Spy vs. Spy: A modern study of microphone bugs operation and detection

Veronica Valeros
MatesLab Hackerspace
Buenos Aires, Argentina
Email: vero.valeros@gmail.com

Sebastian Garcia
MatesLab Hackerspace
Buenos Aires, Argentina
Email: eldraco@gmail.com

***Abstract*—In 2015, artist Ai Weiwei was bugged in his home, presumably by government actors. This situation raised our awareness on the lack of research in our community about operating and detecting spying microphones. Our biggest concern was that most of the knowledge came from fictional movies. Therefore, we performed a deep study on the state-of-the-art of microphone bugs, their characteristics, features and pitfalls. It included real life experiments trying to bug ourselves and trying to detect the hidden mics. Given the lack of open detection tools, we developed a free software SDR-based program, called Salamandra, to detect and locate hidden microphones in a room. After more than 120 experiments we concluded that placing mics correctly and listening is not an easy task, but it has a huge payoff when it works. Also, most mics can be detected easily with the correct tools (with some exceptions on GSM mics). In our experiments the average time to locate the mics in a room was 15 minutes. Locating mics is the novel feature of Salamandra, which is released to the public with this work. We hope that our study raises awareness on the possibility of being bugged by a powerful actor and the countermeasure tools available for our protection.**

***Index Terms*—surveillance, microphone bugs, security, espionage.**

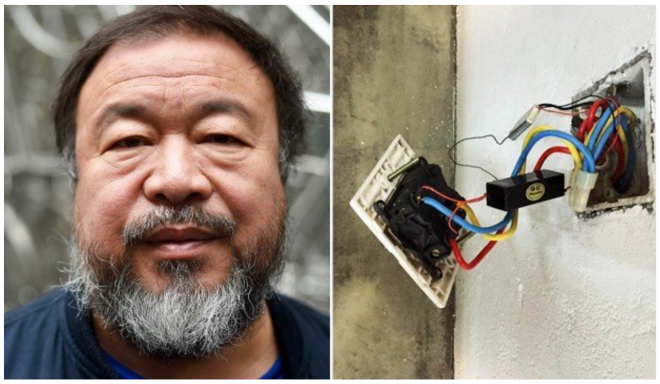
I. Introduction

In October 2015 the activist and artist Ai Weiwei found several microphones bugs hidden in electrical sockets all around his home and studio[1], [2], [3]. It is believed that the microphones were placed when he was detained in 2011, 4 years before their discovery. This event was the trigger of our investigation and it raised our concern about how little we know about the reality of placing, listening and locating microphones.

Most of what the general public knows about microphones bugs comes from movies and other fictional sources, which usually is far from real. An example of these inaccuracies is the public speculation made by the Counselor of the United States President, Kellyanne Conway, who expressed that a microwave oven can spy as a camera [29]; the answer is NO, as refuted in article by WIRED [30]. The current literature about microphones bugs is disturbingly scarce, leaving most people to believe the myths distributed by the media. One of the goals of this work is to debunk the fictional beliefs around mics bugs by performing a thorough study and real life experiments with them.

This paper is divided into three phases. First, we perform a survey of the state-of-the-art of mic bugs and their characteristics. Second, we develop our own free software detection tool, called Salamandra. Third, we perform several real life experiments on placing and detecting bugs to examine how difficult it was. Finally, we conclude with a thorough analysis of our experience.

The first phase makes a deep survey of all the civilian-accessible microphone bugs. It takes into account physical characteristics, frequencies, transmission modes, battery options, operational lifetime, operational listening distance, easiness of listening by the operator, advantages & disadvantages, configurations if any, and easiness of detection by various means. The end goal of the first phase is to show the difficulty in using microphone bugs.



