
See no evil, hear no evil

Hacking invisibly and silently with light and sound

Matt Wixey – PwC UK

September 2017



- 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

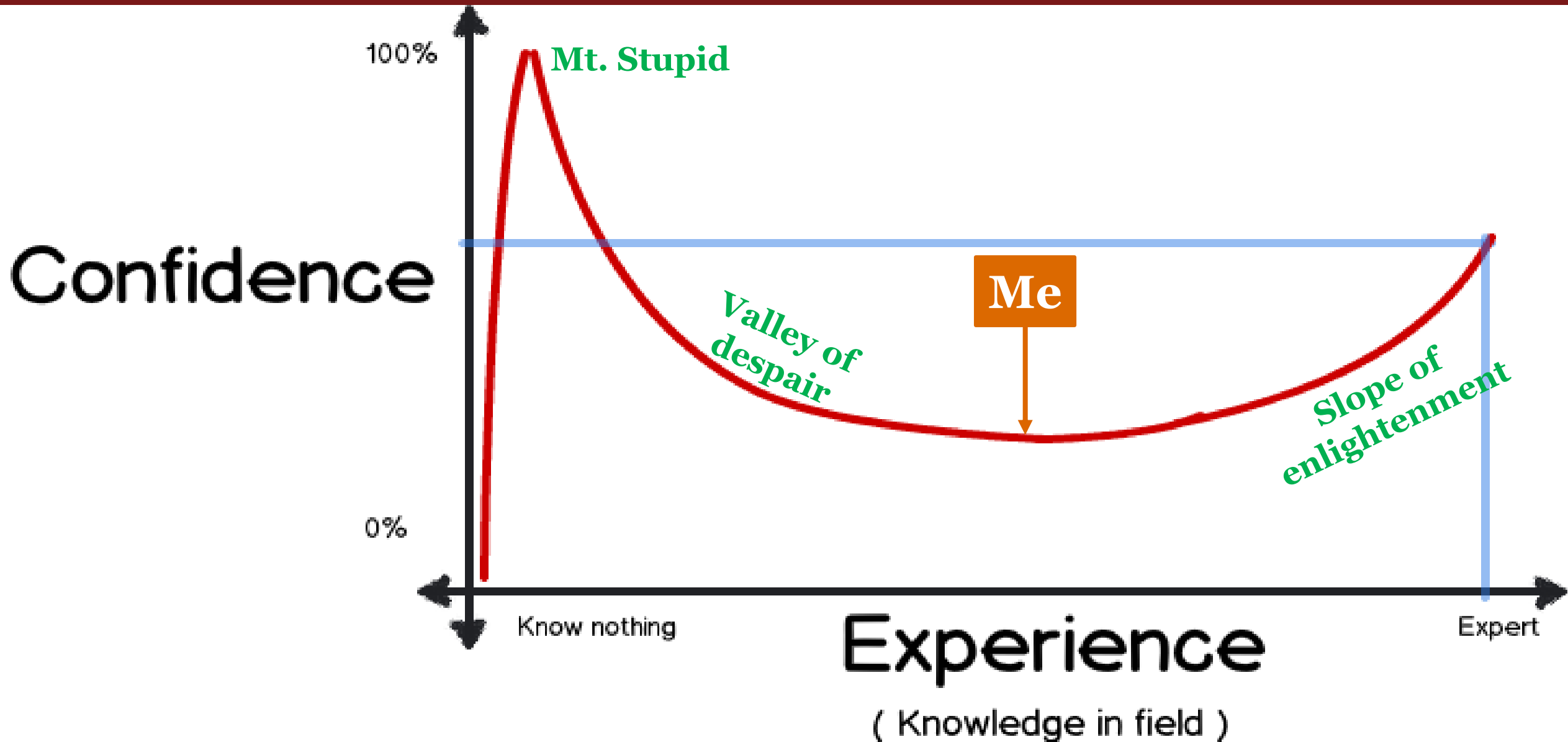
Agenda

- **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 educational purposes only. 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

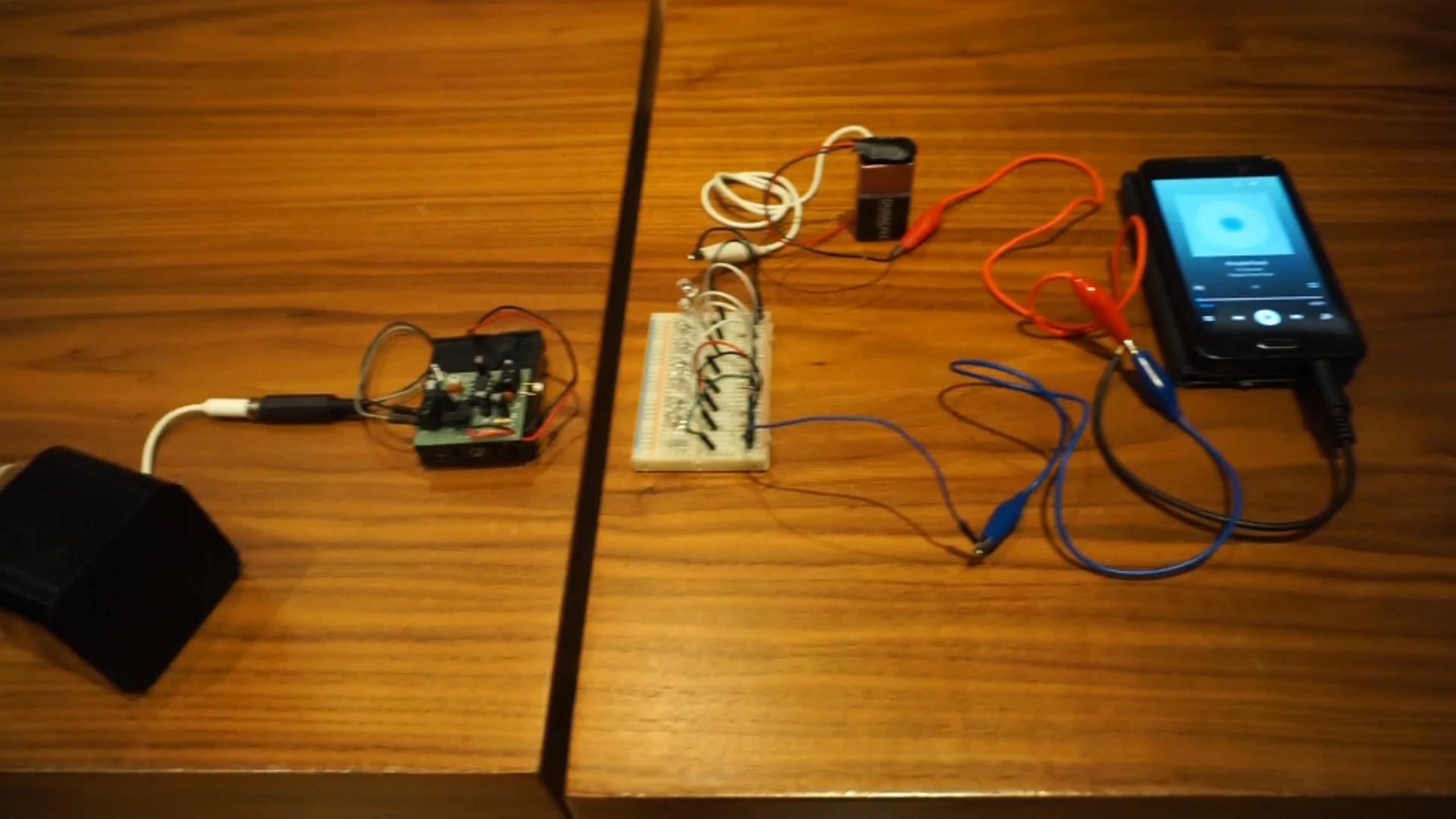
Dunning-Kruger Curve







What sorcery is this?!



Part I

Jumping air-gaps

- *A Sensor Darkly*
- *Dreadphone*
- *Spectrogram*

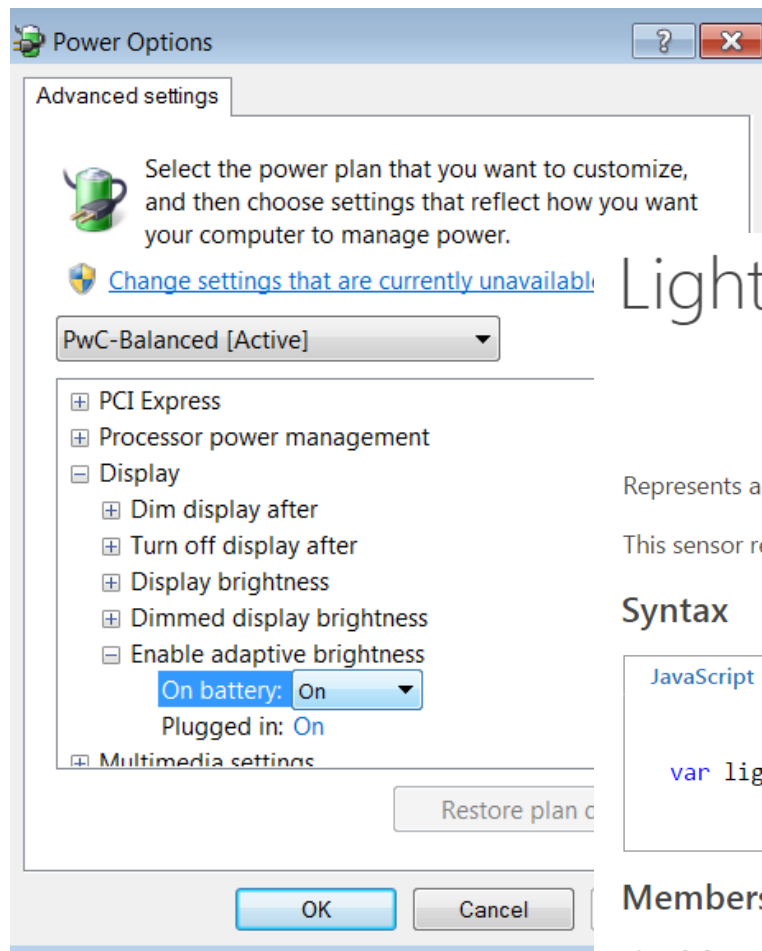
Caveats

- 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!**

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



LightSensor class

Represents an ambient-light sensor.

This sensor returns the ambient-light reading as a LUX value.

Syntax

JavaScript

C#

C++

VB

```
var lightSensor = Windows.Devices.Sensors.LightSensor;
```

Members

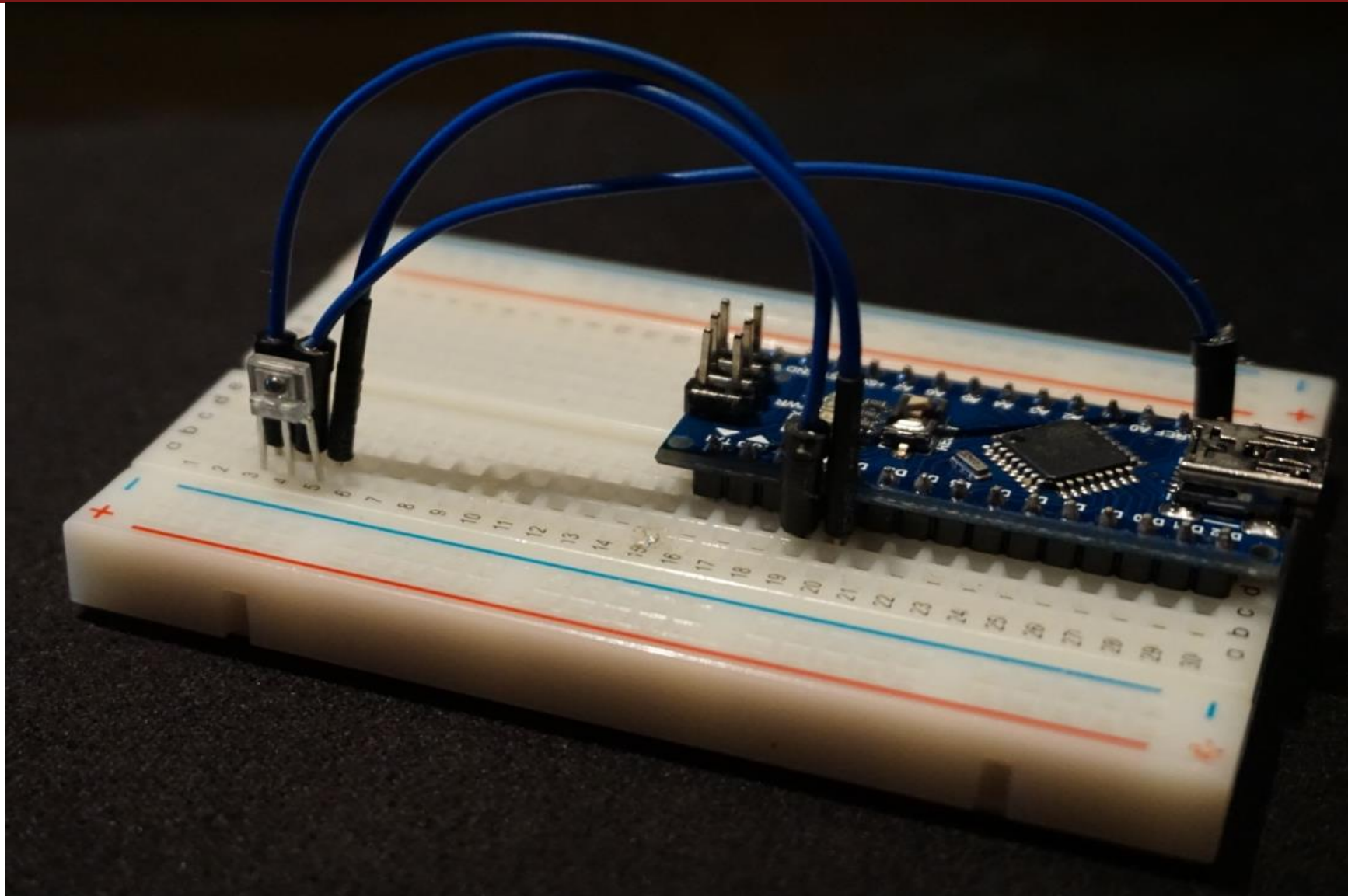
The **LightSensor** class has these types of members:

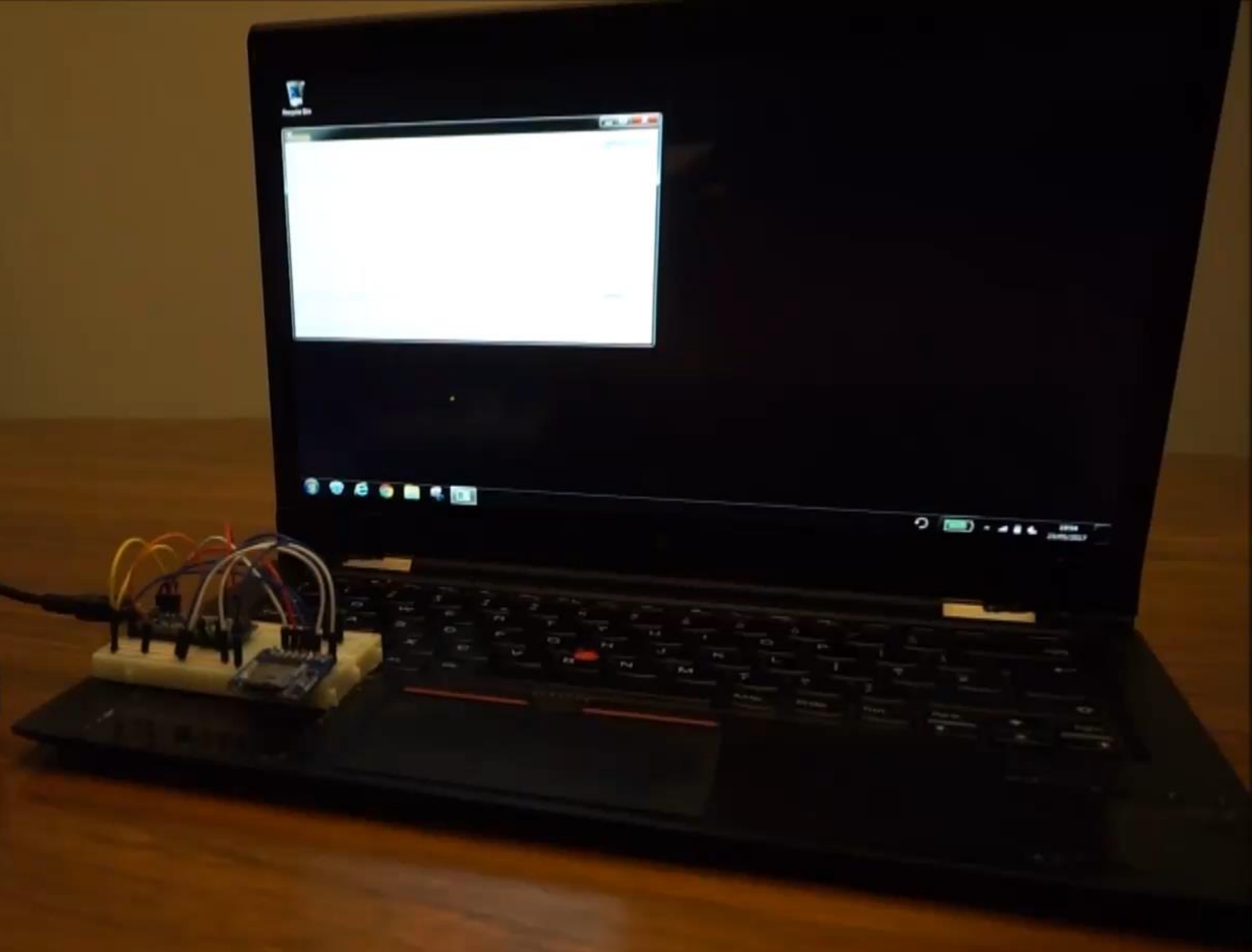
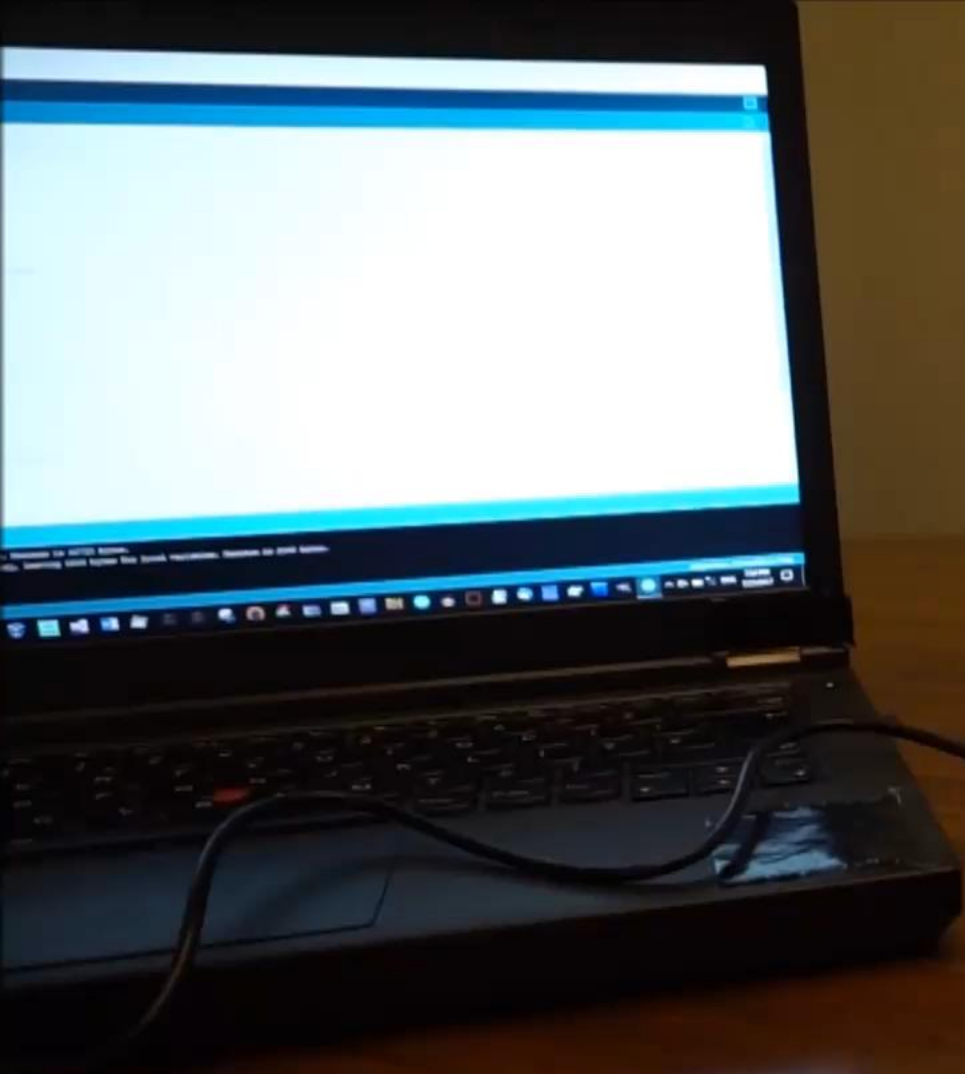
- [Events](#)
- [Methods](#)
- [Properties](#)

