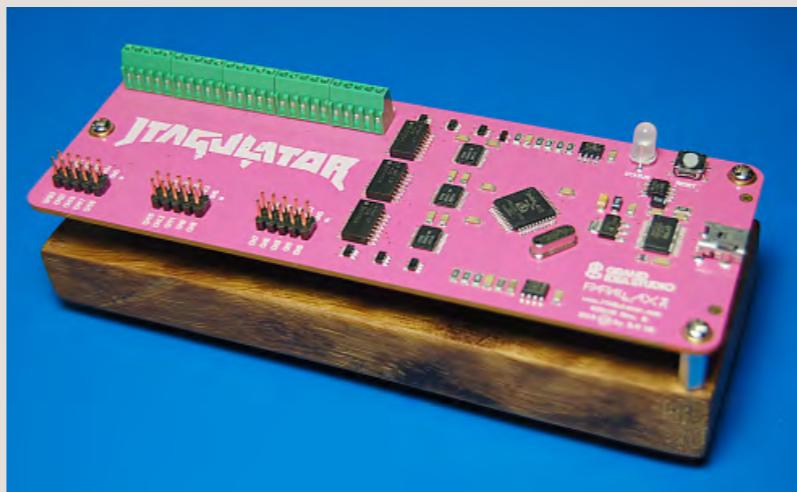
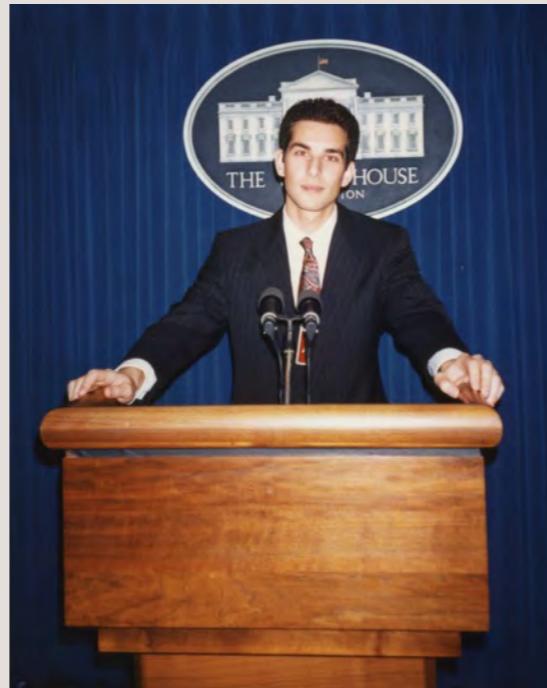
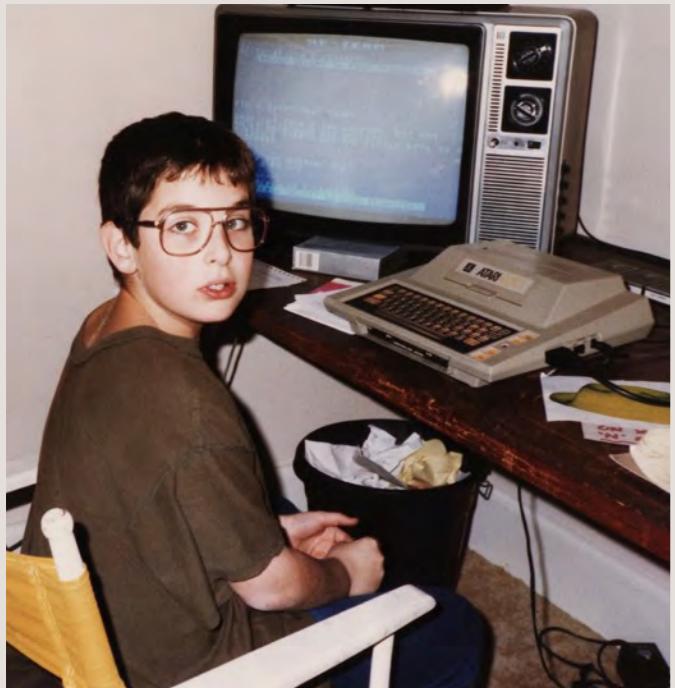




Searching for the Light: Adventures w/ OpticSpy

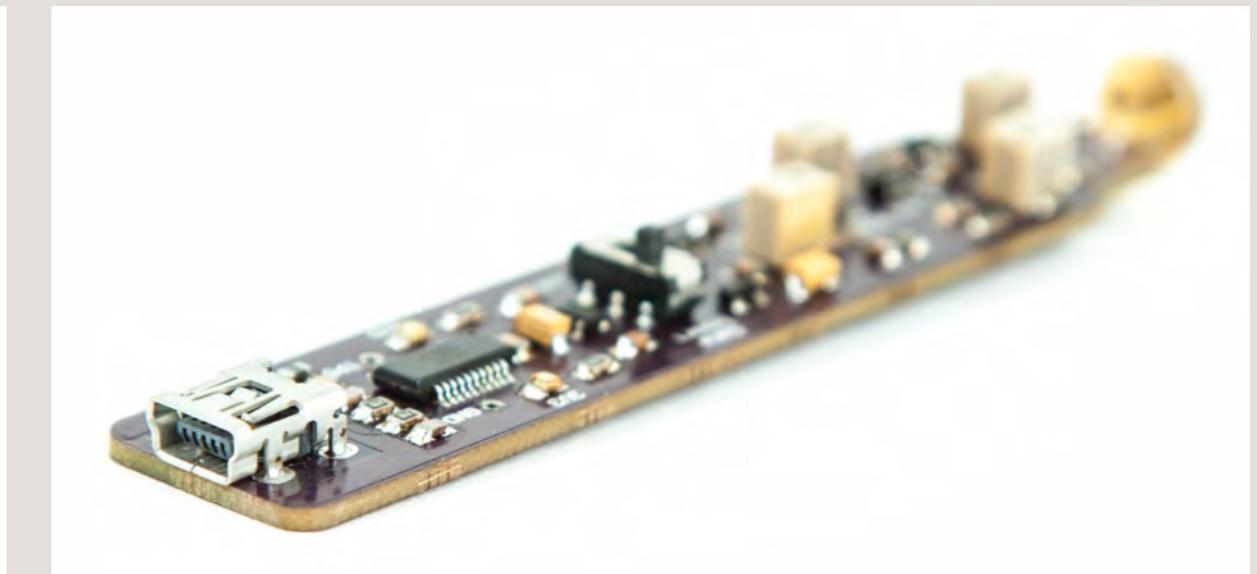
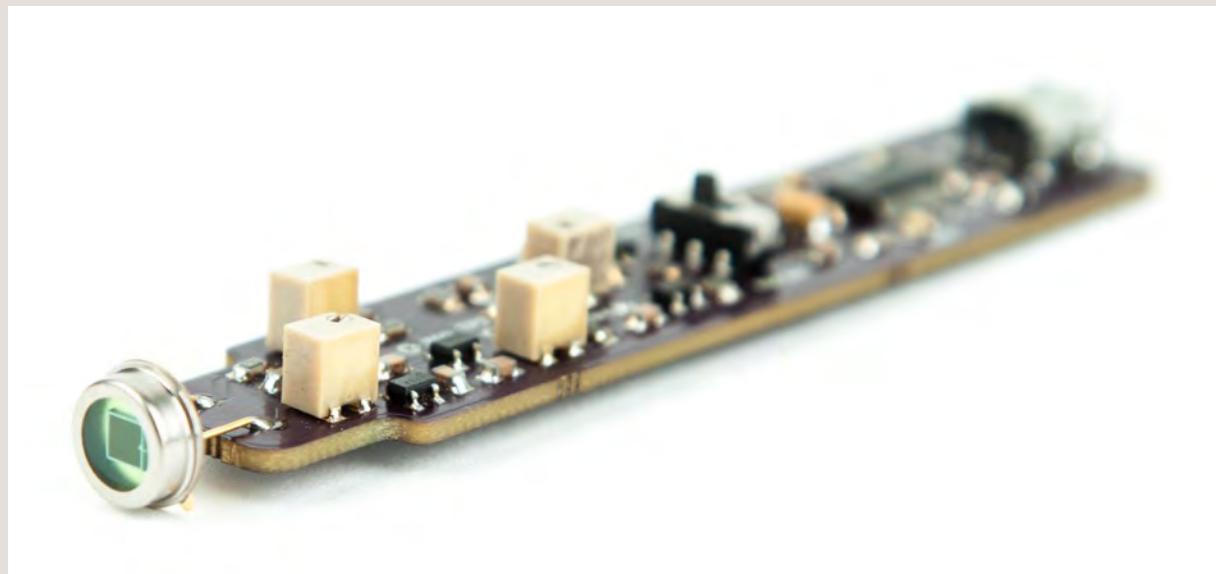
Joe Grand (@joegrand)

Hacker, Engineer, Daddy



OpticSpy

- Optical receiver to convert light into voltage
- Wavelength: Visible and near IR light (420-940nm)
- Signal speed: 100Hz-1.5MHz
- Data stream polarity: Select normal v. inverted
- Gain and threshold adjustment via potentiometers
- USB interface for direct connection to host PC



Covert Channels

- Hidden methods to intentionally exfiltrate/transfer data from a normally functioning system
- Could be achieved with HW and/or FW modification
 - Specifications modified or misdesigned before manufacturing
 - On physical device during manufacturing or in-the-field
 - Hardware implant via interdiction

Exploiting the Environment

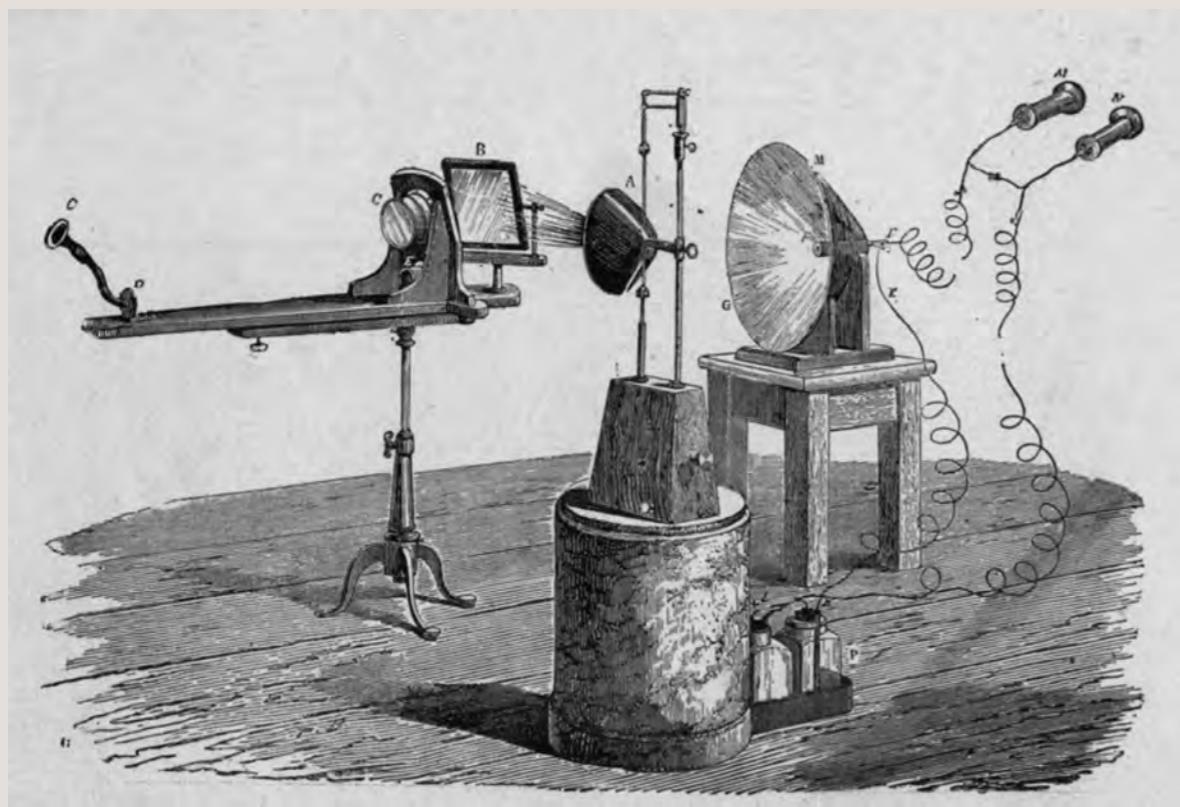
- Leakage based on optical, acoustic, thermal, or RF characteristics of a system
 - Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations (Kuhn, Anderson)
 - Emanate Like a Boss: Generalized Covert Data Exfiltration with Funtenna (Cui)
 - Inaudible Sound as a Covert Channel in Mobile Devices (Deshotels)
 - BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations (Guri et al.)

Blinkenlights

- Using LEDs to exfiltrate/send data
 - Modulation faster than the human eye can detect
- Optical covert channels
 - Information Leakage from Optical Emanations (Loughry and Umphress, 2002)
 - Silence on the Wire: A Field Guide to Passive Reconnaissance and Indirect Attacks (Zalewski)
 - Extended Functionality Attacks on IoT Devices: The Case of Smart Lights (Ronen, Shamir)
 - xLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs (Guri et al.)

A Selection of Optical History

- Alexander Graham Bell's Photophone (1880)
- Fiber optic communications (~1963)
- Laser tag (~1979)
- Optical networking systems (VLC, Li-Fi, FSO) (2011)



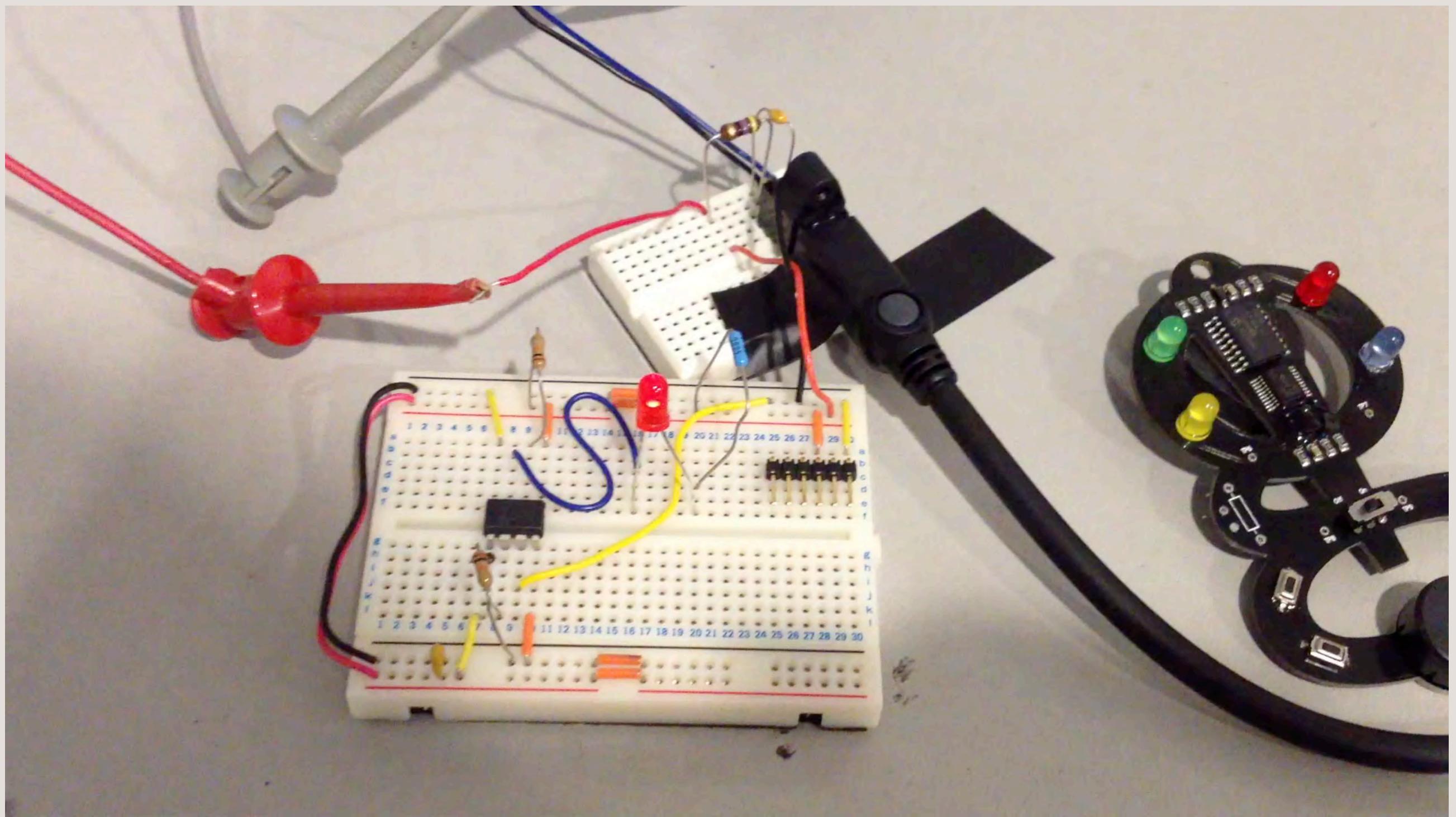
Related Projects

- Heathkit Laser Trainer/Receiver (1985)
- Engineer's Mini Notebook: Optoelectronics Circuits (Forest Mims III, 1985)
- IRis (Craig Heffner, 2016)
- See no evil, hear no evil: Hacking invisibly & silently with light & sound (Matt Wixey, 2017)

