blucat

Joseph Paul Cohen
Security BSides Boston 2013
http://blucat.sf.net
SOCKETS!
Interposition?
Primary Objective of the Internet
Streams are awesome!
Locally we can just stream files to applications
On the internet this gets a bit of abstraction with sockets
Now we can think about Bluetooth this way too
Use case

cat foo.mpg | Internet | vlc -
cat foo.mpg | Bluetooth | vlc -
with netcat

| nc machine1 123 |

nc -l 123 |
Usage:
  blucat devices : Lists devices
  blucat services : Lists all RFCOMM services
  blucat services <device> : List RFCOMM services for one device
  blucat scan <device> : Scan all RFCOMM channels
  blucat -l : Listen for RFCOMM connection
  blucat -l <port> : Listen for RFCOMM connection on port
  blucat -uuid <uuid> : Listen for UUID and attempt RFCOMM
  blucat -l <port> -e <command>: Listen for RFCOMM connection, execute <command> when connection
  blucat <server args> -k : Keep the connection alive
  blucat -url <url> : Connect to RFCOMM URL
  blucat doctor : Run this if it’s not working
with blucat

| blucat -url btspp://0002723E6A6A:4

blucat -l 4 |
with nmap

Starting Nmap 5.21 ( http://nmap.org )
Nmap scan report
Not shown: 846 closed ports, 152 filtered ports
PORT    STATE SERVICE
22/tcp   open    ssh
80/tcp   open    http
Discovery

$blucat devices
Searching for devices
  123456789000, "Nexus 7", Trusted: true, Encrypted: false
  012345678900, "GT-P1010", Trusted: false, Encrypted: false
  001234567890, "Android Dev Phone 1", Trusted: true, Encrypted: false
Found 3 device(s)
Discovery

$blucat services
Listing all services
Searching for services on 123456789000 Nexus 7
123456789000, "Nexus 7", "Test Service Name", ",", btspp://123456789000:20
123456789000, "Nexus 7", "Hello world!!!", ",", btspp://123456789000:27
123456789000, "Nexus 7", "OBEX Object Push", ",", btgoep://123456789000:12
Searching for services on 012345678900 GT-P1010
012345678900, "GT-P1010", "OPP Server", ",", btgoep://012345678900:2
012345678900, "GT-P1010", "FTP Server", ",", btgoep://012345678900:1
Searching for services on 001234567890 Android Dev Phone 1
001234567890, "Android Dev Phone 1", "Voice Gateway", ",", btspp://001234567890:10
Scanning

$blucat scan 123456789000
Scanning RFCOMM Channels 1-30
btssp://123456789000:1 -> connection timeout
btssp://123456789000:2 -> connection timeout
btssp://123456789000:3 -> connection timeout
btssp://123456789000:4 -> connection timeout
btssp://123456789000:5 -> connection timeout
btssp://123456789000:6 -> connection timeout
btssp://123456789000:7 -> Failed to open baseband connection(2)
btspp://123456789000:8 -> connection timeout
btssp://123456789000:9 -> connection timeout
btssp://123456789000:10 -> Open Channel!!! BluetoothRFCommClient
btssp://123456789000:11 -> Open Channel!!! BluetoothRFCommClient
btssp://123456789000:12 -> Open Channel!!! BluetoothRFCommClient
btssp://123456789000:13 -> Failed to open connection(2) [0xe000]
btspp://123456789000:14 -> connection timeout
btssp://123456789000:15 -> Failed to open connection(2) [0xe000]
btspp://123456789000:16 -> Failed to open baseband connection(2)
btspp://123456789000:17 -> connection timeout
btssp://123456789000:18 -> connection timeout
Bluetooth URI Moniker:
btssp://10643FC98386:17

btssp - Bluetooth serial port profile
RFCOMM

btl2cap - Logical link control and adaptation protocol

btgoep - OBEX Generic Object Exchange profile (GOEP)
Bluetooth URI Moniker

btsspp://10643FC98386:17

Instead of IP's we have MAC addresses

Can be looked up here:
Bluetooth URI Moniker
btspan://10643FC98386:17

There are 30 channels to choose from

Bluetooth channel width is 1MHz
+,1362010219433, 000C55F8FBEE, "Officejet 6300 series"

