www.pwc.co.uk

See no evil, hear no evil

Hacking invisibly and silently with light and sound

Matt Wixey – PwC UK

July 2017

pwc

Intro

- Matt Wixey
- Lead the research function on PwC's UK pentesting team
- Run The Dark Art Lab research blog
- Previously worked in LEA, leading R&D team

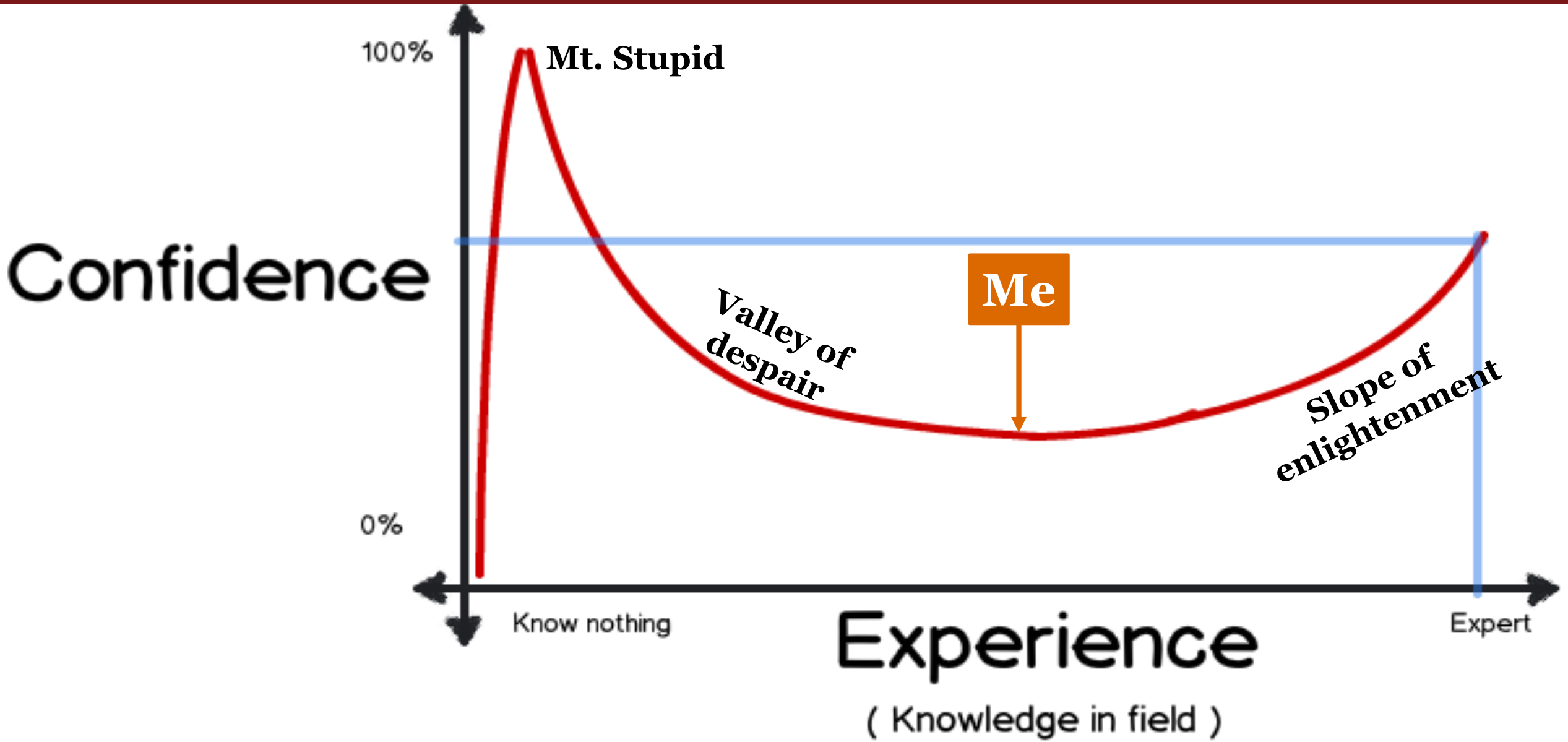
Agenda

- **Part I:** Jumping air-gaps
- **Part II:** Surveillance and counter-surveillance
- **Part III:** Bantz
- **Part IV:** Summary and future research

Disclaimers

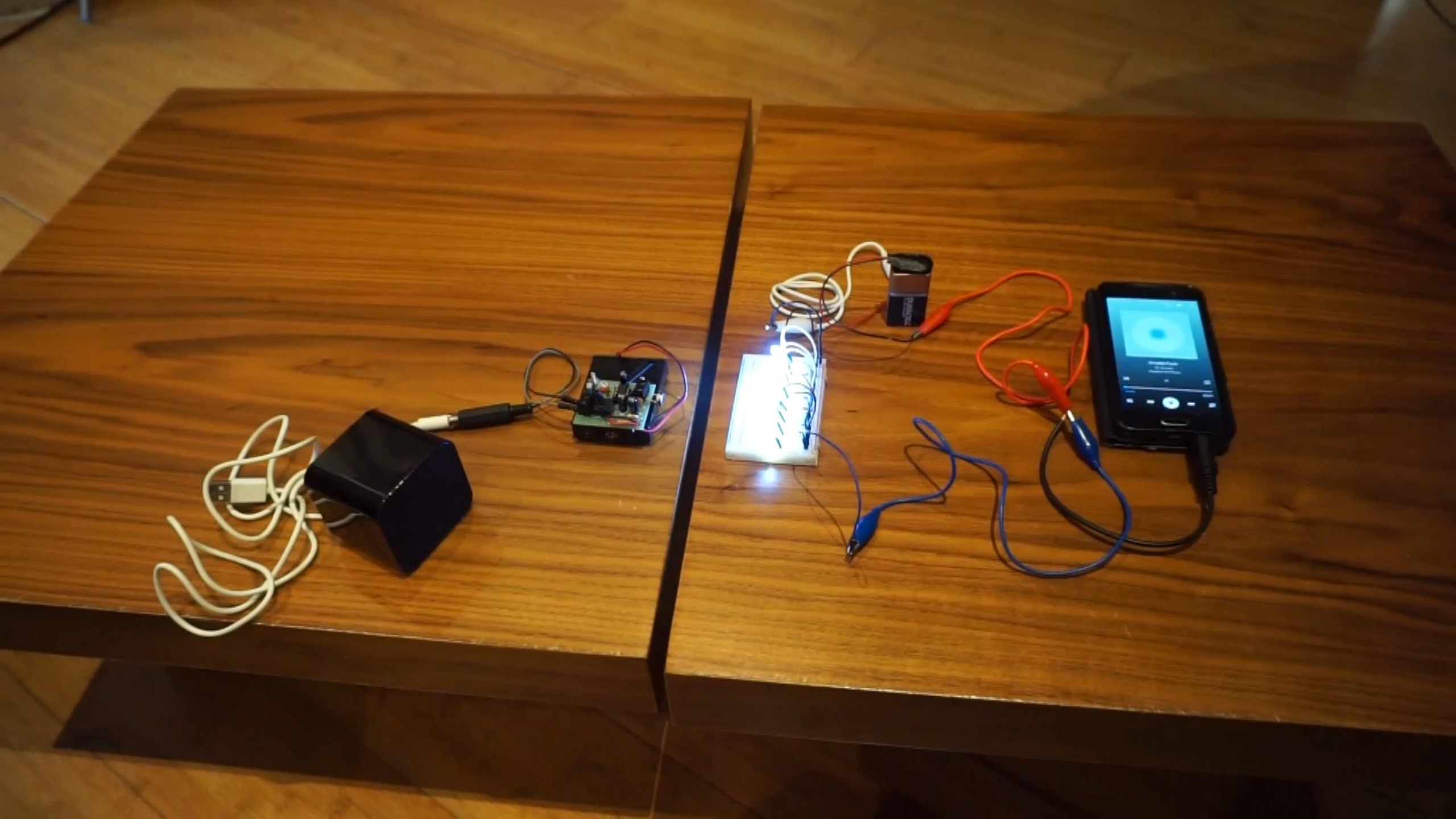
- The views and opinions expressed in this talk are not necessarily those of PwC
- **All content is for <u>educational purposes only</u>. Read up on relevant laws, only attack systems you own or have permission to attack!**
- What this presentation isn't
- I am in no way an electronics expert

Dunning-Kruger Curve

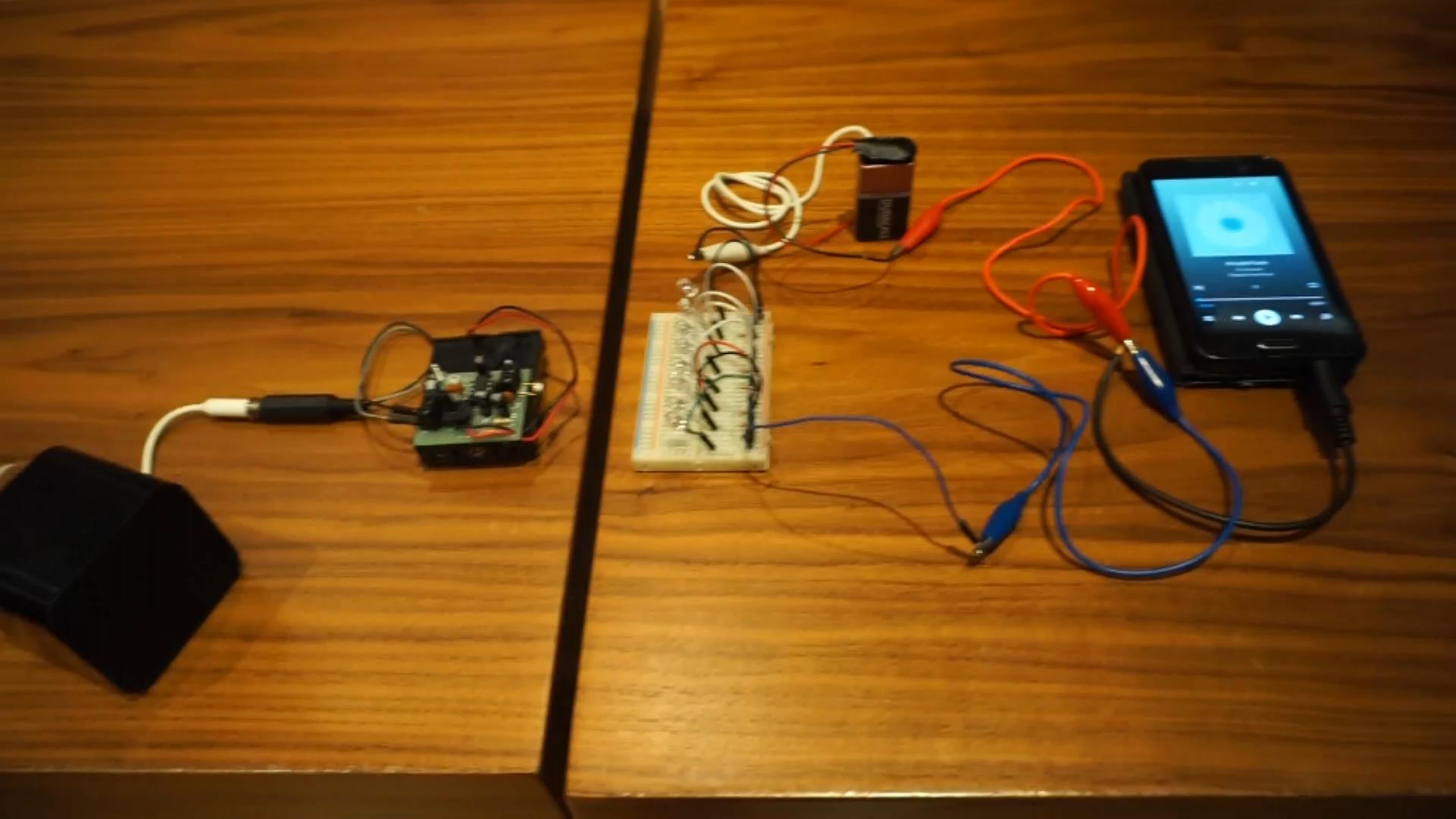


Key terms

- Modulation
- Ultrasonic
- Near-ultrasonic
- Spectrogram
- Infrared




What sorcery is this?!



Part I

Jumping air-gaps

- *A Sensor Darkly*
- *Dreadphone*
- *Spectregram*

Caveats

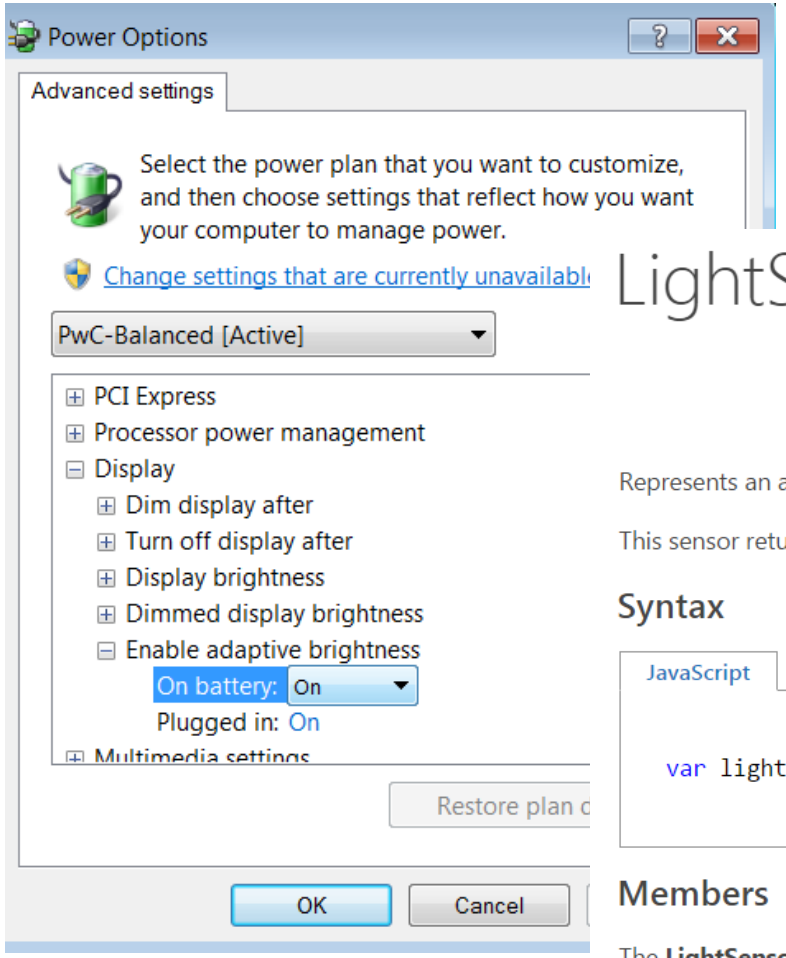
- Virtually all research in this area assumes that the attacker has already managed to infect at least one host
- Attacker has physical or near-physical access
- Exfiltration is of small pieces of data