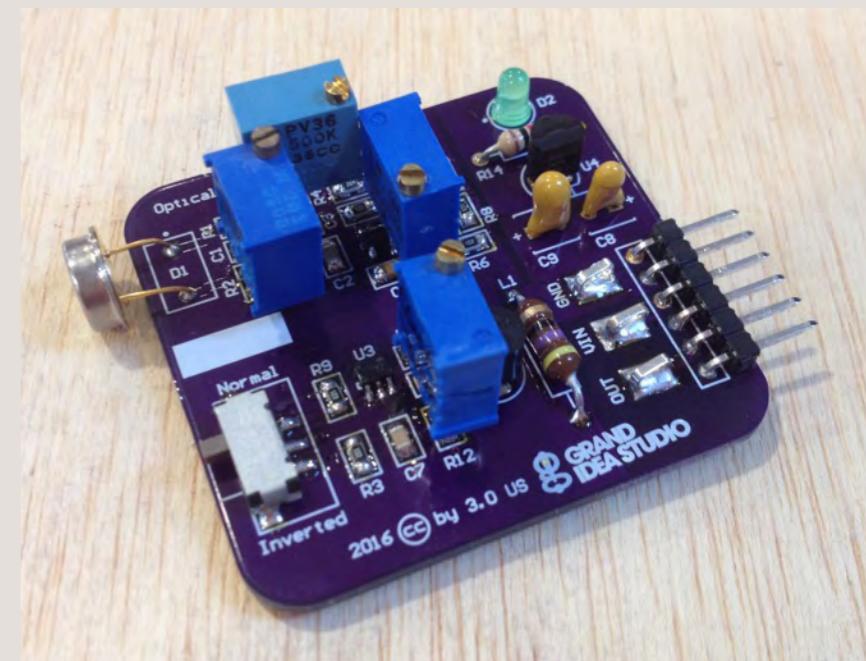
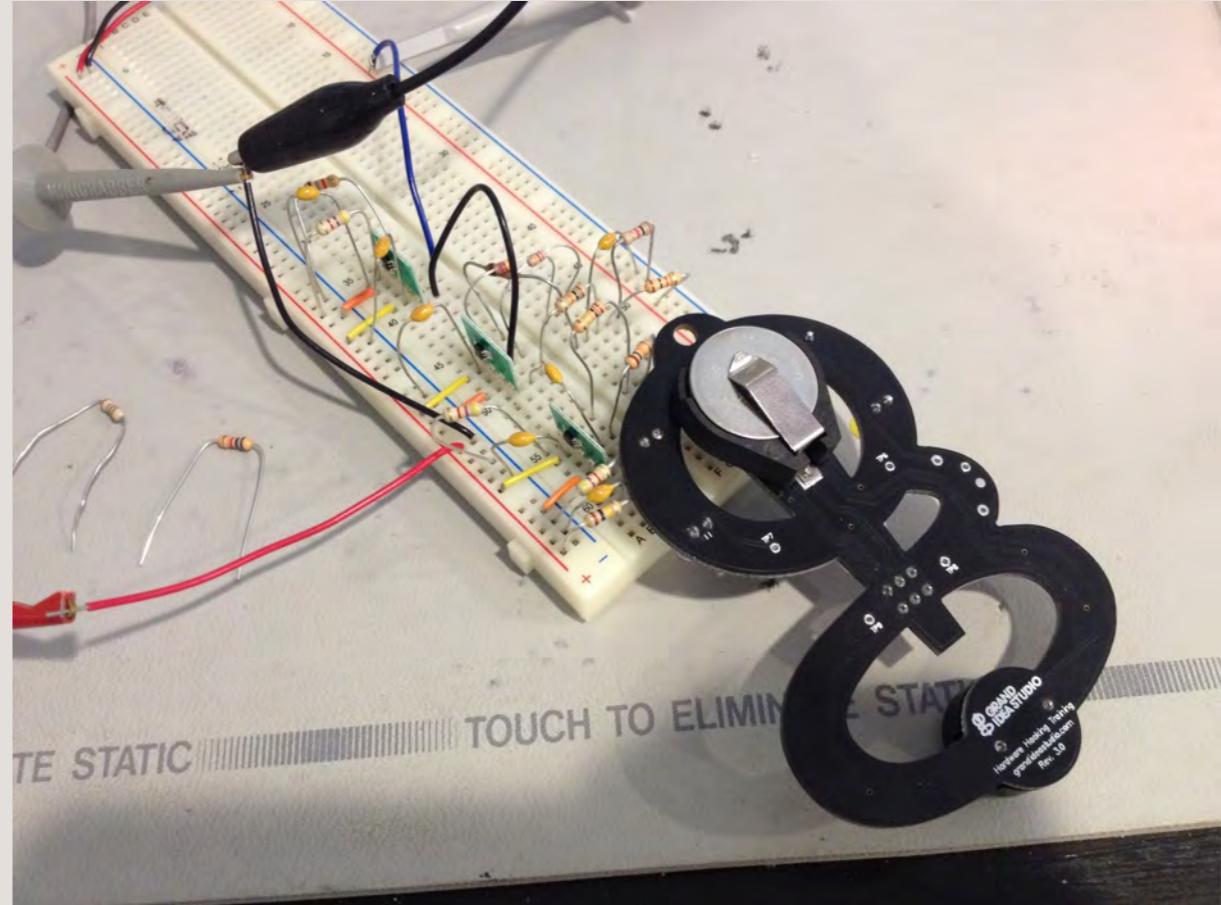
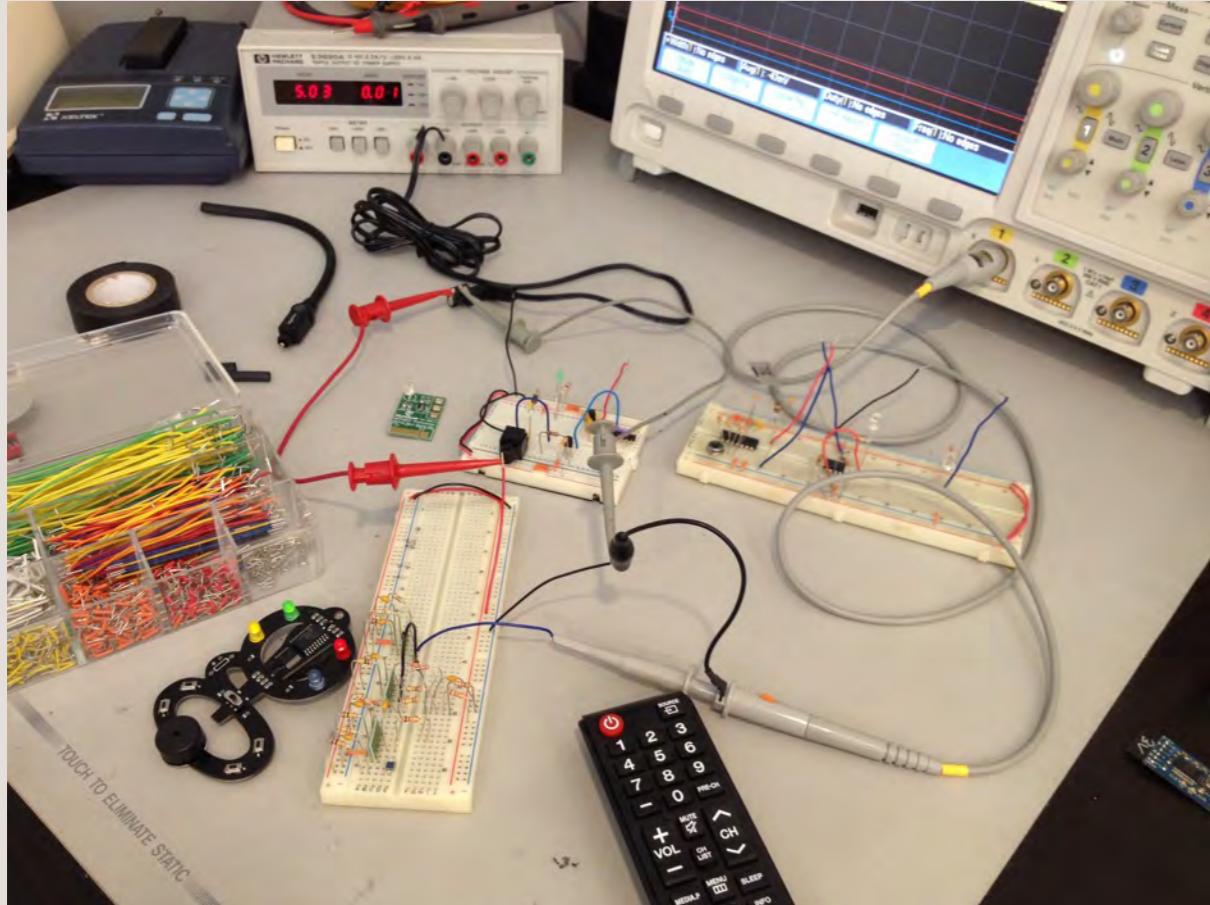
Design Goals

- Open source tool for optoelectronic experimentation
 - Easy to understand theory
 - Off-the-shelf components
 - Hand solderable
- Raise awareness of other interesting communication/exfiltration methods

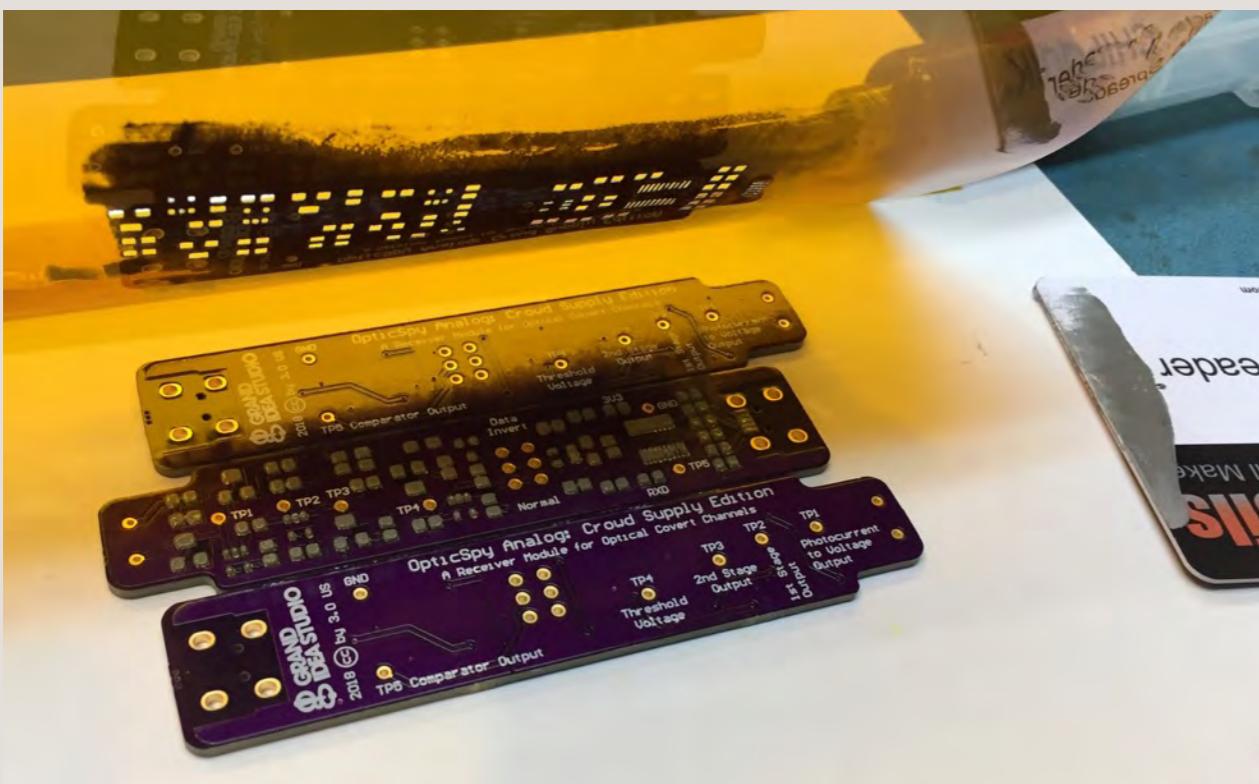
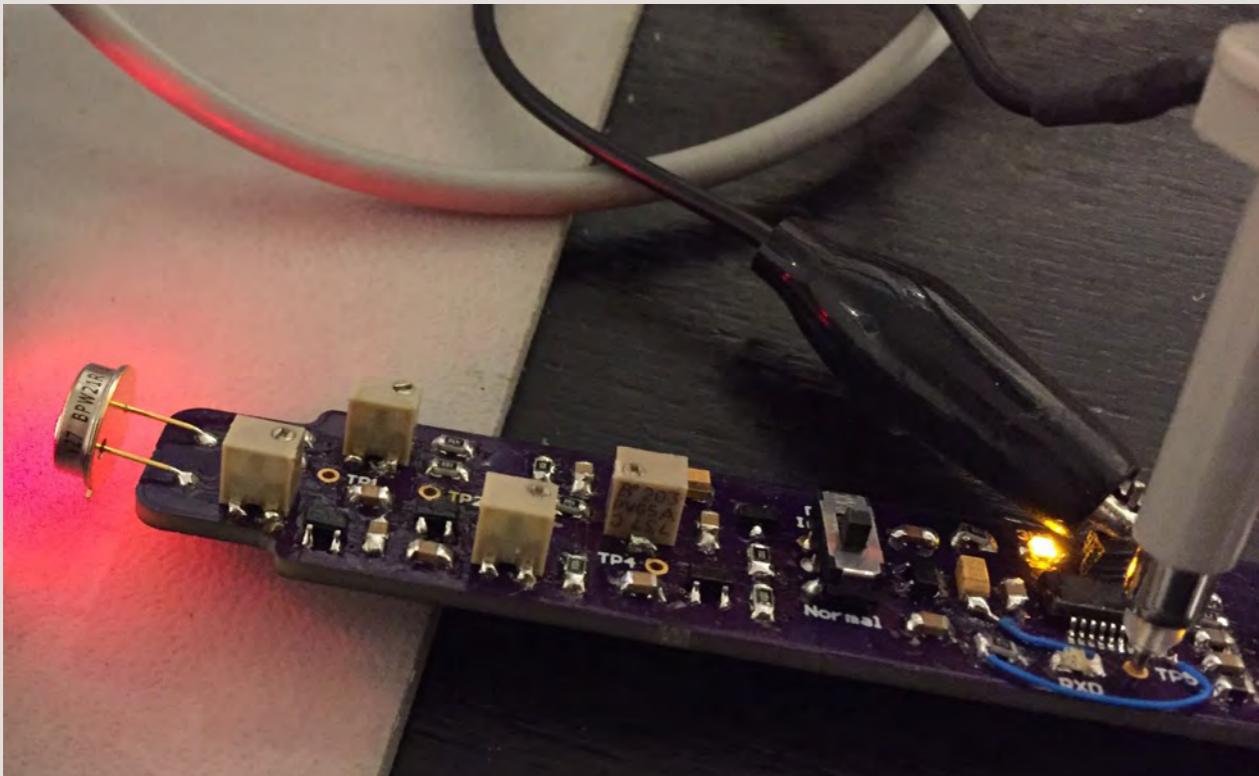
Proof of Concept