- **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

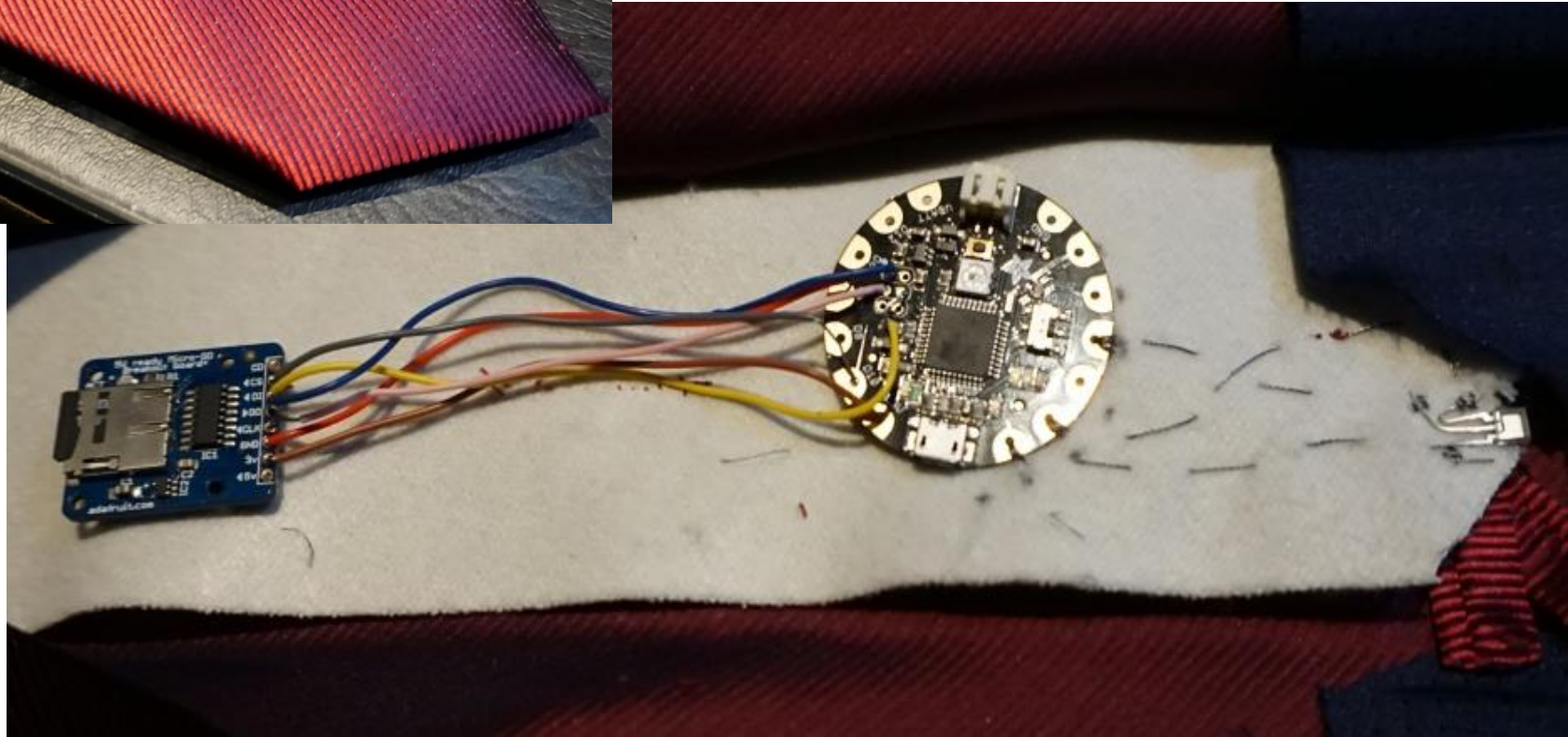


Exfiltration



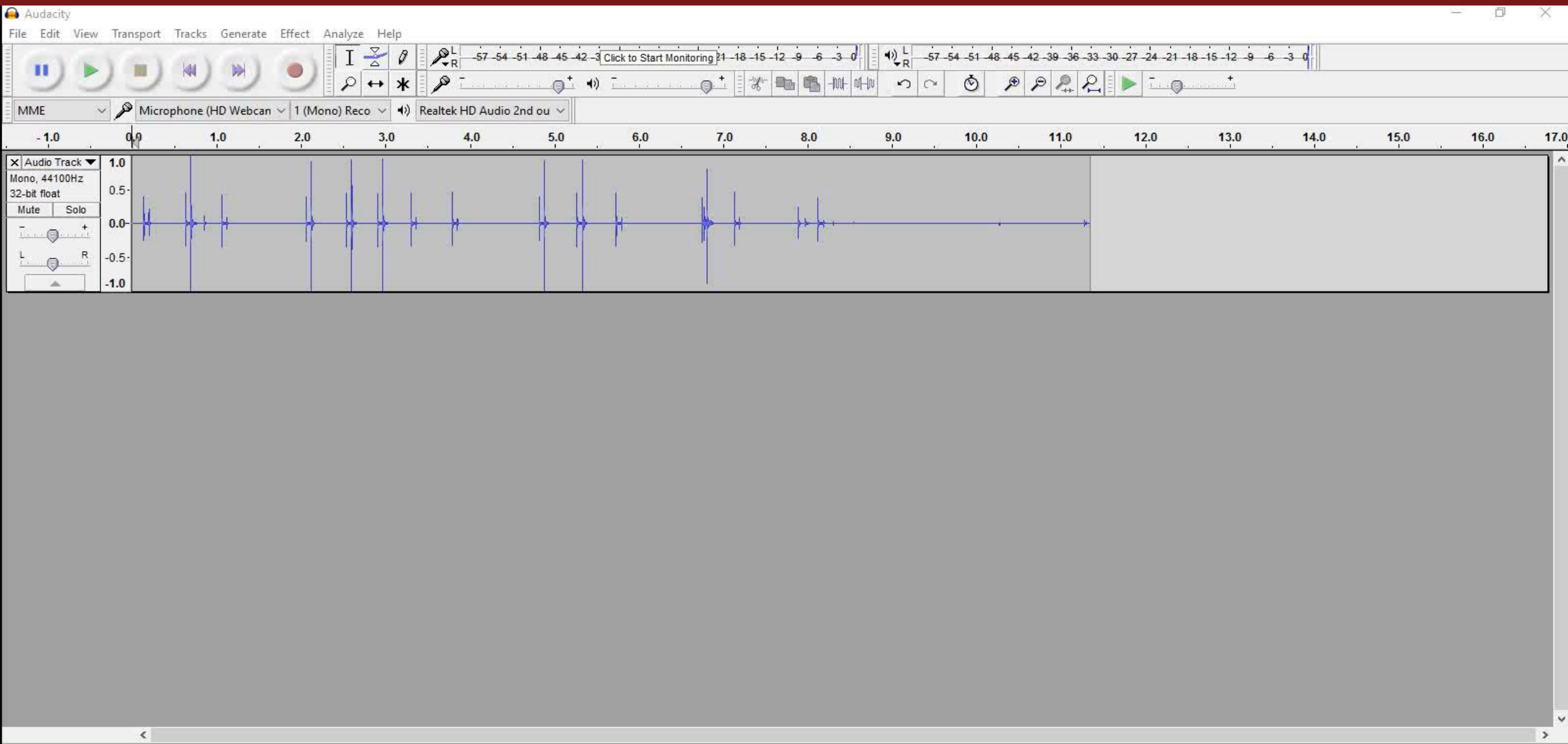


Prototype 2



- 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

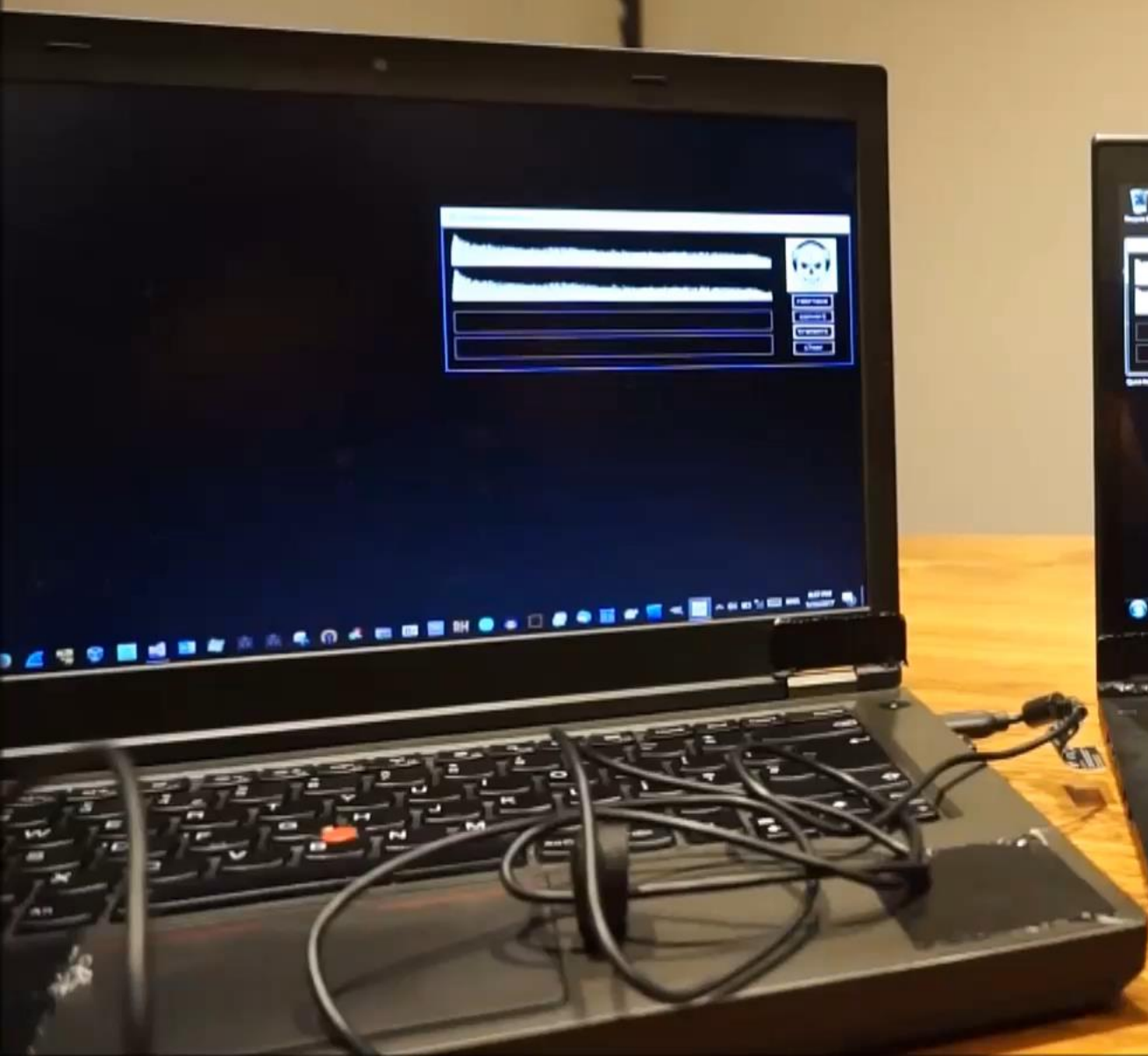
Soundcard woes



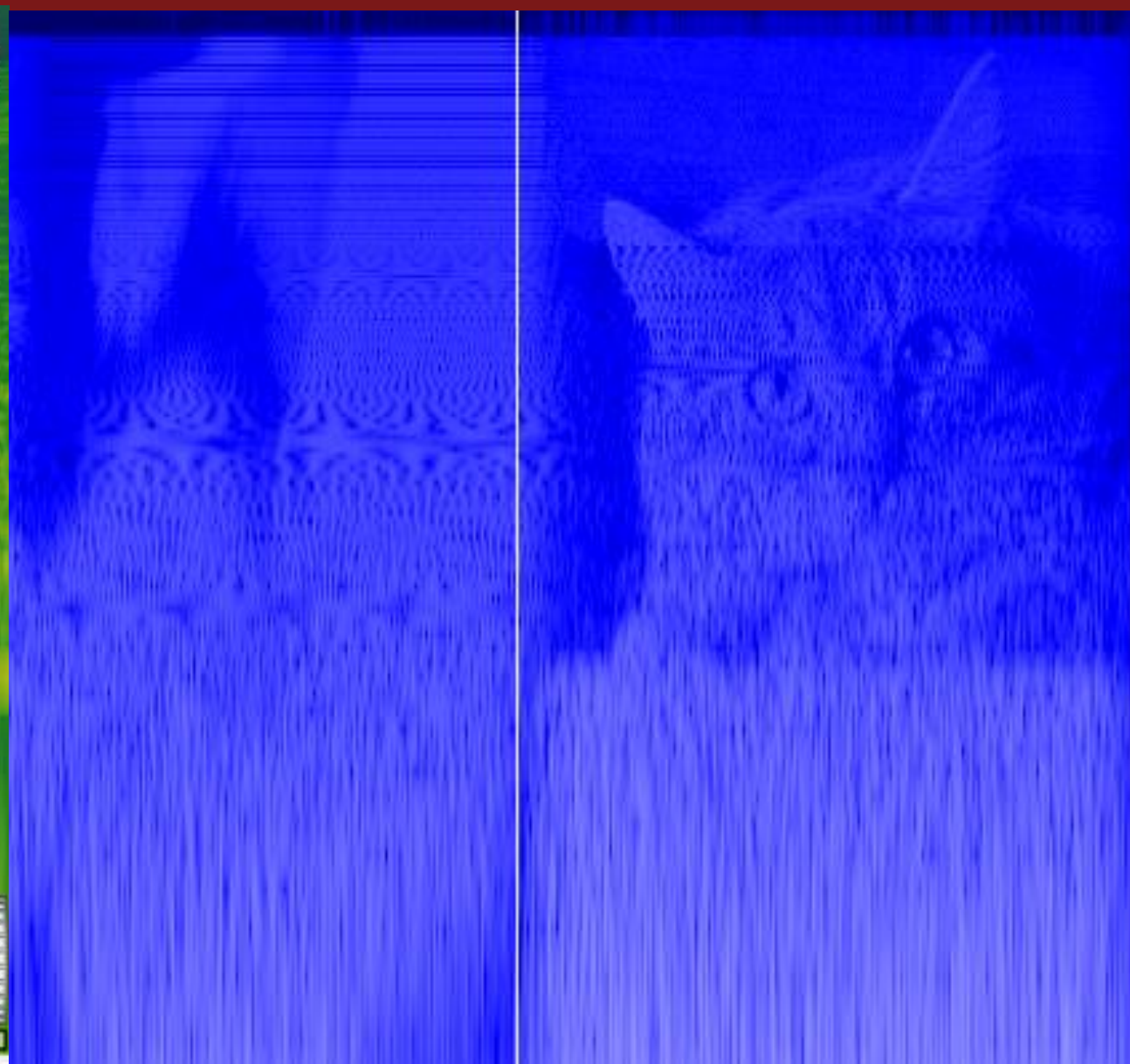
Soundcard woes

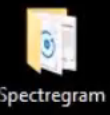
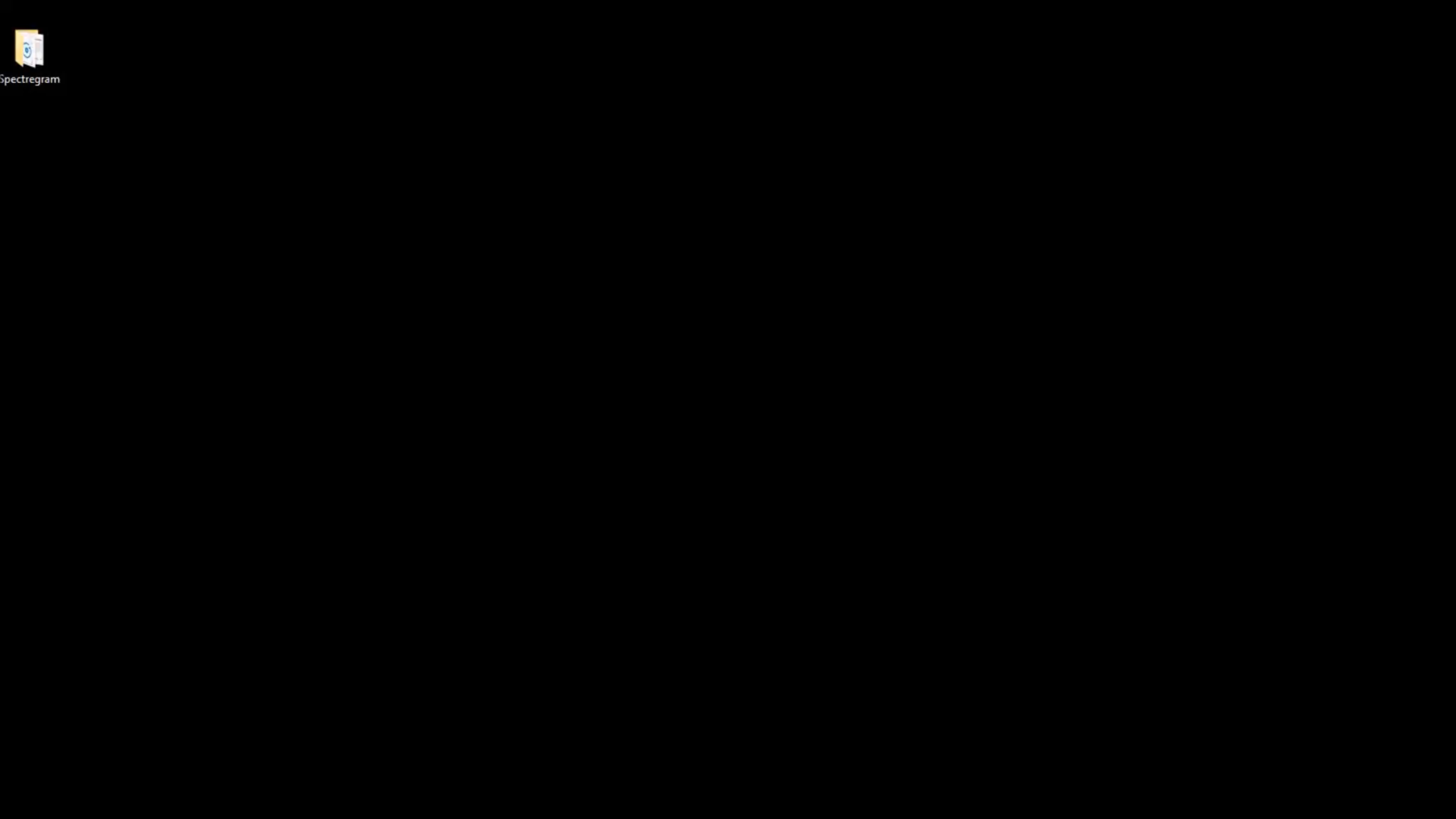
- Apply multiple fade-ins / fade-outs
- Then amplify the track:





