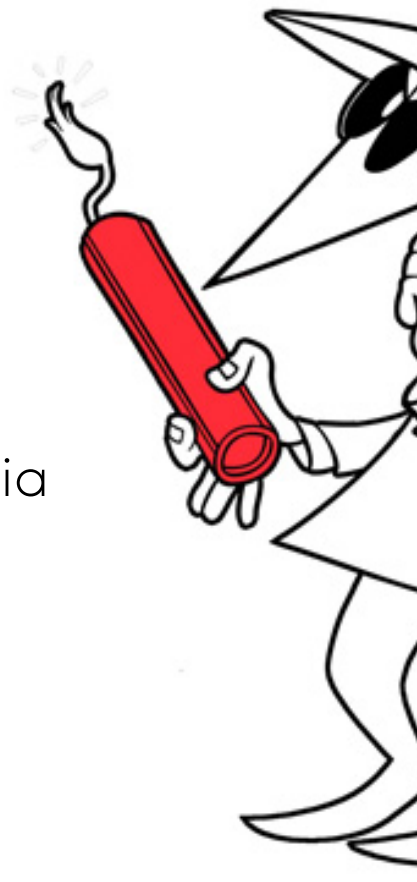
Spy vs. Spy

A modern study of mic bugs operation and detection



Veronica Valeros

@verovaleros

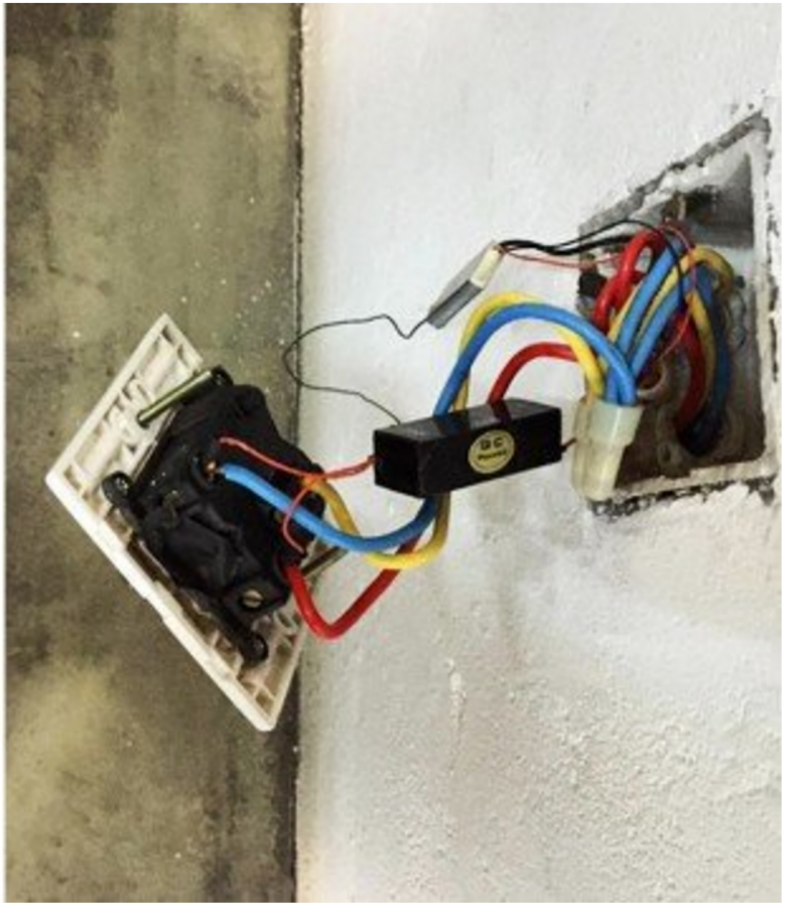
Sebastian Garcia

@eldracote

MatesLab Hackerspace

bit.ly/SpyBud

Audio eavesdropping is a threat



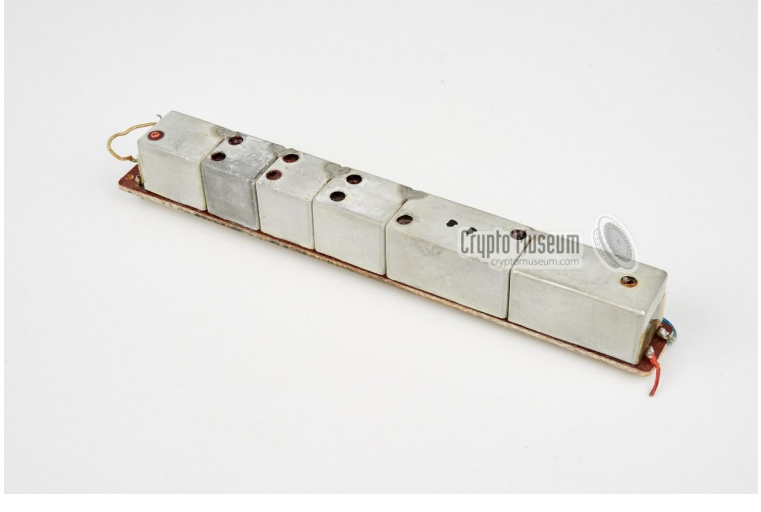
BEIJING - Dissident Chinese artist Ai Weiwei has posted photos on his Instagram account that suggest listening devices were planted in his Beijing studio.