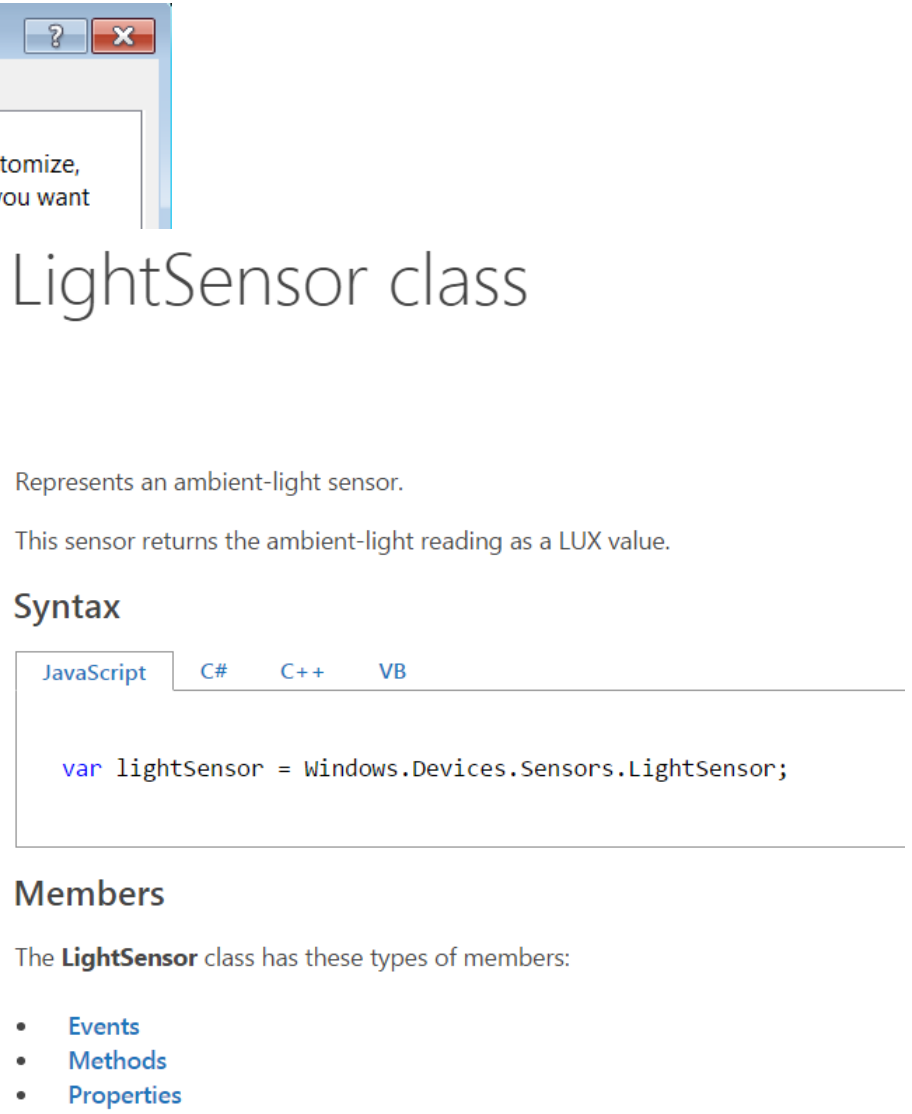
Previous research

- Van Eck phreaking – e.g. Kuhn (2003); Halevi and Saxena (2012)
- AirHopper (Guri et al 2014) – radio frequencies
- BitWhisper (Guri et al 2015) – heat
- VisiSploit (Guri et al 2016) – codes & camera
- Fansmitter (Guri et al 2016) – acoustic
- SPEAKE(a)R (Guri et al 2016) – speakers to mics
- xLED (Guri et al 2017)
- Hasan et al (2013) – great overview of techniques
  - Including ALS for mobile devices
- **Lots more!**

ALS

- Ambient Light Sensor
- Increasingly common
  - Laptops
  - Monitors
  - Smartphones
  - Tablets
  - Smartwatches



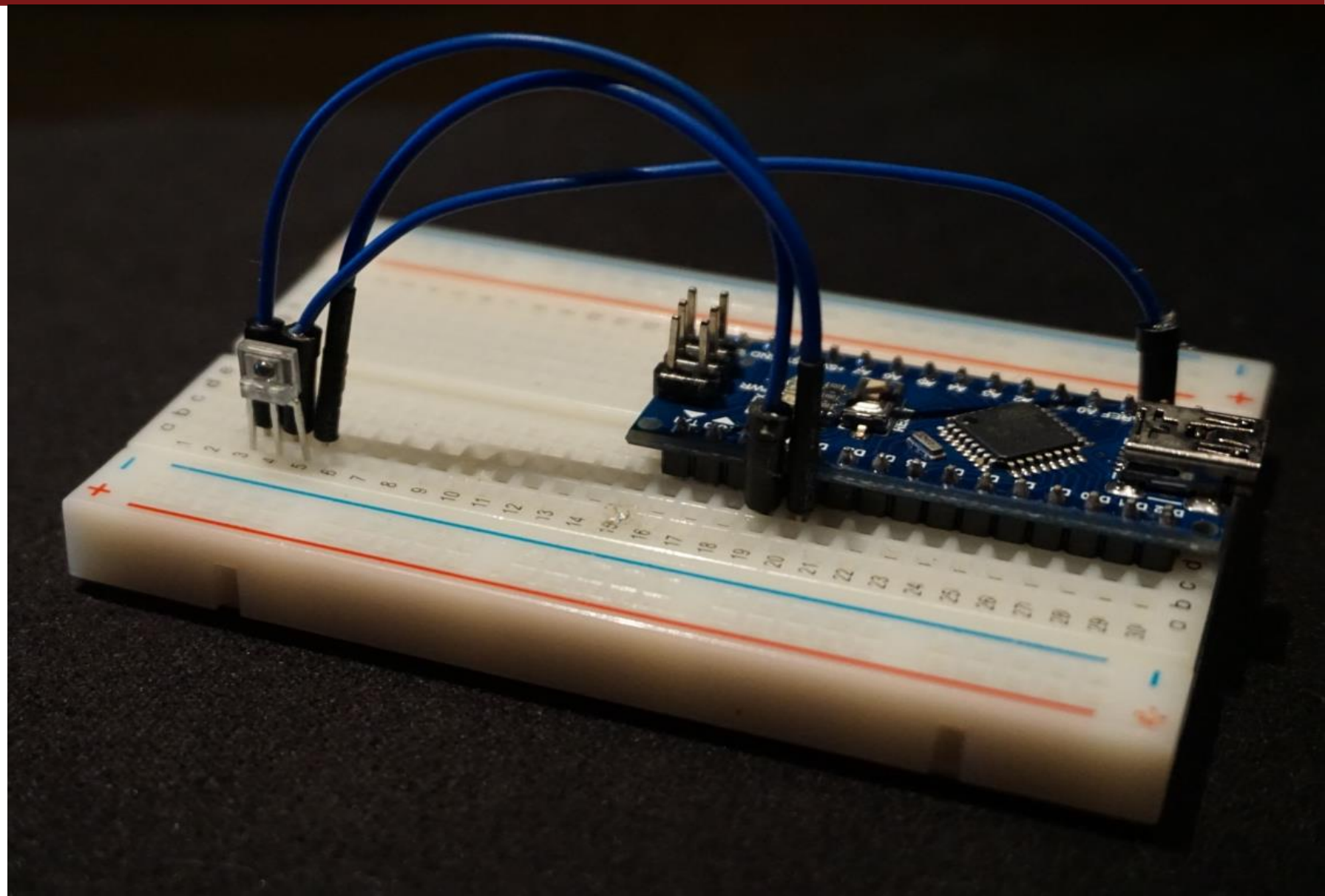


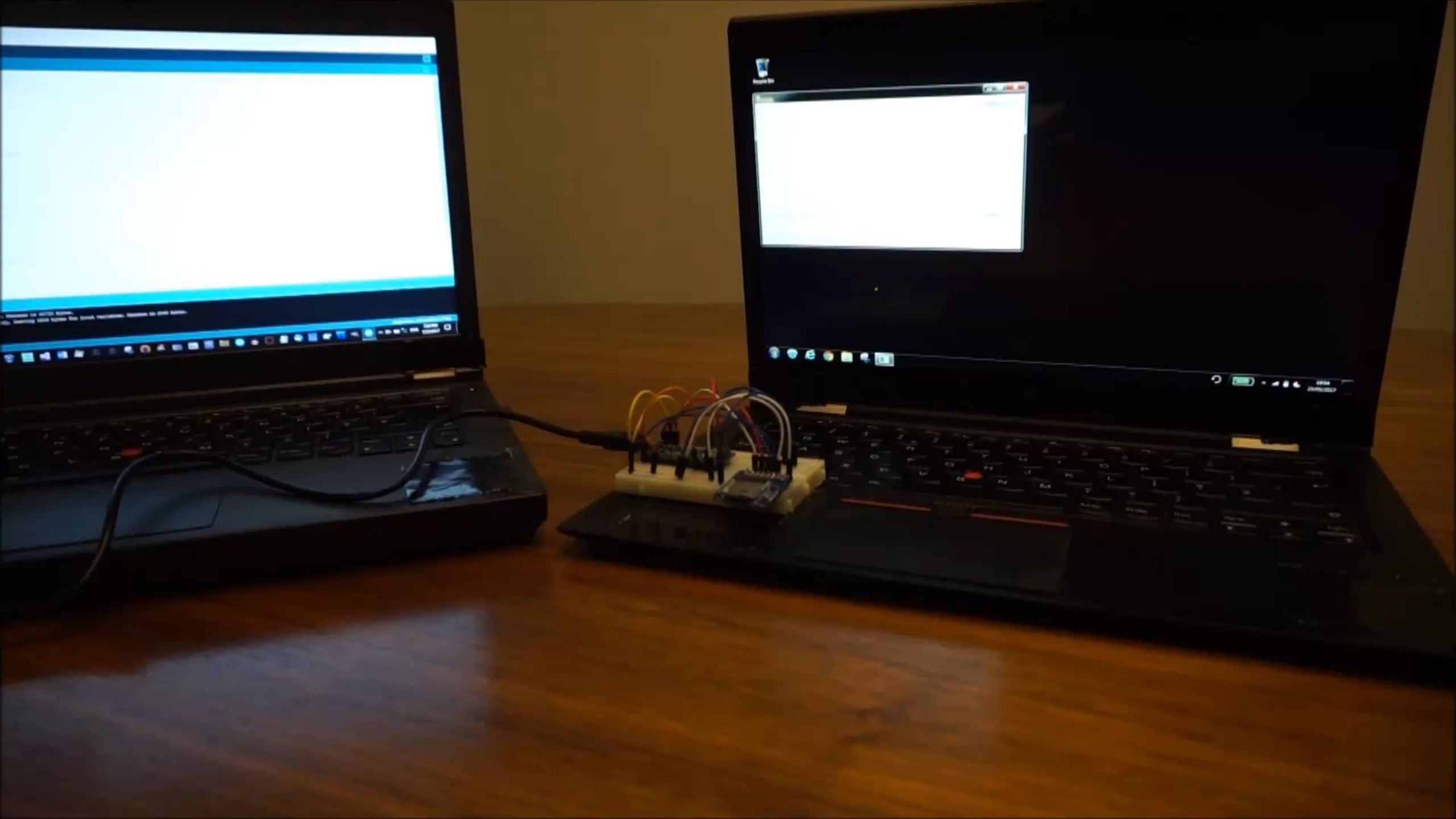
Design

- **The plan:**
  - Create malware to read light (lux) values from the ALS through the API
  - Malware executes different commands according to changes in the intensity

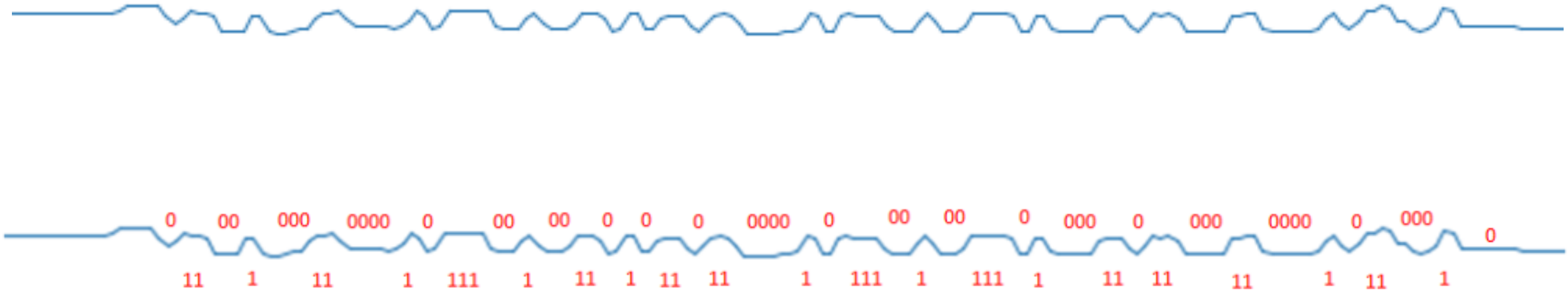
- **Problems:**
  - Hurr durr, I'll just shine this massive torch onto my laptop to execute commands
  - Need exfil capability

