USBProxy

USB tinkering for hackers and makers

Dominic Spill
dominicgs@gmail.com

Dominic Spill

USBProxy developer

Work on Ubertooth, BTBB, gr-bluetooth, Daisho, Unambiguous Encapsulation

Other projects include fcc.io, BeagleDancer, PS/2 tap, EMF Camp

Introduction to USB

2 billion USB devices sold each year (2008)

Most common device interface

Low / Full / High / Super speed

SuperSpeed Plus coming soon

Introduction to USB

- Descriptors (usbdescriptors.com)
- Host → Device architecture
- Speak when spoken to
- Device classes
  - HID
  - Mass Storage
  - Network
  - Vendor Specific

USB IDs

16 bit Vendor ID

16 bit Product ID

Expensive to become a vendor

OpenMoko give away product IDs

USBProxy

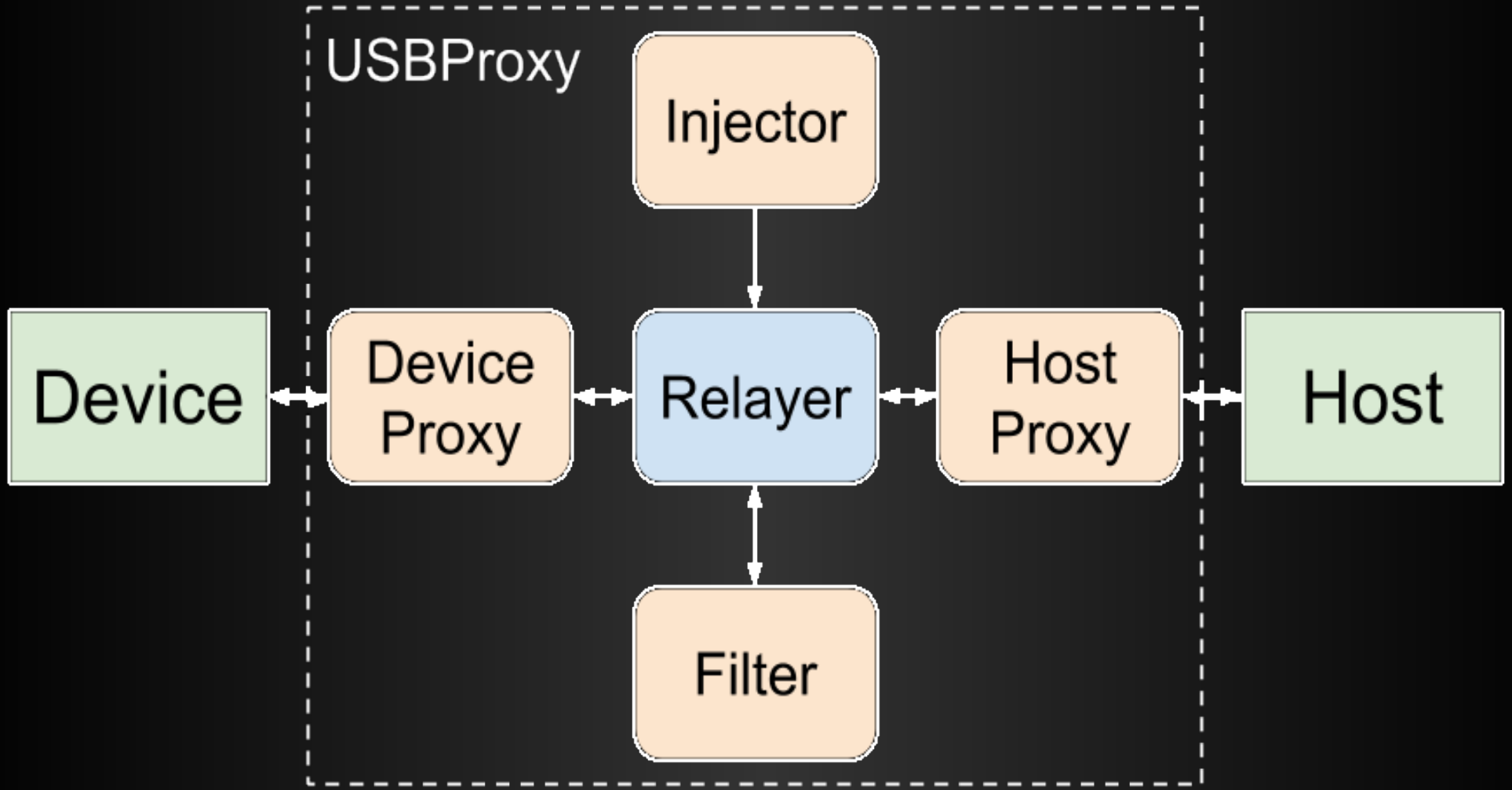
Open source C++ framework

Flexible / extensible architecture

Built upon:

- GadgetFS
- libUSB
- BeagleBone Black

USBProxy Structure



BeagleBone Black

Cheap / powerful

Built in USB OTG interface

Open source hardware

Demo

USBProxy

Mass Storage Devices

Bulk Only

- Two Bulk Eps – one IN, one OUT
- Wrapped SCSI commands
- Small subset of commands (read/write)