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

Fig. 1. Bangkok Post (6 Oct 2015 at 00:41) - Dissident Chinese artist Ai Weiwei has posted photos on his Instagram account that suggest listening devices were planted in his Beijing studio.[4]

The second phase presents our free-software, SDR-based[7] tool to detect hidden microphones called Salamandra. Although a professional microphone search usually requires more complex hardware, we show that a simple SDR USB device and our tool can be used to detect the mic bugs accurately. Moreover, Salamandra has a novel location feature to find mics quickly; a feature that is not available in most commercial detectors. The two most important limitations of the hardware detection solutions are their false detection of mics and their false positive detections of ghost mics.

Salamandra uses several novel techniques to detect mics by taking advantage of its execution in a computer, including continuous discovery and location of mics.

The third phase consists in a group of offensive/defensive experiments on placing and detecting bugs in real life. While one of the researchers places the mics and tries to listen to meaningful spoken passwords, the other runs Salamandra to try to know if there was a mic and where. These real life experiments shone light about the difficulty of placing mics and how easy is to find them.

As far as we know this work is one of the few on the topic of analyzing the real performance of placing and detecting spying microphones. The main contributions of this paper are:

- As far as we know, the first scientific research on the topic of real life spy microphones.
- A novel free software SDR-based detection tool to locate microphone bugs, called Salamandra. A tool trained with real experiments.
- The first comparison of mic bugs characteristics, ranges and performance, based on field experiments in real life scenarios.
- The first experiments of real-life placing and detection of mics to analyze their performance, quality and time to detection.
- The first analysis of spy mics audio quality and improvement.

II. Microphone Bugs State-of-the-Art

The activity of eavesdropping can be considered as old as human civilization. Eavesdropping techniques were, and are, employed by different sectors of our society: governments, organizations, families, and individuals. The main motivation behind the use of these techniques is always the same, the *need to know* directly from the source.

The advances on eavesdropping techniques went hand by hand with the advances in audio communication. In 1844, as explained in the Audiosurveillance chapter by the CIA operative Alfreed Hubest [9], the first telegraph for commercial purposes was installed in the US. It was quickly followed by the civilian interception of such messages. In 1862, the Telegraph messages interception was prohibited in some states of the US. Similarly, commercial telephones were installed in 1878, soon followed by telephone tapping, which was finally prohibited, on the State of New York, in 1892 [9]. In 1902, the first wireless radio message across the Atlantic was sent by Guglielmo Marconi[10]. Shortly after, Rudyard Kipling published a fictional tale in the Scribner's Magazine [11], where he described the eavesdropping of wireless radio transmissions. From this moment on, audio surveillance became widely used by intelligence agencies and other parties [10], [9] until today.

The area of audio surveillance has been very prolific in the last century. Hundreds of different devices have been manufactured for public consumption and for government purposes. Audio eavesdropping devices can be classified in four broad categories: microphone bugs, phone wire taps, wires (on your body), and malicious spying software, known as Spyware.

Fig. 2. The Great Seal Bug, also known as The Thing, was a passive listening device invented by the Soviet Union at the end of the Second World War.

Microphone bugs can also be portable, wearable, or stationary. This work will focus on wireless stationary microphone bugs, primarily FM and GSM devices, which are the most accessible in today's market. An exhaustive enumeration of such devices is out of the scope of this work. Instead, we highlight devices that stood out and are worth mentioning.

A. FM Audio Transmitters

FM transmitters were heavily used in the past and are still used today at some extent. The simplest devices transmit on a fixed frequency, while others allow an adjustment of the range of frequencies. Most of the commercial mics are powered by 9v removable batteries, which may last from 6hs to 5 days after placing the microphone (see Subsection VII for more details). The performance of these devices strongly depends on the general location (indoor, outdoor, residential location or workplace), surroundings of the mic bug (placed near cables, radios or hardware equipment), and the positioning of the antenna (stretched, coiled). Audio quality will depend on the physical distance between the surveillance team and the target; most microphones have a good working range of 500 meters or more in an open field.