A brief tour through the last century FM mic bugs

The Thing

KGB bug

TI-574A



OPEC

Mic Technology Advances

From lasers in the air to malware

Try all the Mics!

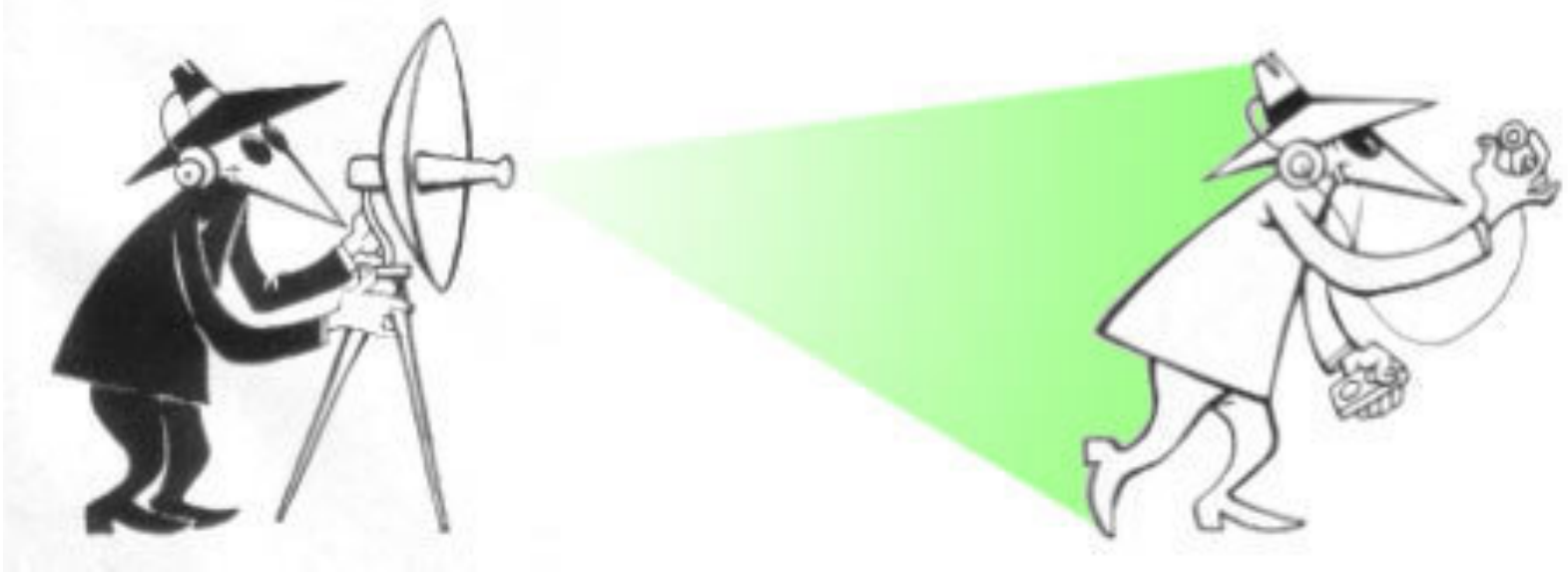
Comparison

Device	Type	Frequency	Range	Battery	Price
MicroSpy	Mic Bug	102MHz	500m	9v battery	15 USD
F-908	Mic Bug	113.5MHz	500m	9v battery	33 USD
EAR-1	Mic Bug	102.2MHz	500m	9v battery	18 USD
Beurer BY 84	Baby Monitor	864MHz	800m	3x AAA	65 USD
MiniA8	GSM bug /tracker	EU GSM	worldwide	3.7V 500mAh Li-ion	9.29 USD