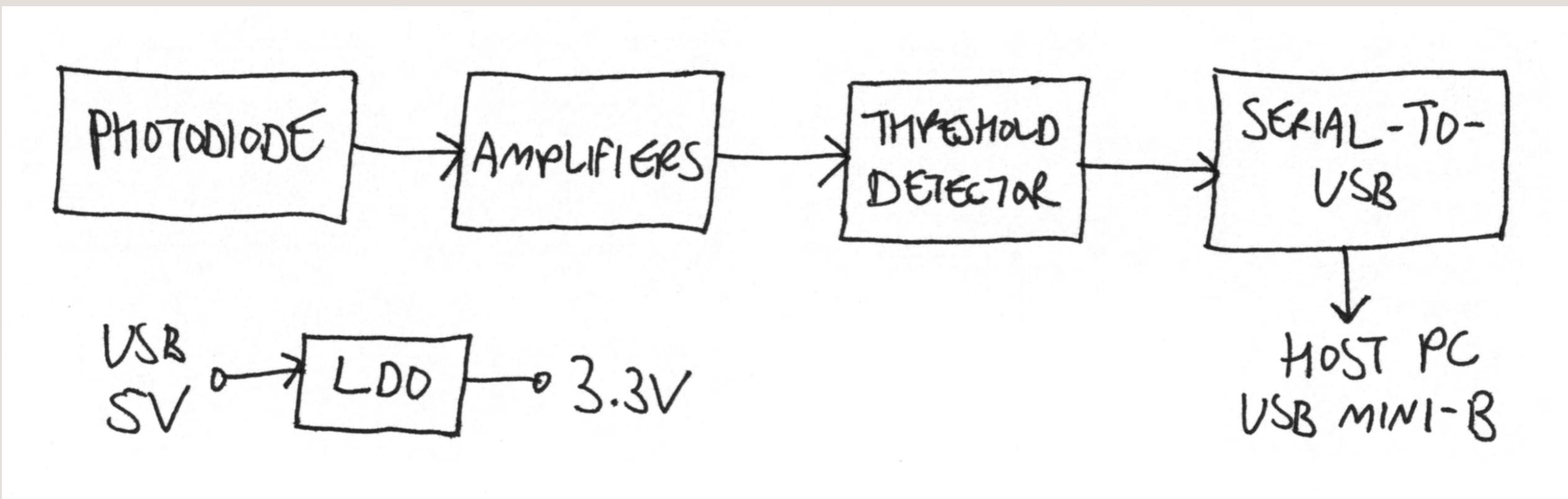
Early Versions



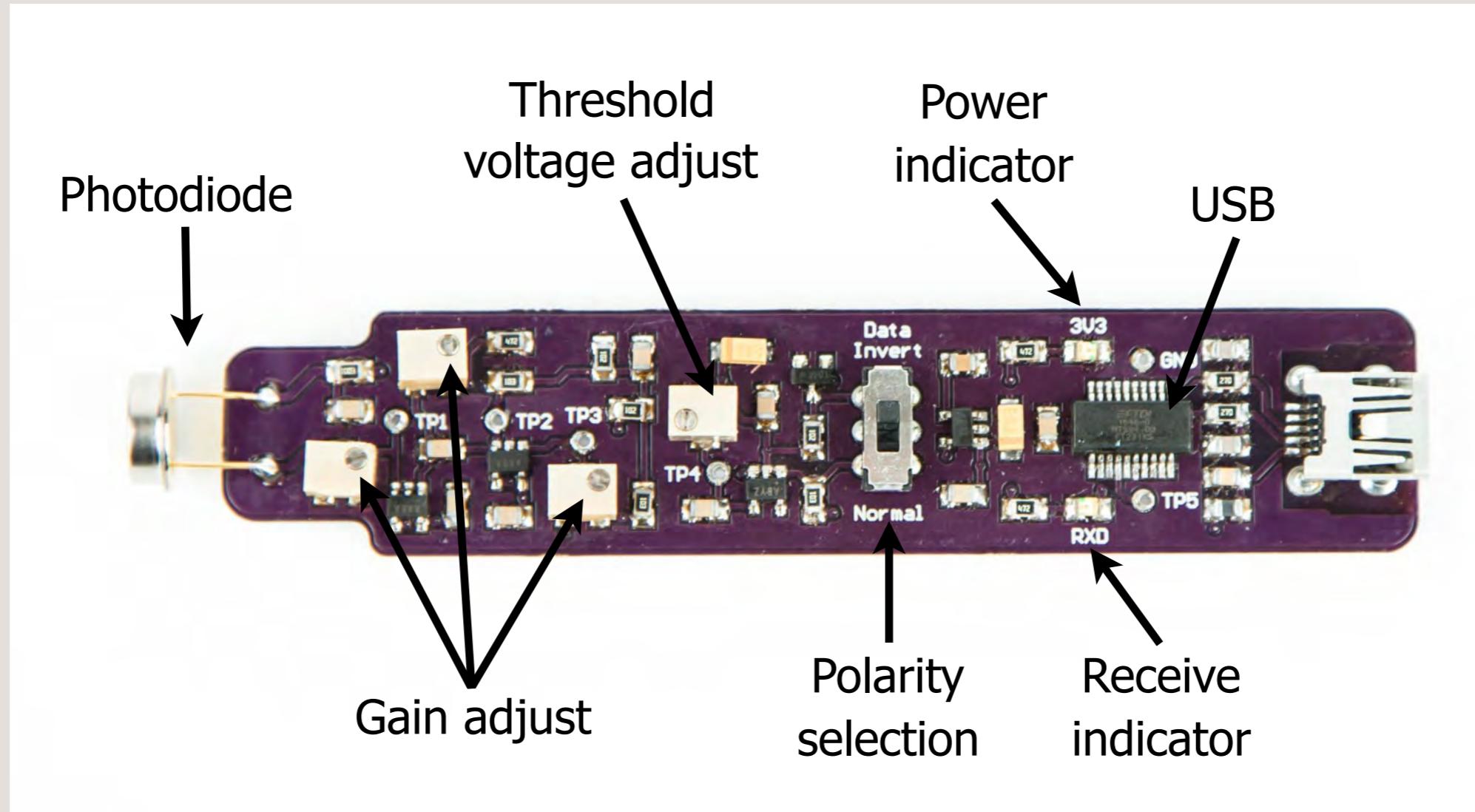
Development



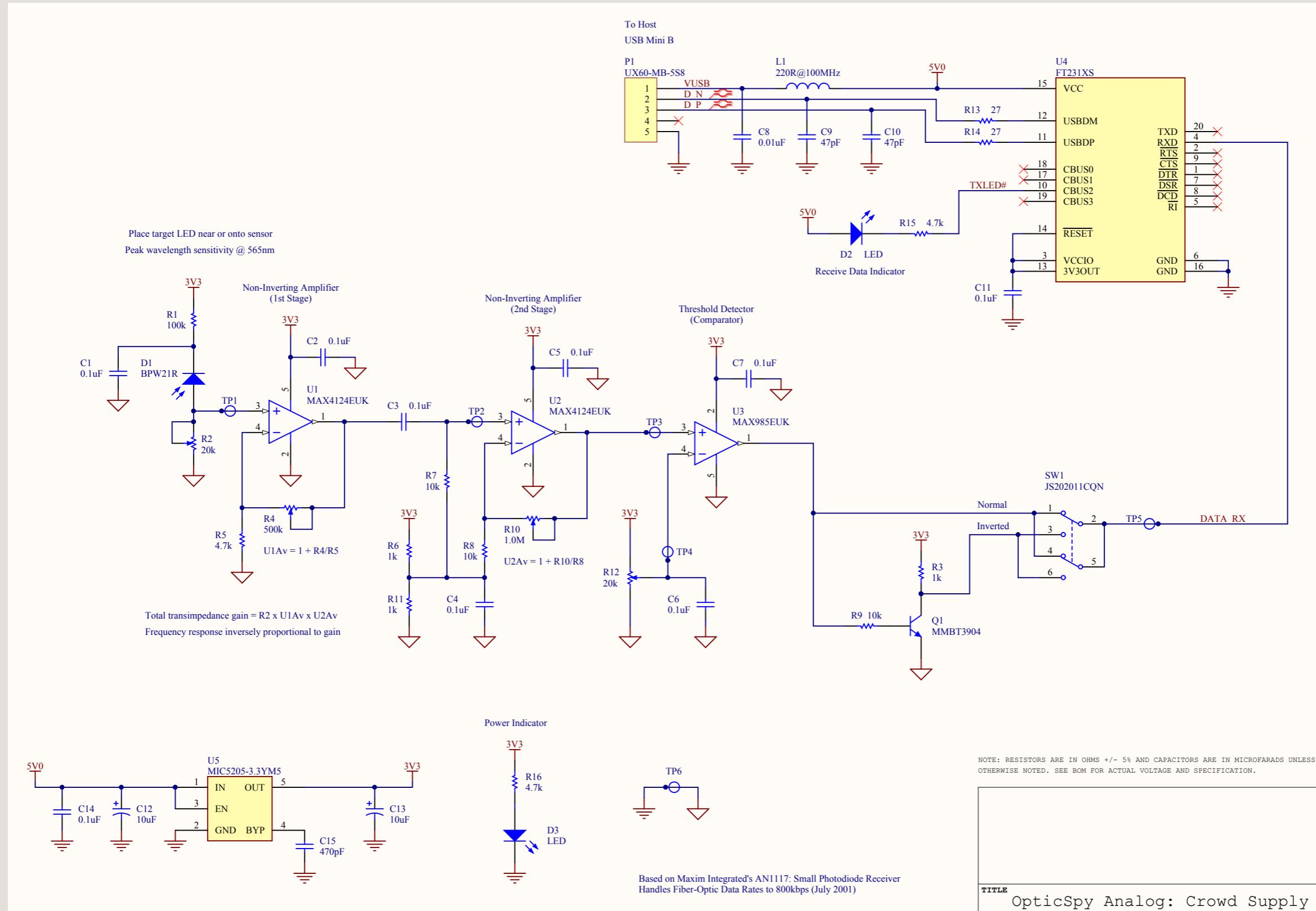
Block Diagram



Points of Interest

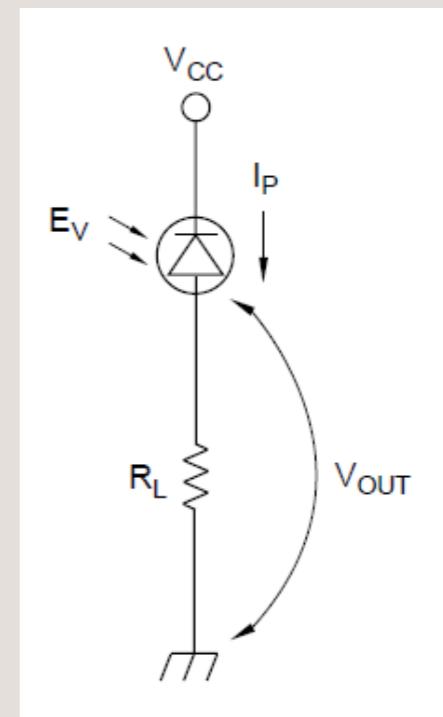
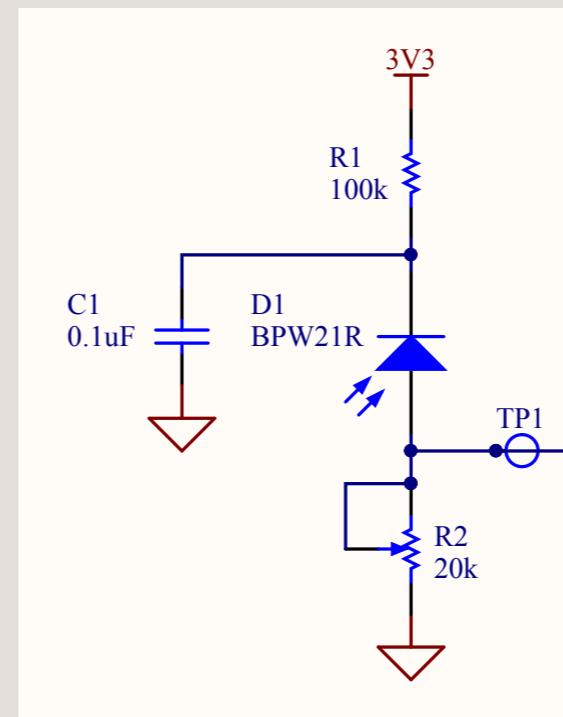
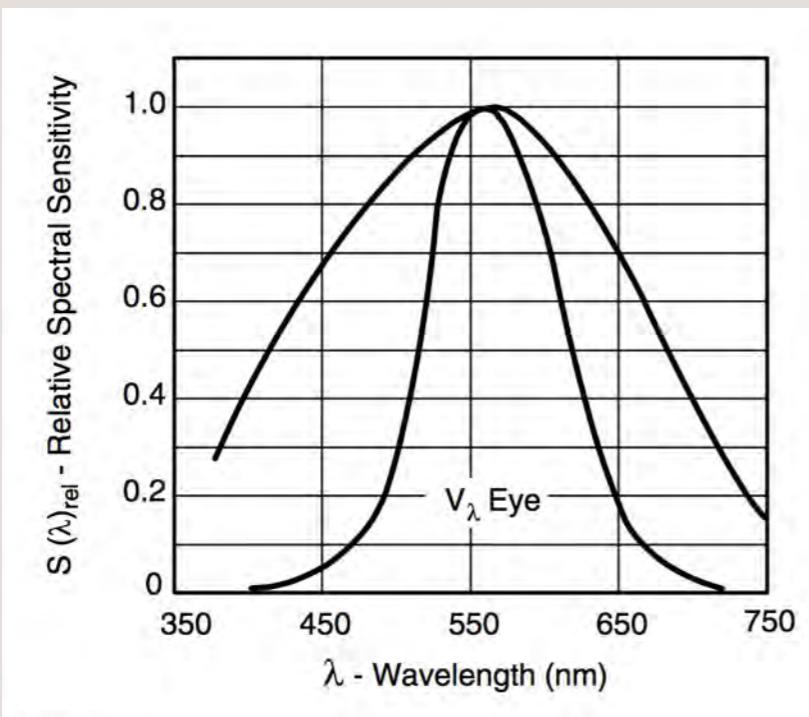
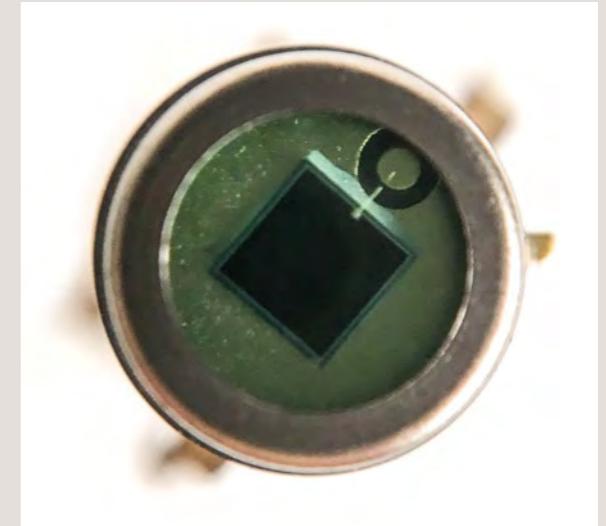