Exfiltration

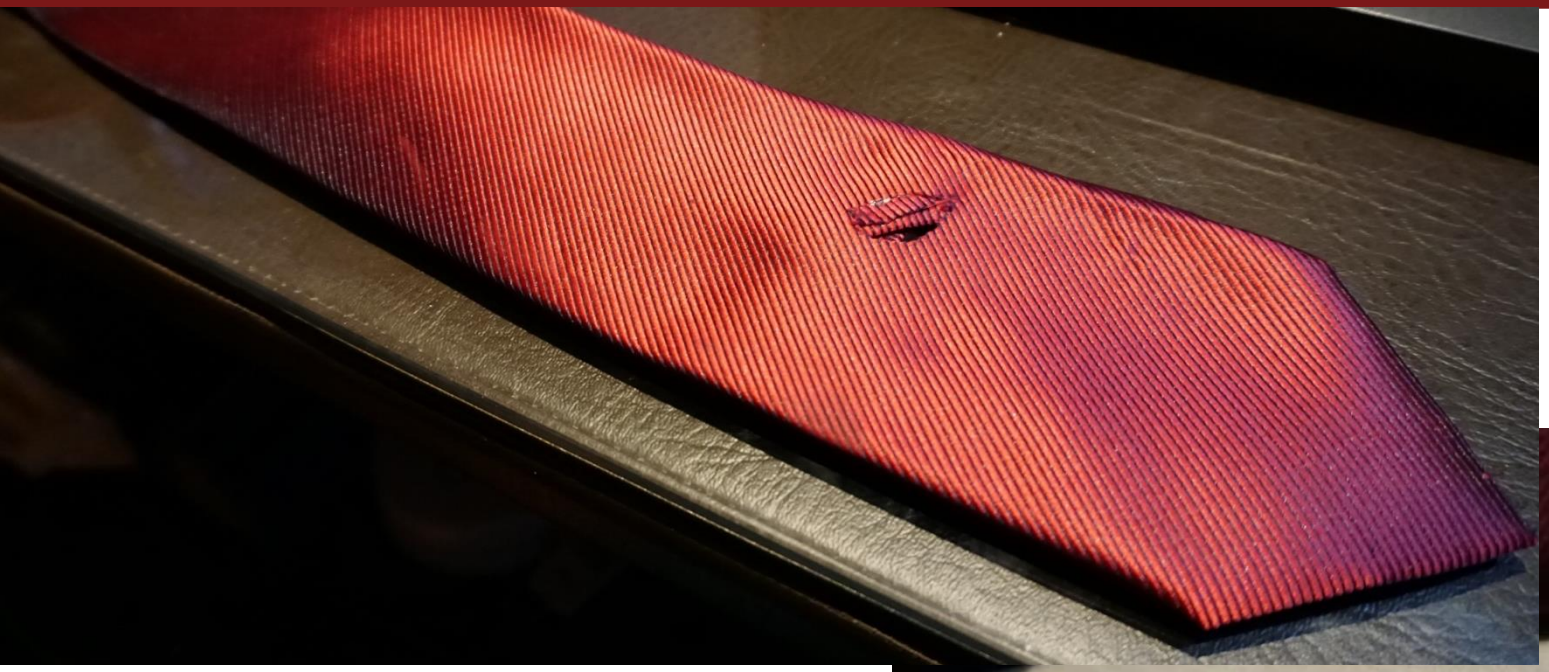


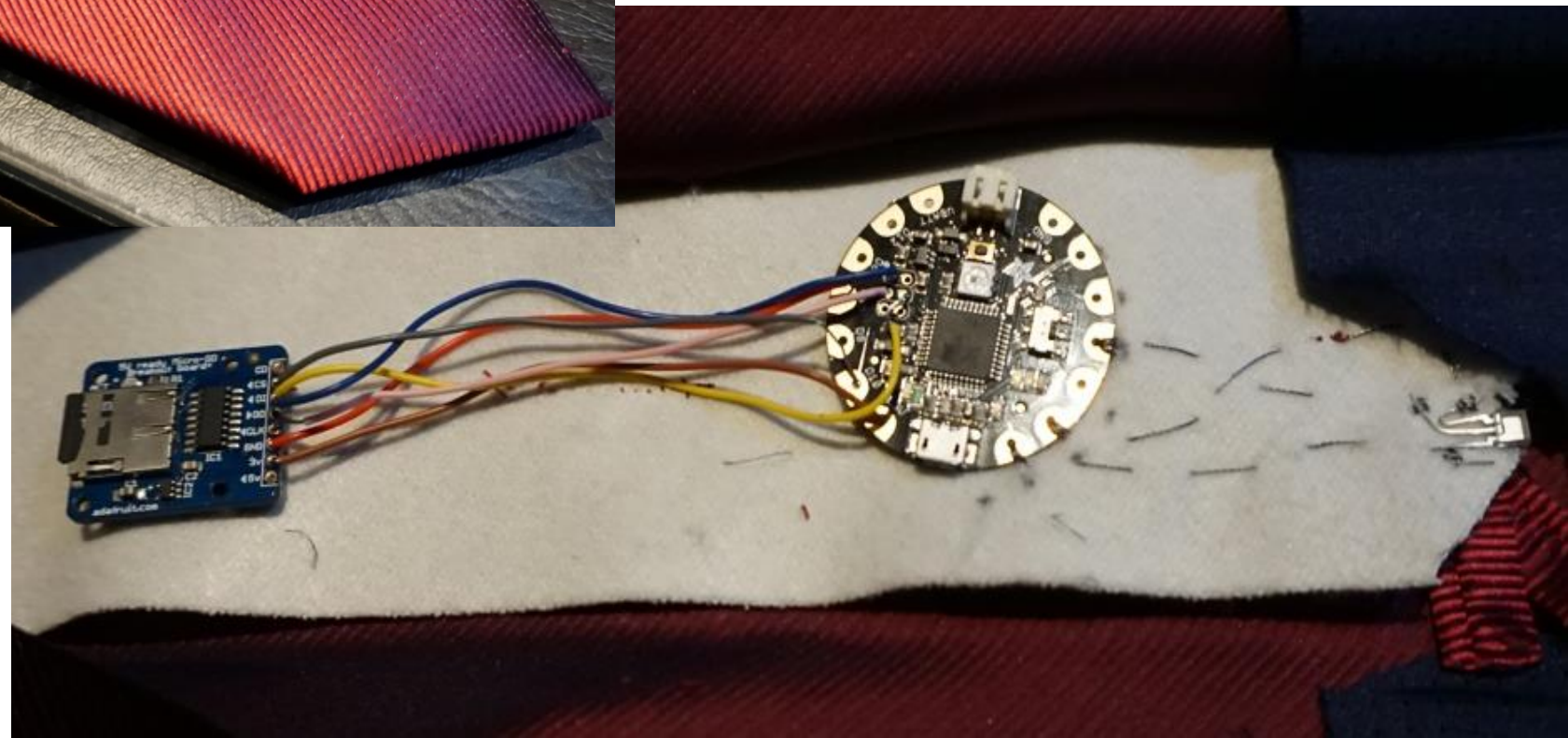


Results


0 00 000 0000 0 00 00 0 0 0 0000 0 00 00 0 000 0 000 0000 0 000 0
11 1 11 1 111 1 11 1 11 11 1 111 1 111 1 11 11 11 1 11 1

Prototype 2

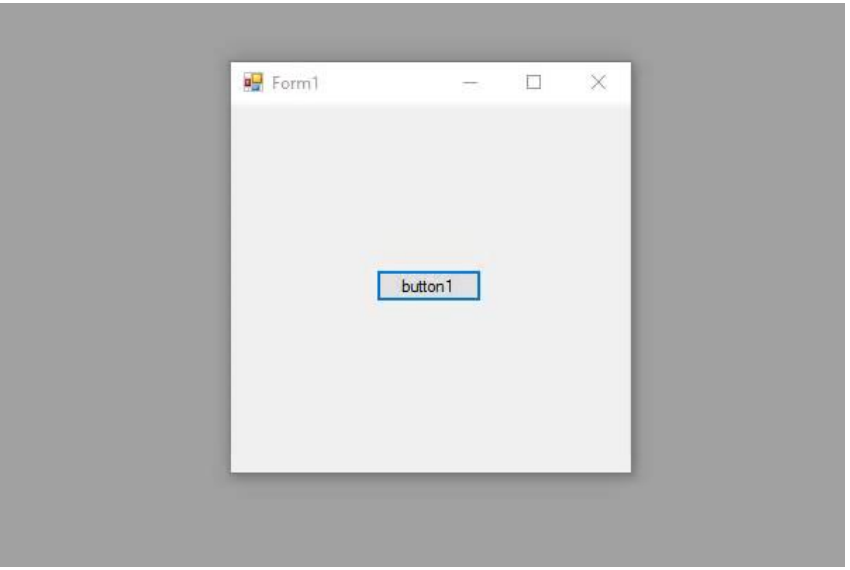


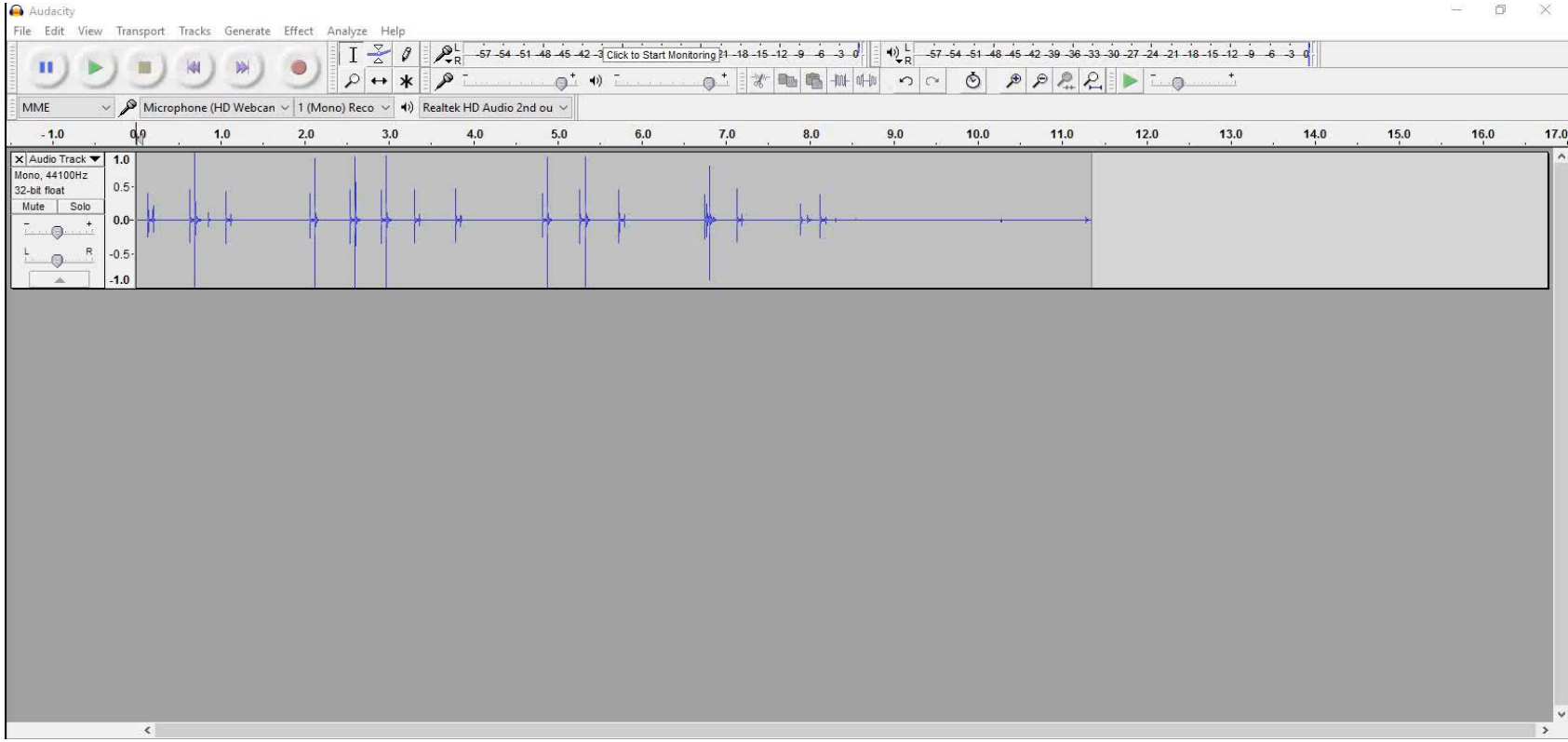


Dreadphone

- C2 using near-ultrasonic sounds (18-19KhZ)
- Standard laptop soundcard
- Toftsed et al (2010) – Army Research Laboratory
- Hanspach and Goetz (2014)
  - Used system designed for underwater communication
  - Covert acoustical mesh networks