MicroSpy **F-908** **EAR-1** **Beurer BY** **MiniA8**

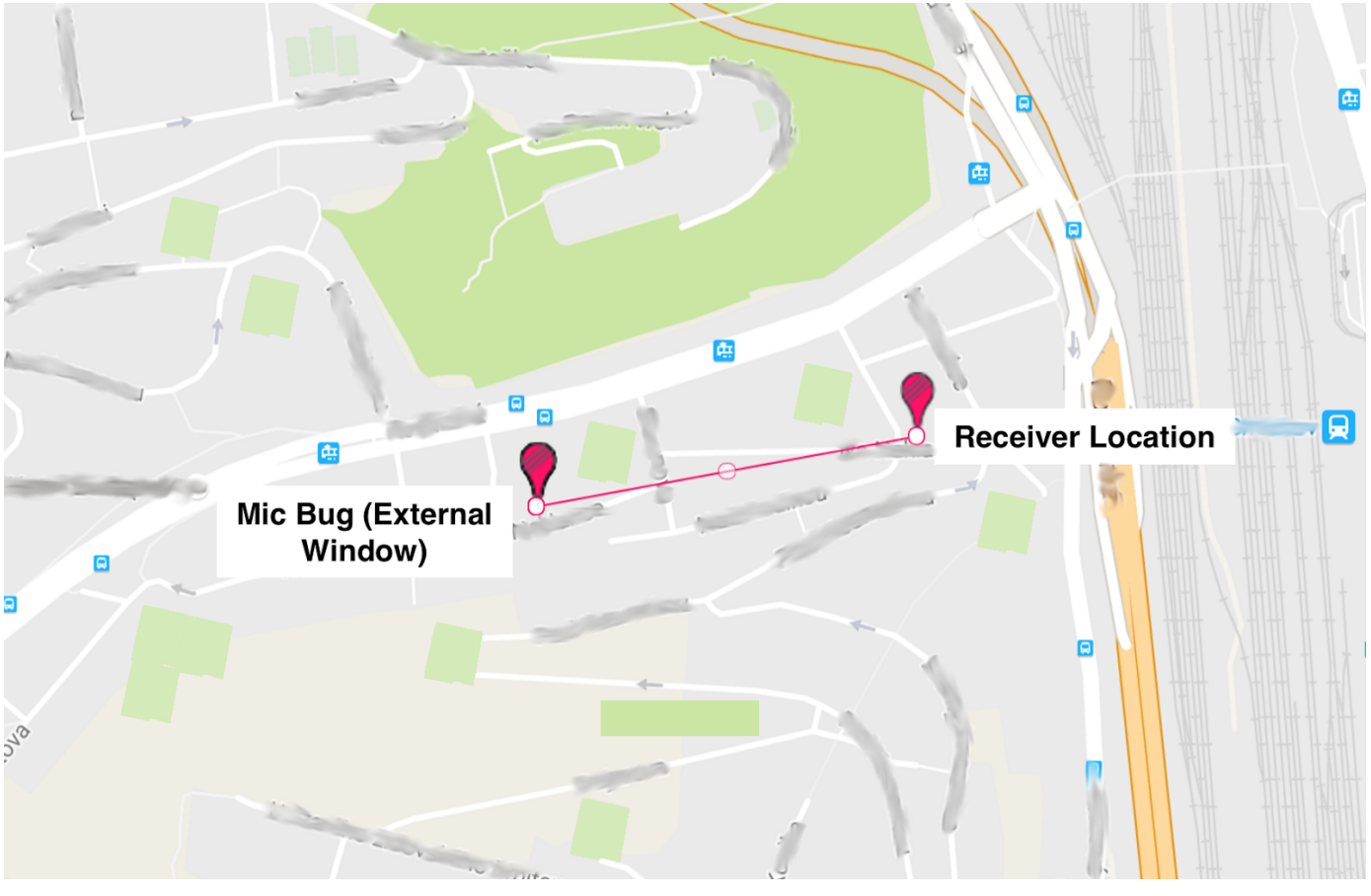


Listening Experiments



Listening Experiments

No need for a van in front of your house



Listening Experiments

Mic Bug Location	Receiver Location	Distance	Quality	Target
T_1	R_1	0.30Km	4/5	20cm from mic bug
T_1	R_2	0.32Km	4/5	20cm from mic bug
T_1	R_3	0.29Km	3/5	20cm from mic bug
T_1	R_4	0.23Km	4/5	20cm from mic bug
T_1	R_5	0.14Km	5/5	20cm from mic bug
T_1	R_6	0.07Km	5/5	20cm from mic bug
T_1	R_7	0.18Km	5/5	20cm from mic bug
T_1	R_8	0.31Km	3/5	20cm from mic bug
T_1	R_9	0.30Km	5/5	20cm from mic bug
T_1	$R_10 = T_1$	15m	5/5	5m from mic bug