Schematic



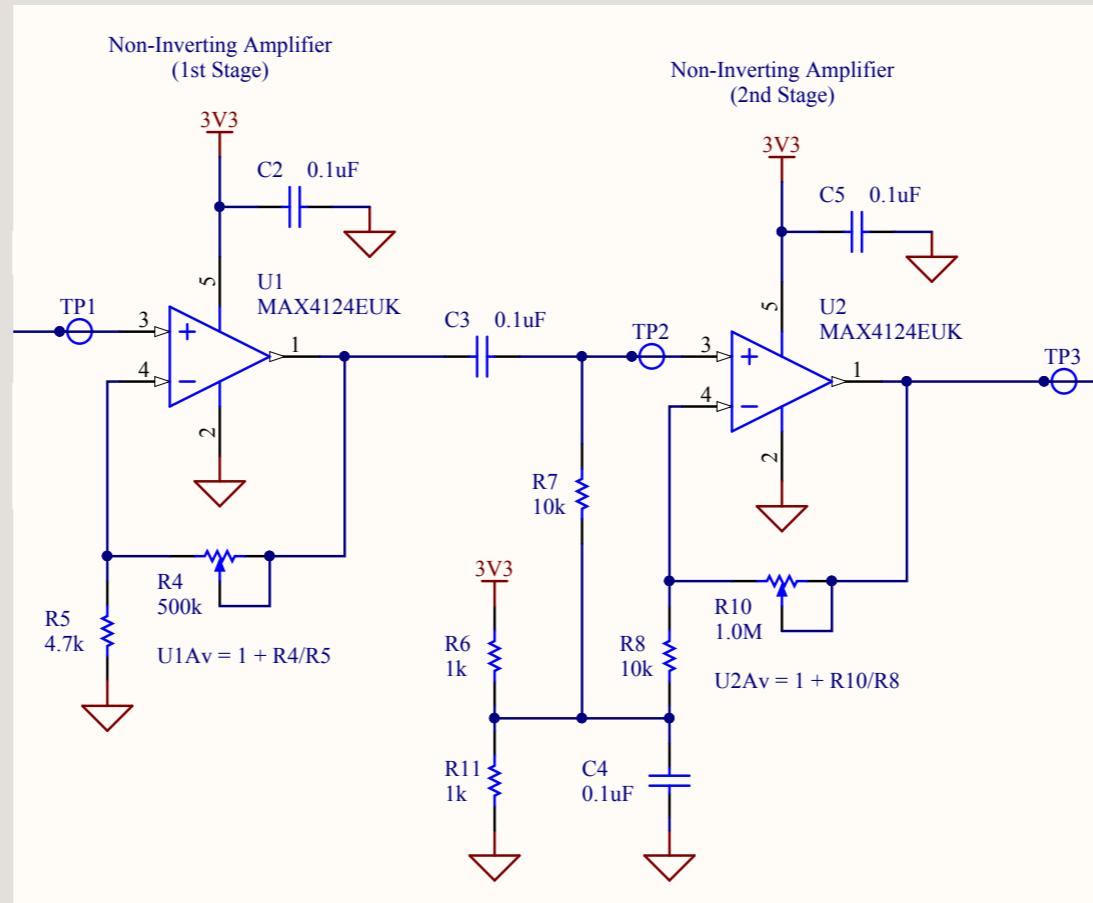
Photodiode

- Vishay Semiconductor BPW21R
- Converts light into current
- Photoconductive mode (reverse bias)
 - Faster response -> higher bandwidth
 - Less sensitivity, increased dark current
 - Bias resistor affects response/sensitivity



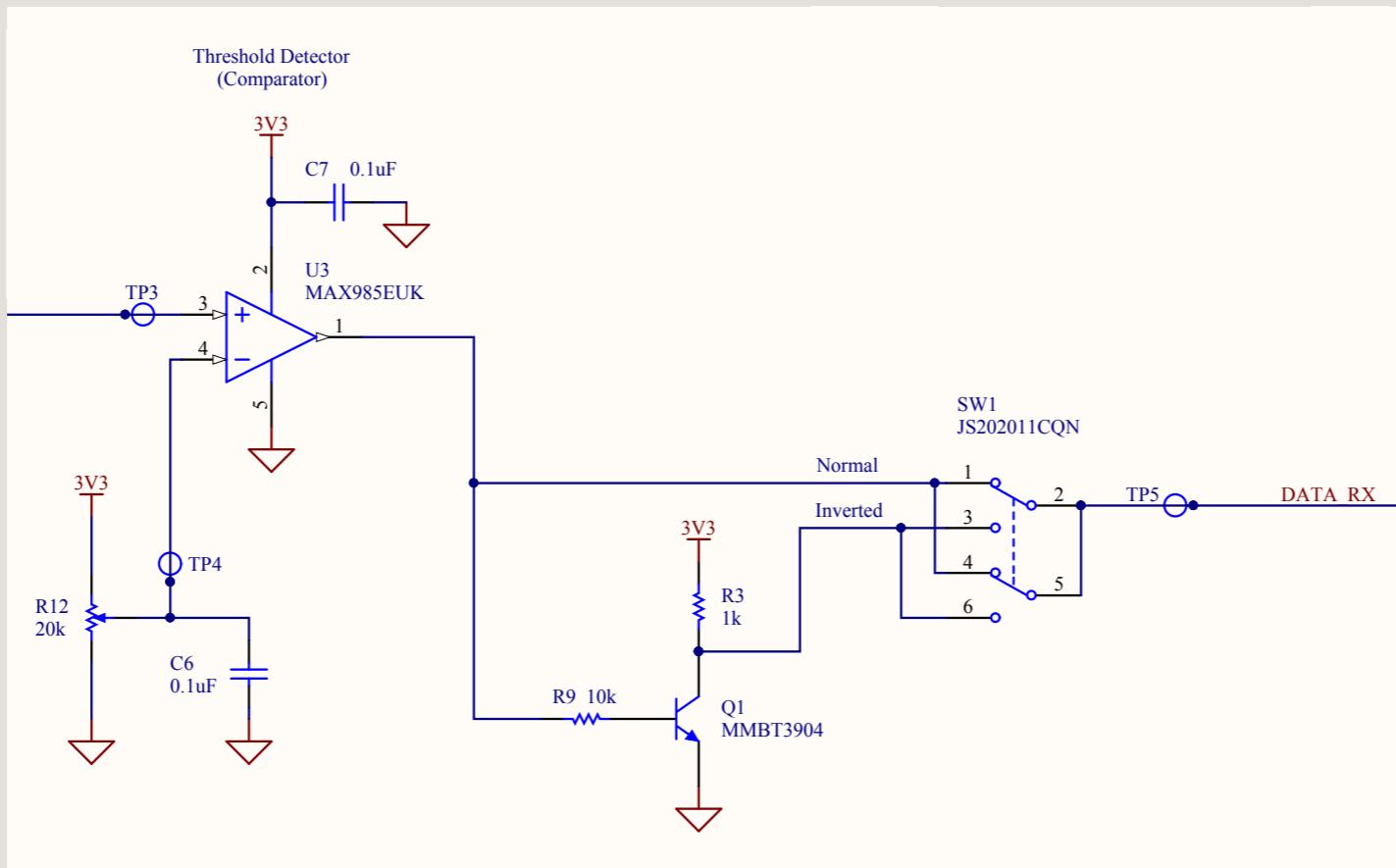
Amplification

- Maxim MAX4124 Wide Bandwidth, Low Power, Rail-to-Rail Operational Amplifier
- Two stages w/ signal massaging in between
 - Lower gain per stage -> less overall noise
- Total transimpedance gain = $R_2 \times U_1 A_v \times U_2 A_v$



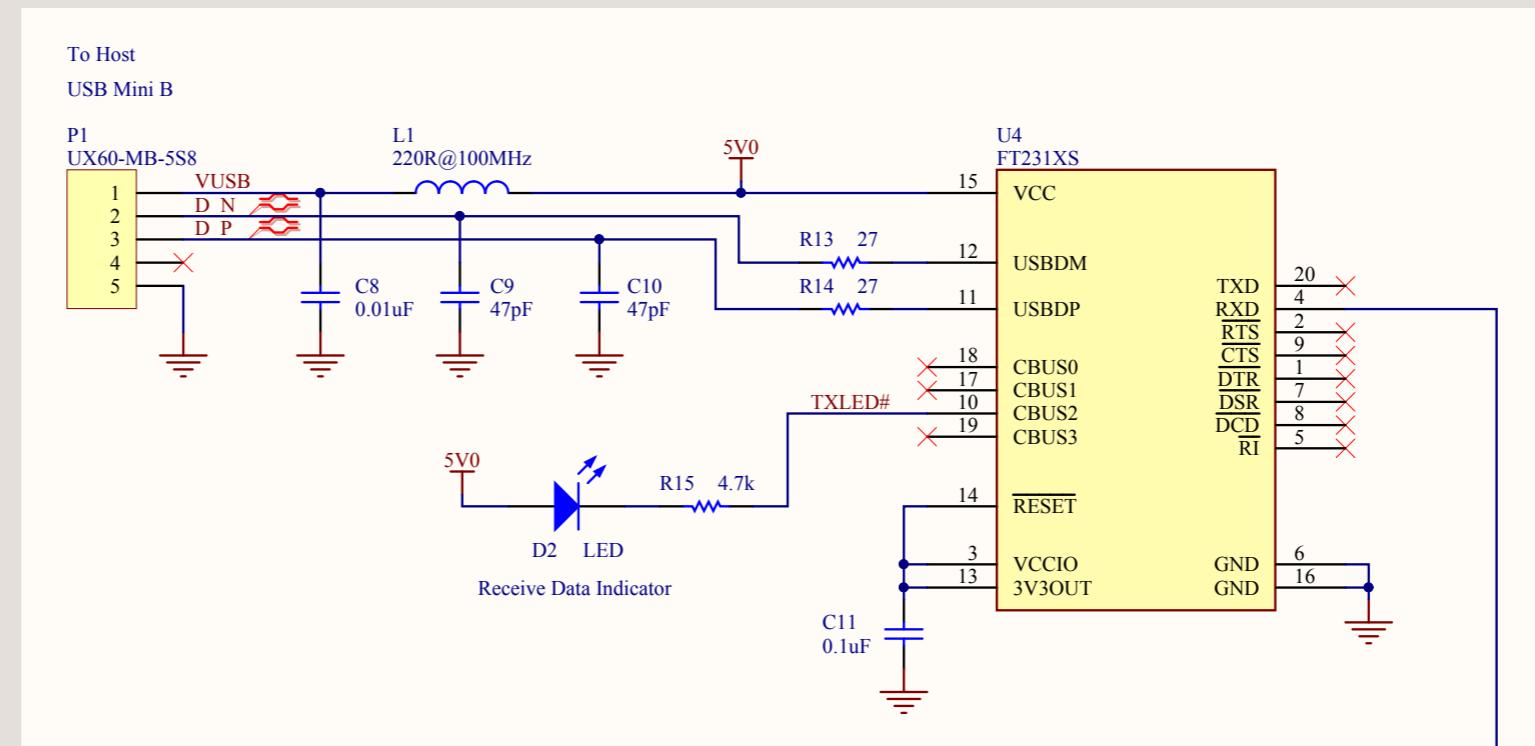
Comparator

- Maxim MAX985 Micropower, Low Voltage, Rail-to-Rail Comparator
- Determine what portion of signal treated as logic level '0' or '1'
- Adjustable threshold voltage w/ potentiometer R12

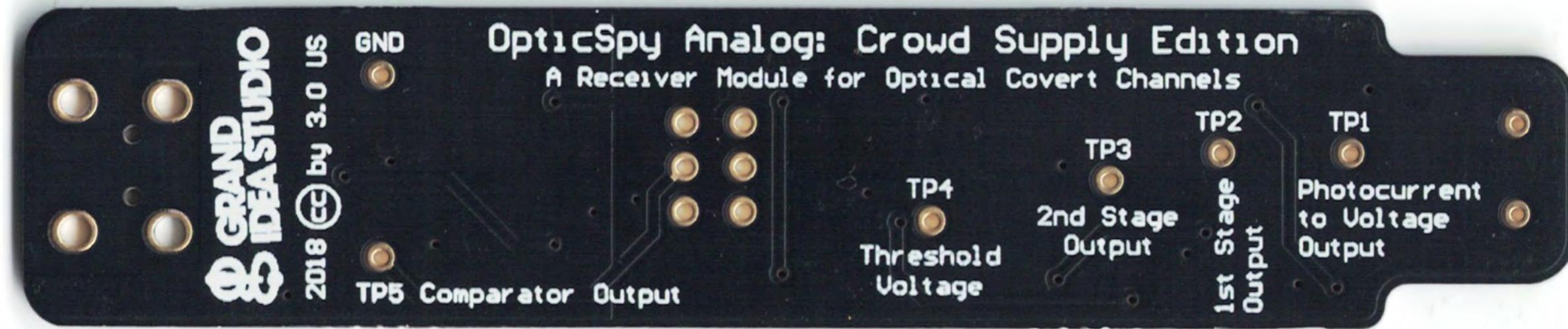
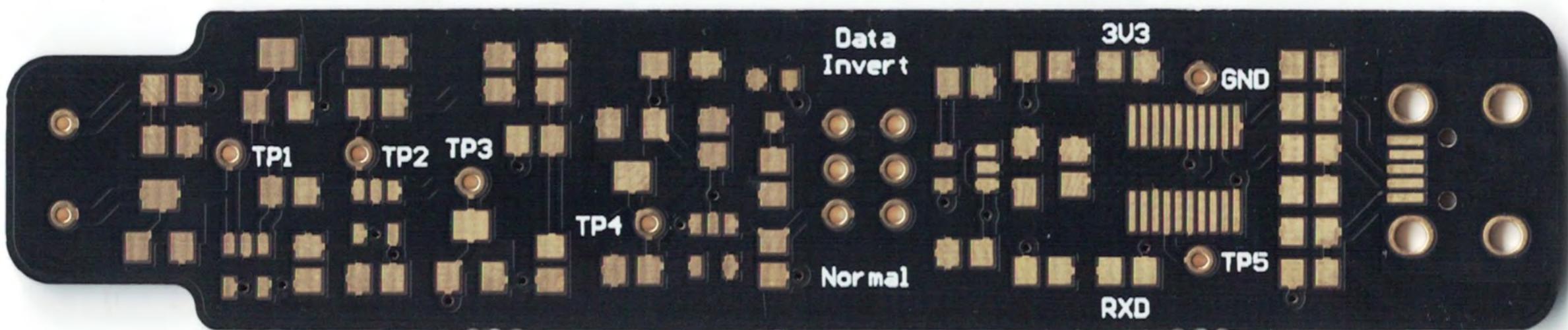