Spectrogram





Spectrogram

Mitigation

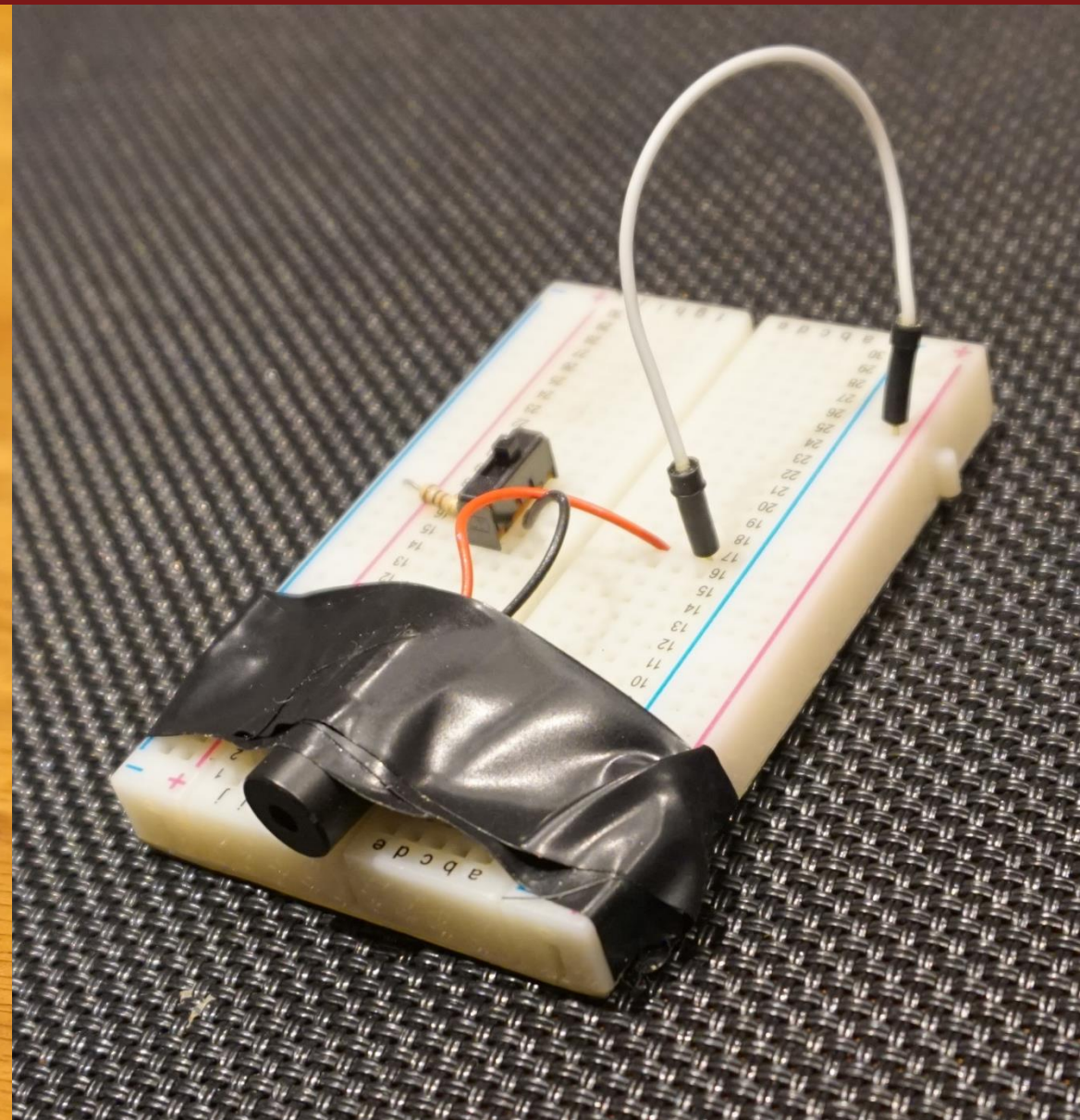
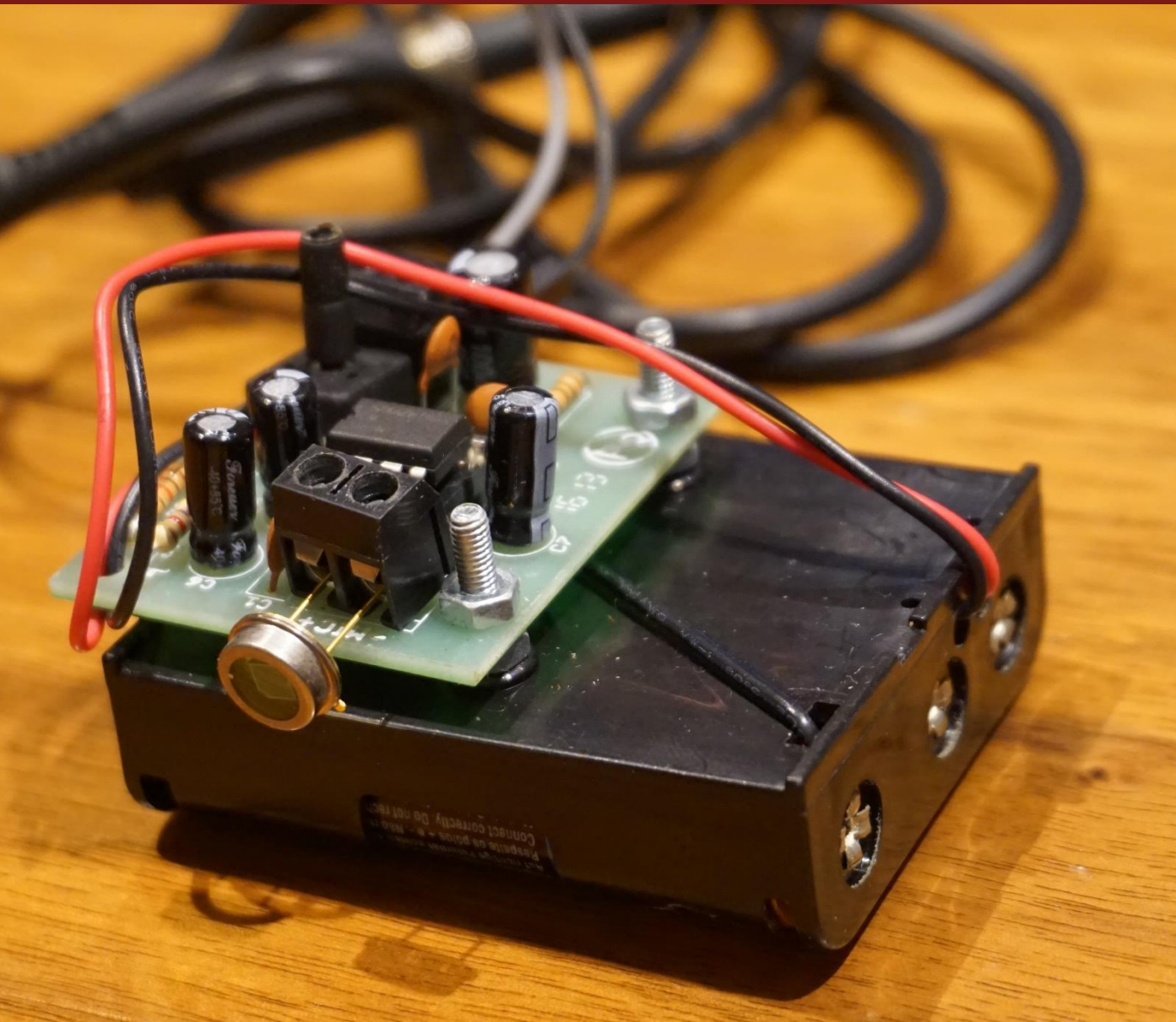
- TEMPEST standards
- Remove/disable ALS
- Screen filters
- White noise
- Ultrasonic detectors
- Disable microphones/speakers

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*

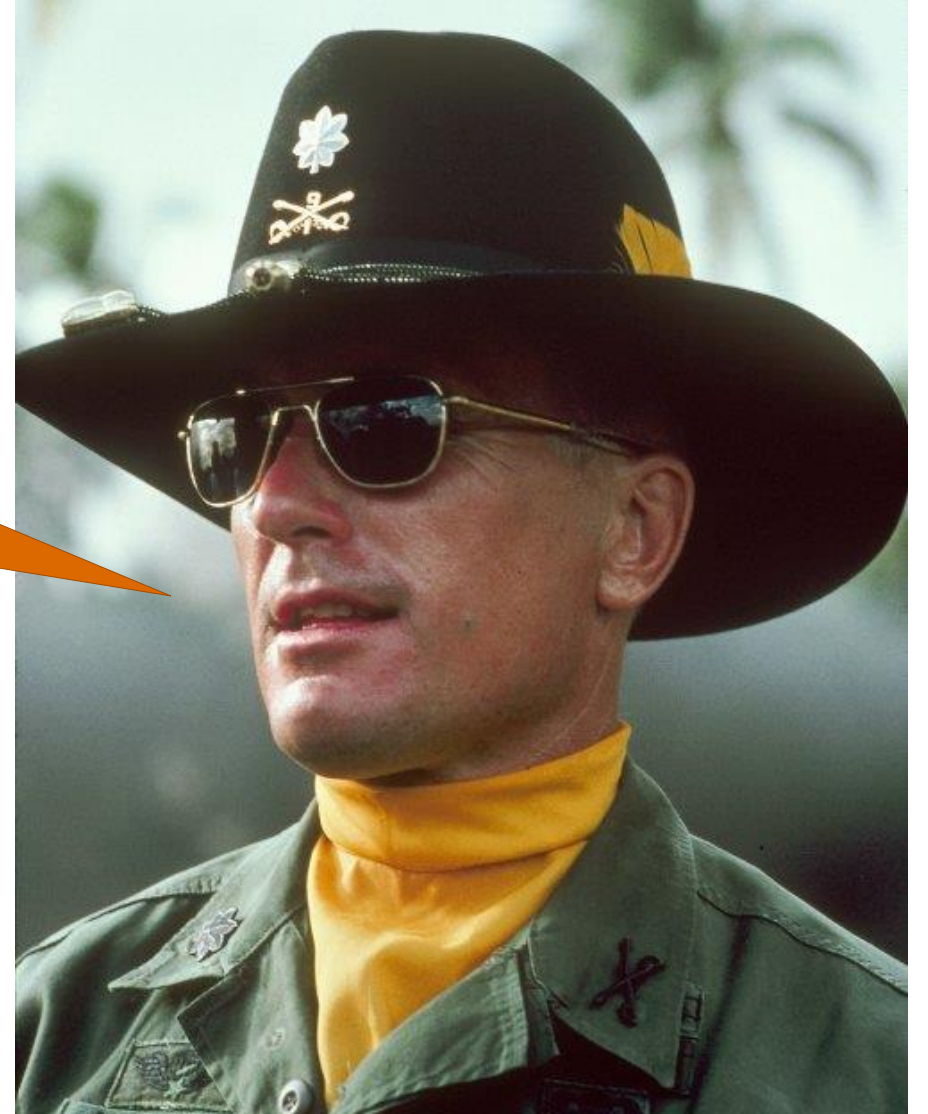
Laser microphone





But that music choice though

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



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

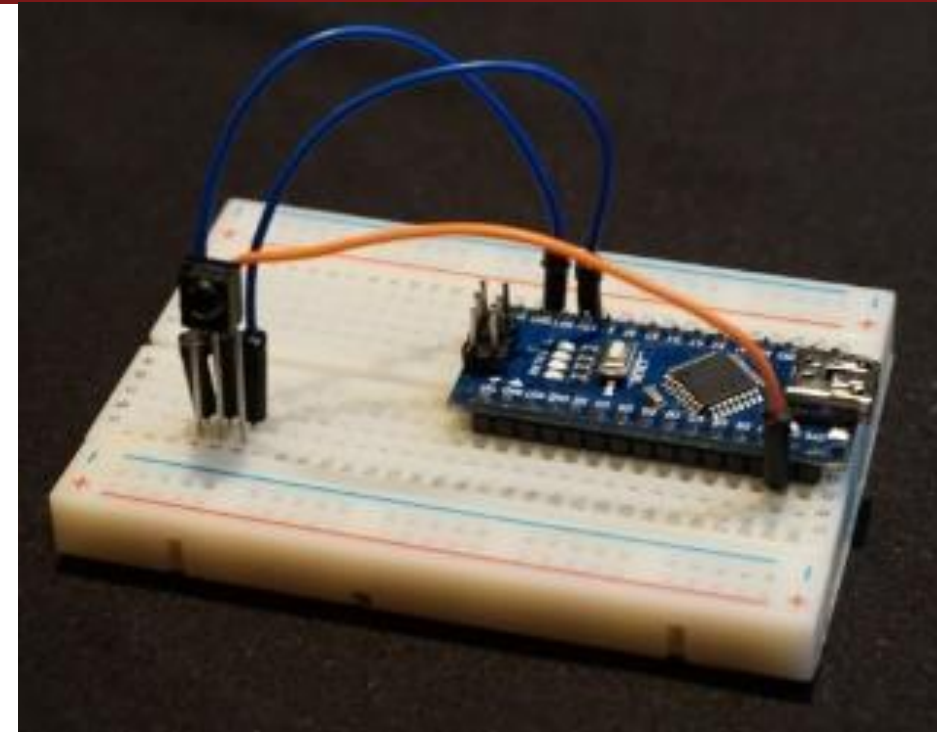
0:m550 s600	1:m500 s600	2:m500 s600	3:m500 s650
4:m450 s600	5:m550 s600	6:m500 s1700	7:m500 s600
8:m500 s1700	9:m550 s1700	10:m500 s1700	11:m500 s1750
12:m500 s1700	13:m500 s1700	14:m550 s550	15:m550 s1700
16:m500 s600	17:m500 s1700	18:m550 s600	19:m450 s650
20:m500 s1700	21:m500 s600	22:m550 s600	23:m450 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