Most mics have a lower battery autonomy than advertised

Geolocation Remarks

- Attackers need to be close
  - Good for you, filters your attackers
  - Bad for them, they need to be close
  - Bad for you, they **are** close
- Nobody can help from the Internet
  - Bad for you

Comparison with Malware

- A successful malware infection is not guaranteed
- Malware leaves traces. Others can find the attack.
- People from the Internet can help with Malware

Comparison with non commercial

- Battery vs. electricity
- Transmit vs. storage
- One-time conversation vs. all the time
- One time access vs. continuous access

Contact a company if you are in a life-threatening situation

Salamandra

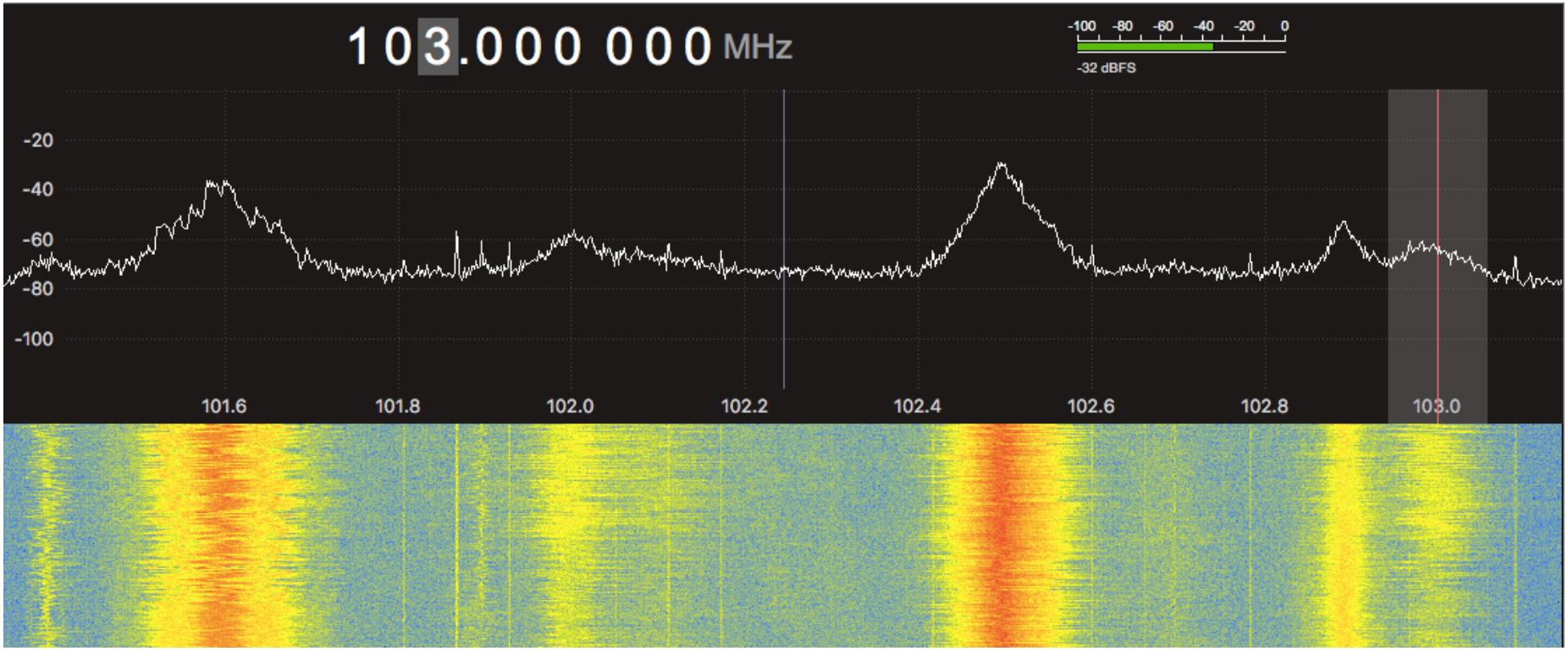
SDR-based, free software detection and location of hidden microphones