USB Interface

- Powers OpticSpy from bus (5V)
- FTDI FT231X USB-to-Serial UART
 - Entire USB protocol handled on-chip
 - Host will recognize as a virtual serial port (Windows, OS X, Linux)
- Decode asynchronous data streams and pass to host PC



PCB



Bill-of-Materials

| Item | Quantity | Reference | Manufacturer | Manuf. Part # | Distributor | Distrib. Part # | Description |
|------|----------|--------------------------------------|----------------------|-------------------|-------------|-------------------|--|
| 1 | 9 | C1, C2, C3, C4, C5, C6, C7, C11, C14 | Kemet | C0805C104K5RACTU | Digi-Key | 399-1170-1-ND | Capacitor, 0.1uF, 50V, Ceramic, 10%, X7R, 0805 |
| 2 | 1 | C8 | Kemet | C0805C103K5RACTU | Digi-Key | 399-1158-1-ND | Capacitor, 0.01uF, 50V, Ceramic, 10%, X7R, 0805 |
| 3 | 2 | C9, C10 | Samsung | CL21C470JBANNNC | Digi-Key | 1276-1156-1-ND | Capacitor, 47pF, 50V, Ceramic, 5%, C0G, 0805 |
| 4 | 2 | C12, C13 | Vishay Sprague | 293D106X0016A2TE3 | Digi-Key | 718-1956-1-ND | Capacitor, 10uF, 16V, Tantalum, 20%, Size A |
| 5 | 1 | C15 | Yageo | CC0805KRX7R9BB471 | Digi-Key | 311-1124-1-ND | Capacitor, 470pF, 50V, Ceramic, 10%, X7R, 0805 |
| 6 | 1 | D1 | Vishay Semiconductor | BPW21R | Digi-Key | 751-1013-ND | Photodiode, Silicon PN, 420-675nm, TO-5 |
| 7 | 2 | D2, D3 | Kingbright | APT2012SYCK | Digi-Key | 754-1134-1-ND | LED, Yellow clear, 150mcd, 2.0Vf, 590nm, 0805 |
| 8 | 1 | L1 | TDK | MPZ2012S221AT000 | Digi-Key | 445-1568-1-ND | Inductor, Ferrite Bead, 220R @ 100MHz, 3A, 0805 |
| 9 | 1 | P1 | Hirose Electric | UX60-MB-5S8 | Digi-Key | H2960CT-ND | Connector, Mini-USB, 5-pin, SMT w/ PCB mount |
| 10 | 1 | Q1 | ON Semiconductor | MMBT3904 | Digi-Key | MMBT3904FSCT-ND | Transistor, NPN, 40V, 200mA, SOT23-3 |
| 11 | 1 | R1 | Any | Any | Digi-Key | P100KACT-ND | Resistor, 100k, 5%, 1/8W, 0805 |
| 12 | 2 | R2, R12 | Bourns | PVG5A203C03R00 | Digi-Key | 490-2667-1-ND | Resistor, Variable Trimmer, 20k, 1/8W, SMD |
| 13 | 3 | R3, R6, R11 | Any | Any | Digi-Key | P1.0KACT-ND | Resistor, 1k, 5%, 1/8W, 0805 |
| 14 | 1 | R4 | Bourns | PVG5A504C03R00 | Digi-Key | 490-2674-1-ND | Resistor, Variable Trimmer, 500k, 1/8W, SMD |
| 15 | 3 | R5, R15, R16 | Any | Any | Digi-Key | P4.7KACT-ND | Resistor, 4.7k, 5%, 1/8W, 0805 |
| 16 | 3 | R7, R8, R9 | Any | Any | Digi-Key | P10KACT-ND | Resistor, 10k, 5%, 1/8W, 0805 |
| 17 | 1 | R10 | Bourns | PVG5A105C03R00 | Digi-Key | 490-2663-1-ND | Resistor, Variable Trimmer, 1.0M, 1/8W, SMD |
| 18 | 2 | R13, R14 | Any | Any | Digi-Key | P27ACT-ND | Resistor, 27 ohm, 5%, 1/8W, 0805 |
| 19 | 1 | SW1 | C&K Components | JS202011CQN | Digi-Key | 401-2001-ND | Switch, DPDT slide, 300mA @ 6VDC, PCB mount |
| 20 | 2 | U1, U2 | Maxim Integrated | MAX4124EUK+T | Digi-Key | MAX4124EUK+TCT-ND | IC, Operational Amplifier, Rail-to-Rail, SOT23-5 |
| 21 | 1 | U3 | Maxim Integrated | MAX985EUK+T | Digi-Key | MAX985EUK+TCT-ND | IC, Comparator, Push-Pull, Rail-to-Rail, SOT23-5 |
| 22 | 1 | U4 | FTDI | FT231XS-R | Digi-Key | 768-1129-1-ND | IC, USB-to-UART Bridge, SSOP20 |
| 23 | 1 | U5 | Microchip | MIC5205-3.3YM5 | Digi-Key | 576-1259-1-ND | Linear Regulator, LDO, 3.3V, 150mA, SOT23-5 |

- All components available from Digi-Key, Mouser
- Total cost per unit @ 100 quantity = ~\$40.77
- High ticket items: Photodiode, op amp, comparator, potentiometers, PCB fab/assembly/test

Target Data Transmission

- Standard LED driver circuit

Target Data Transmission

- Asynchronous serial (UART)
 - No external clock needed
 - NRZ (Non-Return-To-Zero) coding
 - Transfer speed (baud rate) selectable
 - Data bits sent LSB first (D0)

| | | | | | | | | | | |
|-----------|---------------|--------|--------|--------|--------|--------|--------|--------|-------------|----|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Start bit | 5–8 data bits | | | | | | | | Stop bit(s) | |
| Start | Data 0 | Data 1 | Data 2 | Data 3 | Data 4 | Data 5 | Data 6 | Data 7 | Stop | |

*** Start bit + Data bits + Parity (optional) + Stop bit(s)

Target Data Transmission



Target Data Transmission

- Printable ASCII data via standard UART
- printf(message) or equivalent

```
while(1)
{
    #use delay(clock=4000000)
    #use rs232(baud=19200, parity=N, bits=8, xmit=LED_RED, force_sw, stream=LED)
    setup_oscillator(OSC_4MHZ | OSC_INTRC | OSC_PLL_OFF); // increase clock speed
    fprintf(LED, msg_covert); // transmit secret message through the LED
}
```

```
// Set up a new serial port
SoftwareSerial opticSerial = SoftwareSerial(rxPin, txPin);
opticSerial.print(msg_covert); // Transmit secret message through the LED
opticSerial.flush(); // Wait for all bytes to be transmitted
```

TP1: Photocurrent-to-Voltage



TP2: 1st Stage Amp Output

TP3: 2nd Stage Amp Output

TPS: Comparator Output

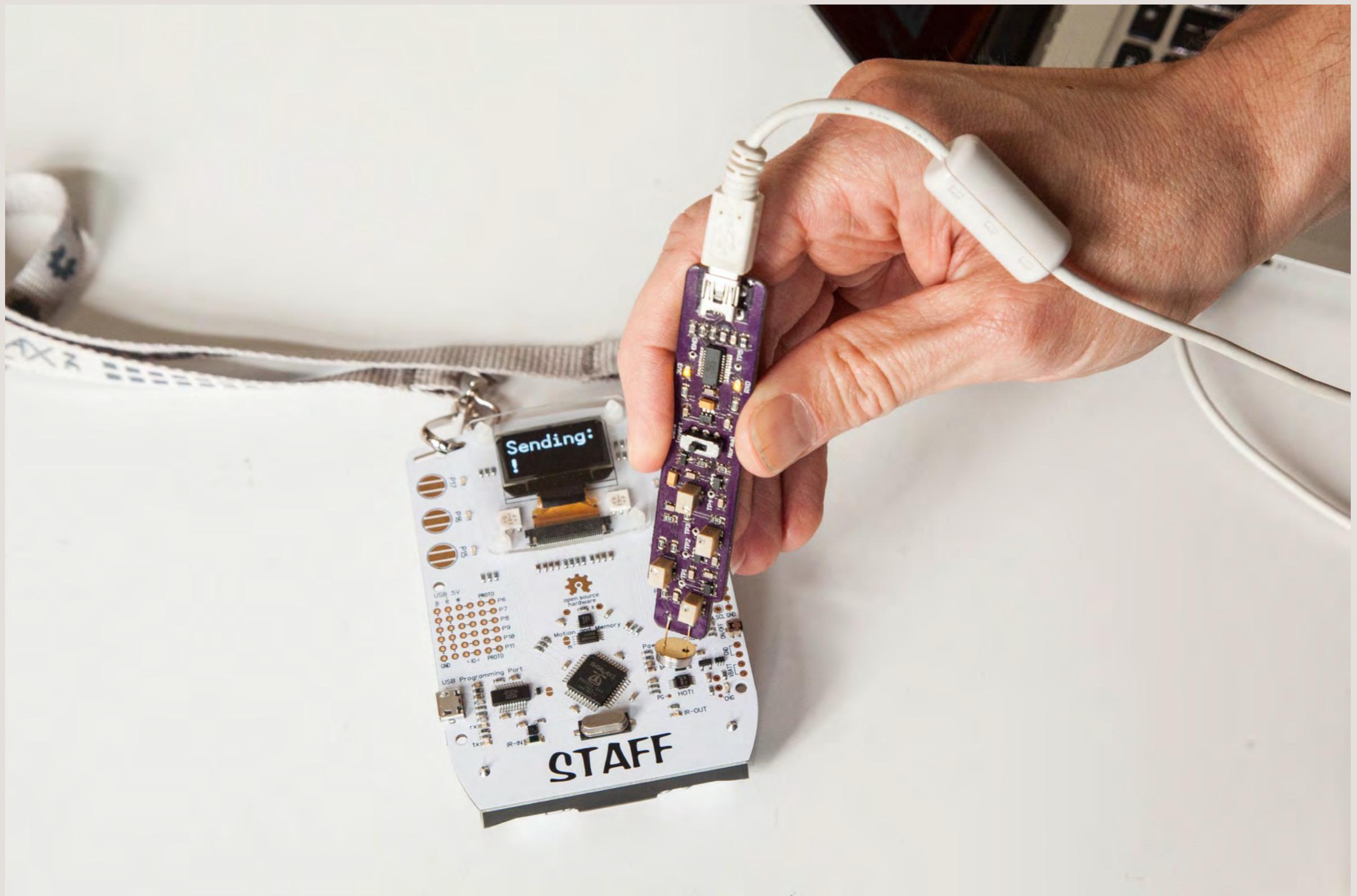
TPS: Comparator Output

Calibration

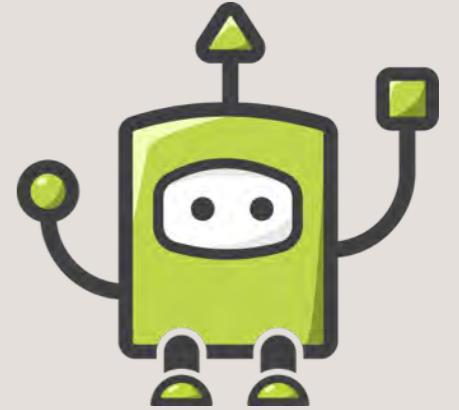
- Adjust settings for a particular target system
 - Reduce ambient noise
 - Increase receive distance
 - Change frequency response/bandwidth
 - Dependent on brightness and wavelength of transmitting signal
- Potentiometers
 - Gain adjustment (three stages)
 - Default setting @ mid-range -> $27.6\text{M}\Omega$
 - Threshold voltage adjustment (for comparator)
 - Set to 2.5V during production

Demonstrations

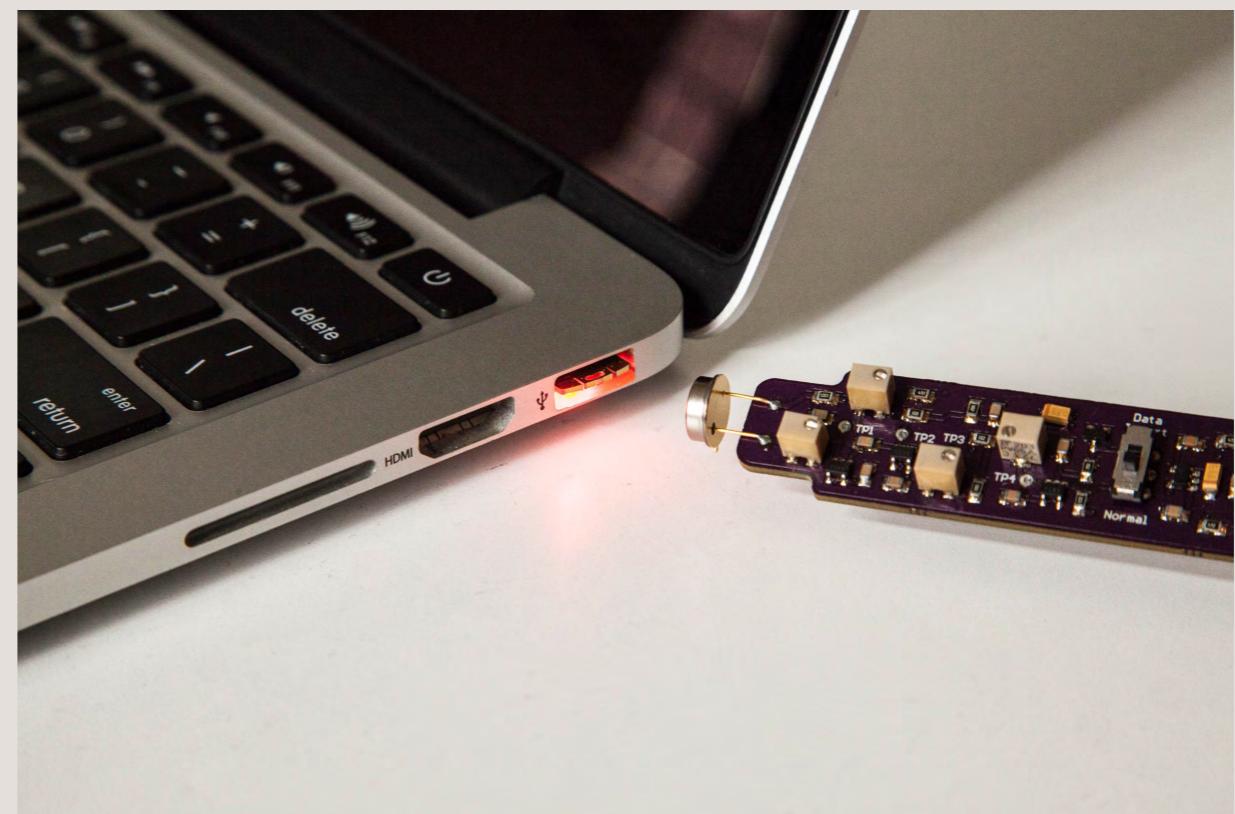
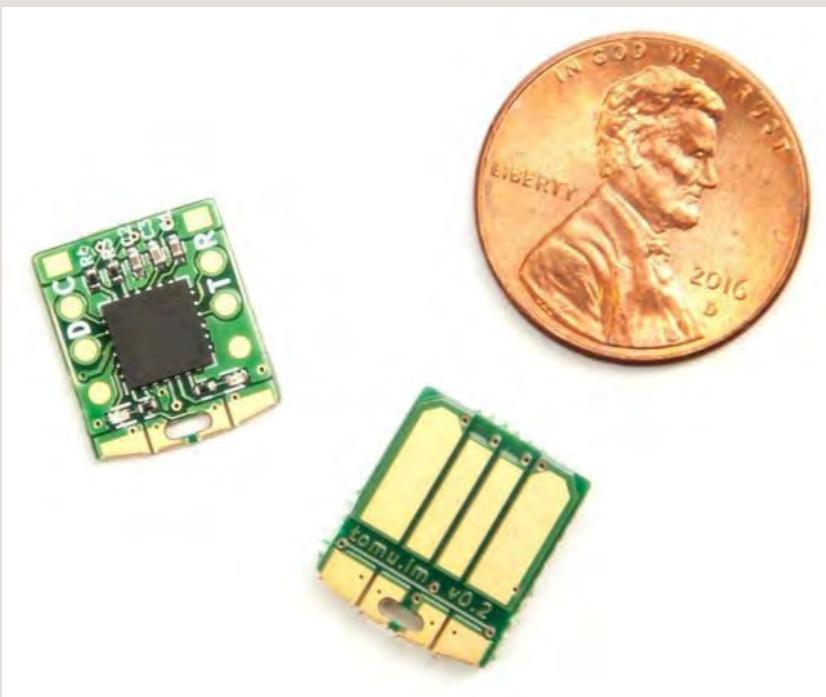
Parallax Electronic Badge