00-0C-55 (hex)  Microlink Communications Inc.
000C55 (base 16) Microlink Communications Inc.
8F, 31, Hsintai Road
Chupei City
Hsinchu 302
TAIWAN, PROVINCE OF CHINA
Searching for services on 30F306598203:2
"Officejet 6300 series", "OBEX Object Push", "", btgoep://30F306598203:2
"Officejet 6300 series", "Basic Printing", "", btgoep://30F306598203:4
"Officejet 6300 series", "Serial Port", "", btgoep://30F306598203:1
"Officejet 6300 series", "Basic Imaging", "", btgoep://30F306598203:3
"Serial Port", ",", \texttt{btspp://30F306598203:1}

\texttt{$./blucat\ -url\ btspp://30F306598203:1$}
Dear Sir,

Your serial port is showing.
Alcatel one touch 665A
Alcatel one touch 665A

Searching for services on 9471ACAAAAAAA, “Alcatel one touch 665A”

“Serial Port0”, “”, btspp://9471ACDBACAD:11
“AUDIO Gateway”, “”, btspp://9471ACDBACAD:1
“OBEX Object Push”, “”, btgoep://9471ACDBACAD:4
“Serial Port0”, “”, btspp://9471ACDBACAD:11
“Dial-up Networking”, “”, btspp://9471ACDBACAD:9
“Voice gateway”, “”, btspp://9471ACDBACAD:2
$ ./blucat -url btspp://9471ACAAAAAA:11
AT+CGMI
+CGMI: Alcatel
OK

AT+CGMM
+CGMM: one touch 665A
OK

AT+CGMR
+CGMR: Alcatel 010 04, 2012/03/05 14:56
OK
More AT Commands?

https://github.com/boos/bluesnarfer/blob/master/src/bluesnarfer.c

http://www.forensicswiki.org/wiki/AT_Commands

http://www.anotherurl.com/library/at_test.htm

http://gatling.ikk.sztaki.hu/~kissg/gsm/at+c.html
On connect execution!

$./blucat -v -l -e /bin/bash
#Listening at btspp://002608D6A03A:4

$./blucat services
"BlueCatPipe","",btspp://002608D6F03F:4

$./blucat -url btspp://002608D6F03F:4 -v
#Connected
Hi
/bin/bash: line 1: Hi: command not found
Details

Java based

Uses BlueCove Java Libraries

Only works with RFCOMM so far

Tested on Mac, Ubuntu with Bluez
svn co http://svn.code.sf.net/p/blucat/code/trunk/blucat/
x86, x64, ARM
blucat and bluecat.arm

$.blucat
$.blucat.arm

if [[ $OSTYPE == *darwin* ]]; then
  LIBS=build/blucat.jar:lib/bluecove-2.1.1-SNAPSHOT.jar
  ...
elif [[ $OSTYPE == *linux* ]]; then
  arm/bluecove-gpl-2.1.1-SNAPSHOT.jar
fi

java -cp $LIBS Main $@ 2>&1 | grep -v -E '(Pool|BlueCove)'
Java Native Interface

==Somewhere in the program:
System.loadLibrary("bluecove")
// Searched for file
// libbluecove.so
// in LD_LIBRARY_PATH

==BluetoothStackBlueZ.java:
private native int rfServerGetChannelIDImpl(long handle) throws IOException;

==Some C file
JNIEXPORT void JNICALL Java_bluecove_rfServerGetChannelIDImpl(JNIEnv *env, jobject obj, jlong handle){...}
Bluetooth Backdoor?

POC Android Bluetooth backdoor demo
(no code released)

$pm list packages -f

$am start 'http://josephpcohen.com'

More: http://www.anddev.org/using_the_am-tool_start_activities-intens_from_a_shell-t368.html
End