https://github.com/eldraco/Salamandra

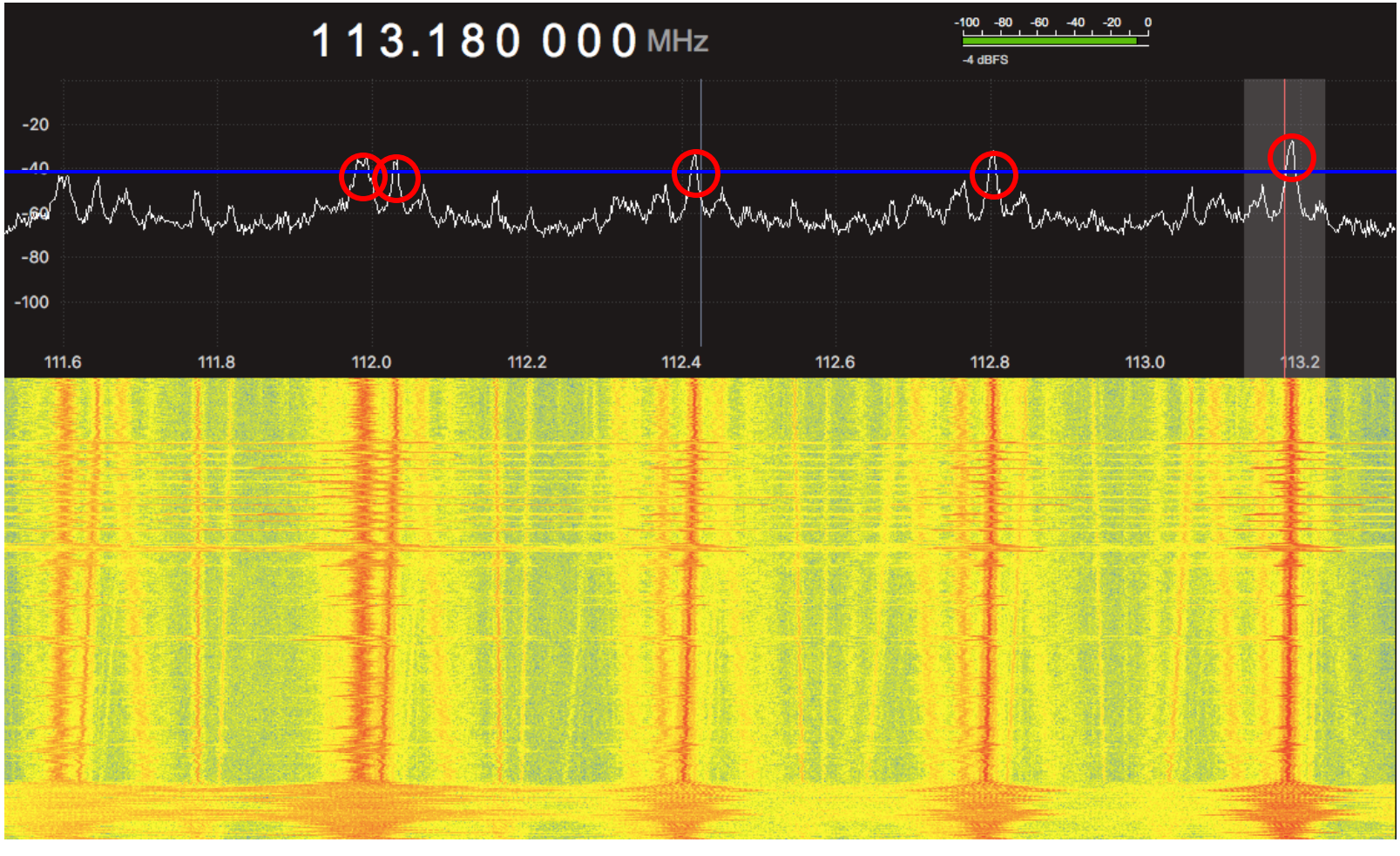
USB SDR device

DVB-T+DAB+FM

Normal FM Radio Station



Mic F908

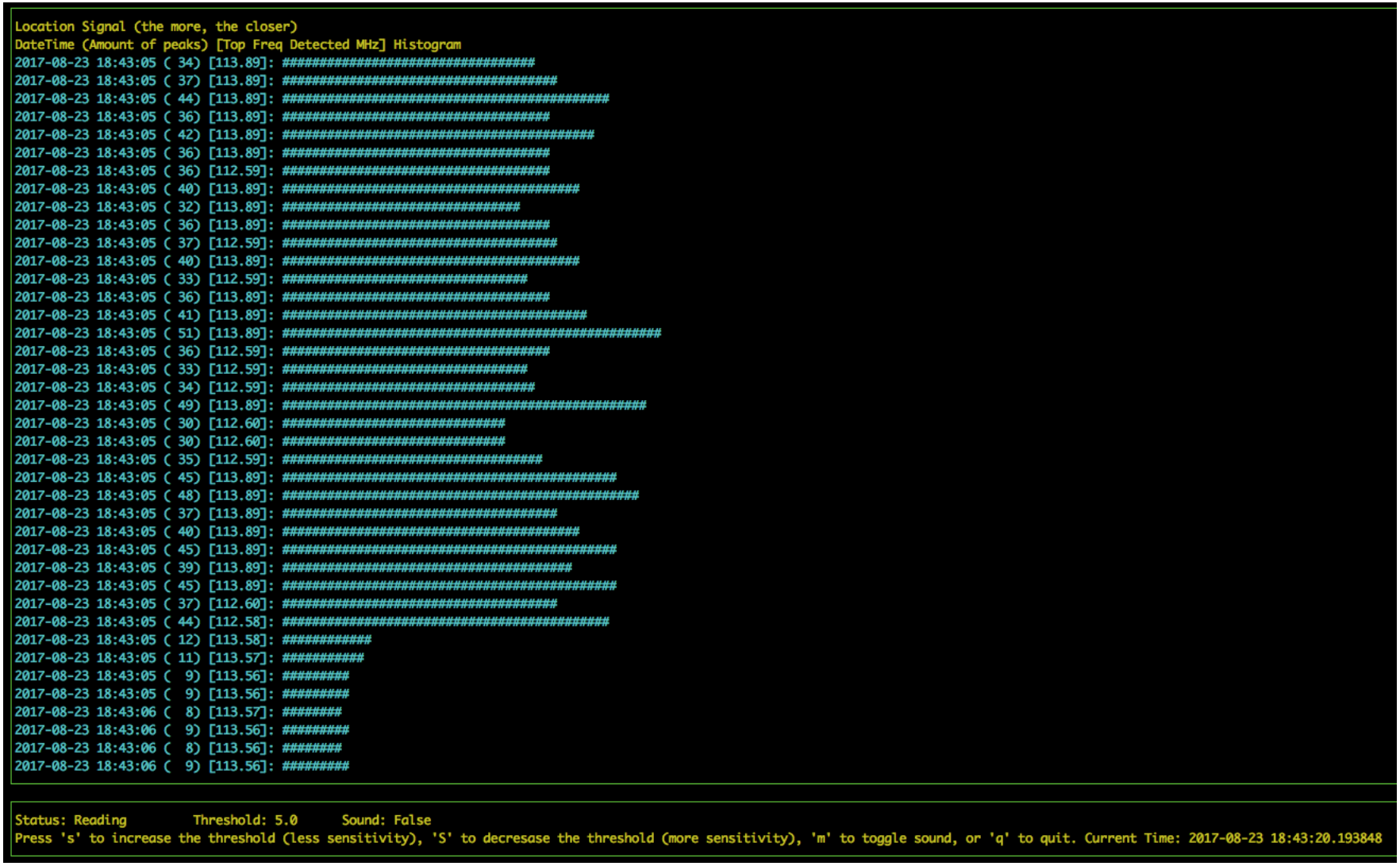

113.180 000 MHz
-100 -80 -60 -40 -20 0
-4 dBFS
-20
-40
-60
-80
-100
111.6
111.8
112.0
112.2
112.4
112.6
112.8
113.0
113.2

Detection Feature

- Trained thresholds with ~85 experiments
- Fixed the thresholds for the best detection

Th1	Th2	FM1	FPR	Acc	Prec	TPR	FP	TP	FN	TN
15	2	0.551	0	0.67	0.38	0.38	0	16	26	37
15.3	**2**	**0.5**	**0**	**0.645**	**0.333**	**0.333**	**0**	**14**	**28**	**37**
13	3	0.472	0	0.632	0.309	0.309	0	13	29	37
15	1	0.676	0.02	0.734	0.523	0.523	1	22	20	36
10	5	0.436	0.02	0.607	0.285	0.285	1	12	30	36
10.8	3	0.53	0.05	0.645	0.38	0.38	2	16	26	35
Ghost	**-**	**0.727**	**0.08**	**0.756**	**0.888**	**0.651**	**3**	**24**	**15**	**32**
7	3	0.714	0.08	0.746	0.595	0.595	3	25	17	34
10	2	0.704	0.108	0.734	0.595	0.595	4	25	17	33
10.8	1	0.735	0.114	0.756	0.862	0.641	4	25	14	31

Location Feature



Salamandra new features

- Detect and **locate** microphones
- You can use **rtl_power** to record and send the signal to others with Salamandra
- Profile your environment in different times and compare

