USB write blocking with USBProxy

Dominic Spill
dominicgs@gmail.com
@dominicgs

Dominic Spill

Open source software developer for Great Scott Gadgets

Ubertooth, Daisho, FCC.io, USBProxy

Dabble in hardware, BeagleDancer, PS/2tap

Adam Stasiak

USBProxy developer

.Net port of FaceDancer codebase

controllingxbox.blogspot.com

Background

2 billion USB devices sold each year (2008)

Most common device interface

Low / Full / High / Super speed

SuperSpeed Plus coming soon

Background

Huge surface for security assessment

- Host drivers
- Device firmware
- Connection between

I build tools for packet sniffing/injection

- Seems like USB might be fun to try

FaceDancer

'It's not a bus, it's a network' - Sergey Bratus

Designed by Travis Goodspeed

- An extension to the GoodFET
- Prototype devices in Python
- Some great examples
- NCC Group 'umap' tool

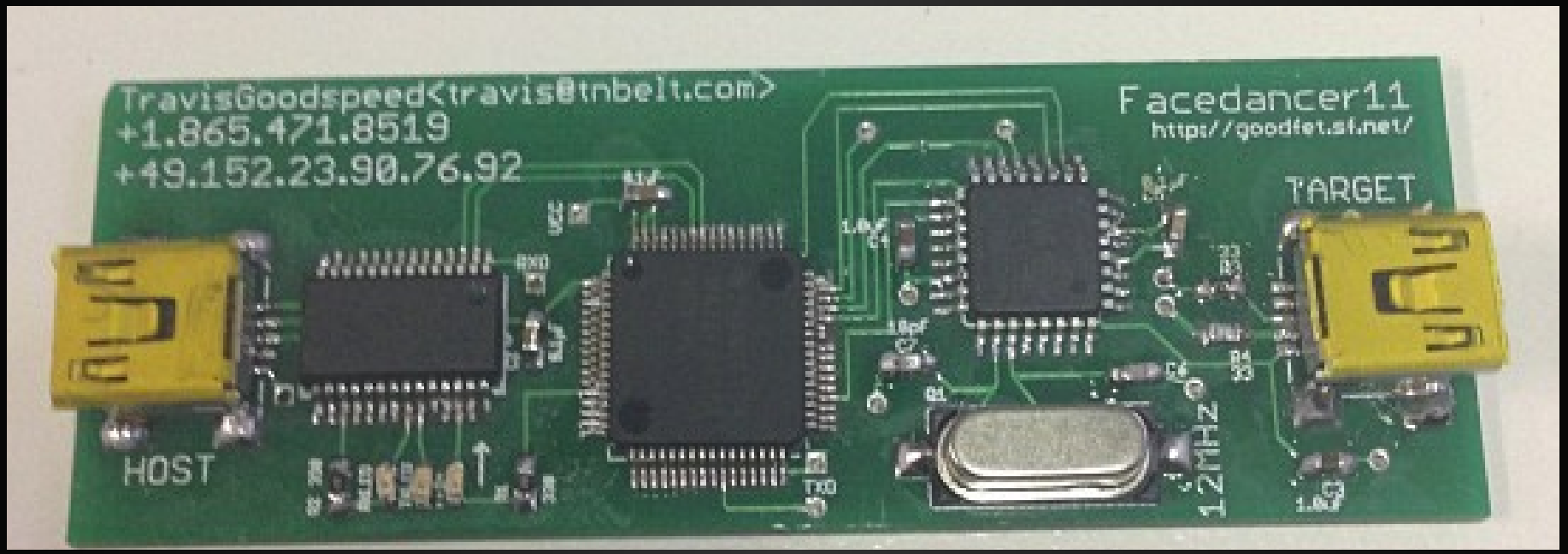
FaceDancer


Facedancer21
USB Device Emulator:
Mass Storage
FTDI Serial
HP49G+ Serial
Firmware Update (DFU)
Keyboard (HID)
http://goodfet.sf.net/
44CON
HOST
TARGET
12MHz
TravisGoodspeed<travis@tnbelt.com>
+1.865.471.8519
+49.152.23.90.76.92

FaceDancer Drawbacks

Speed / latency / limited endpoints / cost

Soldering skills?