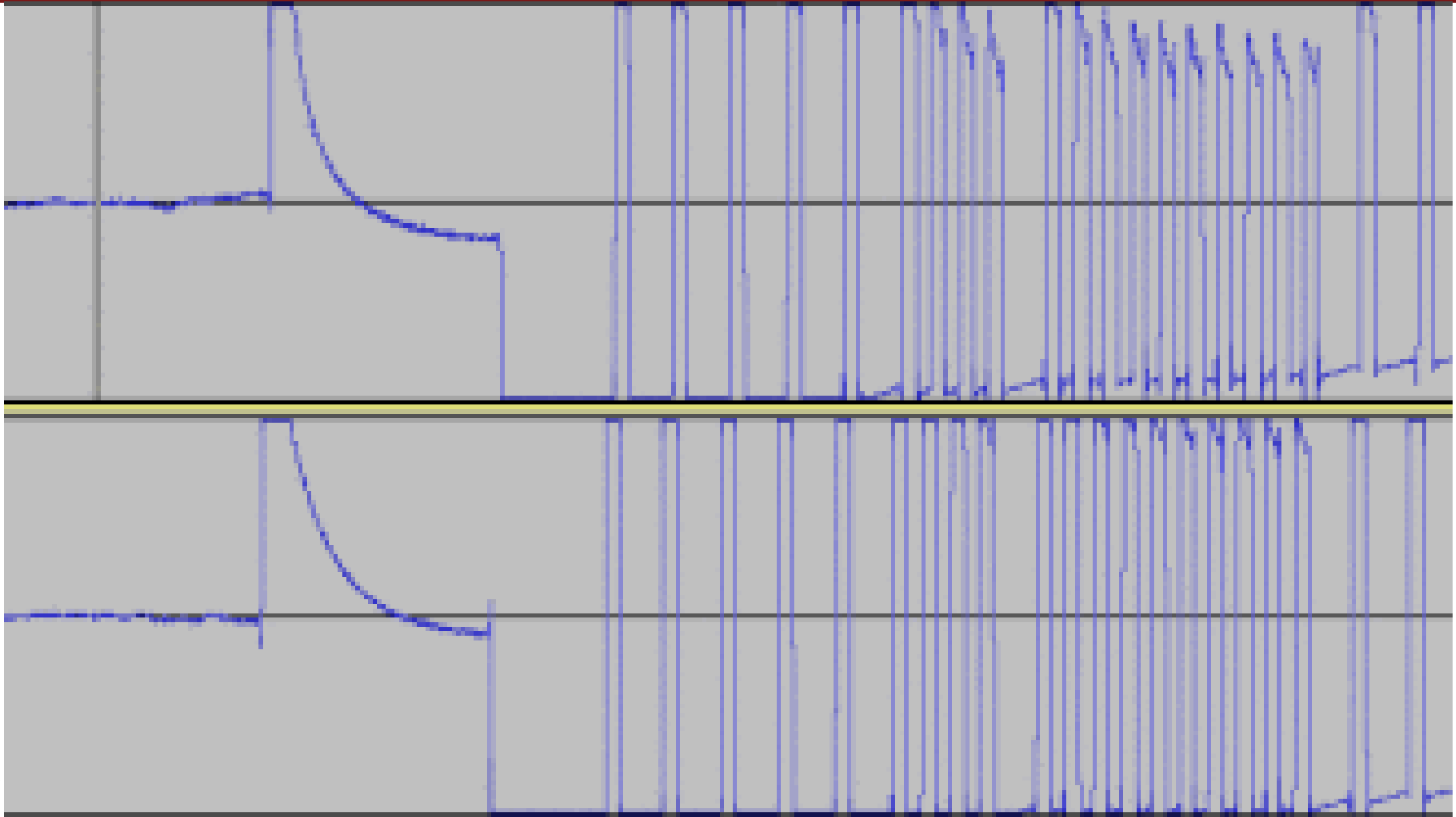
Mark min:450 max:550

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**

```
1  #include <IRremote.h>
2
3  IRsend irsend;
4
5  void setup()
6  {
7    Serial.begin(9600);
8  }
9
10 void loop() {
11   for (int i = 0; i < 3; i++) {
12     irsend.sendNEC(0x2FD48B7, 32);
13     delay(40);
14   }
15   Serial.println("Sent!");
16   delay(5000); //5 second delay between each signal burst
17 }
```


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);
}

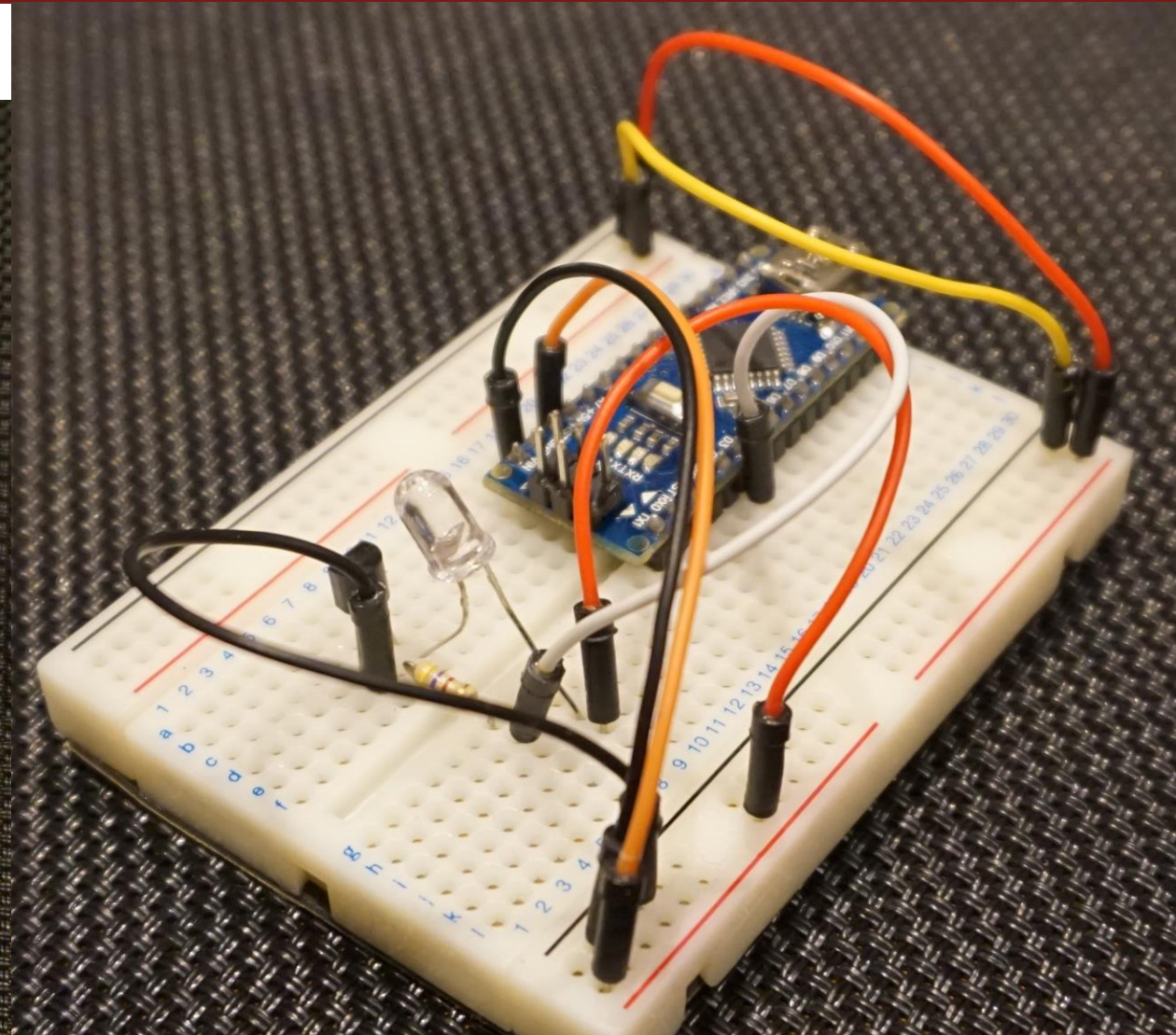
void loop() {
  int khz = 38;
  unsigned int irSignal[] = { 8900, 4600, 500, 1750, 400, 1800, 550, 1700, 500, 1700, 450,