Real Life Experiments

Experiments Methodology

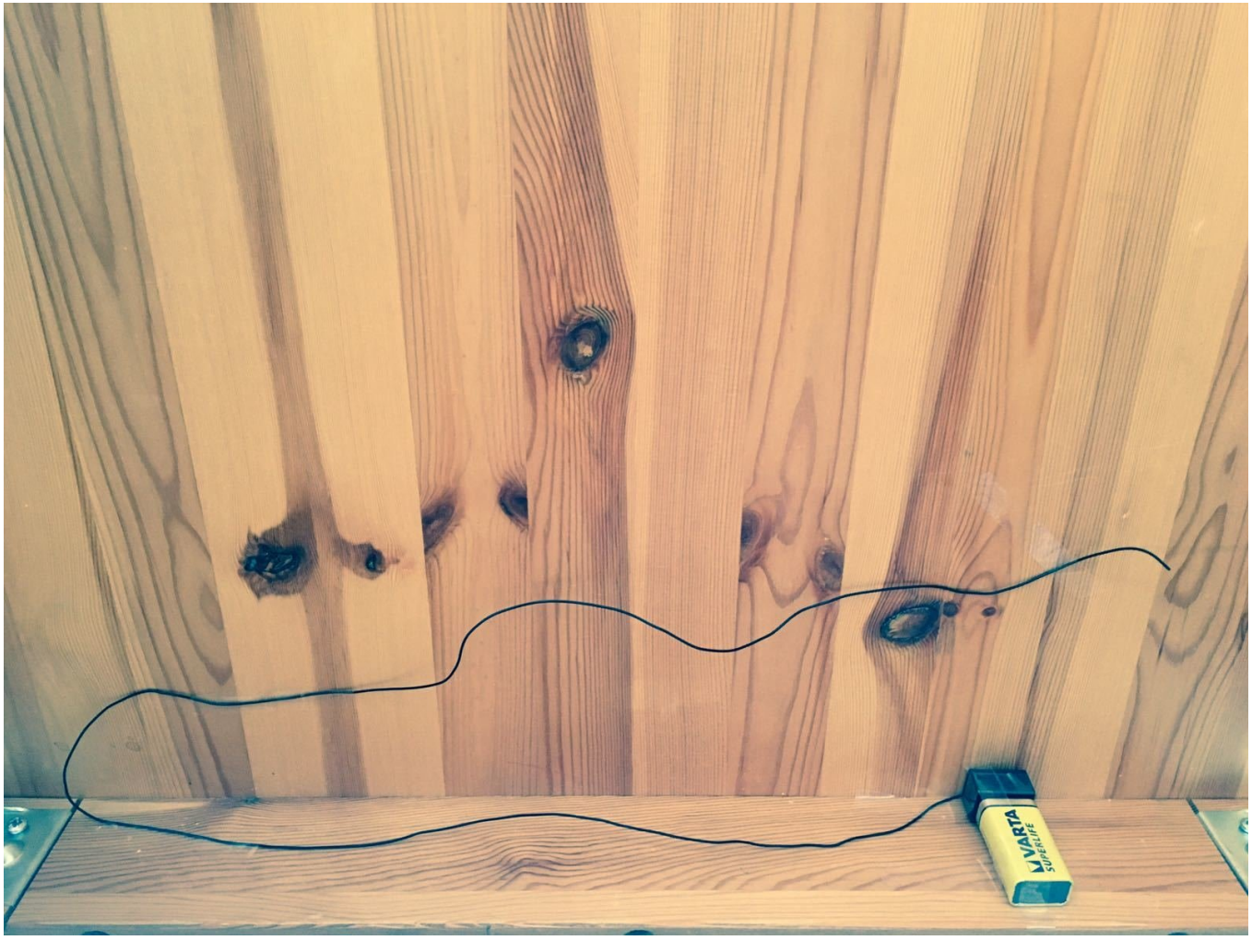
1. Seeker goes out. Hider hides mic (or **not**)
2. Seeker gets in. Speaks passwords. Hider tries to catch them
3. Measure time to detection
4. Measure time to location
5. Measure recall: (passwords heard / total passwords)