The Great Seal Bug, also known as The Thing, was a passive listening device invented by the Soviet Union and used at the end of the Second World War. The device "(...) carving contained an HF radio bug of a novel design, in that it didn't have its own power source and was not connected via wires. Instead, the device was *illuminated* by a strong radio signal from the outside, which powered and activated it. It gave the bug a virtually unlimited life and provided the Soviets with the best possible intelligence." [15]. The size of The Great Seal Bug was extraordinary (See Figure 2) and still fulfilled its purpose. The bug was hiding in plain sight on the US Embassy in Moscow and it was discovered, by accident, after seven years [15]. Another example is the device known as Satyr [16], that was developed by the British government shortly after the discovery of The Great Seal Bug, sharing the same characteristics.

The development of the transistor in 1947 [17] enabled the creation of smaller listening devices. The KGB Bug, one of the first Soviet transistor-based bugs, was created around 1964. It was very small, 75mm x 23mm x 10mm, and contained three

Fig. 3. The KGB Bug, one of the first Soviet transistor-based bugs, created circa 1964. Size 75mm x 23mm x 10mm. Adjustable frequency.

Fig. 4. The Czechoslovak TI-574A was a modular FM transmitter, could be combined to achieve different functions, such being as transceiver, remote control unit, remote control bug and homing beacon. Size 150mm x 20mm x 15 mm.

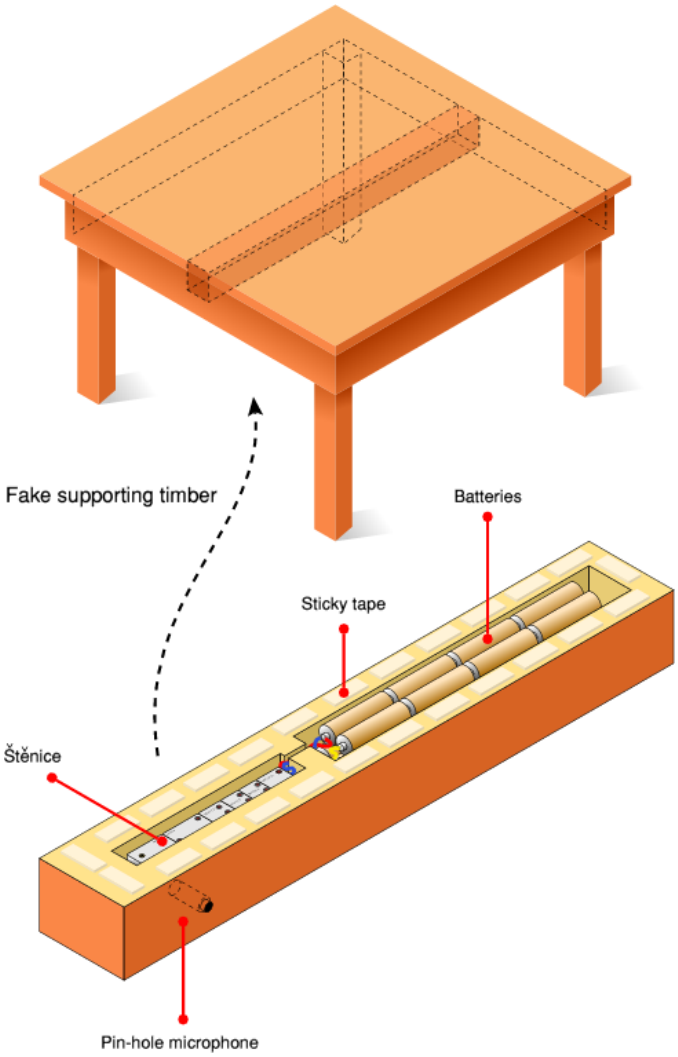


Fig. 5. The Czechoslovak TI-574A was widely used for domestic surveillance, used in common places such as tables.

pins, two of them for power supply and one for connecting the antenna. This device contained two small screws for tuning and adjusting the frequency. An example of this type of device is shown in Figure 3.

A very interesting example is the modular FM microphone bug that was designed in the Czechoslovak Republic in 1968 [12]. This bug, known as TI-574A, consisted in a customizable and modular transmitter that could be combined with other pieces to provide more functions. Modular functions were for example, being "part of a transceiver, a remote control unit, a homing beacon or even a remote controlled bug." [12]. A leaked design of the bug can be observed in Figure 4, and an example of how it was commonly used can be seen in Figure 5. The device was able to transmit, by adjusting the frequency, in the 74-88MHz range, which was ideal for not interfering with normal FM radio frequencies.