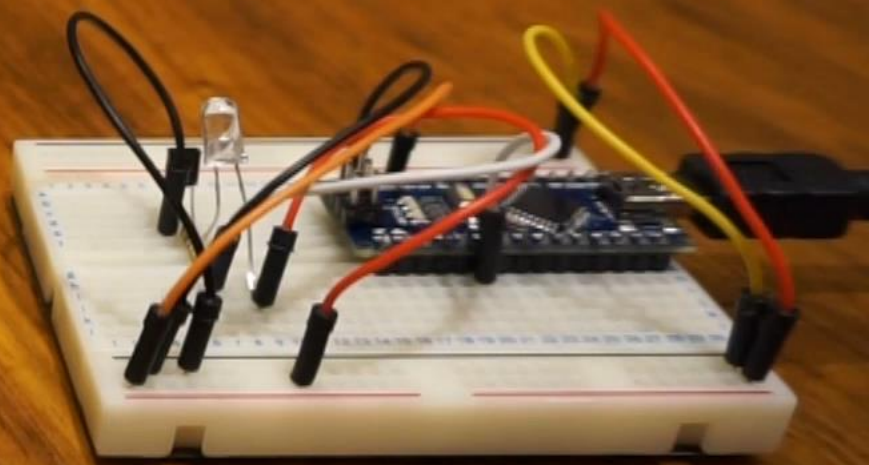
  irsend.sendRaw(irSignal, sizeof(irSignal) / sizeof(irSignal[0]), khz);
  Serial.println("Sending evil signal!");
  delay(3000);
}
```

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

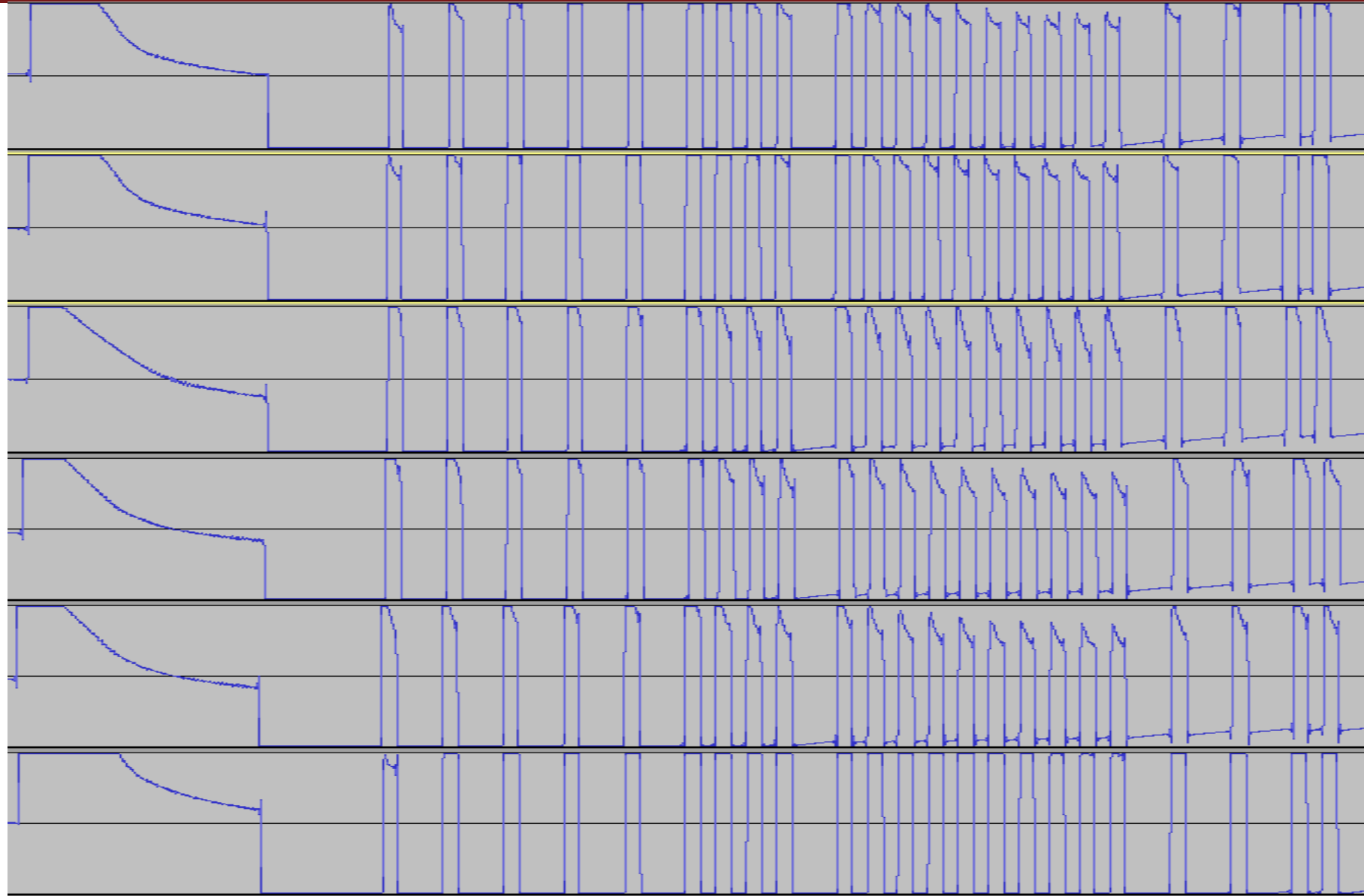
Remote 2

Remote 3

Remote 4

Remote 5

Remote 6



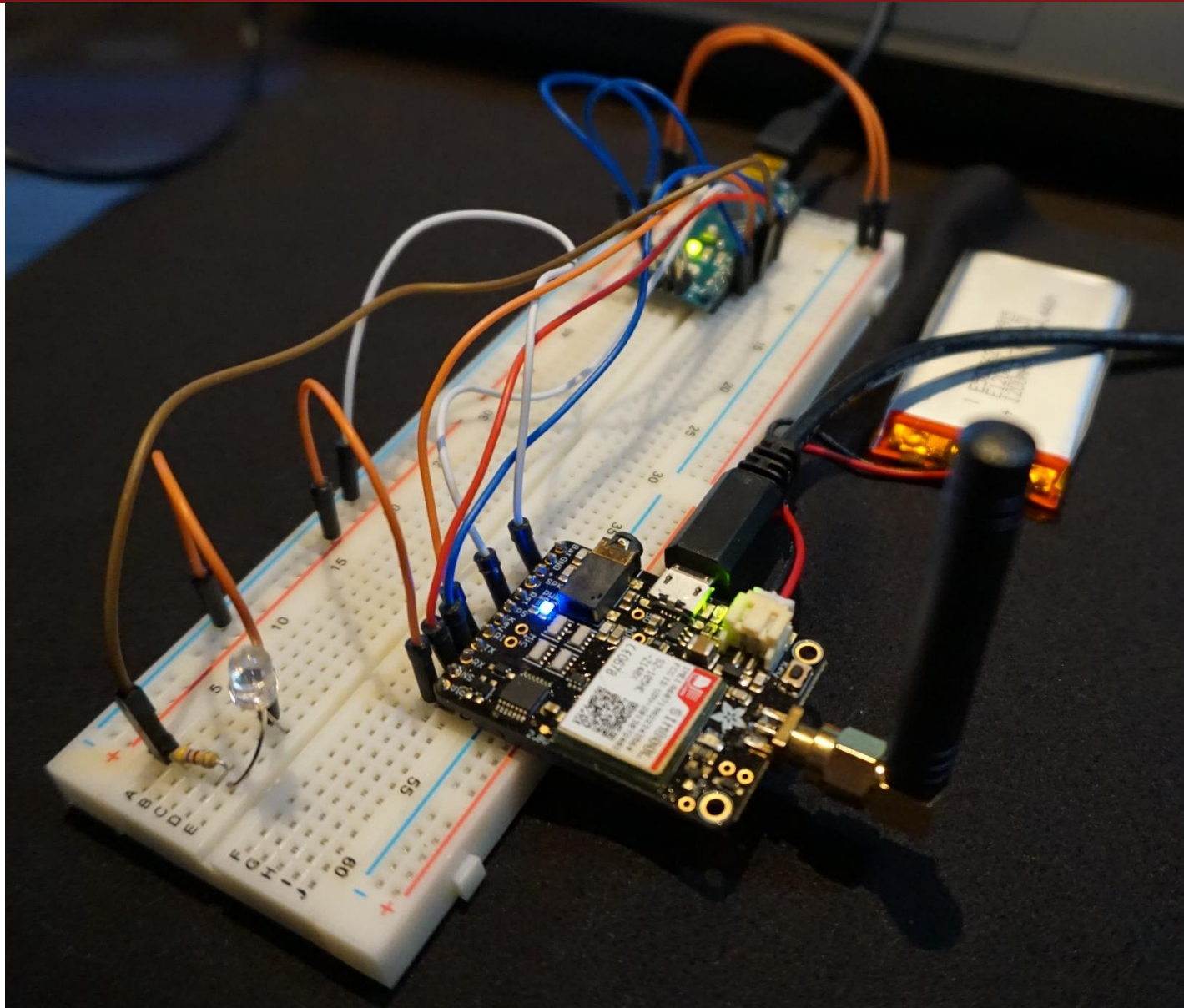


Drone to clone to pwn





Phone to clone to pwn





Active IR motion detector





Mitigation

- Vibrations/speakers/wire screens/coverings on windows
- Detect IR lasers with unfiltered cameras
- 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

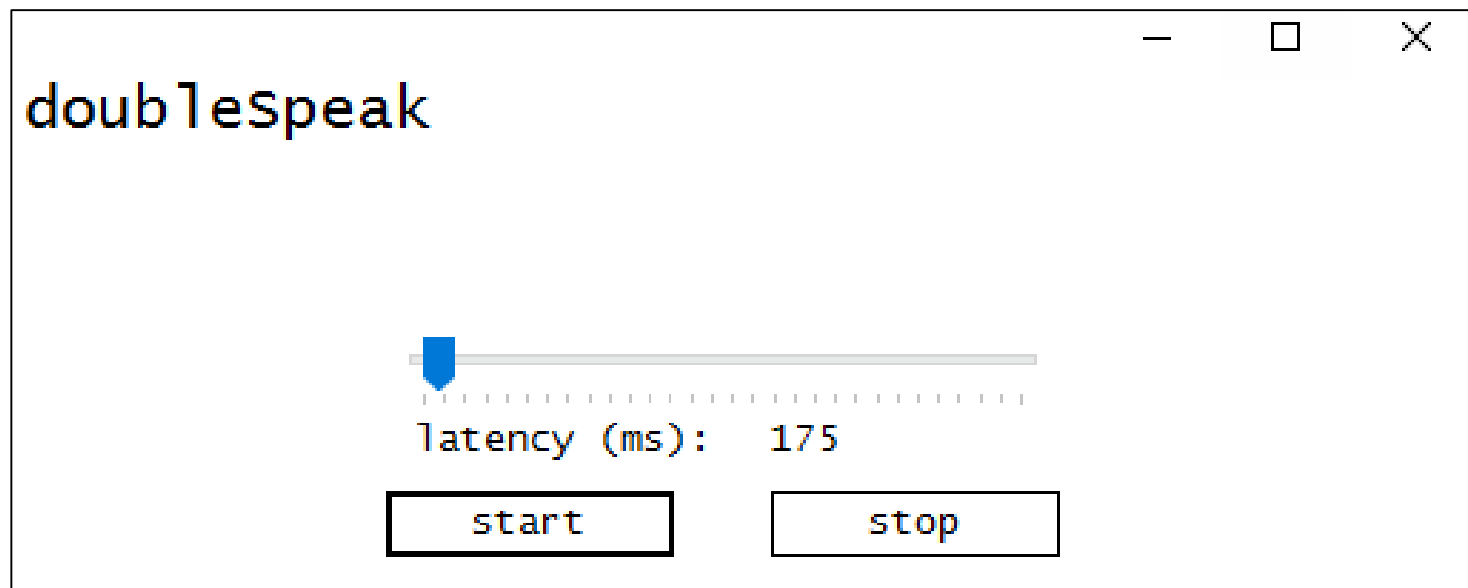
Part III

Bantz

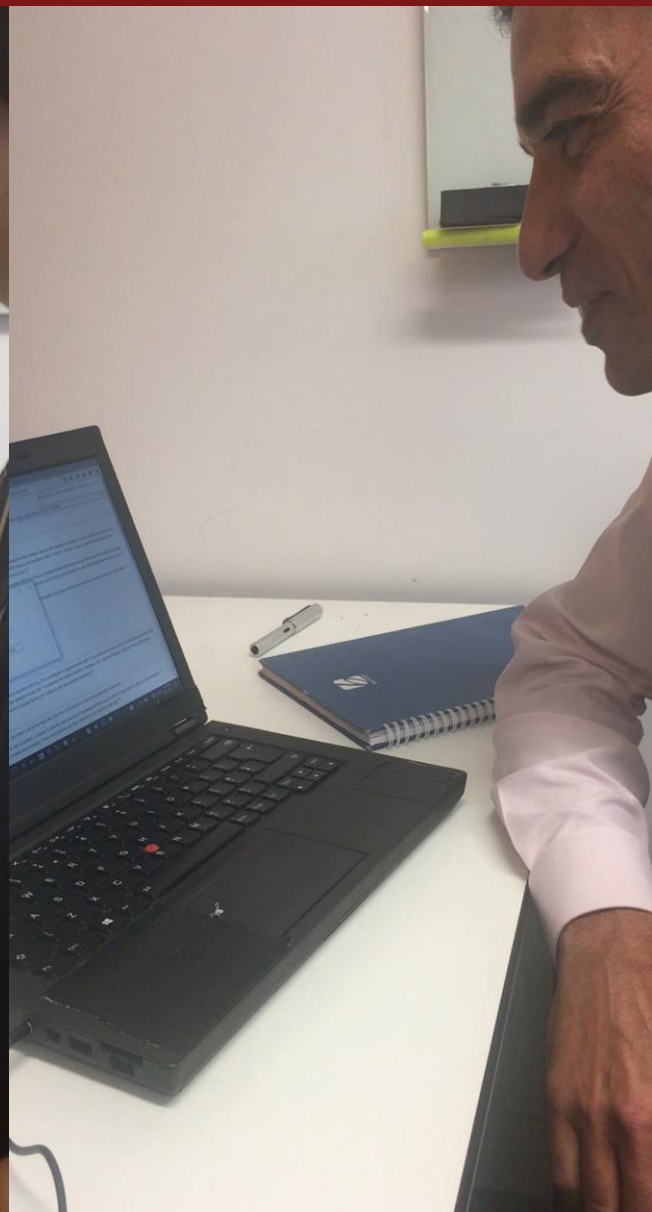
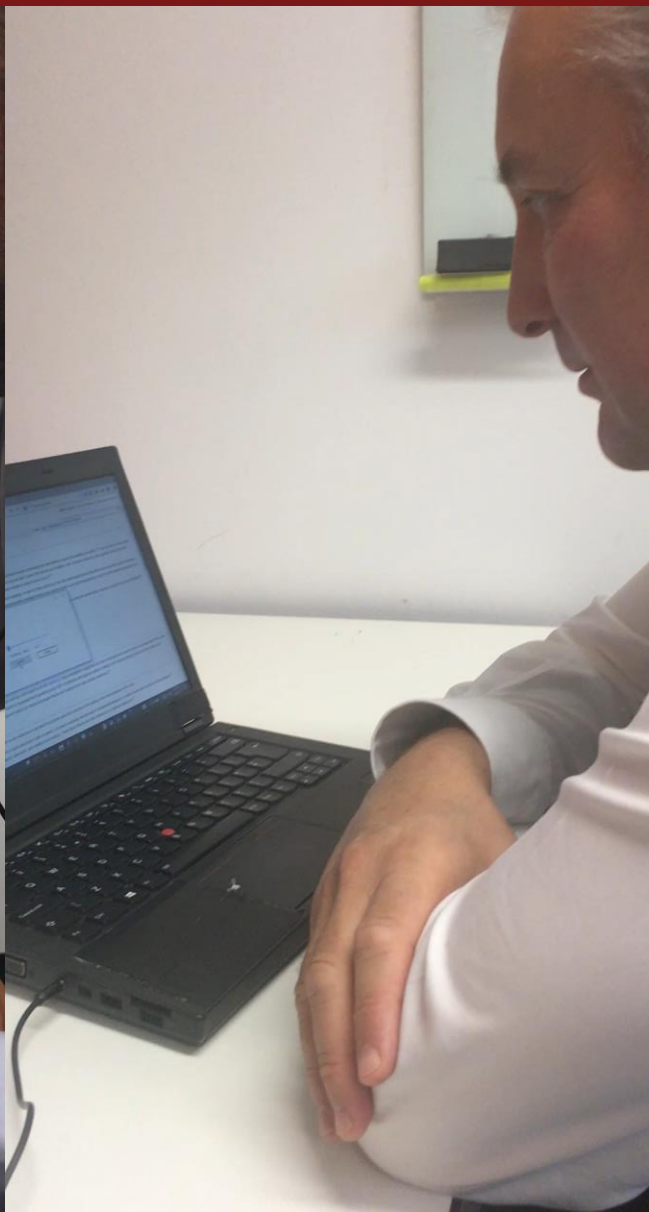
- *doubleSpeak*
- *Annoying malware analysts*
- *Kill More Gilmore*
- *AstroDrone*

Delayed Auditory Feedback (speech jamming)

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

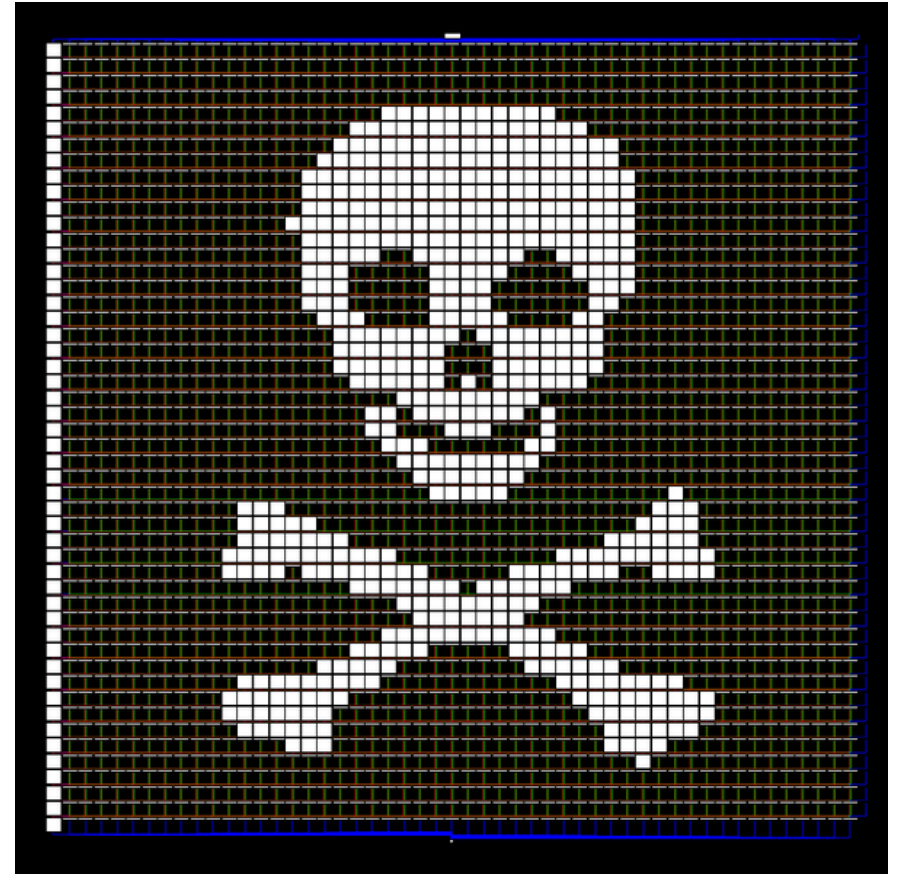


Speech jamming



Demotivating malware analysts

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





Kill More Gilmore

A promotional photograph of the cast of the TV show 'Gilmore Girls'. The cast members are posed in two rows against a background of autumn foliage. The title 'THE GILMORE GIRLS' is overlaid in large white letters.

THE GILMORE GIRLS

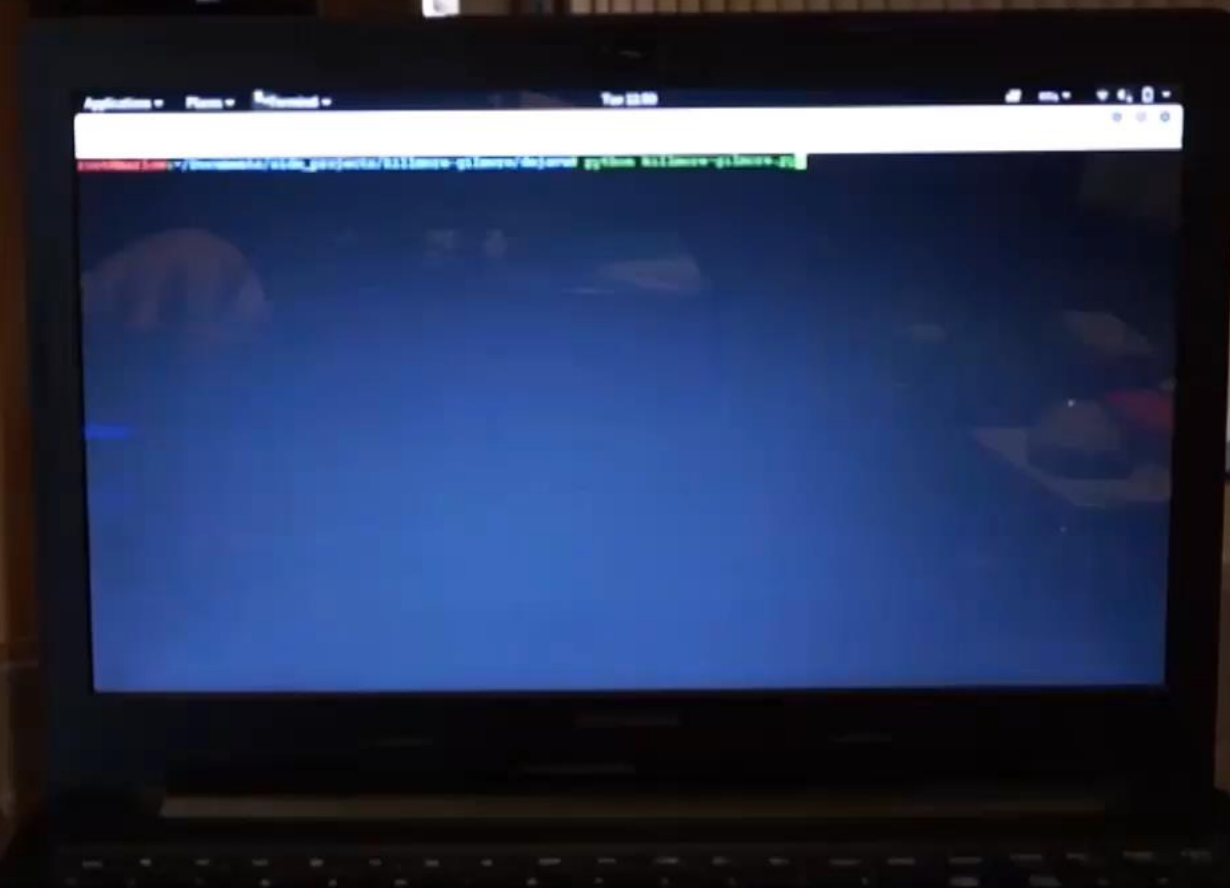
ONE AWFUL SHOW, ONE HELL OF A LOT OF TALKING

Kill More Gilmore

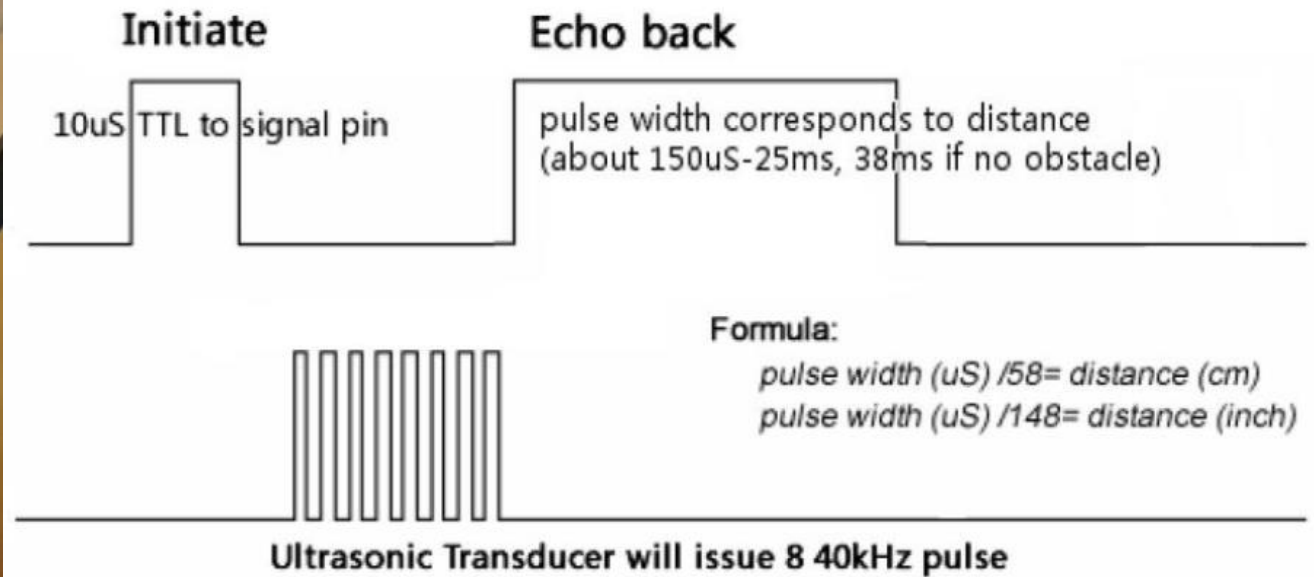
```
while True:
    counter += 1
    djv = Dejavu(config)
    song = djv.recognize(MicrophoneRecognizer, seconds=10) # longer period provides more accuracy
    os.system('clear')
    match = song.get('song_name')
    confidence = song.get('confidence')
    if match == 'evil' and confidence > 10: # we've 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