Real Life Experiments

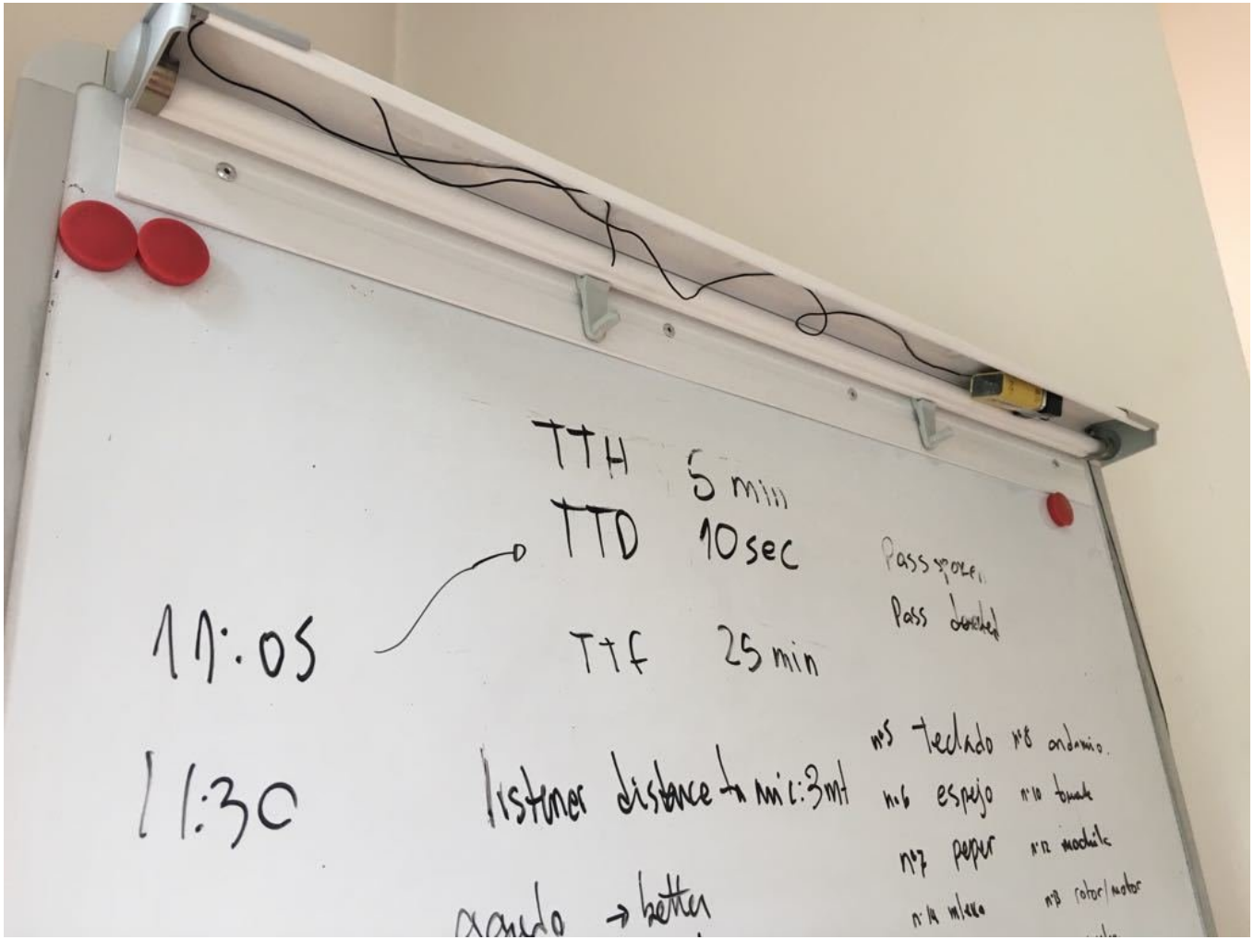
Exp. Id	# Mics Hidden	# Mics found	TTD	TTF
1	1	1	3s	40min
2	1	1	7s	40min
3	1	1	10s	25min
4	1	1	25min	-
5	1	1	3min	20min

Exp. Id	Passwords spoken	Passwords listened	Distance of the Hider	Ghost
1	10	10	5m	Yes
2	-	-	4m	Yes
3	16	13	2m	Yes
4	10	0	4m	No
5	10	5	6m	Yes

Real Life Experiments



Real Life Experiments



Experiments Conclusions

- Hiding is **hard**
  - Power, behavior, know your target, physical access
- Location is **hard**
- Listening is **hard**
- Detection is **fast** (w/Salamandra)
- Music doesn't hide your voice

Conclusions

- Audio eavesdropping is a real threat. Don't be fooled.
- Now you know how it works.
- Now you know how to protect yourself.

Try Salamandra, find mics.

Advance the field. Help others.

Questions?

Veronica Valeros

@verovaleros

vero.valeros@gmail.com

Sebastian Garcia

@eldracote

eldraco@gmail.com