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

PHOTODIODE → AMPLIFIERS → THRESHOLD DETECTOR → SERIAL-TO-USB

USB SV

LDO 3.3V

HOST PC
USB MINI-B
Points of Interest

- Photodiode
- Gain adjust
- Threshold voltage adjust
- Power indicator
- Polarity selection
- Receive indicator
- USB
OpticSpy Analog: Crowd Supply

To Host
USB Max B

1 USB
4 D
5 G

Place target LED near or onto sensor
Peak wavelength sensitivity @ 565nm

Non-Inverting Amplifier (1st Stage)
- U1 MAX4124EUK
- C2 0.1uF
- R2 20k
- R3 4.7k
- U1Av = 1 + R4/R5
- Total transimpedance gain = R2 x U1Av x U2Av
- Frequency response inversely proportional to gain

Non-Inverting Amplifier (2nd Stage)
- U2 MAX4124EUK
- C3 0.1uF
- R6 1k
- R8 10k
- R11 1k

Threshold Detector (Comparator)
- U3 MAX8605EU
- C7 0.1uF
- R10 10k
- U2Av = 1 + R10/R8

Power Indicator
- LED
- D3
- TP3

Based on Maxim Integrated’s AN1117: Small Photodiode Receiver Handles Fiber-Optic Data Rates to 400Kbps (July, 2003)

NOTE: RESISTORS ARE IN OHMS +/- 5% AND CAPACITORS ARE IN MICROFARADS UNLESS OTHERWISE DOTTED. SEE BOM FOR ACTUAL VOLTAGE AND SPECIFICATION.
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 = $R_2 \times U_{1Av} \times U_{2Av}$
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
# Bill-of-Materials