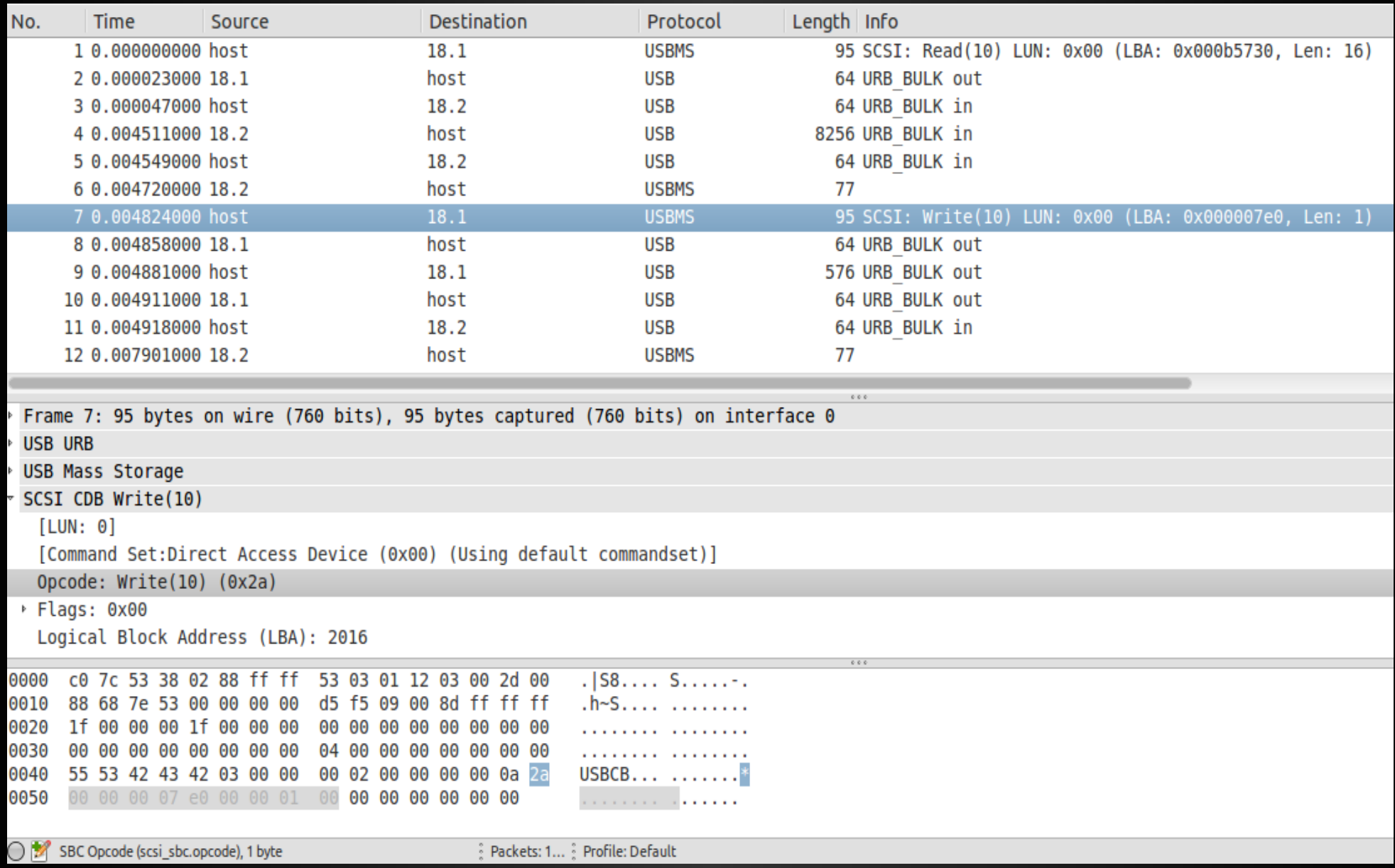
USB Attached SCSI

- Introduced in USB 3.0
- Faster, but not common yet

Bulk Only Mass Storage

- Three stage read/write
  - Command block
    - SCSI opcode, length, location
  - Data
    - Bytes to be written
  - Status
    - Device status

Wireshark


No. Time Source Destination Protocol Length Info
1 0.000000000 host 18.1 USBMS 95 SCSI: Read(10) LUN: 0x00 (LBA: 0x000b5730, Len: 16)
2 0.000023000 18.1 host USB 64 URB_BULK out
3 0.000047000 host 18.2 USB 64 URB_BULK in
4 0.004511000 18.2 host USB 8256 URB_BULK in
5 0.004549000 host 18.2 USB 64 URB_BULK in
6 0.004720000 18.2 host USBMS 77
7 0.004824000 host 18.1 USBMS 95 SCSI: Write(10) LUN: 0x00 (LBA: 0x000007e0, Len: 1)
8 0.004858000 18.1 host USB 64 URB_BULK out
9 0.004881000 host 18.1 USB 576 URB_BULK out
10 0.004911000 18.1 host USB 64 URB_BULK out
11 0.004918000 host 18.2 USB 64 URB_BULK in
12 0.007901000 18.2 host USBMS 77
Frame 7: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
USB URB
USB Mass Storage
SCSI CDB Write(10)
[LUN: 0]
[Command Set:Direct Access Device (0x00) (Using default commandset)]
Opcode: Write(10) (0x2a)
Flags: 0x00
Logical Block Address (LBA): 2016
0000 c0 7c 53 38 02 88 ff ff 53 03 01 12 03 00 2d 00 .|S8.... S.....-.