One strong limitation of typical microphone bugs is the power supply. Devices such as The Thing were rare, and typical FM mic bugs need a power supply to work. This need of power was, in many cases, very limiting. In this area, the OPEC bug was innovative. Its name was after its first discovery in Vienna in the late 1970s, in the headquarters of the Organization of the Petroleum Exporting Countries (OPEC). The OPEC bug was one of a kind because it did not have its own power, but instead it got powered by electromagnetic induction by placing it near electric wiring [19]. This innovative way of powering itself made it very difficult to be detected. An picture of this device is shown in Figure 6.

Nowadays, FM microphone bugs for commercial use are widely available in online stores such as Ebay [20] and Amazon [21]. The devices available on such sites and similar vary slightly on size, prices and range. For this research, restricted by a limited budget, we selected four devices to study: MicroSpy, F-908, EAR-1 and a Beurer BY 84 FM baby monitor. A common characteristic of these devices is that all of them are powered by removable batteries, giving them more

Fig. 6. The OPEC Bug, discovered in the late 1970s, was powered by electromagnetic induction.

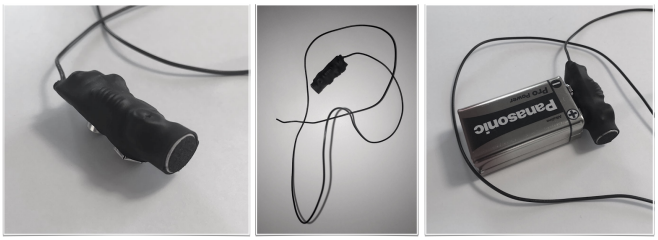


Fig. 7. Microphone Bug 01 - MicroSpy FM transmitter. Size 35mm x 10mm, 3-12v. Adjustable frequency. Advertised range up-to 500m in open field. One week of life on battery. Price: 15 USD.

flexibility for hiding and moving them to different locations. Other FM microphone bugs that use a different power supply method, such as those designed to be placed in wall power sockets, have the advantage of being more standalone in terms of battery but they are harder to hide and replace.

The MicroSpy is a FM transmitter available in Ebay for 15 USD [22]. This model is very small, with a size of 35mm x 10mm. It is powered by a 3-12v battery, which can last up-to one week. It allows the frequency to be tuned by adjusting a small screw near the extreme of the microphone. In theory, this model can transmit in a range up-to 500 meters in an open field. The MicroSpy can be observed in Figure 7.

The F-908 is a FM transmitter available in Ebay at 33 USD [24]. The device comes with a receiver, which is tuned to listen to the same frequency as the device. The device is slightly bigger than the MicroSpy, measuring 78.8mm x 50.0mm x 16.5mm. The F-908 is powered by a 9v battery. Its frequency cannot be adjusted. In theory, this model can transmit in a range up-to 500 meters in an open field. The F-908 model can be observed in Figure 8.

The EAR-1 is available in Ebay at 18 USD [23]. This model is bigger in size as the transmitter and the battery are slightly separated. It is powered by a 9v battery, which is advertised to last for 100 hours in continuous use (4-5 days). The frequency of the device can be adjusted through a screw in the base of

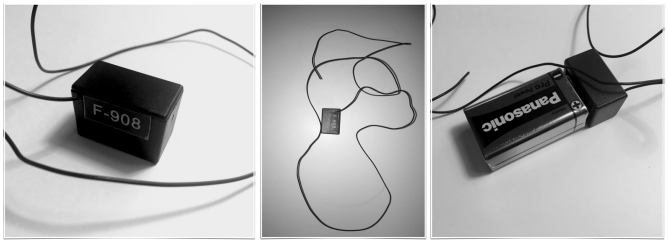


Fig. 8. Microphone Bug 02 - F-908 FM transmitter. Size 78.8mm 50.0mm 16.5mm, 9v. Not adjustable frequency. Advertised range up-to 500m in open field. Price: 33 USD.