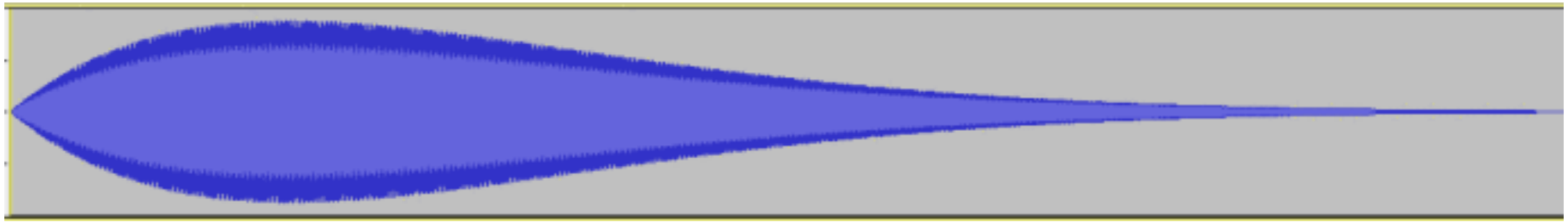
Soundcard woes

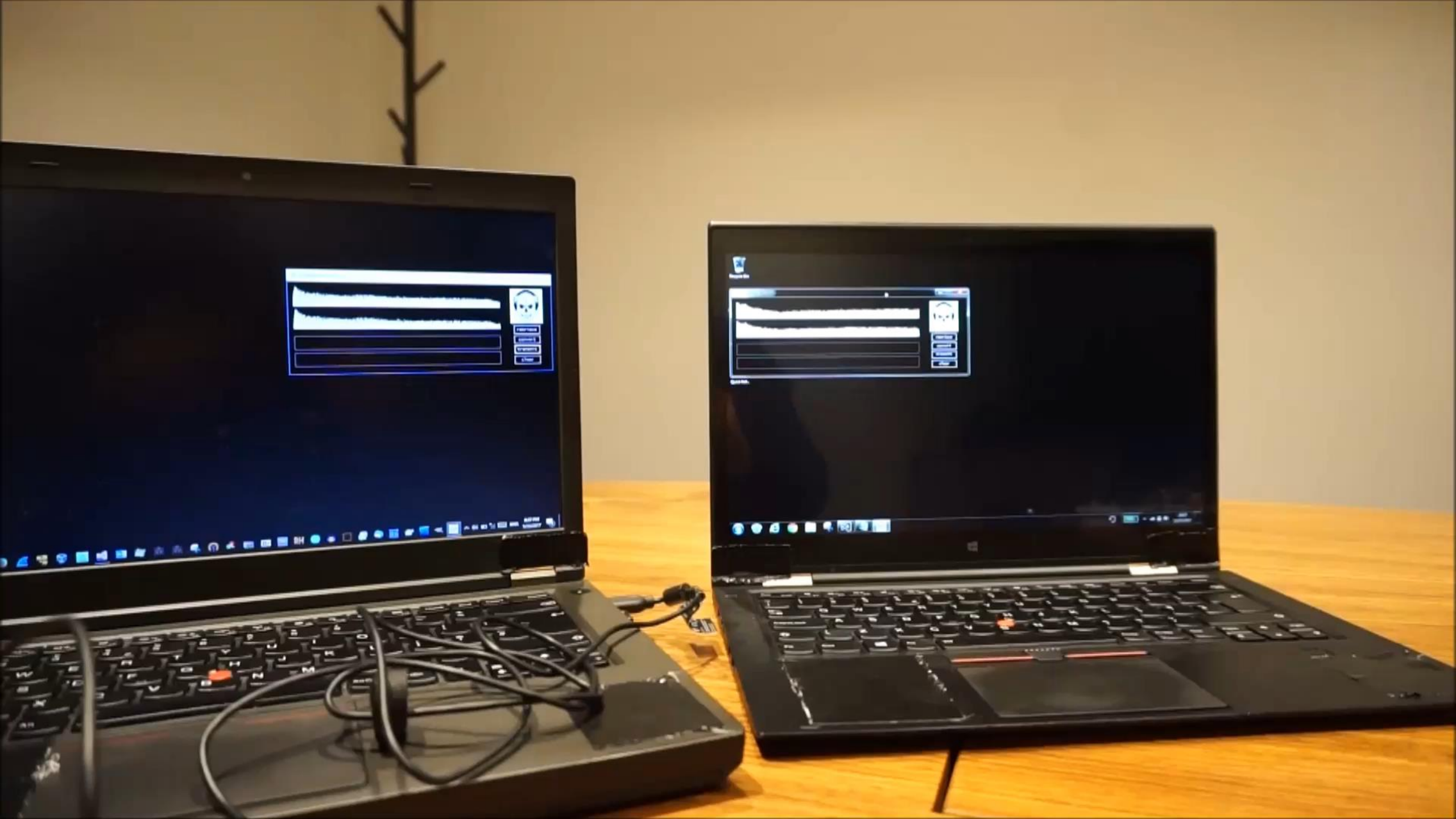




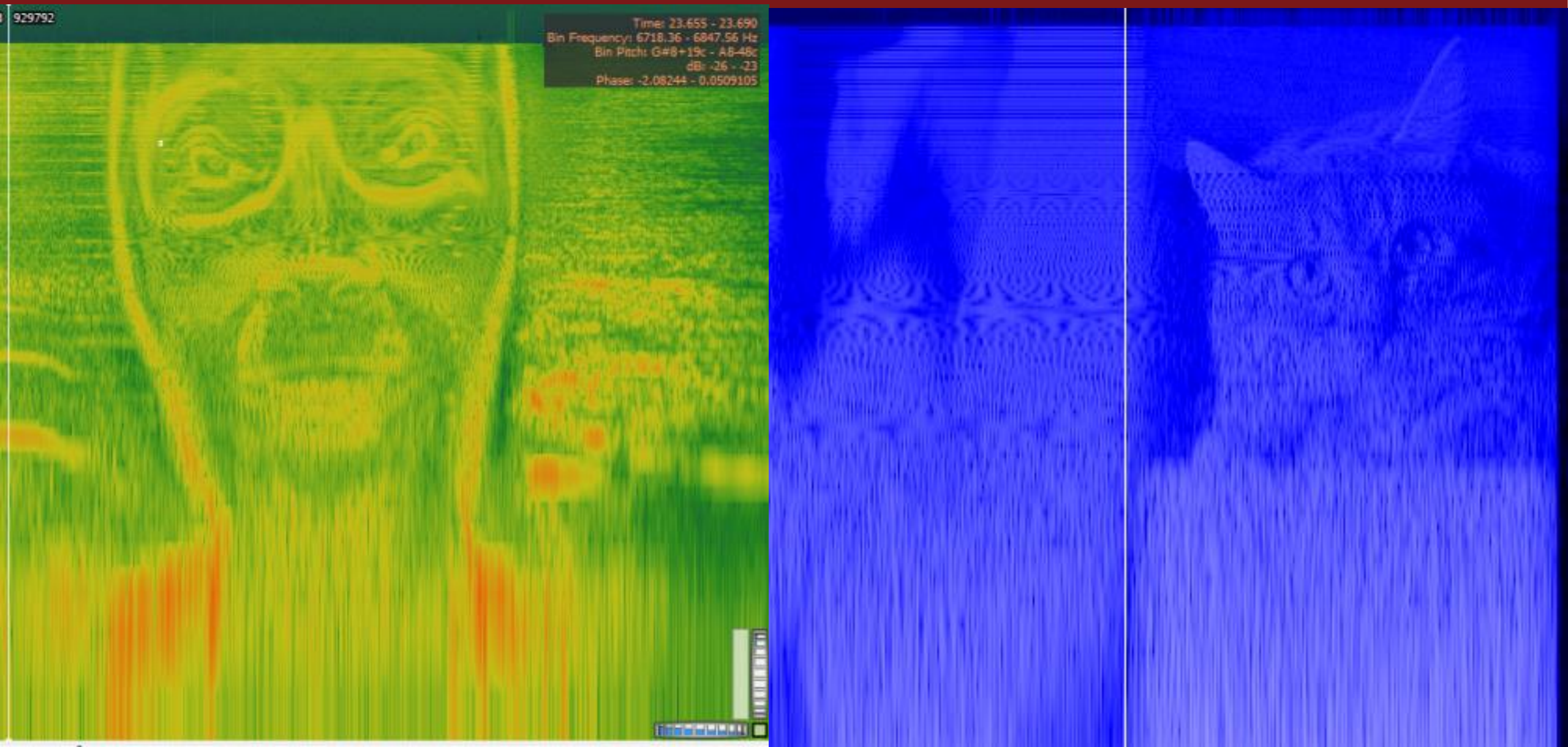
Soundcard woes

- Apply multiple fade-ins / fade-outs
- Then amplify the track:





In music


929792
Time: 23.655 - 23.690
Bin Frequency: 6718.36 - 6847.56 Hz
Bin Pitch: G#8+19c - A8-46c
dB: -26 - -23
Phase: -2.08244 - 0.0509105


Spectregram

Mitigation

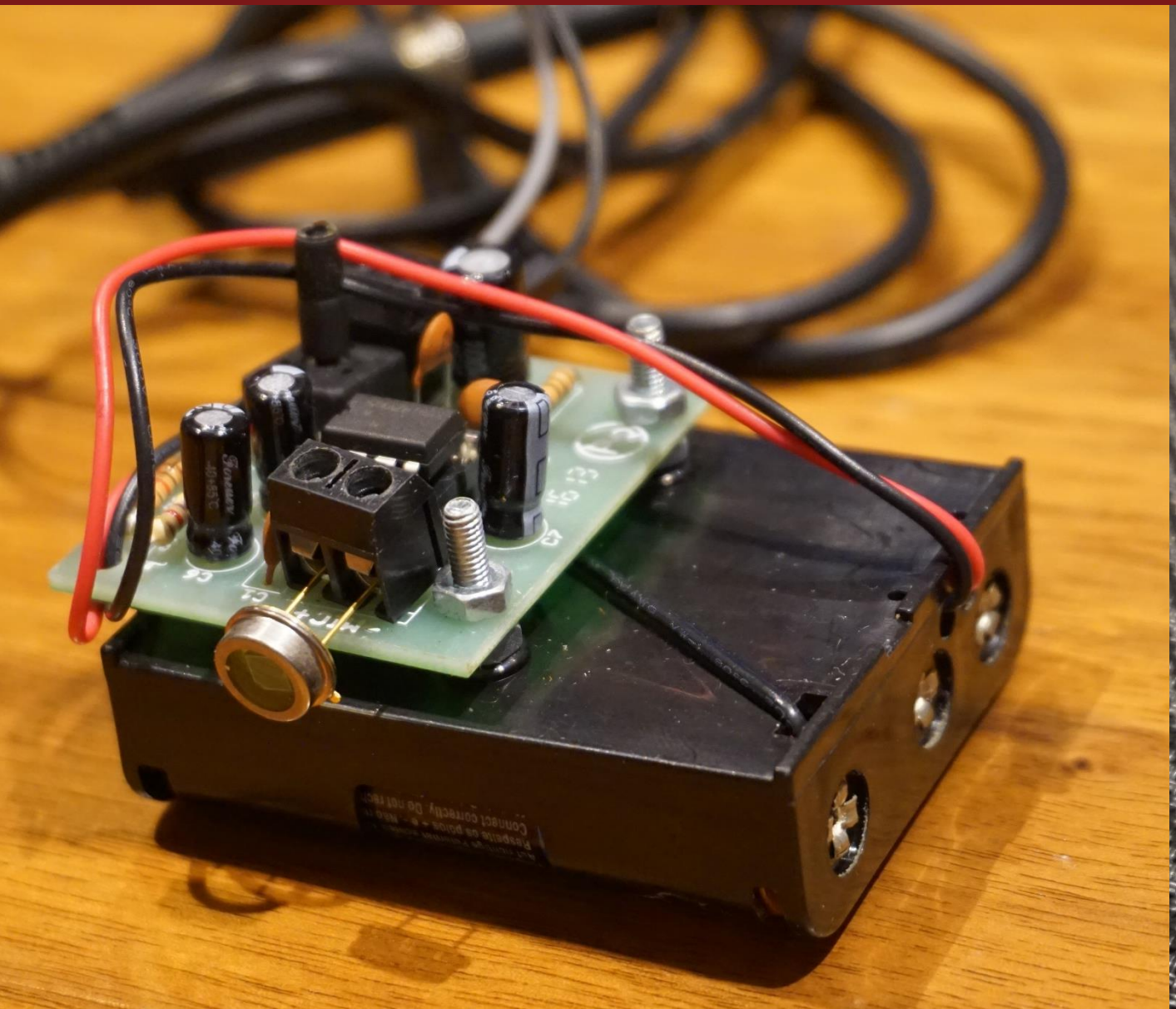
- TEMPEST standards
- Remove/disable ALS
- Screen filters
- White noise
- Ultrasonic detectors
- Disable microphones/speakers

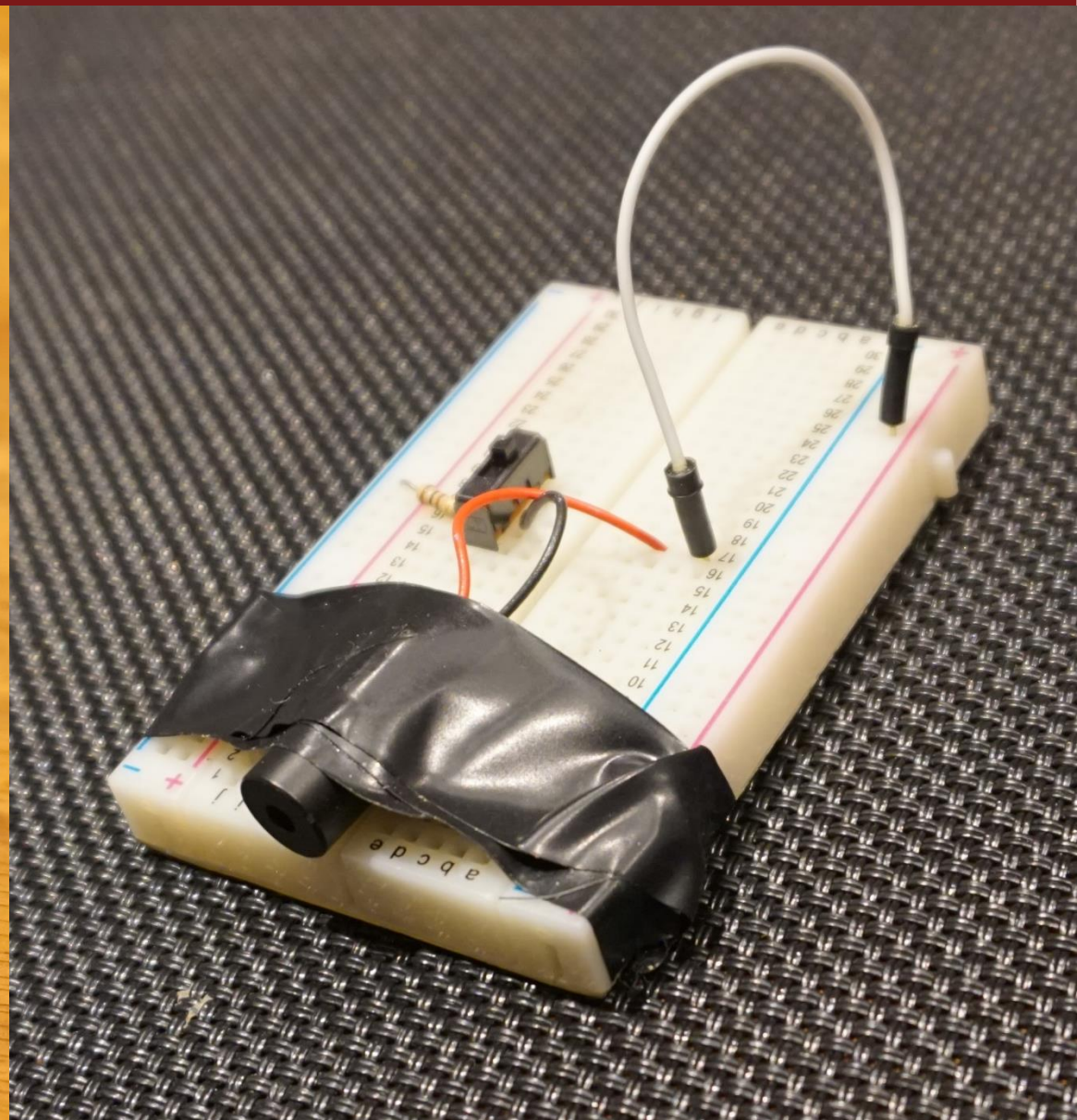
Part II

Surveillance and counter-surveillance

- *Laser microphone*
- *Passive infrared motion detector*
  - *Drone to clone to pwn*
  - *Phone to clone to pwn*
- *Active infrared motion detector*

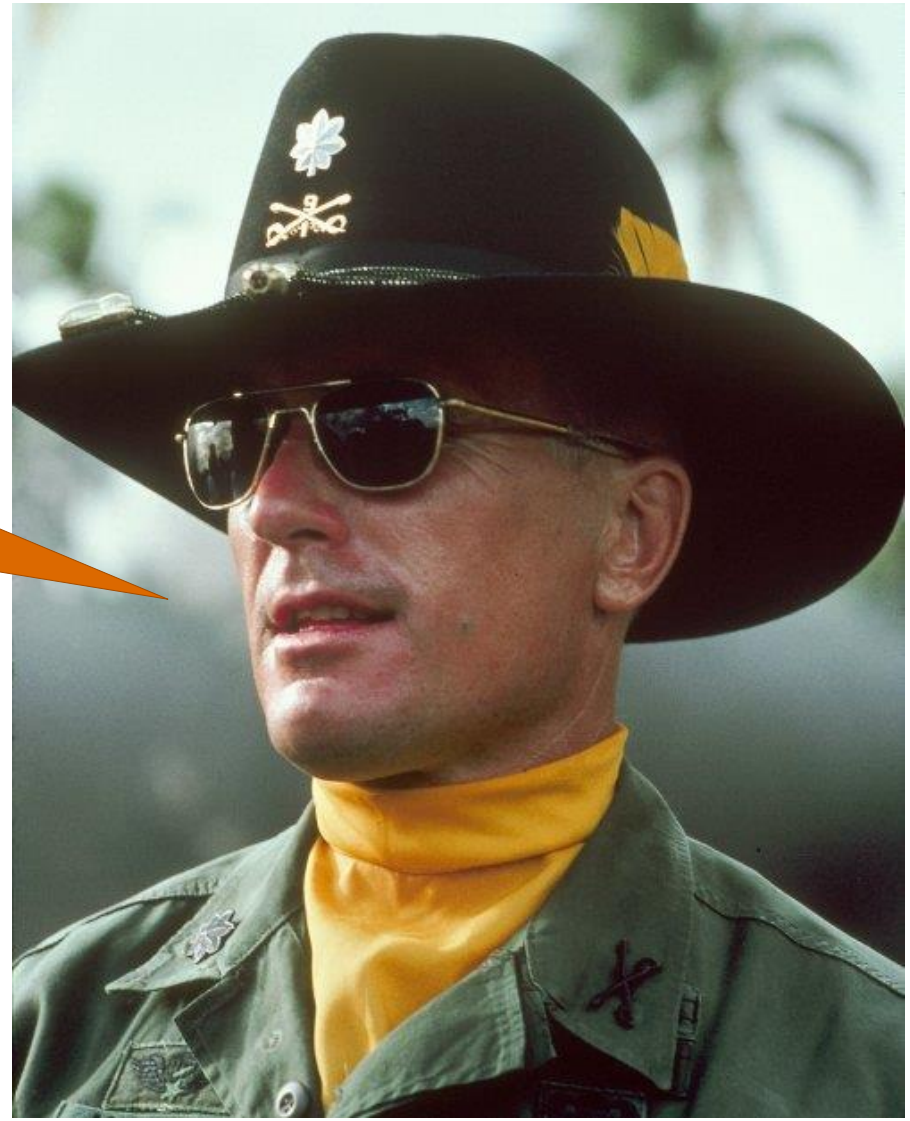
Laser microphone





But that music choice though

I love the sound of sound converted to light and then converted back to sound again in the morning.