<table>
<thead>
<tr>
<th>Item</th>
<th>Quantity</th>
<th>Reference</th>
<th>Manufacturer</th>
<th>Manuf. Part #</th>
<th>Distributor</th>
<th>Distrib. Part #</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9</td>
<td>C1, C2, C3, C4, C5, C6, C7, C11, C14</td>
<td>Kemet</td>
<td>C0805C104K5RACTU</td>
<td>Digi-Key</td>
<td>399-1170-1-ND</td>
<td>Capacitor, 0.1uF, 50V, Ceramic, 10%, X7R, 0805</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>C8</td>
<td>Kemet</td>
<td>C0805C103K5RACTU</td>
<td>Digi-Key</td>
<td>399-1158-1-ND</td>
<td>Capacitor, 0.01uF, 50V, Ceramic, 10%, X7R, 0805</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>C9, C10</td>
<td>Samsung</td>
<td>CL21C470JBA7N6C</td>
<td>Digi-Key</td>
<td>1276-1156-1-ND</td>
<td>Capacitor, 47pF, 50V, Ceramic, 5%, C0G, 0805</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>C12, C13</td>
<td>Vishay Sprague</td>
<td>293D106X0016A2TE3</td>
<td>Digi-Key</td>
<td>718-1956-1-ND</td>
<td>Capacitor, 10uF, 16V, Tantalum, 20%, Size A</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>C15</td>
<td>Yageo</td>
<td>CC0805KRX7R9BB471</td>
<td>Digi-Key</td>
<td>311-1124-1-ND</td>
<td>Capacitor, 470pF, 50V, Ceramic, 10%, X7R, 0805</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>D1</td>
<td>Vishay Semiconductor</td>
<td>BPW21R</td>
<td>Digi-Key</td>
<td>751-1013-ND</td>
<td>Photodiode, Silicon PN, 420-675nm, TO-5</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>D2, D3</td>
<td>Kingbright</td>
<td>APT2012SYCK</td>
<td>Digi-Key</td>
<td>754-1134-1-ND</td>
<td>LED, Yellow clear, 150mcd, 2.0Vf, 590nm, 0805</td>
</tr>
<tr>
<td>8</td>
<td>1</td>
<td>L1</td>
<td>TDK</td>
<td>MPZ2012S221AT000</td>
<td>Digi-Key</td>
<td>445-1568-1-ND</td>
<td>Inductor, Ferrite Bead, 220R @ 100MHz, 3A, 0805</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>P1</td>
<td>Hirose Electric</td>
<td>UX80-MB-SSS</td>
<td>Digi-Key</td>
<td>H2960CT-ND</td>
<td>Connector, Mini-USB, 5-pin, SMT w/ PCB mount</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>Q1</td>
<td>ON Semiconductor</td>
<td>MMBT3904</td>
<td>Digi-Key</td>
<td>MMBT3904FSCT-ND</td>
<td>Transistor, NPN, 40V, 200mA, SOT23-3</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>R1</td>
<td>Any</td>
<td>Any</td>
<td>Digi-Key</td>
<td>P100KACT-ND</td>
<td>Resistor, Variable Trimmer, 10k, 5%, 1/8W, 0805</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>R2, R12</td>
<td>Bourns</td>
<td>PVG5A203C03R00</td>
<td>Digi-Key</td>
<td>490-2667-1-ND</td>
<td>Resistor, Variable Trimmer, 20k, 1/8W, SMD</td>
</tr>
<tr>
<td>13</td>
<td>3</td>
<td>R3, R6, R11</td>
<td>Any</td>
<td>Any</td>
<td>Digi-Key</td>
<td>P1.0KACT-ND</td>
<td>Resistor, 1k, 5%, 1/8W, 0805</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>R4</td>
<td>Bourns</td>
<td>PVG5A504C03R00</td>
<td>Digi-Key</td>
<td>490-2674-1-ND</td>
<td>Resistor, Variable Trimmer, 50k, 1/8W, SMD</td>
</tr>
<tr>
<td>15</td>
<td>3</td>
<td>R5, R15, R16</td>
<td>Any</td>
<td>Any</td>
<td>Digi-Key</td>
<td>P4.7KACT-ND</td>
<td>Resistor, 4.7k, 5%, 1/8W, 0805</td>
</tr>
<tr>
<td>16</td>
<td>3</td>
<td>R7, R8, R9</td>
<td>Any</td>
<td>Any</td>
<td>Digi-Key</td>
<td>P10KACT-ND</td>
<td>Resistor, 10k, 5%, 1/8W, 0805</td>
</tr>
<tr>
<td>17</td>
<td>1</td>
<td>R10</td>
<td>Bourns</td>
<td>PVG5A105C03R00</td>
<td>Digi-Key</td>
<td>490-2663-1-ND</td>
<td>Resistor, Variable Trimmer, 10M, 1/8W, SMD</td>
</tr>
<tr>
<td>18</td>
<td>2</td>
<td>R13, R14</td>
<td>Any</td>
<td>Any</td>
<td>Digi-Key</td>
<td>P27ACT-ND</td>
<td>Resistor, 27 ohm, 5%, 1/8W, 0805</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>SW1</td>
<td>C&amp;K Components</td>
<td>JS202011CQN</td>
<td>Digi-Key</td>
<td>401-2001-ND</td>
<td>Switch, DPDT slide, 300mA @ 6VDC, PCB mount</td>
</tr>
<tr>
<td>20</td>
<td>2</td>
<td>U1, U2</td>
<td>Maxim Integrated</td>
<td>MAX4124EUK+T</td>
<td>Digi-Key</td>
<td>MAX4124EUK+TCT-ND</td>
<td>IC, Operational Amplifier, Rail-to-Rail, SOT23-5</td>
</tr>
<tr>
<td>21</td>
<td>1</td>
<td>U3</td>
<td>Maxim Integrated</td>
<td>MAX9885EUK+T</td>
<td>Digi-Key</td>
<td>MAX9885EUK+TCT-ND</td>
<td>IC, Comparator, Push-Pull, Rail-to-Rail, SOT23-5</td>
</tr>
<tr>
<td>22</td>
<td>1</td>
<td>U4</td>
<td>FTDI</td>
<td>FT231XS-R</td>
<td>Digi-Key</td>
<td>768-1129-1-ND</td>
<td>IC, USB-to-UART Bridge, SSOP20</td>
</tr>
<tr>
<td>23</td>
<td>1</td>
<td>U5</td>
<td>Microchip</td>
<td>MIC5205-3.3YM5</td>
<td>Digi-Key</td>
<td>576-1259-1-ND</td>
<td>Linear Regulator, LDO, 3.3V, 150mA, SOT23-5</td>
</tr>
</tbody>
</table>

- 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)

<table>
<thead>
<tr>
<th>Start bit</th>
<th>Data 0</th>
<th>Data 1</th>
<th>Data 2</th>
<th>Data 3</th>
<th>Data 4</th>
<th>Data 5</th>
<th>Data 6</th>
<th>Data 7</th>
<th>Stop bit(s)</th>
</tr>
</thead>
</table>

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

Mark (Idle)

Space

Bit width = ~8.7uS
Target Data Transmission

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

```cpp
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
TP5: Comparator Output
TP5: 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 -> 27.6MΩ
- 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 + Laz0r!@**

- 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](oshpark.com/shared_projects/WV8fBzyW)
Arduino + Laz0r!@
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)
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

- ~313\textup{u}S 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_gnulinux/

• Asus ROG Strix Z370 Gaming Mini-ITX Motherboard
  • Addressable AURA sync RGB LED lighting
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.