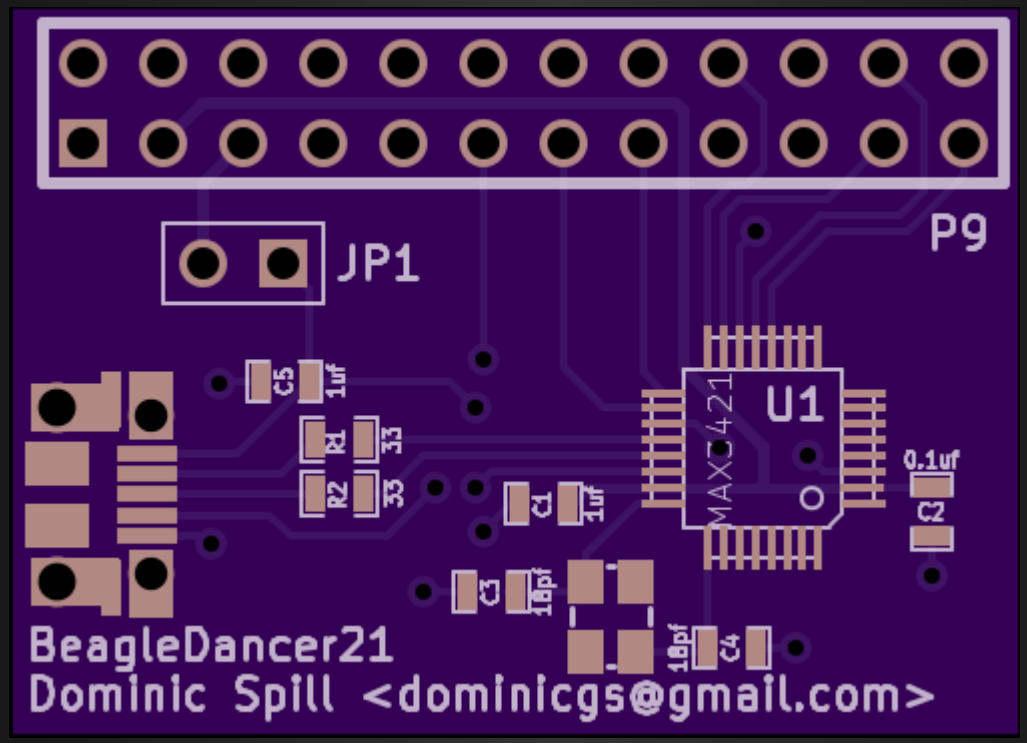
RaspDancer / BeagleDancer

RaspDancer – Phillipe Teuwen

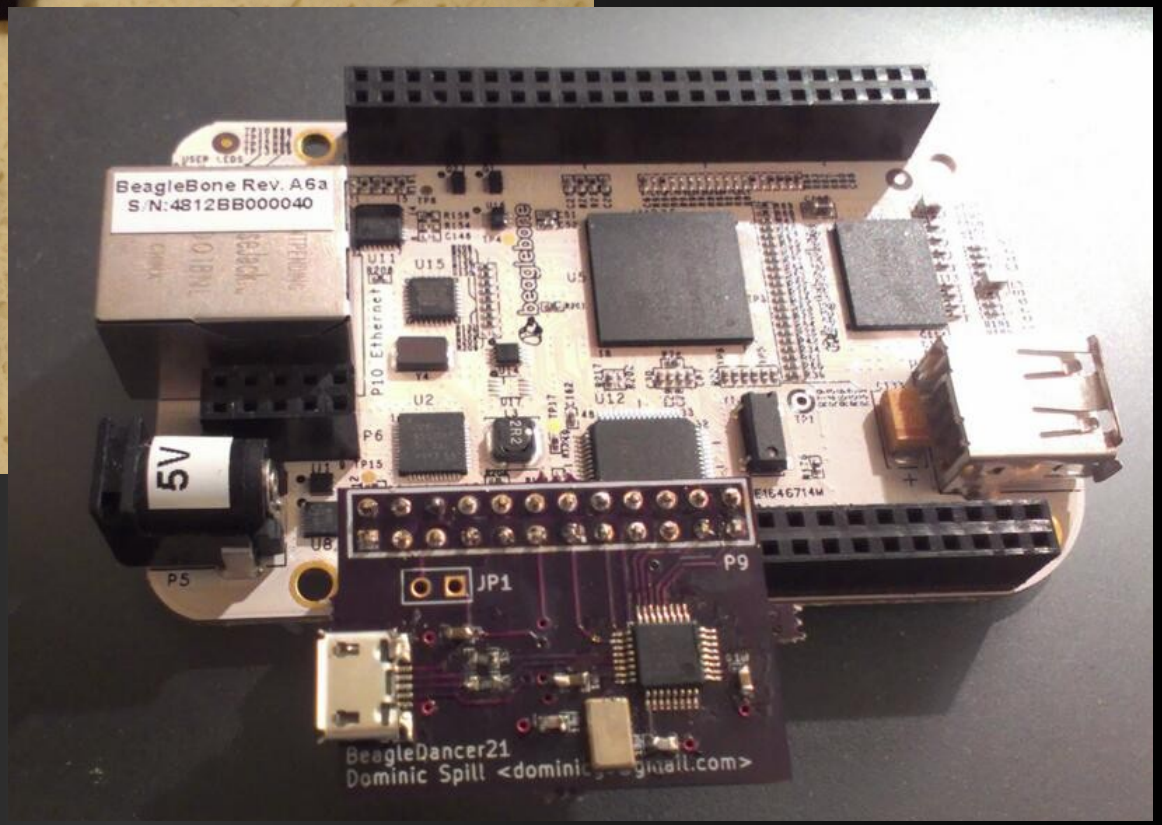
Increases SPI to 26MHz

Fewer parts – cheaper

BeagleDancer



BeagleDancer



BeagleDancer is pointless

MAX3421 USB OTG IC

BBB has OTG built in to TI am3359

<dominicgs> I made a FaceDancer for the BBB!

<mossmann> Great! You know the BBB can probably do FaceDancery things anyway?

USBProxy

Open source C++ framework

Flexible / extensible architecture

Built upon:

- GadgetFS
- libUSB
- BeagleBone Black

BeagleBone Black

Cheap / powerful

Built in USB OTG interface

Open source hardware

Other platforms

Olimex Lime

Parallela

Anything with USB host + device ports

Demo

USB man in the middle

USBProxy Structure

Relayer moves packets around

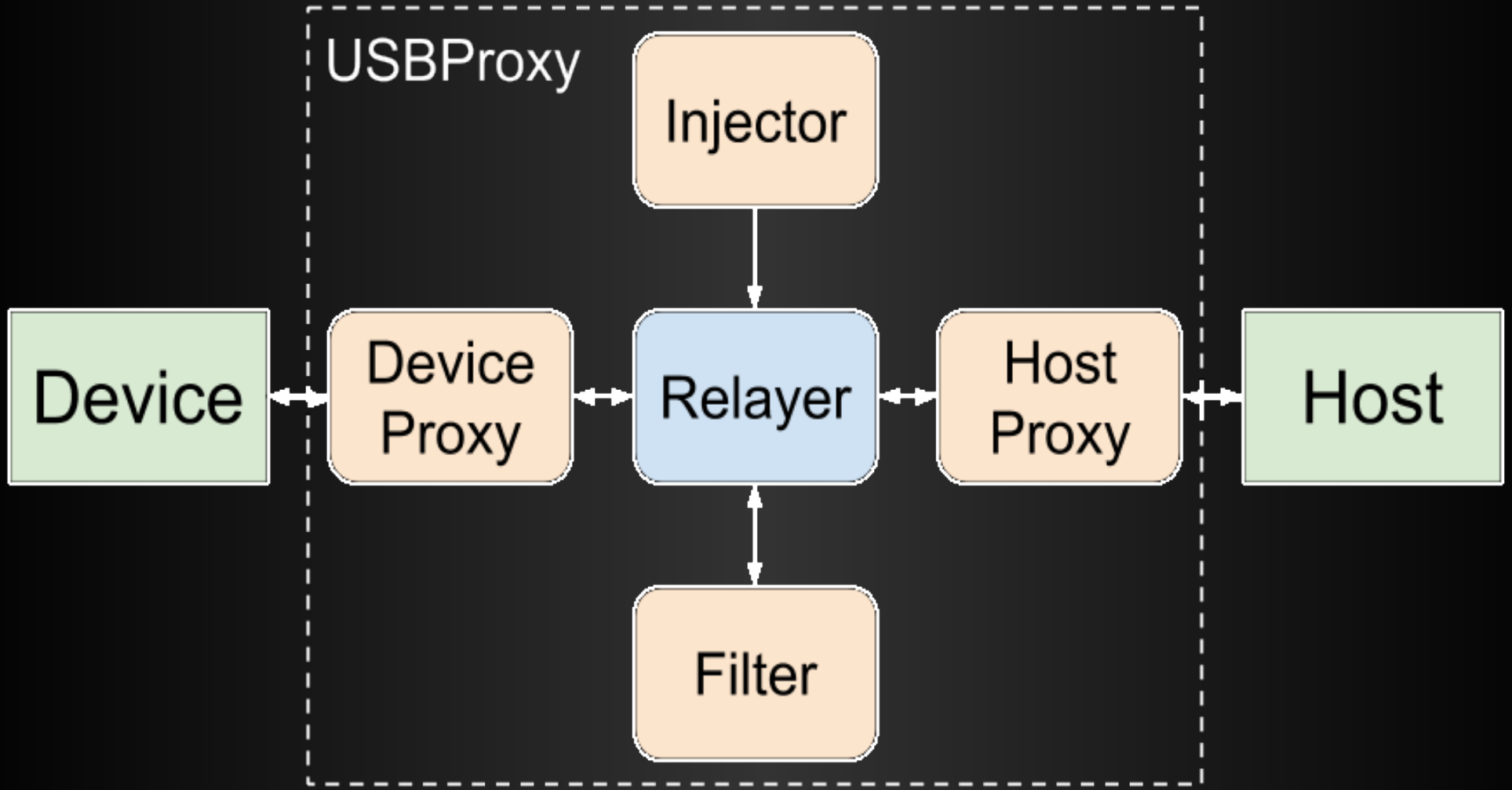
Manager handles setup and teardown

Proxies for talking to devices and hosts

Filters for modifying packets

Injectors for injecting arbitrary packets

USBProxy Structure



USB Mass Storage

SCSI over USB bulk endpoints

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

Three stage process:

- Command block (out)
- Data (in/out)
- Status block (in)

USB Mass Storage

Read:

READ:LOCATION:SIZE →

DATA ←

STATUS:OK ←

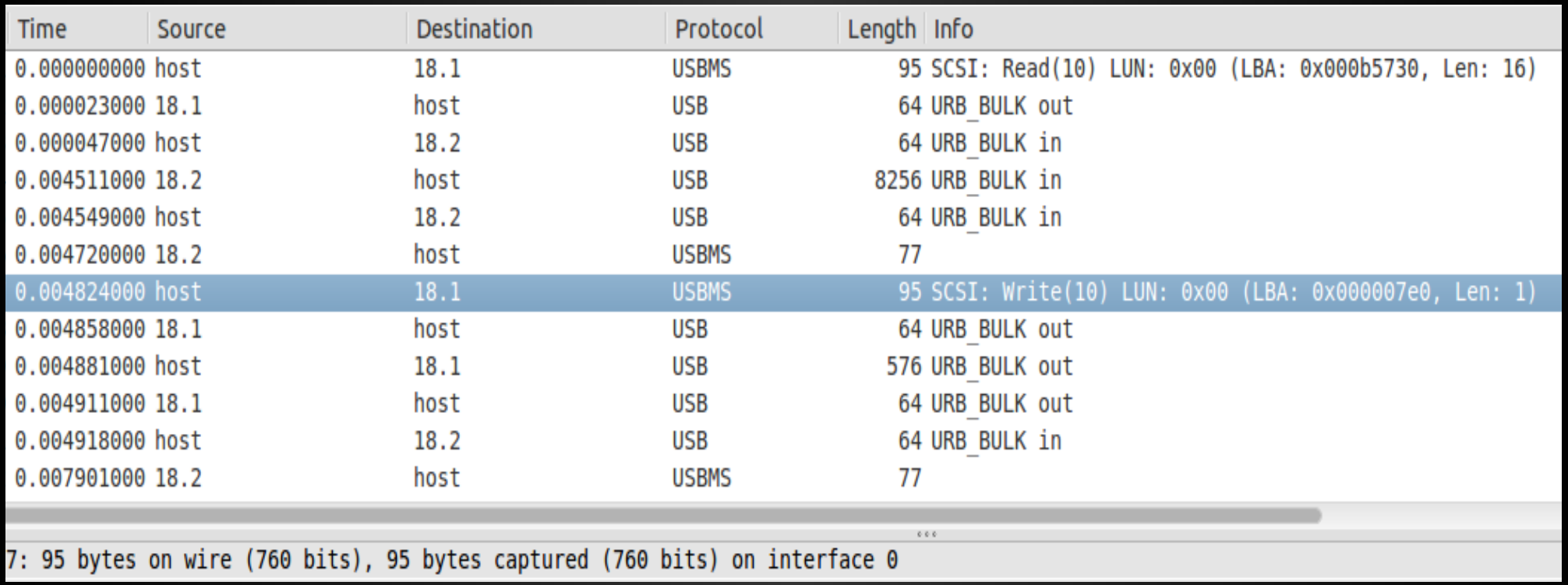
Write:

WRITE:LOCATION:SIZE →

DATA →

STATUS:OK ←

Wireshark



Time	Source	Destination	Protocol	Length	Info
0.000000000	host	18.1	USBMS	95	SCSI: Read(10) LUN: 0x00 (LBA: 0x000b5730, Len: 16)
0.000023000	18.1	host	USB	64	URB_BULK out
0.000047000	host	18.2	USB	64	URB_BULK in
0.004511000	18.2	host	USB	8256	URB_BULK in
0.004549000	host	18.2	USB	64	URB_BULK in
0.004720000	18.2	host	USBMS	77	
0.004824000	host	18.1	USBMS	95	SCSI: Write(10) LUN: 0x00 (LBA: 0x000007e0, Len: 1)
0.004858000	18.1	host	USB	64	URB_BULK out
0.004881000	host	18.1	USB	576	URB_BULK out
0.004911000	18.1	host	USB	64	URB_BULK out
0.004918000	host	18.2	USB	64	URB_BULK in
0.007901000	18.2	host	USBMS	77	

7: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0

Blocking Writes

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

Demo

Write blocking
+
Write blocking with caching

Caching Blocks

Cache blocks on first read

Drop write command

Update cache with writes

Log changes

Drop write data

Return fake OK status message

In-band Signalling

Enable / disable write blocking

Instruction sent in-band

Use filesystem write

Demo

In-band Signalling
(super-sketchy demo written this morning)

Things we're working on

- USB 3
  - Requires suitable device interface
  - Most likely Daisho
- Language bindings
  - Python at first
  - Looking for volunteers to help with others

FaceDancer Compatibility

Waiting on Python bindings

Hope to work with existing software tools

Some slight differences in design, but should work

Thanks

Adam Stasiak

Travis Goodspeed & Sergey Bratus

Michael Ossmann

Questions

github.com/dominicgs/USBProxy

#USBProxy on freenode

@dominicgs / dominicgs@gmail.com