Tomu

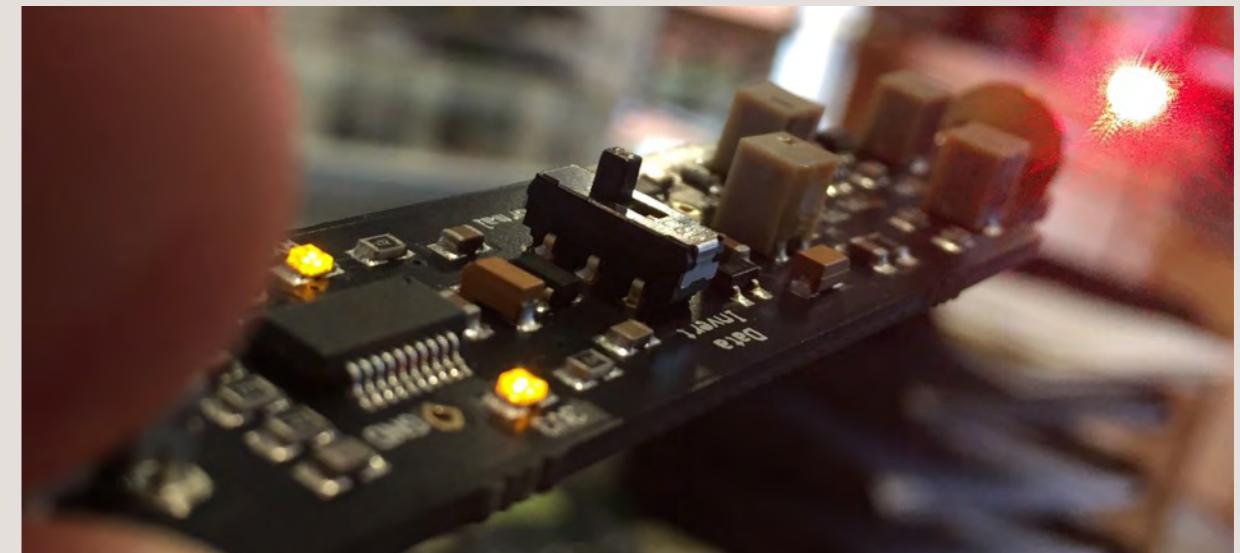
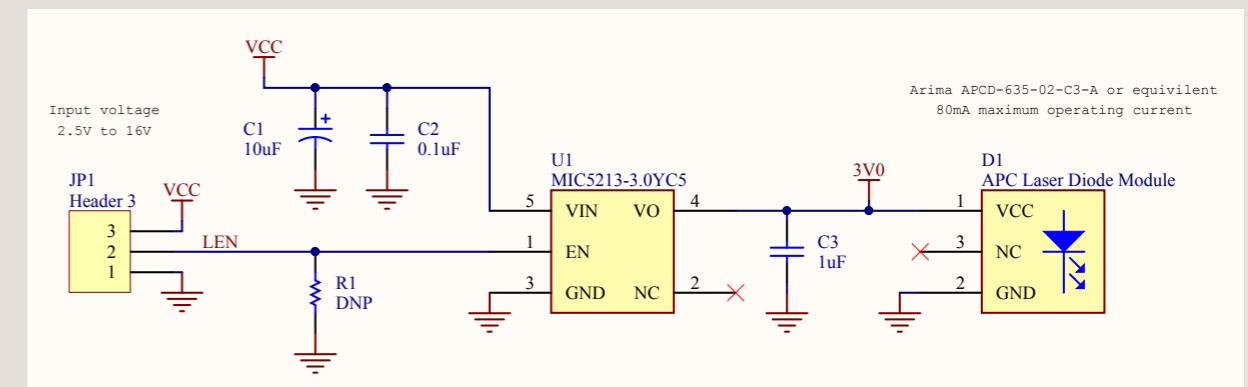
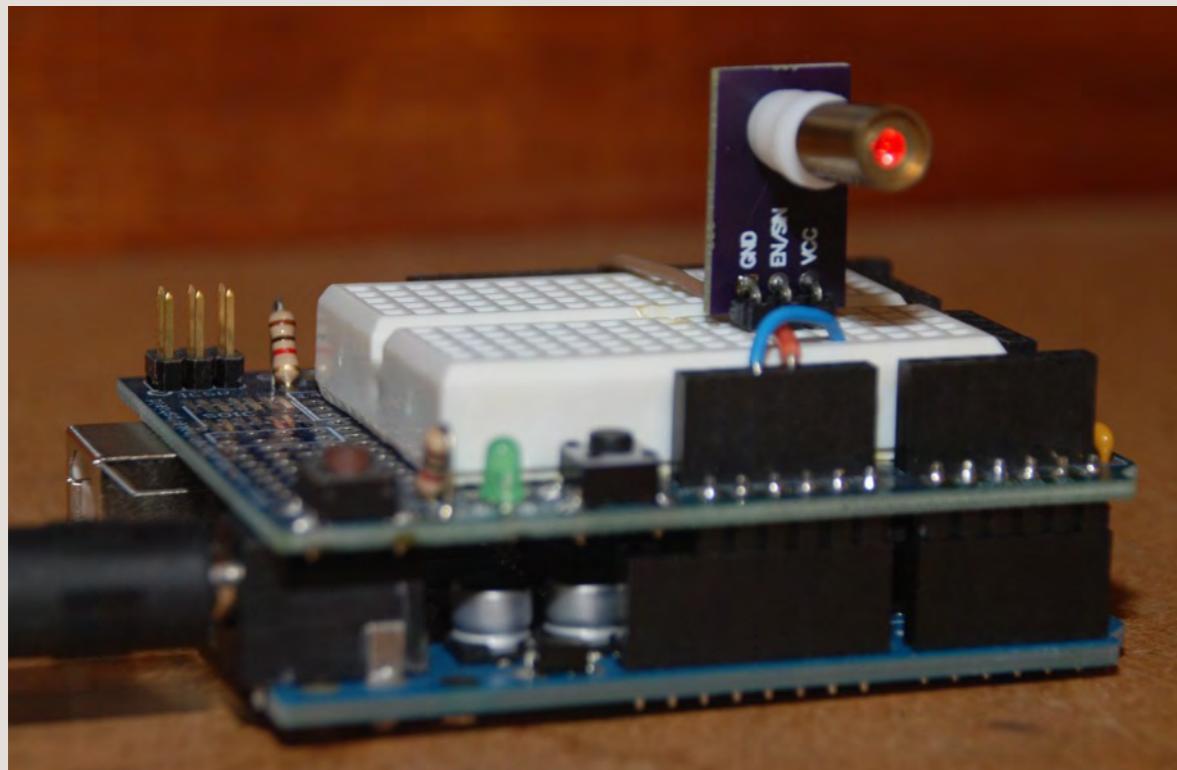


- Silicon Labs Happy Gecko EFM32HG309
- Total 12 components (incl. plastic case)
- 100% Open Source (w/ KiCad)
- <http://tomu.im>
- <https://github.com/im-tomu/tomu-quickstart/tree/master/opticspy>

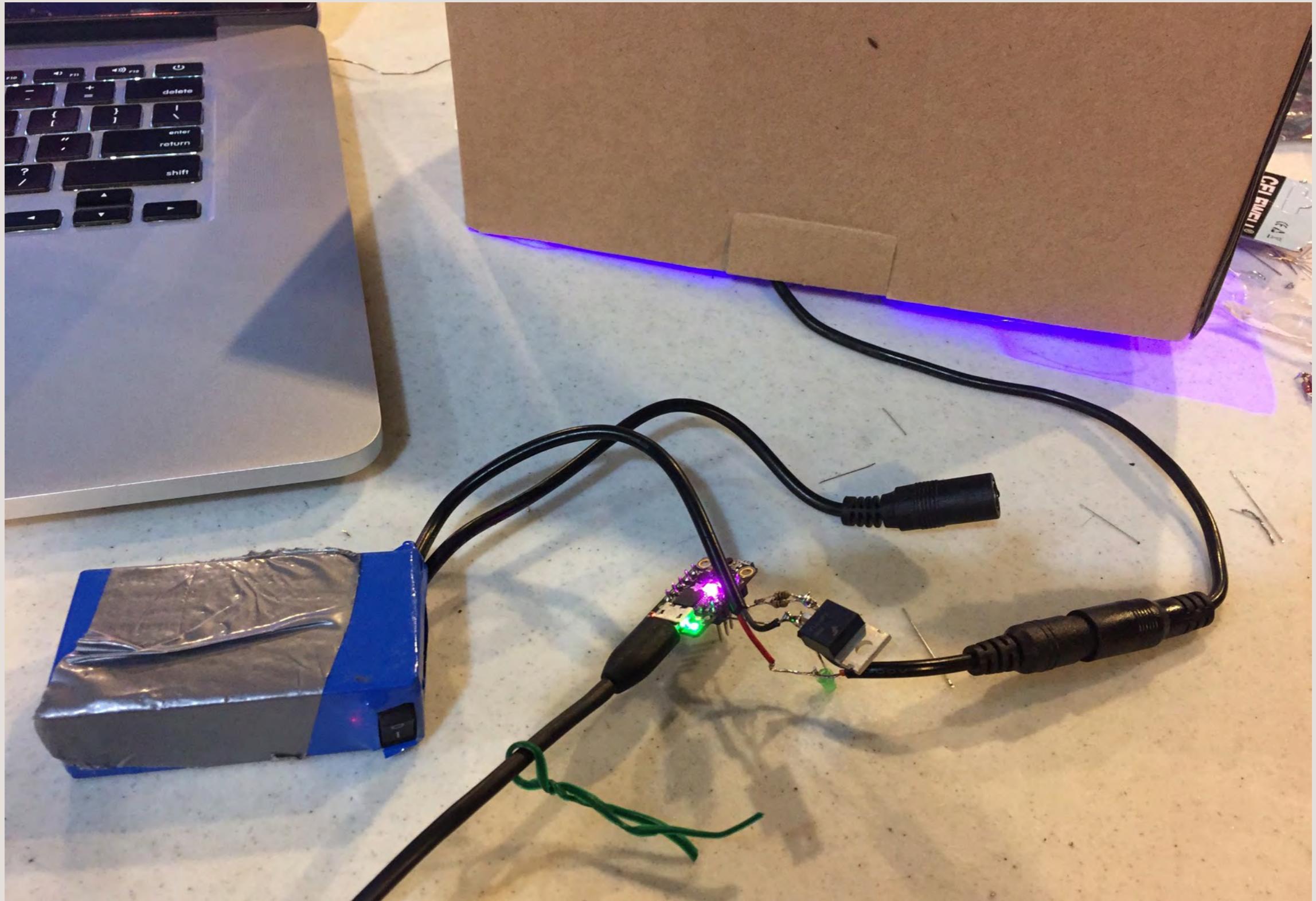


Arduino + LazOr!®

- Long-range data transmission w/ laser diode module
- Data sent to LDO Enable (EN) pin
- Distance limited by laser diffusion + output power
- oshpark.com/shared_projects/WV8fBzyW