AstroDrone



- Either *launches* the drone upwards at speed
- 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) – using resonant frequencies to affect gyroscopic sensors
 - Luo (2016)

Animal repellent alarm

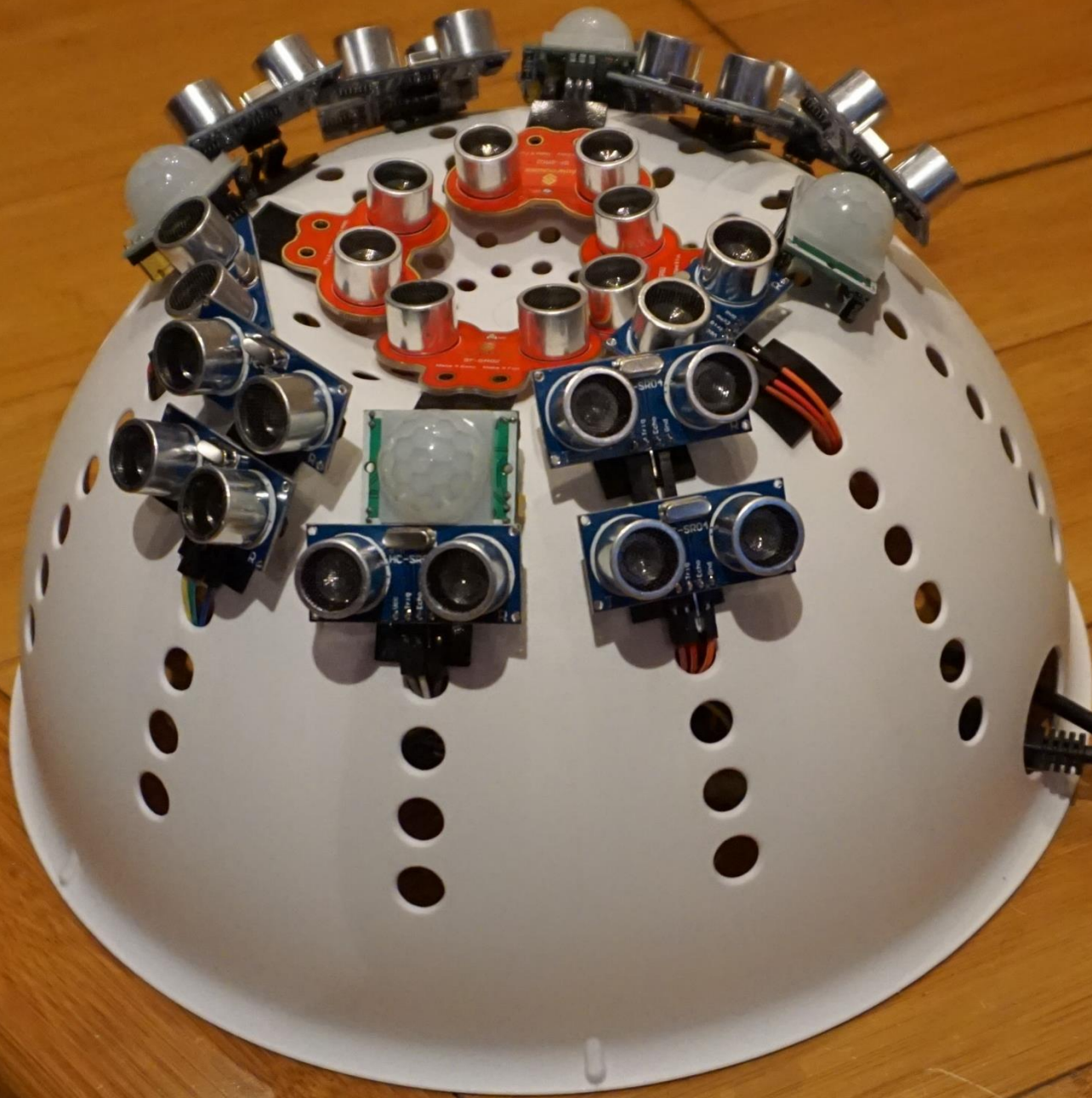
- PIR
- If high, sends out an ultrasonic pulse
- Adjustable frequency (0-50Khz)
- Adjustable sensitivity