Laser microphones

Original version

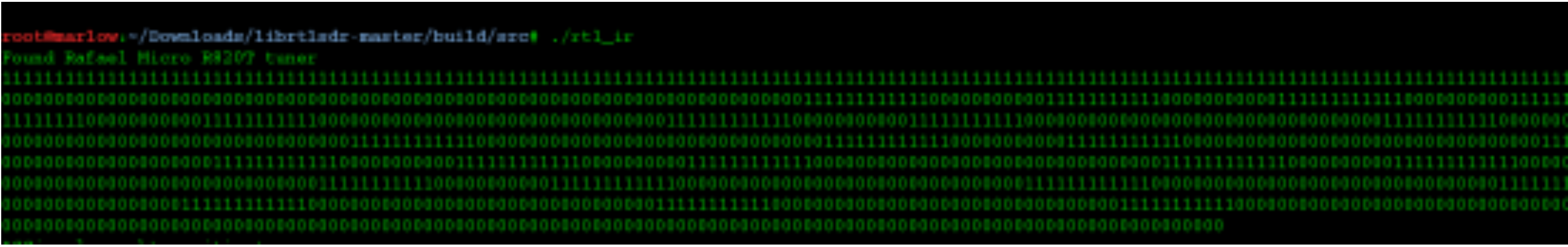
Laser mic version

Sniffing, analysing and cloning IR signals

- Similar principle to RF signals
- Assuming fixed codes (not rolling)
- Need to listen to the signal
- Analyse
- Replay the cloned signal on an Arduino
- See Major Malfunction (2005) – compromising hotel payment systems via infrared TV remotes

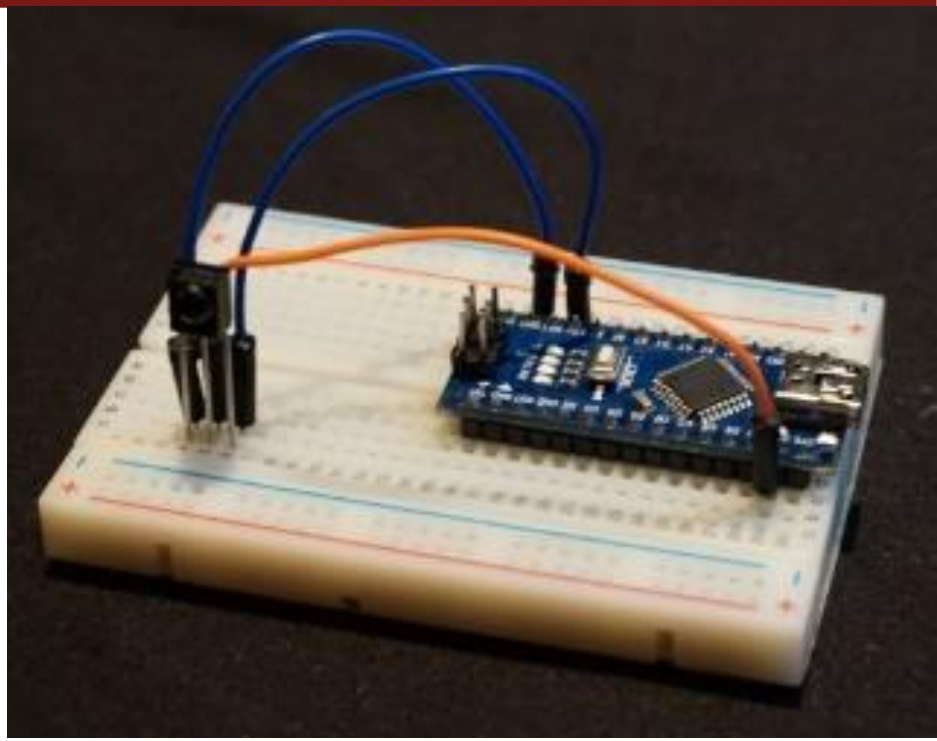
Sniffing the signal

- Use an RTL-SDR
- rtl_ir
  - Forked from librtlsdr



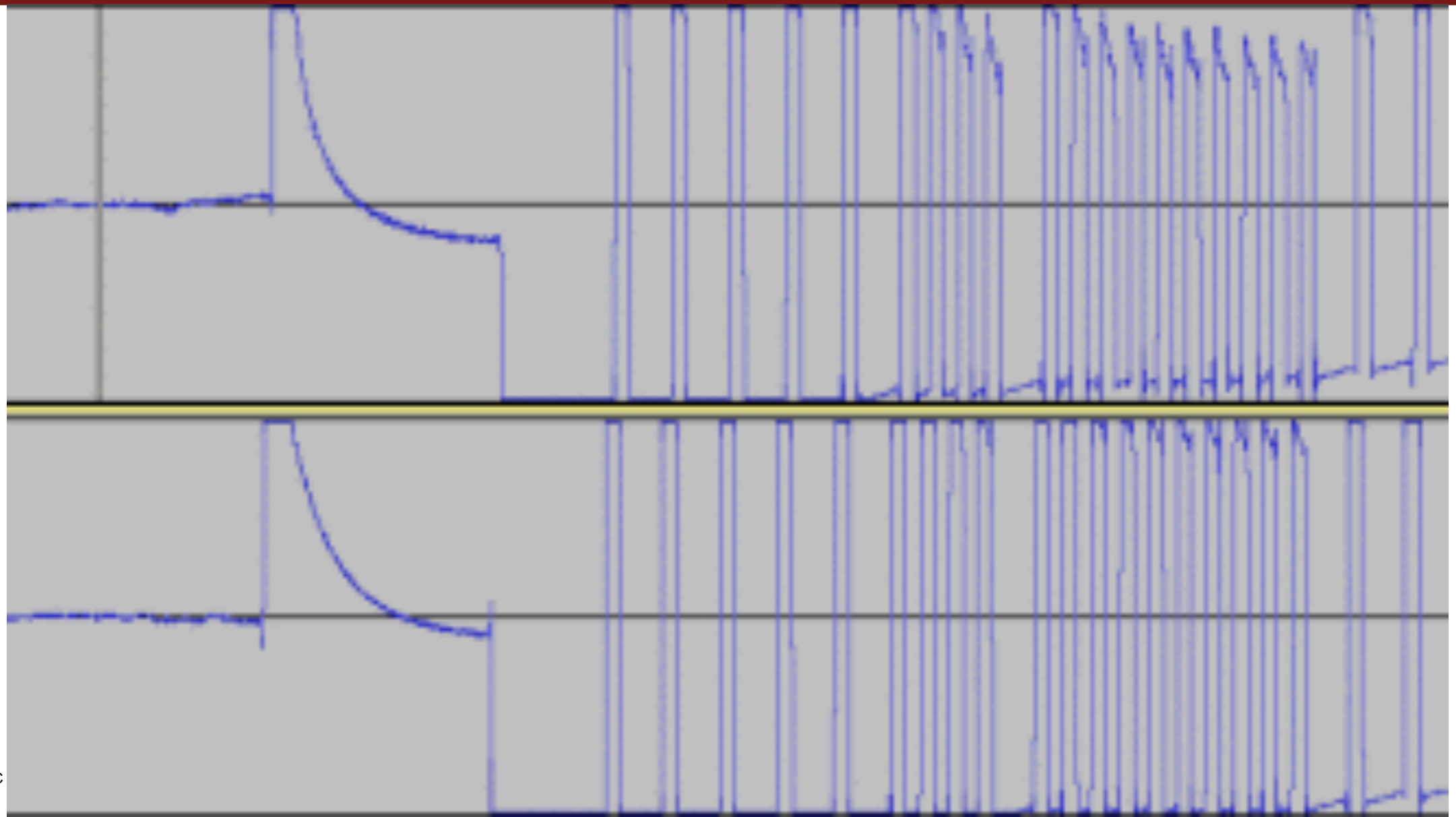
Sniffing the signal

- IR receiver and Arduino
- IRLib library



```
Decoded NEC(1): Value:2FD48B7 (32 bits)
Raw samples(68): Gap:4050
  Head: m8850  s4450
0:m550 s600     1:m500 s600             2:m500 s600    3:m500 s650
4:m450 s600     5:m550 s600             6:m500 s1700   7:m500 s600
8:m500 s1700    9:m550 s1700            10:m500 s1700  11:m500 s1750
12:m500 s1700   13:m500 s1700           14:m550 s550   15:m550 s1700

16:m500 s600    17:m500 s1700           18:m550 s600   19:m450 s650
20:m500 s1700   21:m500 s600            22:m550 s600   23:m450 s650
24:m500 s1700   25:m500 s600            26:m550 s1650  27:m550 s1700
28:m500 s600    29:m550 s1650           30:m550 s1700  31:m500 s1700

32:m500
Extent=67050
Mark  min:450    max:550
Space min:550    max:1750
```

Analysis and replay



Analysis and replay

- If signal is a known protocol, can just play back the code
- e.g. standby signal from my TV remote:
  - **NEC 0x2FD48B7**

```
#include <IRremote.h>

IRsend irsend;

void setup()
{
Serial.begin(9600);
}

void loop() {
for (int i = 0; i < 3; i++) {
irsend.sendNEC(0x2FD48B7, 32);
delay(40);
}
Serial.println("Sent!");
delay(5000); //5 second delay between each signal burst
}
```

Analysis and replay

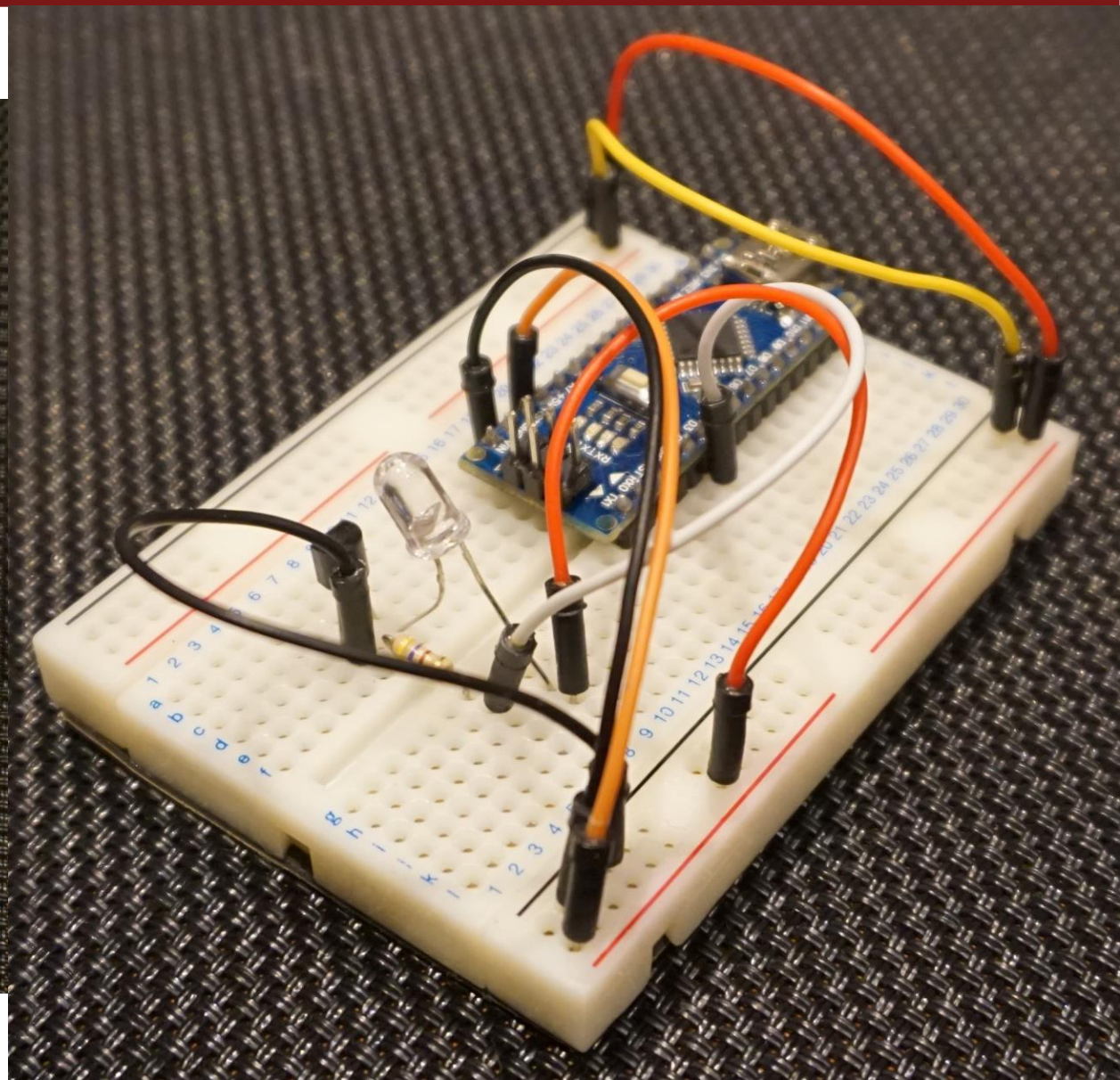
- If signal is unknown, read edges/delays into an array using IRLib or IRremote library
- Play array back

```
#include <IRremote.h>

IRsend irsend;

void setup()
{
Serial.begin(9600);
}

void loop() {
  int khz = 38;
  unsigned int irSignal[] = { 8900, 4600, 500, 1750, 400, 1800, 550, 1700, 500, 1700, 450,

  irsend.sendRaw(irSignal, sizeof(irSignal) / sizeof(irSignal[0]), khz);
  Serial.println("Sending evil signal!");
  delay(3000);
}
```

Passive IR motion detectors

- Bypasses – see Porter and Smith (2013)
  - Move slowly
  - Mask body heat
  - Overwhelm sensor with heat (like a lighter)
  - False alarms