0010 88 68 7e 53 00 00 00 00 d5 f5 09 00 8d ff ff ff .h~S.... ....
0020 1f 00 00 00 1f 00 00 00 00 00 00 00 00 00 00 00 ....
0030 00 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 ....
0040 55 53 42 43 42 03 00 00 00 02 00 00 00 00 0a 2a USBCB... ....*
0050 00 00 00 07 e0 00 00 01 00 00 00 00 00 00 00 00 ....
SBC Opcode (scsi_sbc.opcode), 1 byte
Packets: 1...
Profile: Default

Blocking Writes

- Many options
  - Block entire transaction
  - Convert write to read
  - Read block, write it back
  - Write 0 length data

Demo

USBProxy + Mass Storage
(this demo will fail)

So, you want to get involved in USBProxy?

- USB 3
  - Requires suitable device interface
  - Most likely Daisho
- Shared library
- Configuration parser

Language Bindings

- Starting with Python
  - Some initial filter code exists
  - Nothing to demo yet
- Plan for more languages
  - Looking for volunteers to help write them

FaceDancer Compatibility

Waiting on Python device proxies

Hope to work with existing software tools

Some slight differences in design, but should work

Thanks

Adam Stasiak

Travis Goodspeed & Sergey Bratus

Michael Ossmann

David Formby

Questions

github.com/dominicgs/USBProxy

#USBProxy on freenode

@dominicgs / dominicgs@gmail.com