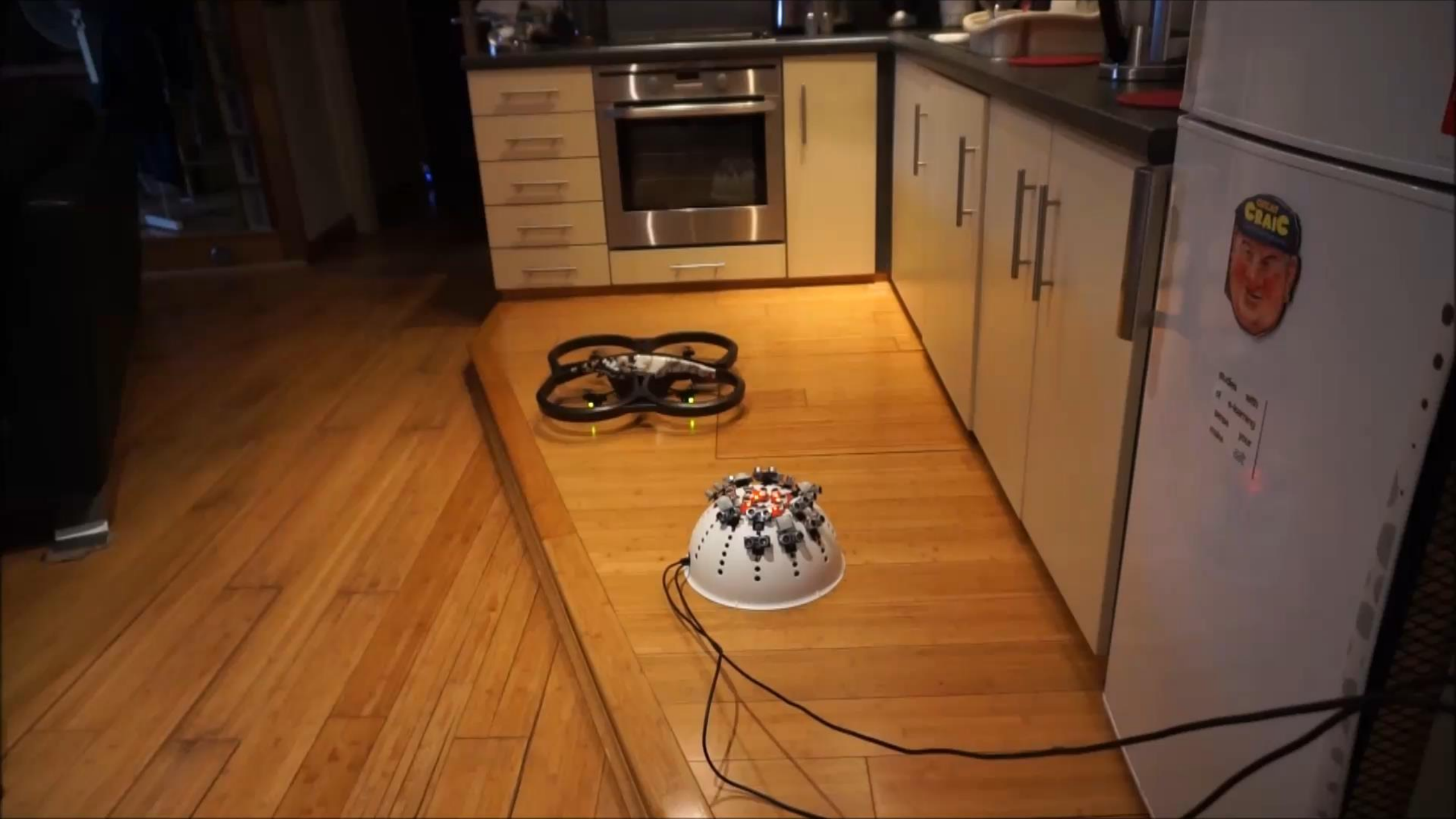




GOODNIGHT SWEET PRINCE







Radio	with
or	4-wire
wire	pin
pin	pin

Real-world applications

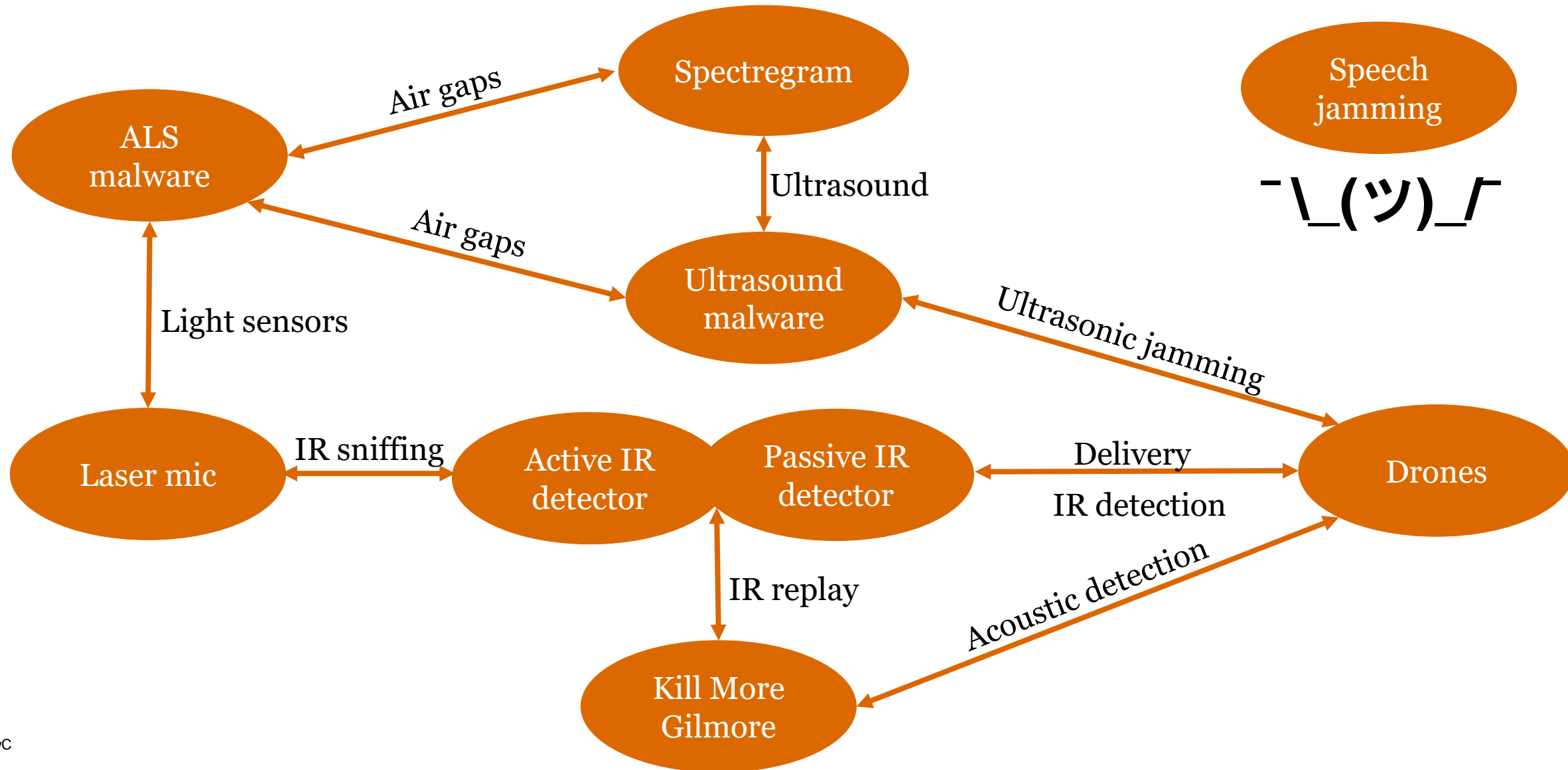
- Deploy on roof to keep drones away
 - Prisons
 - Government buildings
 - Public events
- Further research ongoing
- Personal drone protection 😊



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**

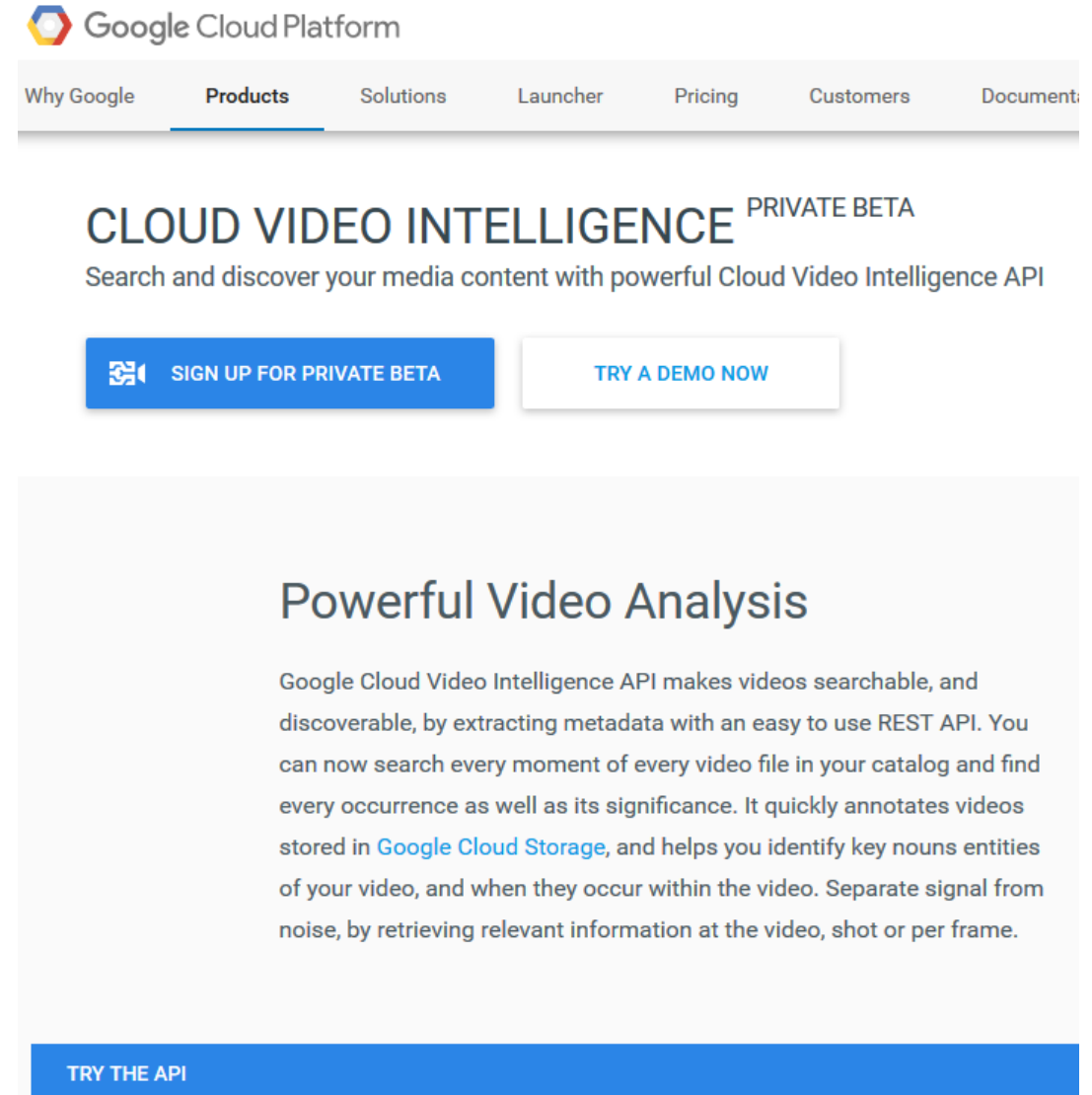
- Usually require proximity to targeted systems
- Subject to interference
- Range and power depend on resources

Mitigation

- 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
- More work on LiFi
- Further work on drone repellents
 - Tracking and targeting
 - Identification through video →
 - Combo of infrared and sound




The screenshot shows the Google Cloud Platform website for Cloud Video Intelligence. The header includes the Google Cloud Platform logo and navigation links: Why Google, Products (selected), Solutions, Launcher, Pricing, Customers, and Documentation. The main heading is 'CLOUD VIDEO INTELLIGENCE' with 'PRIVATE BETA' in smaller text to the right. Below this is the tagline 'Search and discover your media content with powerful Cloud Video Intelligence API'. Two buttons are present: 'SIGN UP FOR PRIVATE BETA' (blue) and 'TRY A DEMO NOW' (white with blue text). A section titled 'Powerful Video Analysis' describes the API's capabilities: making videos searchable by extracting metadata via a REST API, searching every moment of every video file, annotating videos stored in Google Cloud Storage, identifying key nouns/entities, and separating signal from noise. A blue button at the bottom says 'TRY THE API'.

Google Cloud Platform

Why Google Products Solutions Launcher Pricing Customers Document

CLOUD VIDEO INTELLIGENCE PRIVATE BETA

Search and discover your media content with powerful Cloud Video Intelligence API

 SIGN UP FOR PRIVATE BETA TRY A DEMO NOW

Powerful Video Analysis

Google Cloud Video Intelligence API makes videos searchable, and discoverable, by extracting metadata with an easy to use REST API. You can now search every moment of every video file in your catalog and find every occurrence as well as its significance. It quickly annotates videos stored in [Google Cloud Storage](#), and helps you identify key nouns entities of your video, and when they occur within the video. Separate signal from noise, by retrieving relevant information at the video, shot or per frame.

TRY THE API

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/>
- **Spectrogram 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](https://msdn.microsoft.com/en-us/library/windows/desktop/dd318933(v=vs.85).aspx)
- “Stealing sensitive browser data with the 23C Ambient Light Sensor API”. 2017. Olejnik, L.
- “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.
- <https://github.com/worldveil/dejavu>
- “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](https://twitter.com/darkartlab)