Passive IR motion detectors



Oops…

Remote 1

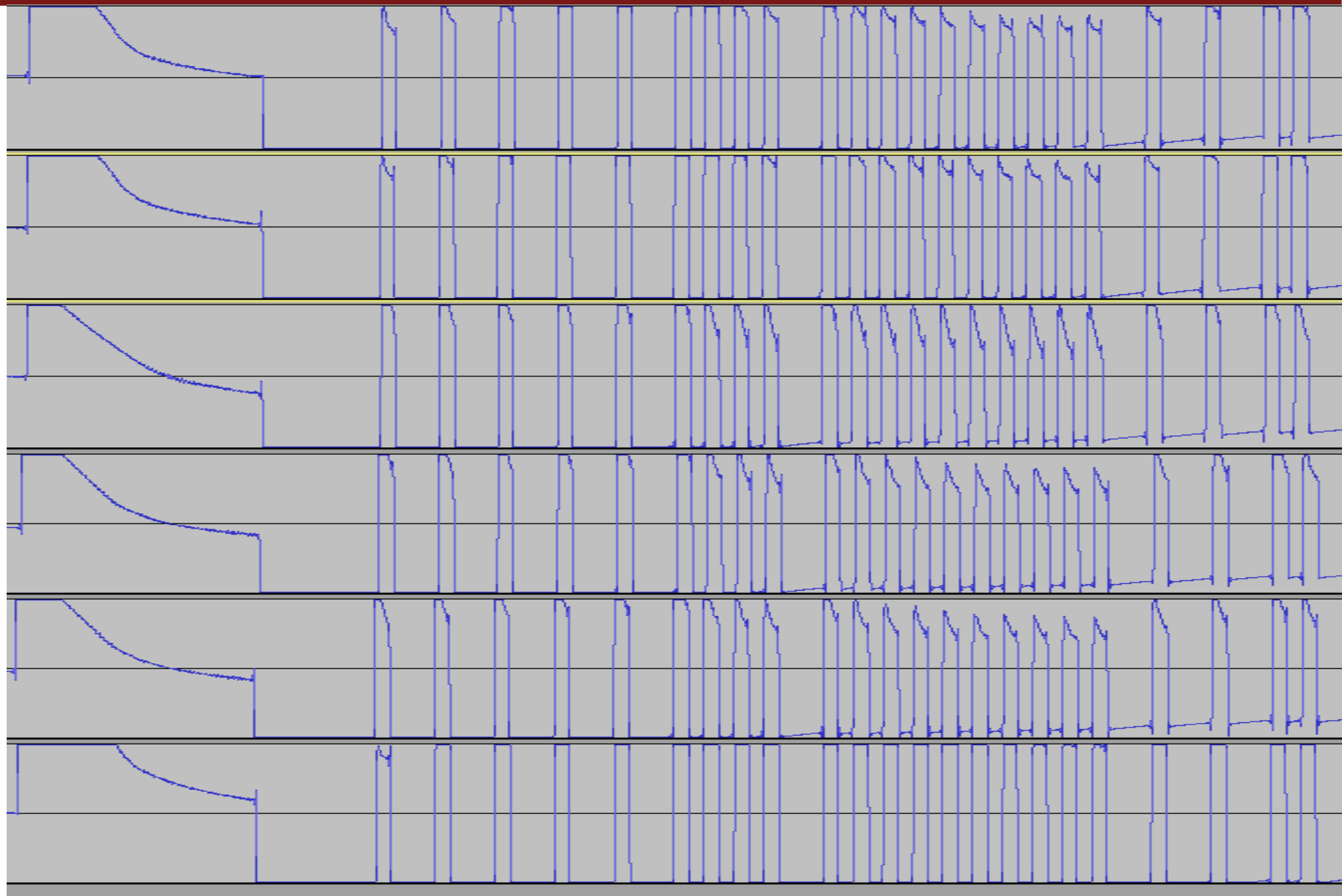
Remote 2

Remote 3

Remote 4

Remote 5

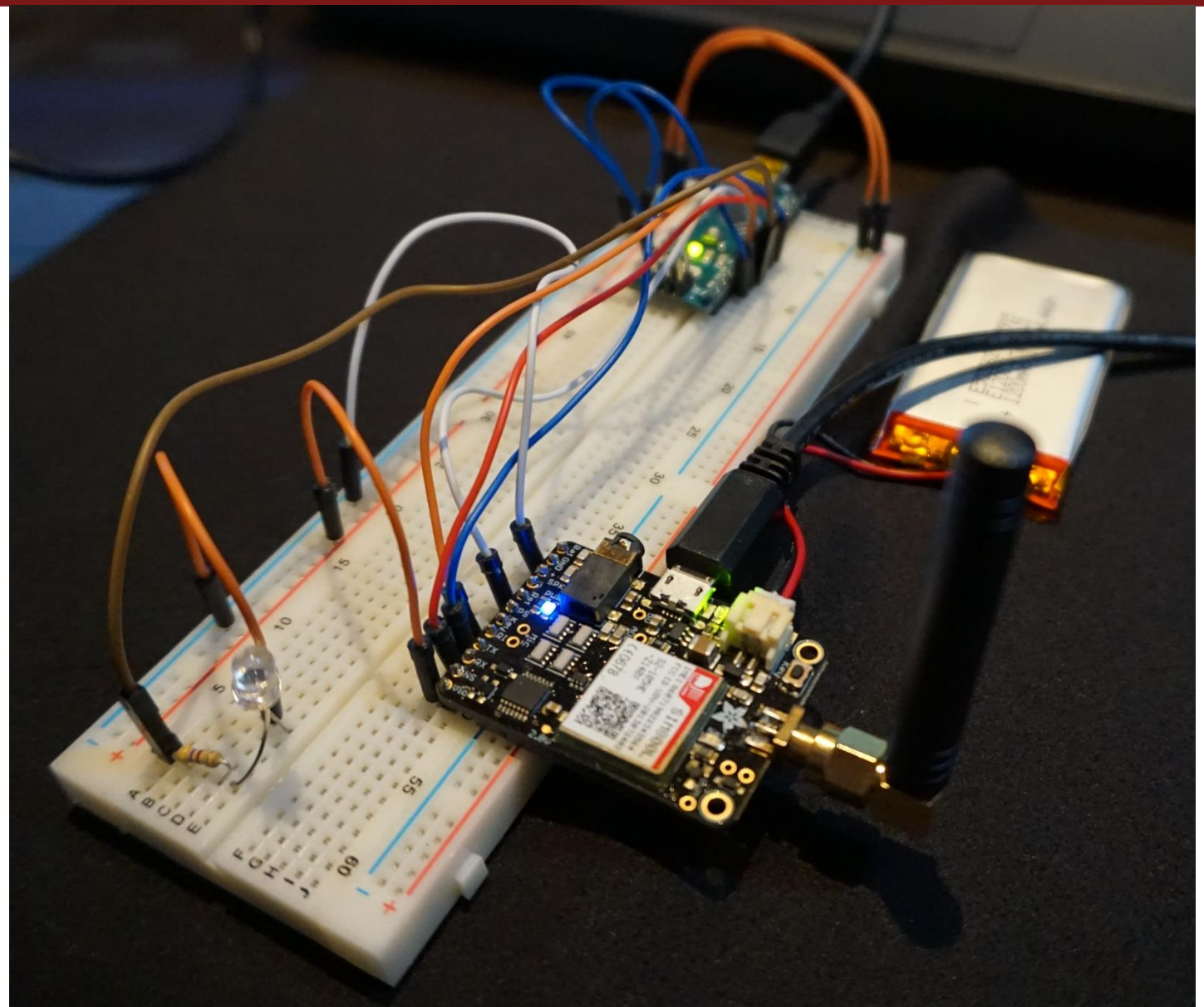
Remote 6




A1
A2
A3
B1
B2
B3

Drone to clone to pwn

Phone to clone to pwn



Active IR motion detector


RECEIVER

Mitigation

- Vibrations/speakers/wire screens/coverings on windows
- Double-glazing or curved glass can cause problems
- Where possible, use alarms with physical keypads to disarm, not remotes
- If using remotes, go for ones which:
  - Use encrypted rolling code algorithms, anti-jamming, etc
  - Are paired uniquely to a device

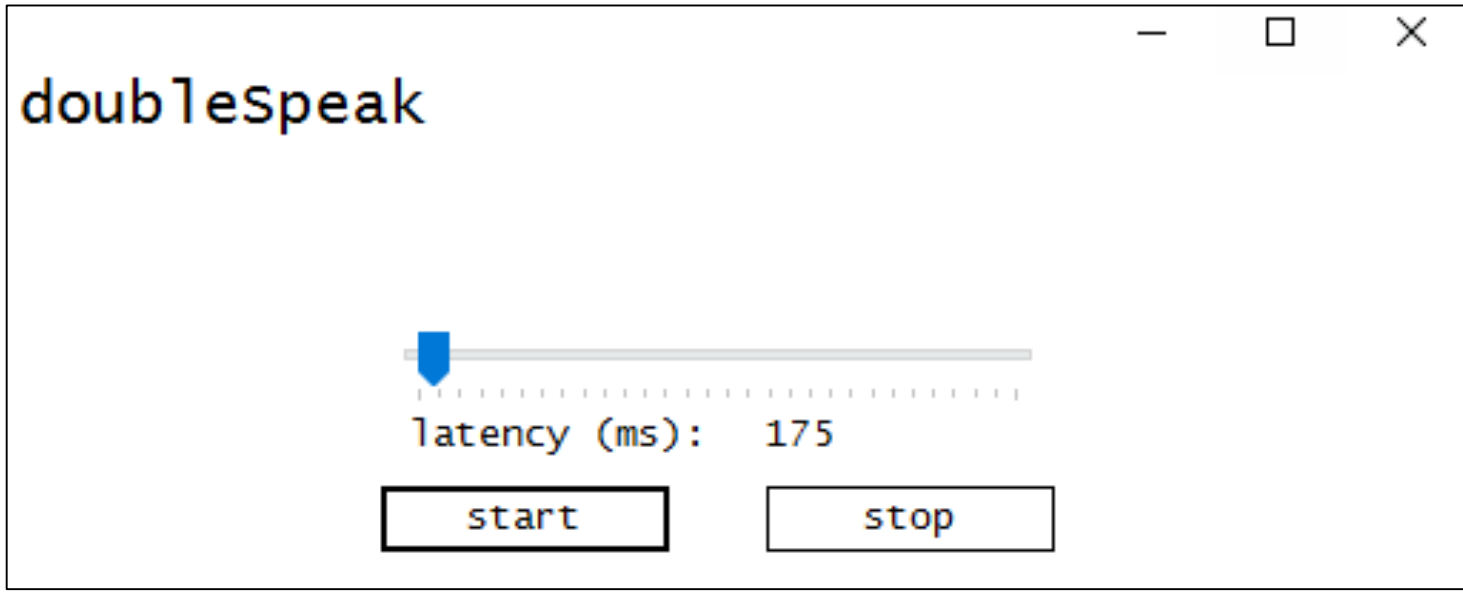
Part III

Bantz

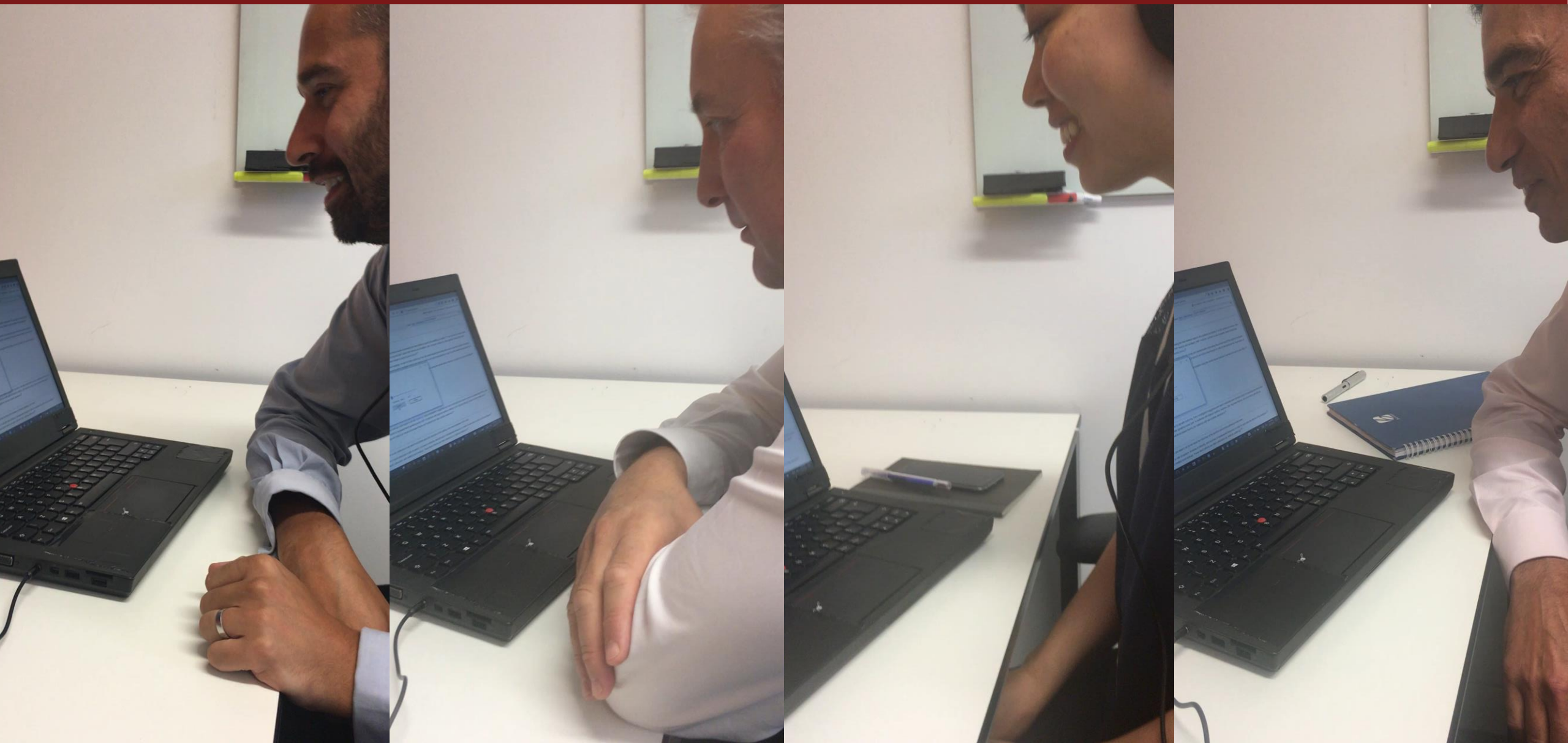
- *doubleSpeak*
- *Annoying malware analysts*
- *Kill More Gilmore*
- *AstroDrone*

Delayed Auditory Feedback (speech jamming)

- Has been around since the 1950s
- SpeechJammer - Kurihara and Tsukada (2012)
- I built a software version

