01 06:05:56	00:21:85:EC:00:70	0x08d0	0x0c010c	theNURSEnetbook
2010/09/01 06:05:56	00:23:AA:E0:66:01	0x27fe	0x5a0204	CHIPHONE

RSSI: +0 LQ: 000 TXPWR: Cur +0
Address: 00:23:AA:E0:66:01
Found by: 00:21:85:EA:C7:EF
OUI owner:
First seen: 2010/09/01 05:30:26
Last seen: 2010/09/01 06:06:48
Name: CHIPHONE
Vulnerable to:
Clk off: 0x27fe
Class: 0x5a0204
Phone/Mobile
Services: Networking,Capturing,Object Transfer,Telephony

HCI Version

LMP Version: 2.0 (0x3) LMP Subversion: 0x0
Manufacturer: MediaTek, Inc. (70)

HCI Features

Features: 0xff 0xff 0x8d 0xf8
<3-slot packets> <5-slot packets> <encryption> <slot offset>
<timing accuracy> <role switch> <hold mode> <sniff mode> <park state>

Found device 00:21:85:EC:00:70
Found device 00:23:AA:E0:66:01
Found device 00:23:AA:E0:66:01
Found device 00:21:85:EC:00:70

■ Channel Proxy

```
root@bt:/pentest# sdptool add --channel=3 DUN
Dial-Up Networking service registered
root@bt:/pentest# sdptool add --channel=6 FTP
OBEX File Transfer service registered
root@bt:/pentest# sdptool add --channel=7 OPUSH
OBEX Object Push service registered
root@bt:/pentest#
```

■ Change Memory

```
root@bt:/pentest/bluetooth# hciconfig hci* revision
hci0:  Type: USB
      BD Address: 00:21:85:EA:C7:EF ACL MTU: 310:10 SCO MTU: 64
      Unified 2le
      Chip version: BlueCore4-ROM
      Max key size: 128 bit
      SCO mapping: HCI
root@bt:/pentest/bluetooth# bccmd psget -s 0x0000 0x02bf
USB product identifier: 0xa97a (43386)
root@bt:/pentest/bluetooth# bccmd psset -s 0x0000 0x02bf 0x0002
root@bt:/pentest/bluetooth# bccmd psget -s 0x0000 0x02bf
USB product identifier: 0x0002 (2)
root@bt:/pentest/bluetooth#
```

Bluesnarfer

```
root@bt:/pentest/bluetooth/bluesnarfer# ./bluesnarfer
bluesnarfer: you must set bd_addr
bluesnarfer, version 0.1 -
usage: ./bluesnarfer [options] [ATCMD] -b bt_addr

ATCMD      : valid AT+CMD (GSM EXTENSION)

TYPE       : valid phonebook type ..
example    : "DC" (dialed call list)
            : "SM" (SIM phonebook)
            : "RC" (recevied call list)
            : "XX" much more

-b bdaddr  : bluetooth device address
-C chan    : bluetooth rfcomm channel

-c ATCMD   : custom action
-r N-M     : read phonebook entry N to M
-w N-M     : delete phonebook entry N to M
-f name    : search "name" in phonebook address
-s TYPE    : select phonebook memory storage
-l         : list aviable phonebook memory storage
-i         : device info
root@bt:/pentest/bluetooth/bluesnarfer#
```

Bluebugger

```
root@bt:~# bluebugger

bluebugger 0.1 ( MaJoMu | www.codito.de )
-----

Usage: bluebugger [OPTIONS] -a <addr> [MODE]

    -a <addr>      = Bluetooth address of target

Options:
-----
    -m <name>      = Name to use when connecting (default: '')
    -d <device>    = Device to use (default: '/dev/rfcomm')
    -c <channel>   = Channel to use (default: 17)
    -n             = No device name lookup
    -t <timeout>   = Timeout in seconds for name lookup (default: 5)
    -o <file>      = Write output to <file>

Mode:
-----
    info           = Read Phone Info      (default)
    phonebook      = Read Phonebook       (default)
    messages       = Read SMS Messages    (default)
    dial <num>     = Dial number
    ATCMD          = Custom Command (e.g. '+GMI')

Note: Modes can be combined, e.g. 'info phonebook +GMI'

* You have to set the target address
```

Securing BT

- Keep BT on “non-discoverable” when not using or Turn OFF
- Keep your device close
- Don't store SSN, credit cards #....
- Use strong PIN (5+ digits)
- Password protect your device
- NIST “**Guide to Bluetooth Security**” 800-121

Review

- Chips
- Low / High level protocols
- Using in Windows
- Does it work in Linux
- Basic command line tools
- Should now be functional for scanning

Additional Help

- Backtrack-Linux.org -> Help on BT tools
- Youtube -> Just search bluetooth
- www.soldierx.com/bbs/201001/Bluetooth-hacking-wth-Backtrack-4
- www.trifinite.org
- <http://en.wikipedia.org/wiki/Bluetooth>
- <http://www.everydaynodaysoff.com/2010/06/03/bluetooth-sniffer-guns-a-good-way-to-get-shot/>

Questions and Thanks

- Easy to crack your tooth!
- More threats every day
- Secure your group Today!

Thanks for attending, Brad (theNURSE)

dir@NationalCyberDefenseForce.org