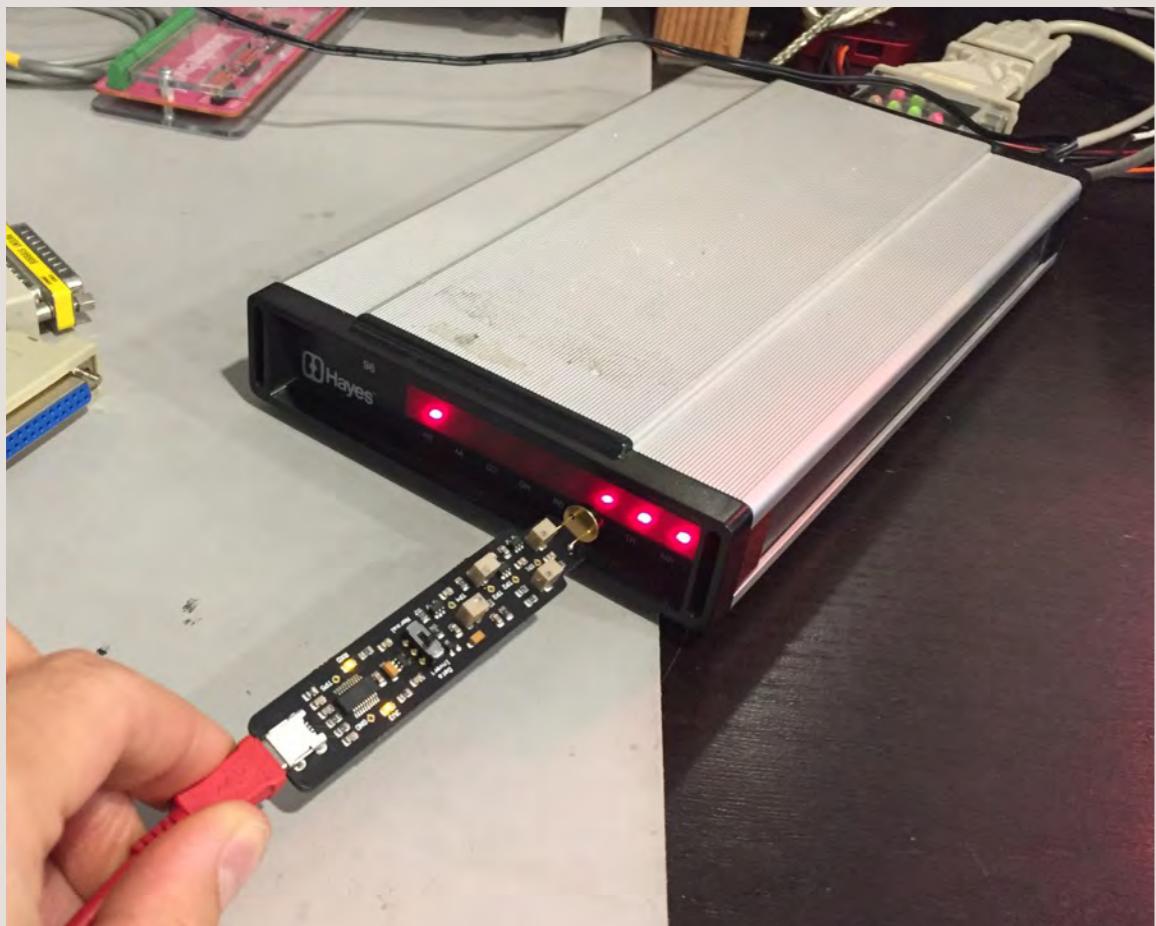


Arduino + LazOr!©



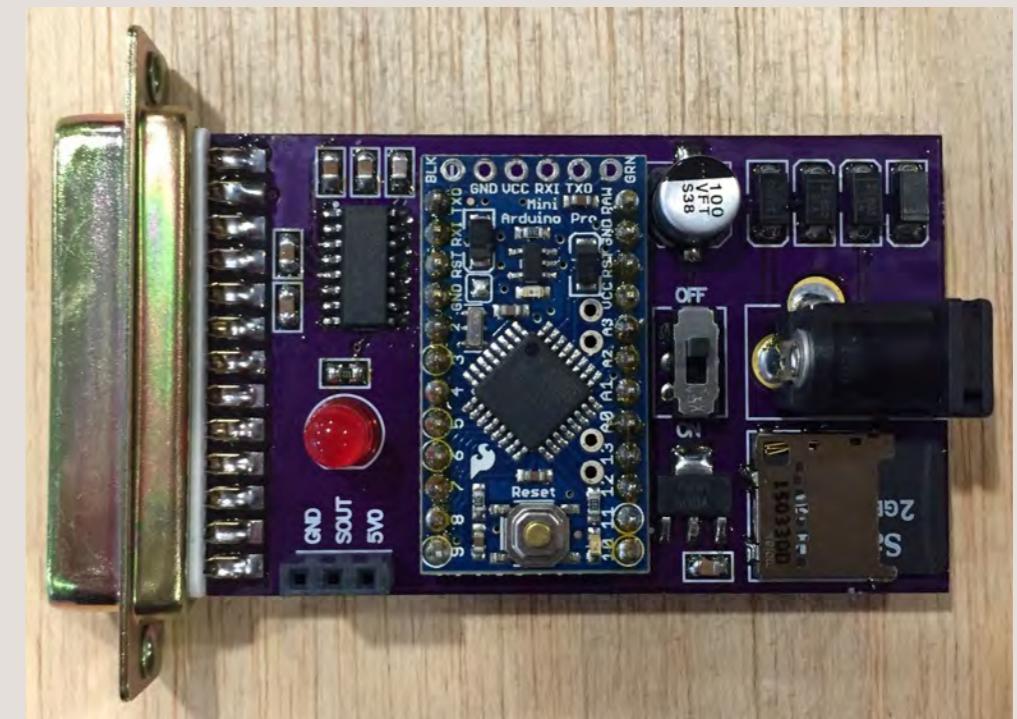
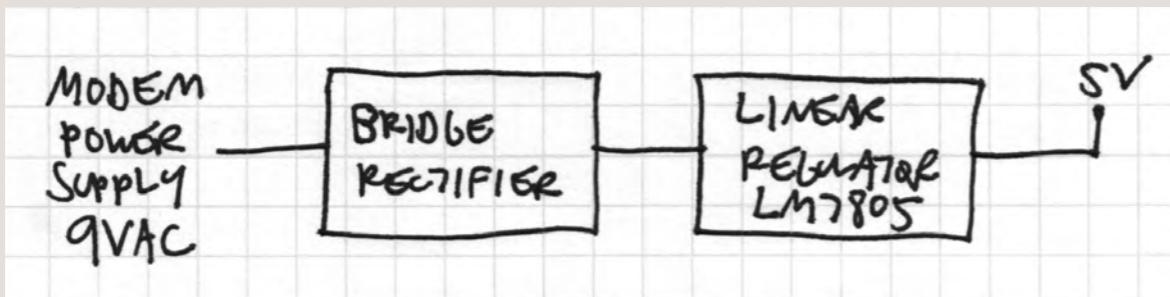
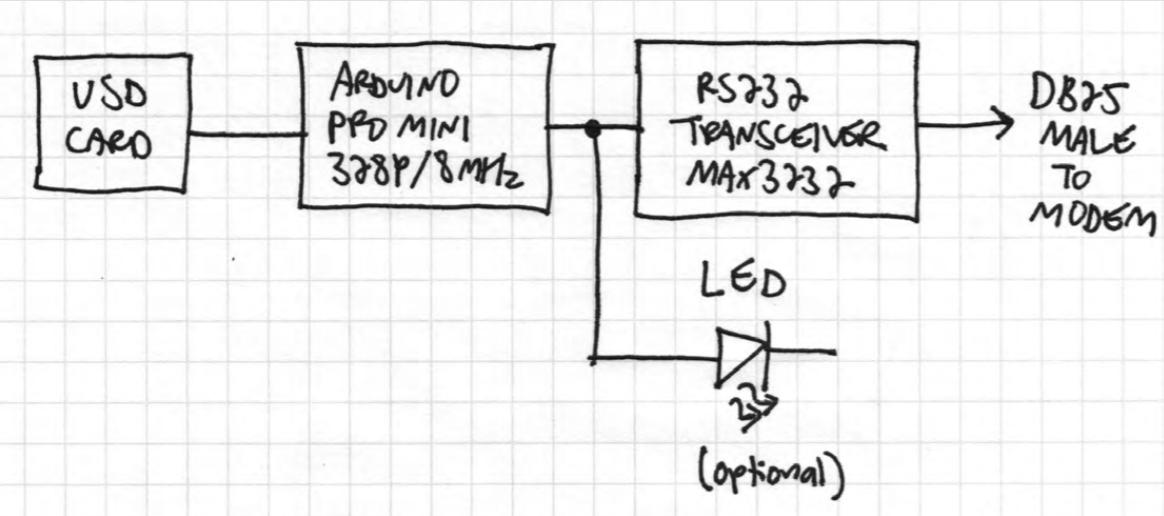
Hayes Smartmodem Optima

- Data leakage through SD (Send Data) LED
- Discovered by Loughry and Umphress 2002
- Indicator LEDs tied to serial port data lines



Hayes Smartmodem Optima

- uSD to Serial Interface
 - Read text file from card, send contents via serial
- DB25 connection for direct connection to modem
- Good for demonstrations, trolling, etc.
- oshpark.com/shared_projects/laP2t8DO

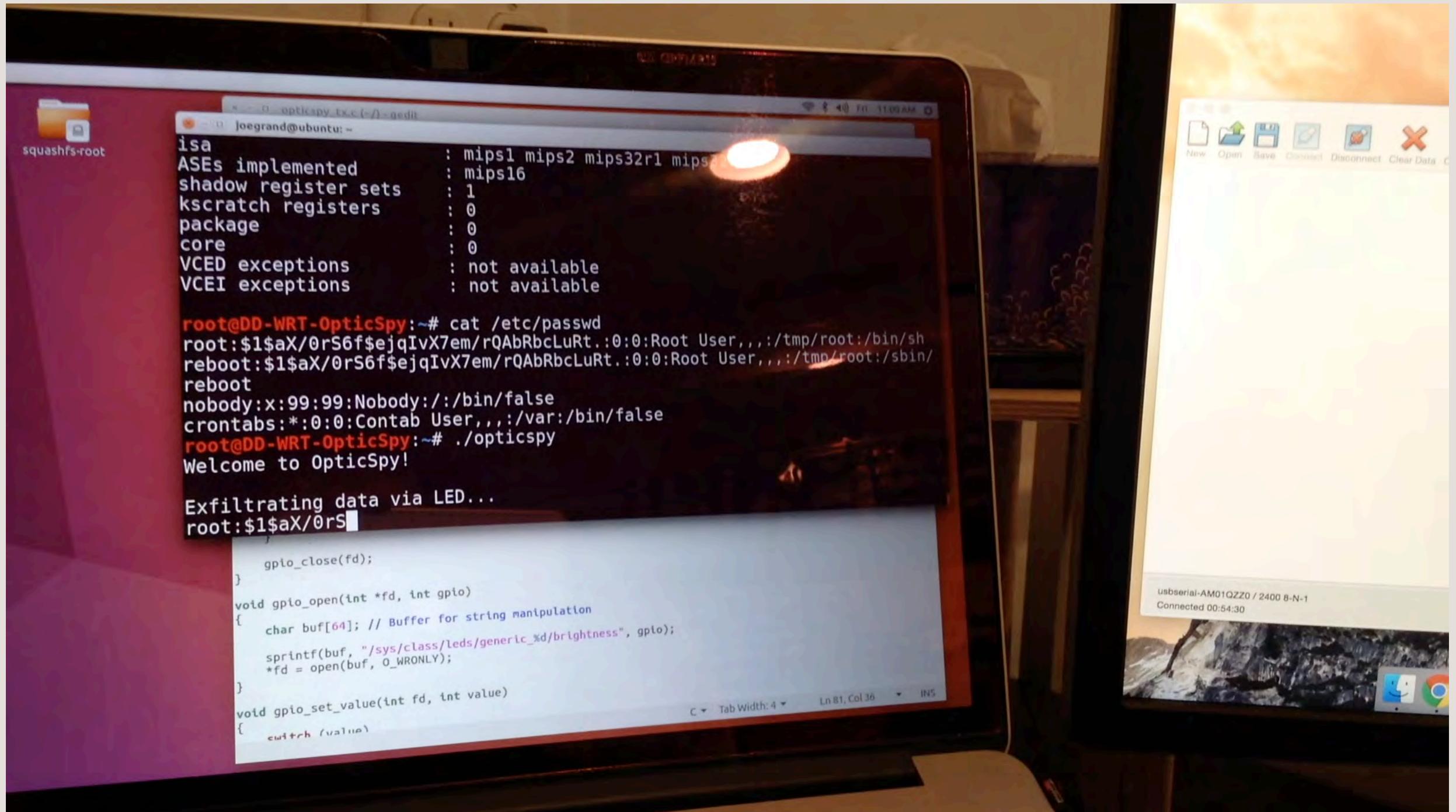


TP-Link TL-WR841N

- Physically unmodified router w/ DD-WRT
- Cross compiled w/ toolchain-mips_24kc_gcc-7.2.0_musl
- Loaded onto the device with known administrator credentials (as proof of concept)

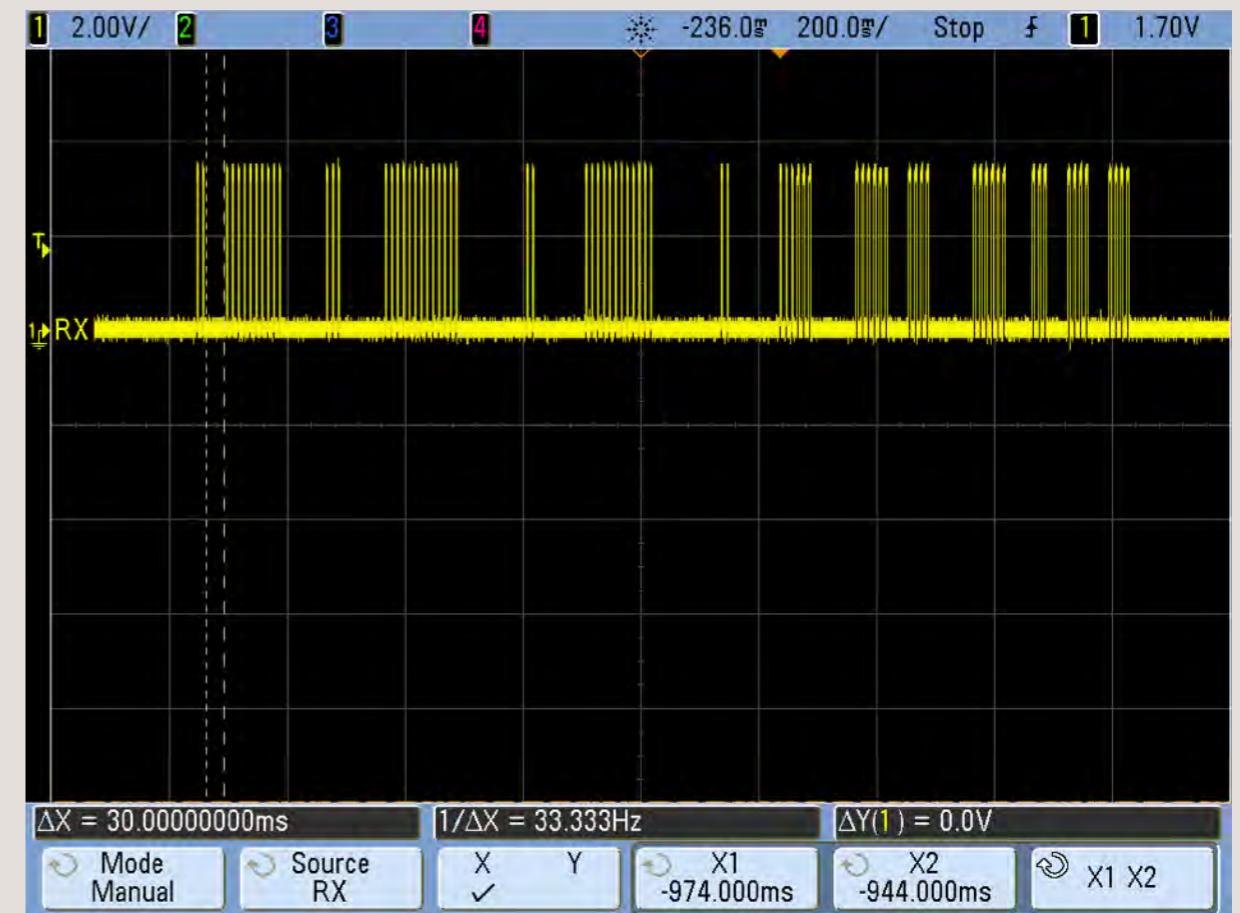
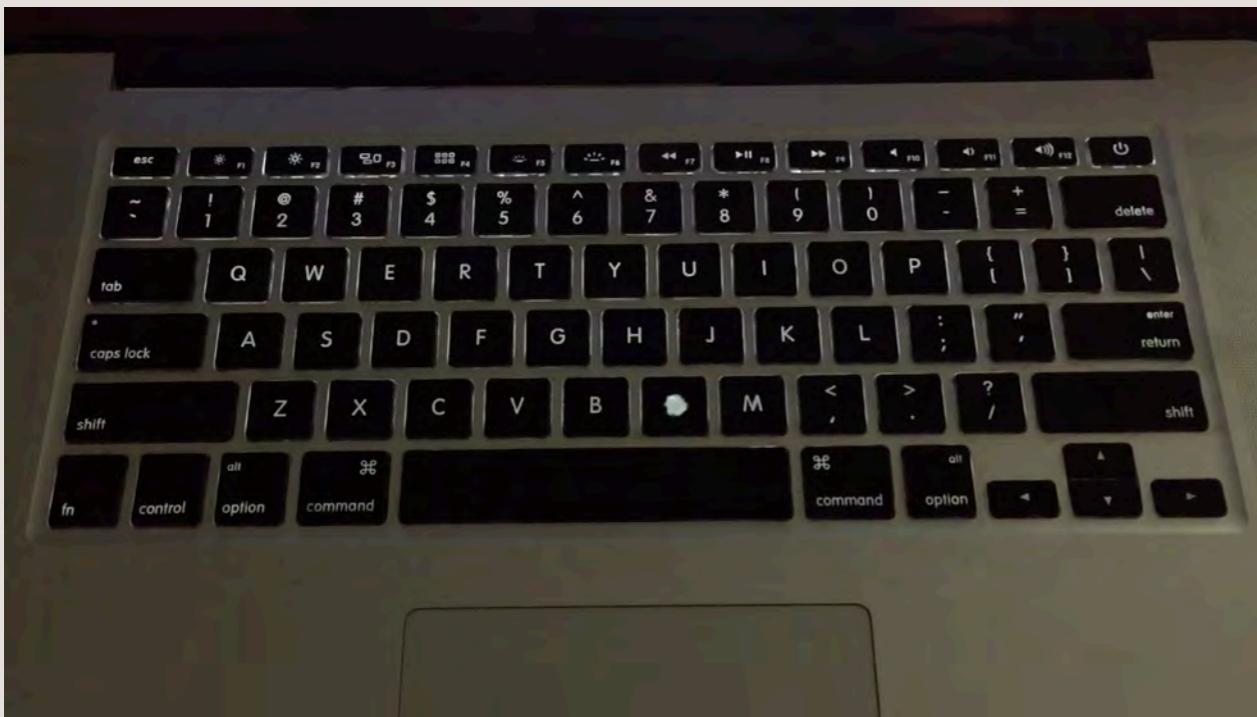