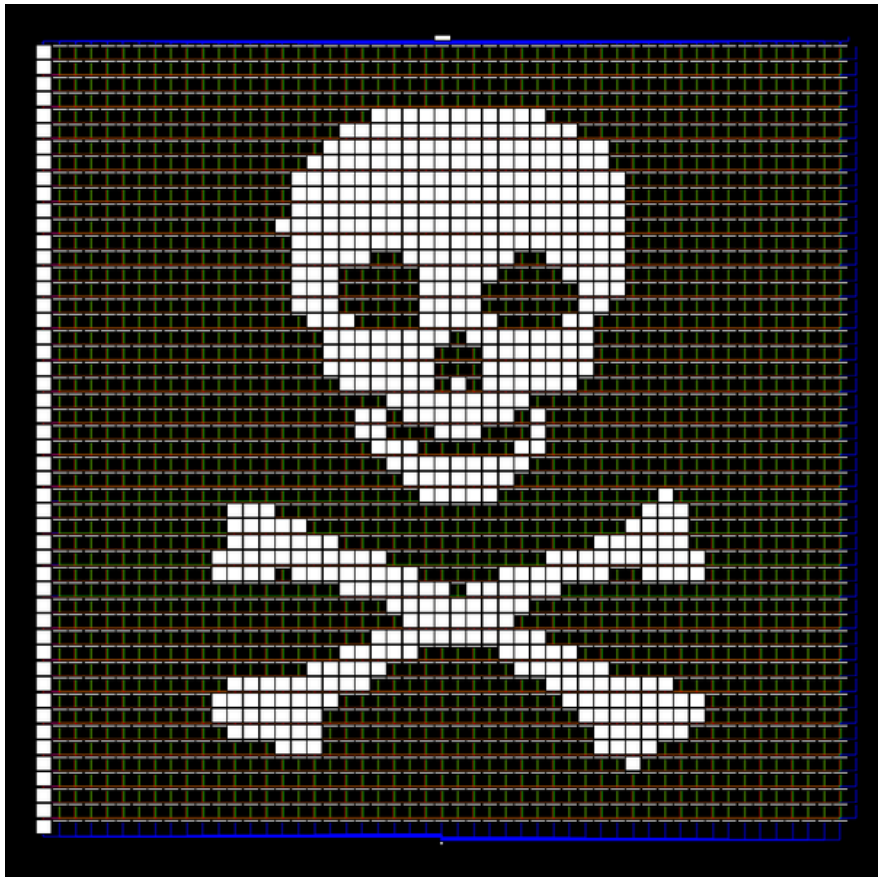


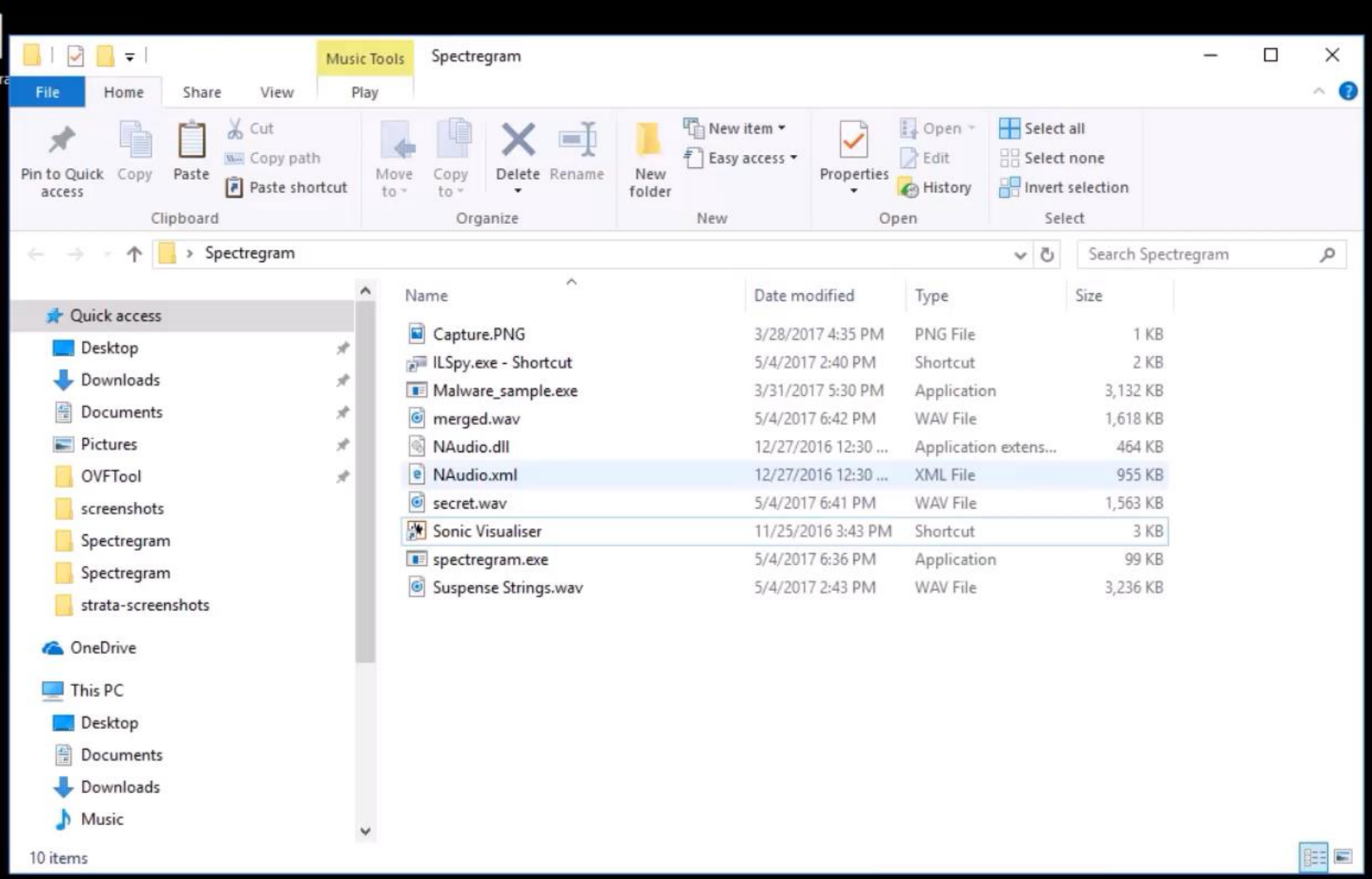
Speech jamming



Demotivating malware analysts

- Inspired by Domas (2015)
- "Psychological warfare in reverse engineering"
- Created malware where the flow graph in disassemblers represents an image




Spectregram
Music Tools
Spectregram
File
Home
Share
View
Play
Pin to Quick access
Copy
Paste
Cut
Copy path
Paste shortcut
Clipboard
Move to
Copy to
Delete
Rename
Organize
New folder
New item
Easy access
New
Properties
Open
Edit
History
Open
Select all
Select none
Invert selection
Select
Spectregram
Search Spectregram
Quick access
Desktop
Downloads
Documents
Pictures
OVFTool
screenshots
Spectregram
Spectregram
strata-screenshots
OneDrive
This PC
Desktop
Documents
Downloads
Music
Name
Date modified
Type
Size
Capture.PNG 3/28/2017 4:35 PM PNG File 1 KB
ILSpy.exe - Shortcut 5/4/2017 2:40 PM Shortcut 2 KB
Malware_sample.exe 3/31/2017 5:30 PM Application 3,132 KB
merged.wav 5/4/2017 6:42 PM WAV File 1,618 KB
NAudio.dll 12/27/2016 12:30 ... Application extens... 464 KB
NAudio.xml 12/27/2016 12:30 ... XML File 955 KB
secret.wav 5/4/2017 6:41 PM WAV File 1,563 KB
Sonic Visualiser 11/25/2016 3:43 PM Shortcut 3 KB
spectregram.exe 5/4/2017 6:36 PM Application 99 KB
Suspense Strings.wav 5/4/2017 2:43 PM WAV File 3,236 KB
10 items

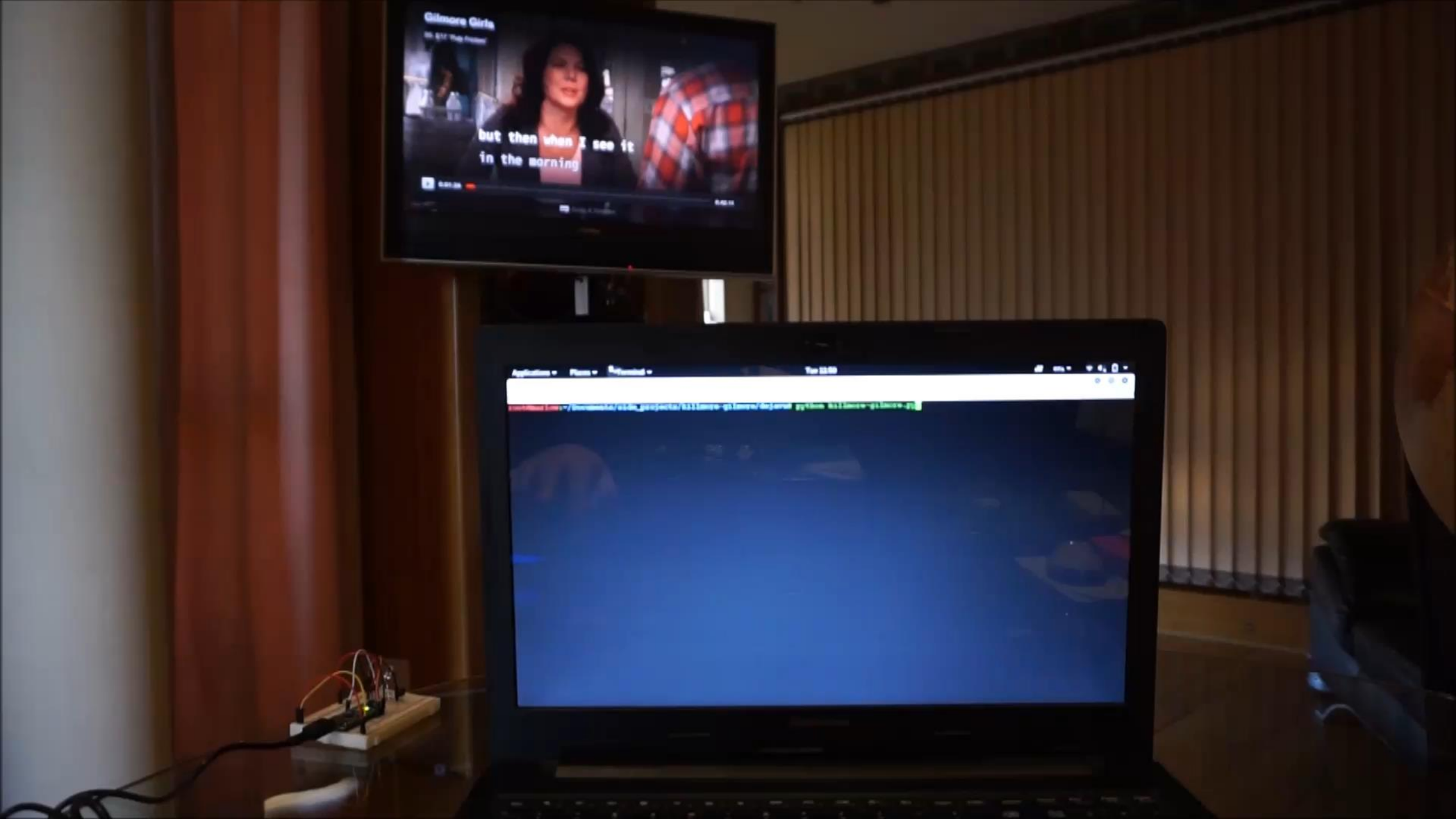
Kill More Gilmore

Kill More Gilmore

```
while True:
    counter += 1
    djv = Dejavu(config)
    song = djv.recognize(MicrophoneRecognizer, seconds=10) # longer period provides more accuracy
    os.system('clear')
    match = song.get('song_name')
    confidence = song.get('confidence')
    if match == 'evil' and confidence > 10: # we've got a match! kill it with fire!
        print 'AAARGH GILMORE GIRLS!'
        counter = 0
        ser = serial.Serial("/dev/ttyUSB0", 9600) # change to whatever serial device is being used
        ser.write('G') # send the byte; the Arduino sketch checks for incoming bytes and compares
        ser.close()
    else:
        freeNum = (counter * 10)
        print 'Rejoice! ', freeNum, 'seconds of Gilmore-free bliss!'
```

If the *Gilmore Girls* theme song plays in our flat, the TV turns itself off

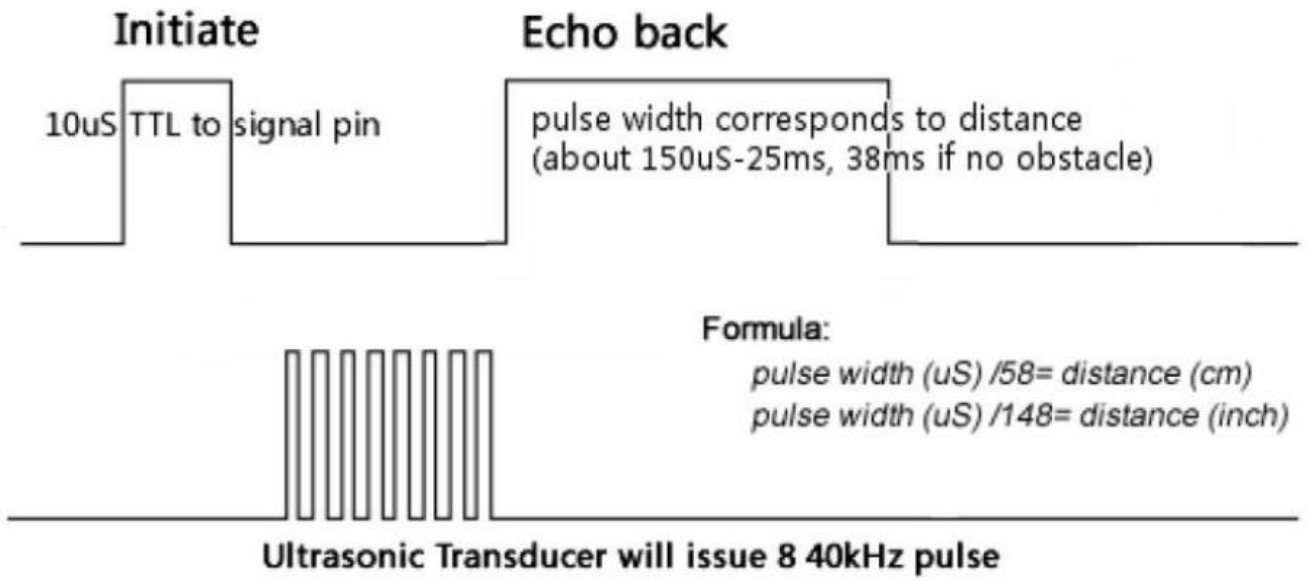
Because not all heroes wear capes


Gilmore Girls
but then when I see it
in the morning

AstroDrone

- Many drones have ultrasonic altimeters
- I’ve demonstrated with the Parrot AR 2.0
  - **But any drone with an ultrasonic altimeter is likely to be affected**
- 22.5Khz or 25Khz (configurable via telnet)

AstroDrone


Initiate
Echo back
10uS TTL to signal pin
pulse width corresponds to distance
(about 150uS-25ms, 38ms if no obstacle)
Formula:
pulse width (uS) /58= distance (cm)
pulse width (uS) /148= distance (inch)
Ultrasonic Transducer will issue 8 40kHz pulse

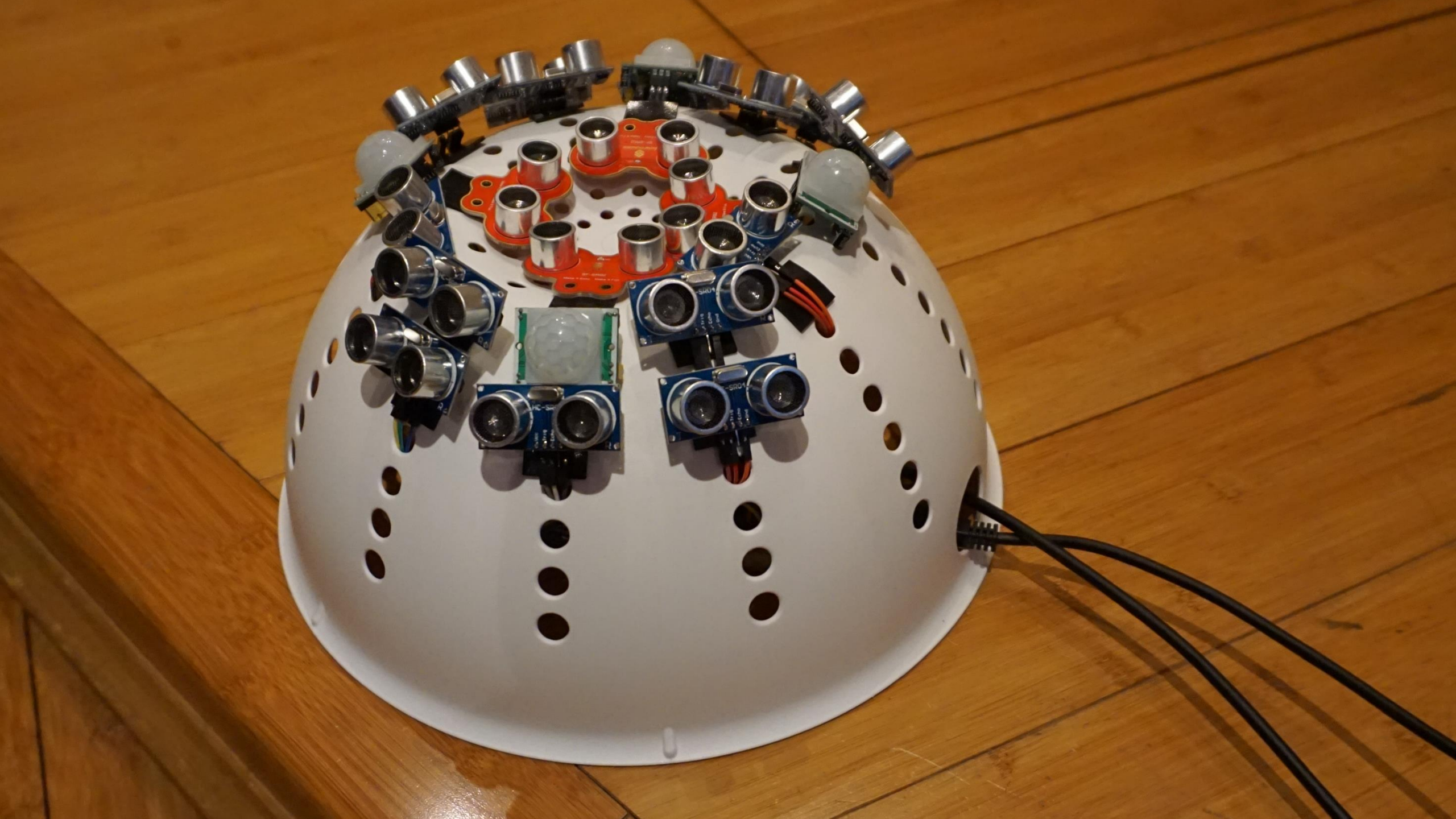
Effects

- Either *launches* the drone upwards at speed
  - I now have a dented ceiling
  - And a broken drone
- Or causes it to stick to the floor
  - But not crash – rotors still turn
- Liu et al (2016) – ultrasonic attacks against autonomous cars
- Lots of attacks against drones generally
  - Robinson (2015)
  - Son et al (2015)
  - Luo (2016)

Animal repellent alarm

- PIR
- If high, sends out an ultrasonic pulse
- Adjustable frequency (0-50Khz)
- Adjustable sensitivity

GOODNIGHT SWEET PRINCE



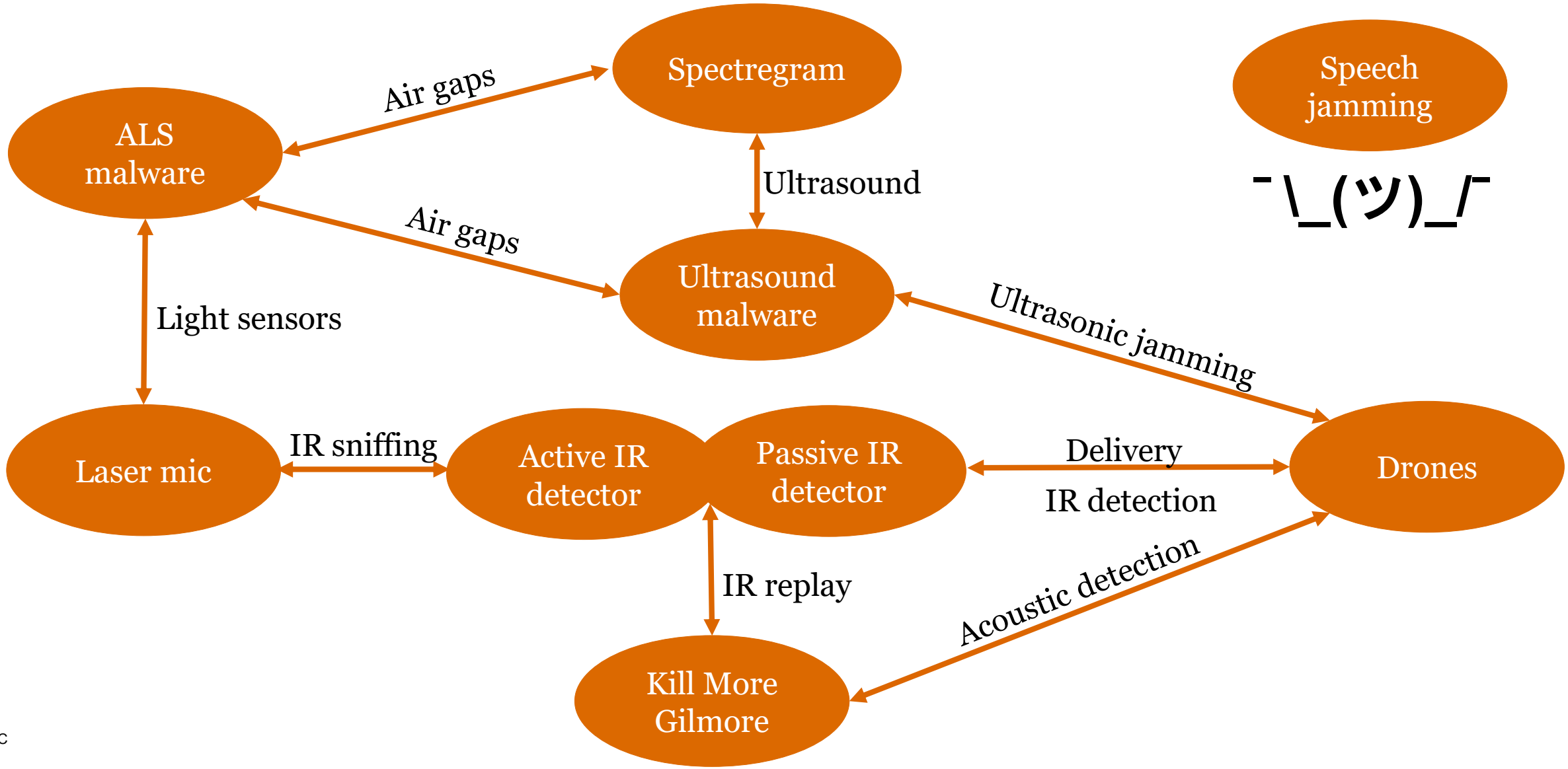

CRAIC

Real-world applications

- Deploy on roof to keep drones away
  - Prisons
  - Government buildings
  - Public events
- Further research ongoing
- Personal drone protection ☺

Part IV
Summary

Research overview



Pros & Cons

- **Pros**
  - Great for physical engagements / air-gaps
  - Difficult to detect / defend against
  - Very little trace
  - Cheap to design and develop

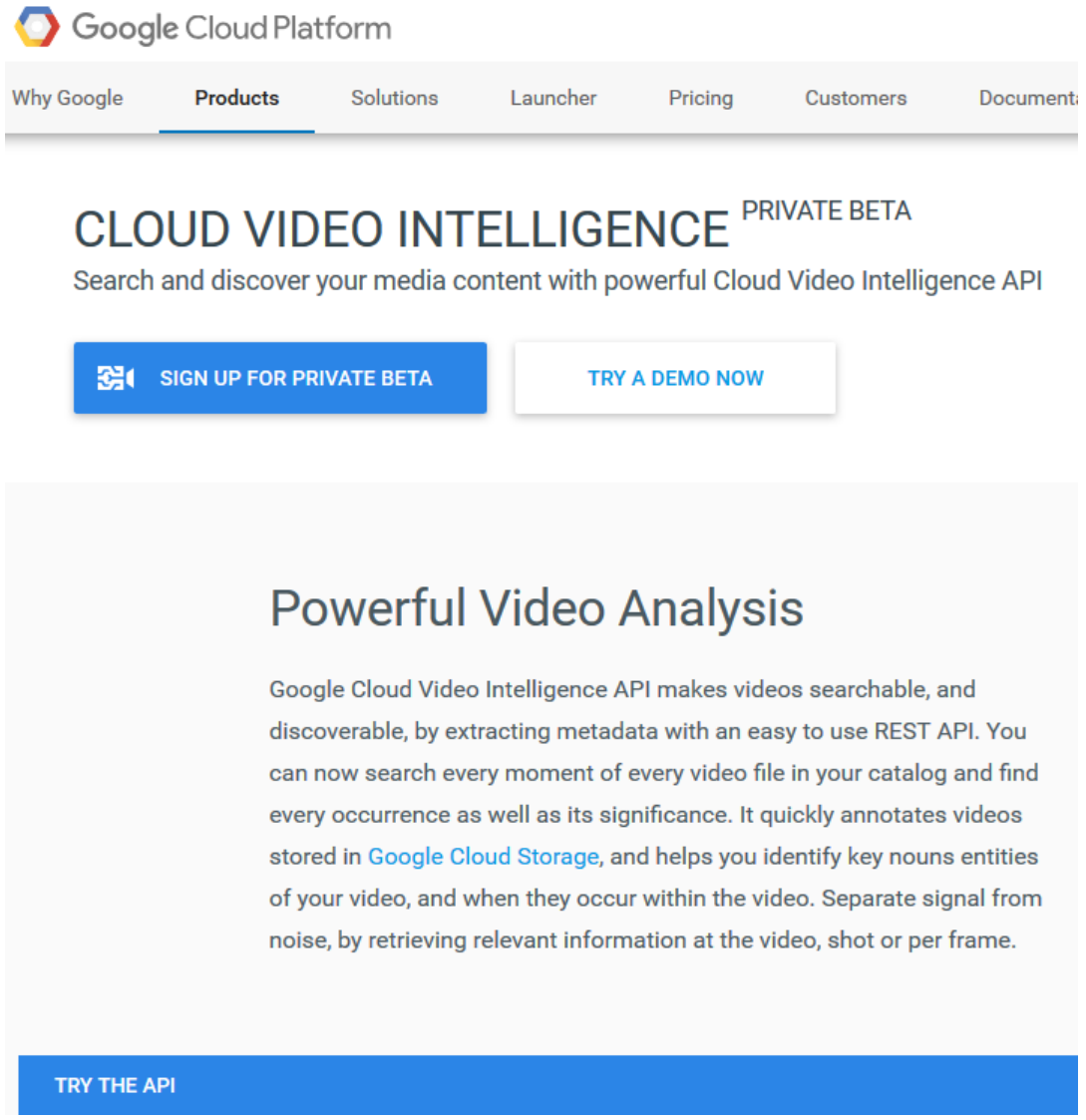
- **Cons**
  - Usually require proximity to targeted systems
  - Subject to interference
  - Range and power depend on resources

Mitigations

- First step is knowing these techniques and attacks exist
- And that inputs/outputs can often be easily manipulated and accepted as genuine
- Where possible/feasible, block inputs/outputs to a system, or ensure they have a reliable failover
- Be aware of clone-and-replay attacks
- Be aware of the limitations of some security products
  - e.g. fixed codes, susceptible to jamming, etc

Future research

- Exfiltration via IR
- Acoustic keylogging
- Further work on drone repellents
  - Tracking and targeting
  - Identification through video →
  - Combo of infrared and sound



Hopefully, you're on the left rather than the right…

Music credits

- **LiFi demo:** “Arcade Funk”: https://www.dl-sounds.com/license/, https://www.dl-sounds.com/royalty-free/arcade-funk/
- **Spectregram demo:** “Suspense Strings”: https://www.dl-sounds.com/license/, https://www.dl-sounds.com/royalty-free/suspense-strings/
- **Laser microphone demo:** “Die Walküre, WWV 86B – Fantasie“: United States Marine Band, CC license, https://musopen.org/music/488/richard-wagner/die-walkure-wwv-86b/

References

Air-Gaps

- https://github.com/cwalk/LiFi-Music
- "BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations". 2015. Guri M., Monitz M., Mirski Y., Elovici Y.
- "VisiSploit: An Optical Covert-Channel to Leak Data through an Air-Gap". 2016. Guri M., Hasson O., Kedma G., Elovici Y.
- "Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers". 2016. Guri M., Solewicz Y., Daidakulov A., Elovici Y.
- "Sensing-enabled channels for hard-to-detect command and control of mobile devices". 2013. Hasan R., Saxena N., Haleviz T., Zawoad S., Rinehart D.
- "Information leakage from optical emanations". 2002. Loughrey, J., Umphress D.A.
- "XLED: Covert Data Exfiltration from Air-Gapped Networks via Router LEDs". 2017. Guri, M., Zadov B., Daidakulov A., Elovici Y.
- "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies". 2014. Guri M., Kedma G., Kachlon A., Elovici Y.
- "SPEAKE(a)R: Turn speakers to microphones for fun and profit". 2016. Guri M., Daidakulov A., Elovici Y.
- "Compromising emanations: Eavesdropping risks of computer displays". 2003. Kuhn, M.G.
- "A closer look at keyboard acoustic emanations: random passwords, typing styles and decoding techniques". 2012. Halevi T., Saxena N.
- https://msdn.microsoft.com/en-us/library/windows/desktop/dd318933(v=vs.85).aspx
- "An Examination of the Feasibility of Ultrasonic Communications Links". 2010. Toftsed D., O'Brien S., D'Arcy S., Creegan E., Elliot S.
- "On Covert Acoustical Mesh Networks in Air". 2014. Hanspach M., Goetz M.
- [Equation] – Aphex Twin
- Look – Venetian Snares

Surveillance and Counter-surveillance

- "Let's Get Physical". 2013. Porter D., Smith S. BH USA 2013.
- "Old Skewl Hacking – Infrared". 2005. Major Malfunction. DEF CON 13.
- "Digital Ding Dong Ditch". 2014. Kamkar, S. https://samy.pl/dingdong/.

References

Bantz

- "Repsych: Psychological warfare in reverse engineering". 2015. Domas, C. DEF CON 23.
- "Knocking my neighbour's kid's cruddy drone offline". 2015. Robinson, M. DEF CON 23.
- "Rocking drones with intentional sound noise on gyroscopic sensors". 2015. Son Y., Shin H., Kim D., Park Y., Noh J., Choi K., Choi J., Kim Y.
- "Drones hijacking: Multi-dimensional attack vectors and countermeasures". 2016. Luo, A. DEF CON 24
- "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles". 2016. Liu J., Yan C., Xu W. DEF CON 24.

Thank you!
Any questions?

email: **matt.wixey@pwc.com**
twitter: **@darkartlab**