TP-Link TL-WR841N



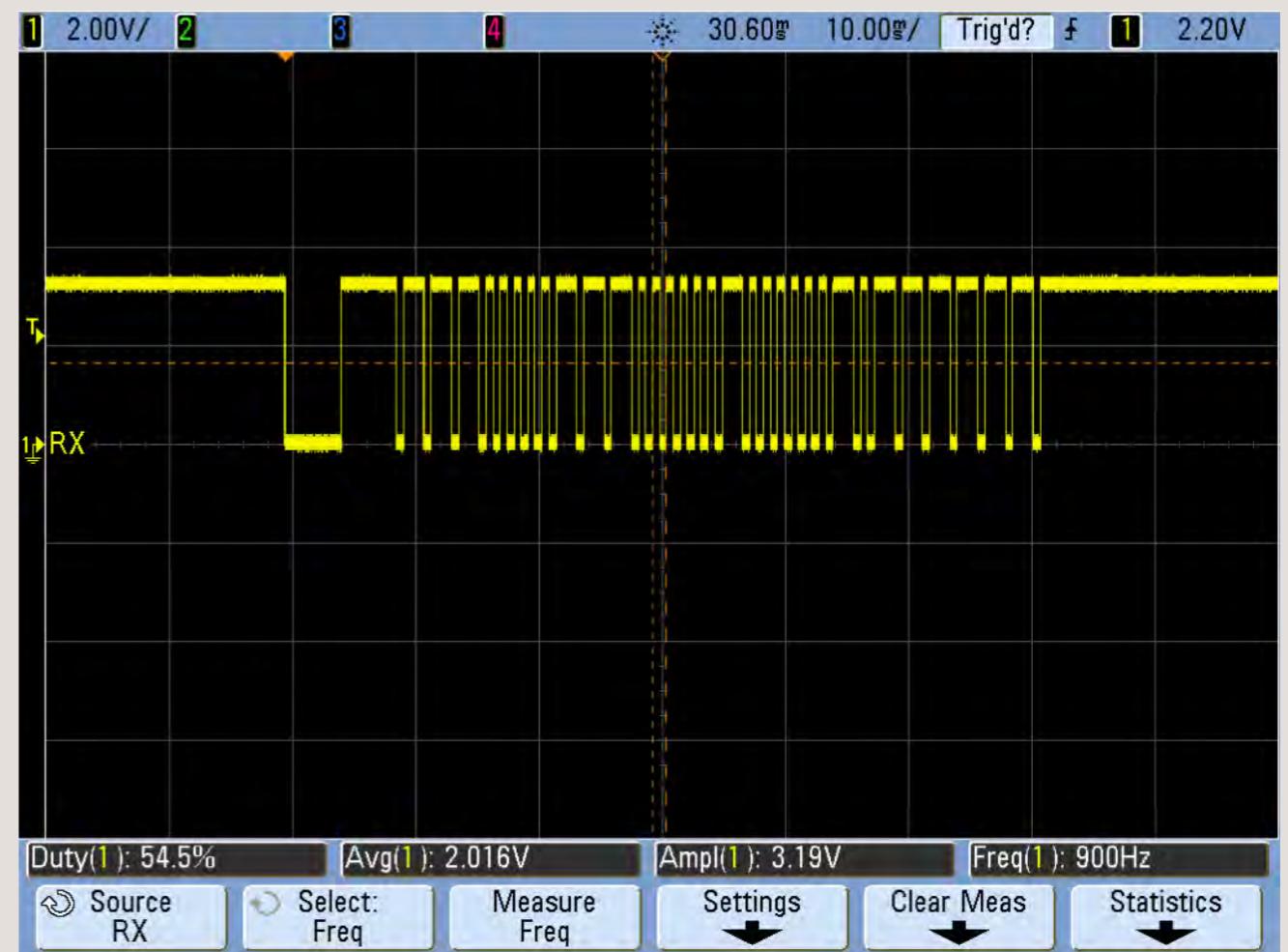
MacBook Pro Keyboard

- Based on <https://github.com/pirate/mac-keyboard-brightness>
- Backlight LEDs @ 100Hz, 75% PWM :(
- Can decode manually or w/ MCU via TP5



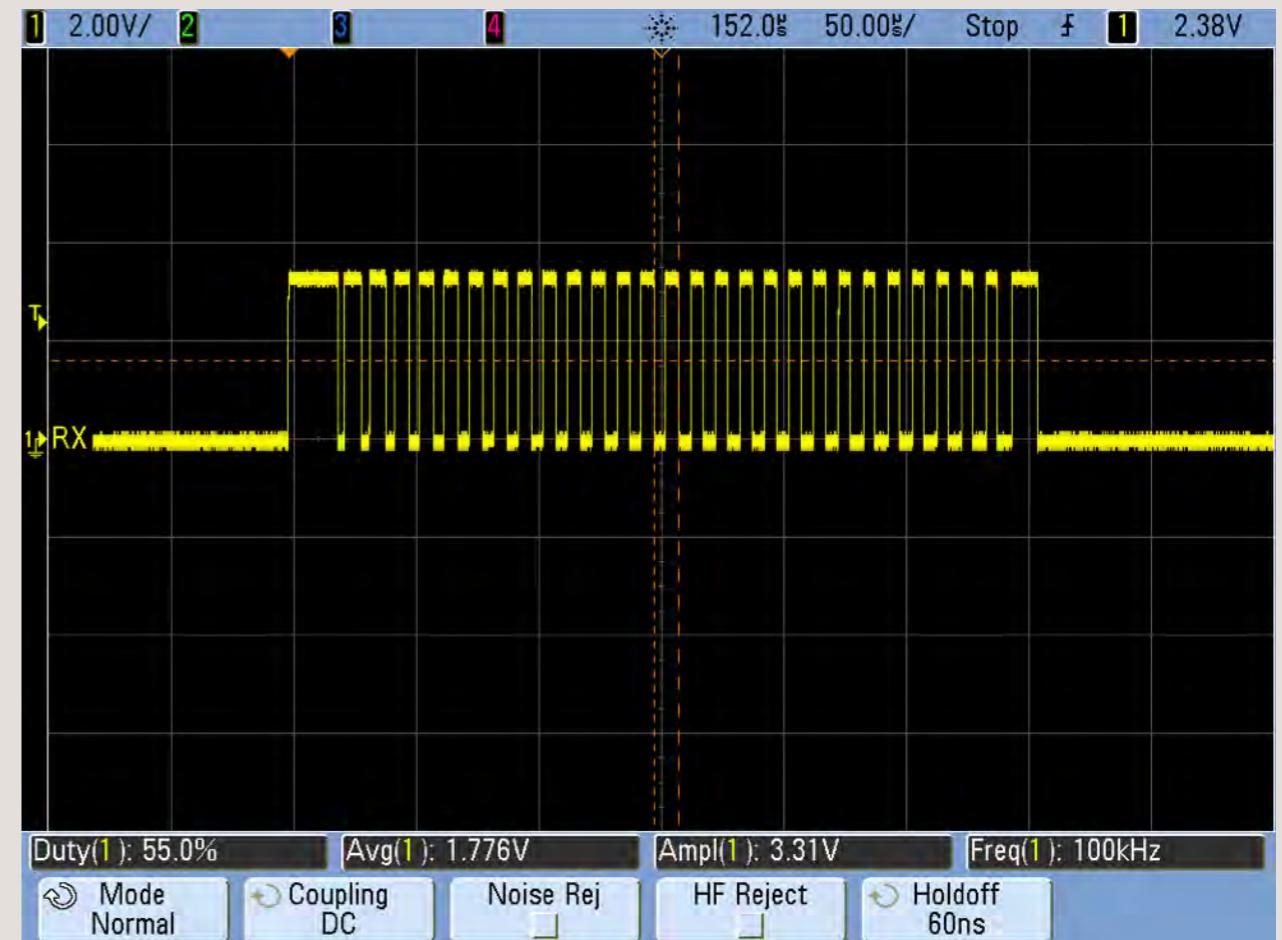
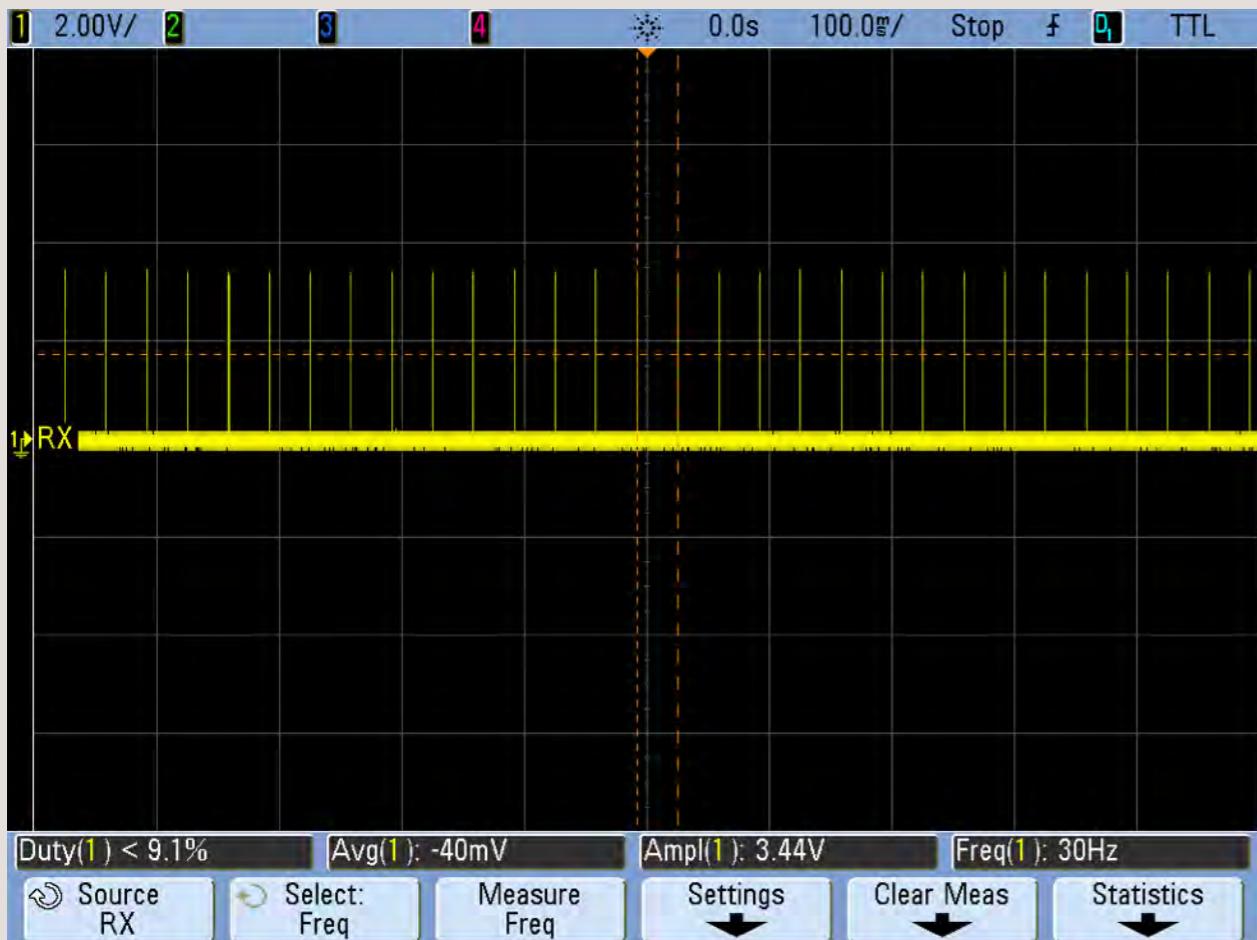
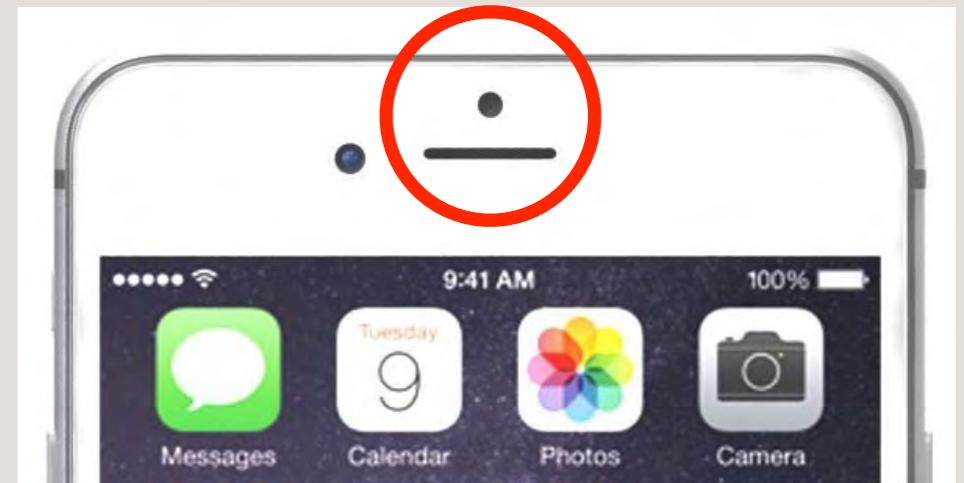
Samsung TV Remote

- 38kHz carrier
- Start: 4.5ms pulse burst, 4.5ms space
- Logic '1': ~544μs pulse, 1.706ms space
- Logic '0': ~544μs pulse, 580μs space
- Measure via TP5



iPhone 6 Proximity Sensor

- ~313uS width @ 100kHz carrier
- 30Hz refresh rate
- Measure via TP5



Application Ideas

- Search for optical covert channels in existing devices
- Discover optical networking/communications systems
- Add data transfer functionality to a project
- Receive/demodulate IR signals
- Measure the world around you

Limitations

- Data must be NRZ encoded in order to pass through USB-to-Serial interface
- Short receive range (up to ~4 inches) w/o additional optics
- Difficult to determine potentiometer settings

Future Work?

- More intelligence to handle non-NRZ data streams (on-board v. off-board)
- Automatic gain control (AGC) to replace potentiometers
- Compromise/communicate with a target device using an LED as an *input*

Other Things

- Photodiode Amplifiers: Op Amp Solutions, Jerald Graeme, McGraw-Hill, 1995
- Sound Camera: NYC Night Drive, Eric Archer, 2010
- The Photophone, Hack-a-Week, 2011
- PWM Laser Audio Transmitter, Tymkrs, 2011

Other Things

- IBM/Lenovo ThinkPad LED Control
 - www.reddit.com/r/thinkpad/comments/7n8eyu/thinkpad_led_control_under_gnulinx/
- Asus ROG Strix Z370 Gaming Mini-ITX Motherboard
 - Addressable AURA sync RGB LED lighting
 - www.asus.com/us/ROG-Republic-Of-Gamers/ROG-STRIX-Z370-I-GAMING/

Come Into the Light

- grandideastudio.com/portfolio/opticspy
*** Schematic, BOM, Gerber plots, test procedure,
user manual, demonstration code
- oshpark.com/profiles/joegrand
*** Bare boards
- crowdsupply.com/grand-idea-studio/opticspy
*** Assembled units



The End.