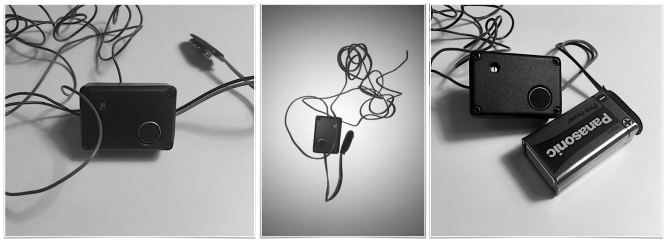


Fig. 9. Microphone Bug 03 - EAR-1 FM transmitter. Powered by 9v battery. Adjustable frequency. Advertised range up-to 500m in open field. Advertised 100 hours of continuous use. Price: 18 USD

the microphone. In theory, this model can transmit in a range up-to 500 meters in an open field. The EAR-1 model can be observed in Figure 9.

The Beurer BY 84 is an audio monitoring device designed to monitor babies, and is available in several online stores [25]. This model comes in peers, one transmitter and one receiver. The size of the devices is 6cm x 4cm x 11cm, weighting 398 grams each.The transmitter is powered by three 1.5v batteries, and is advertised to last 22 hours of continuous use. This model has two available frequencies, operating around 864 MHz. In theory, this model can transmit in a range up-to 800 meters. The Beurer BY 84 can be observed in Figure 10.

Table I summarizes the characteristics of the five selected devices for our experiments, including frequencies used, prices, type of battery used, and advertised range.

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

TABLE I
THIS RESEARCH IS FOCUSED PRIMARILY ON FOUR FM MICROPHONE BUGS AND ONE GSM MICROPHONE BUG. THIS TABLE SUMMARIZES THEIR CHARACTERISTICS, INCLUDING DEVICE TYPE, FREQUENCY, RANGE, BATTERY AND PRICE.

Fig. 10. The Beurer BY 04 is an audio monitoring device designed to monitor babies that operates in the 864 MHz. Size 6cm x 4cm x 11cm. Anyone with a receiver in that frequency can listen to its transmission.

B. GSM Audio Transmiters

While FM radio transmitters were heavily used in the past, nowadays the GSM microphones are more common. One of the main advantages of these devices is the size: no need of a long antenna, and the space of the typically embedded Li-ion battery is far smaller than a normal 9v removable battery.

One of the disadvantages of the GSM microphones is the large data fingerprint they leave. If one of this devices is found, its SIM card can reveal its own phone number and other stored phone numbers. Leveraging this information the phone operator can identify which other numbers communicated with the mic bug, where they were and when they listened. It is also possible to know when and where the number in the mic was active, perhaps during testing operations. In consequence, using a GSM phone can be dangerous in governmental situations.

There is a myriad of ways to conceal GSM microphone bugs: USB drives [27], power adapters [28], and others. GSM microphone bugs cost typically more than three times the price of common FM microphone bugs. In this category, the MiniA8 is one of the most affordable GSM microphones commercially available [26]. This device is small, with a size of 4.2cm x 3cm x 1.2cm. This model is powered by a Li-ion rechargeable battery of 3.7V 500mAh, which is advertised to last 12-15 days in stand-by or 5 hours of continuous use. The device operates in the following GSM frequencies: 850 / 900/ 1800 / 1900 MHz. A model of the MiniA8 can be observed in Figure 11.

III. Salamandra Detection Tool

The discipline of finding microphones is part of a group of techniques usually denoted TSCM [6] (Technical Surveillance Countermeasures). These techniques usually involve complex and expensive hardware used by expert technicians. If there is a very important need for finding mics, we suggest to secure the services of these professional companies. However, with

Fig. 11. Microphone Bug 04 - MiniA8 GSM Transmitter. Size 4.2cm x 3cm x 1.2cm, 3.7V 500mAh Li-ion battery. Advertised 2 hours of continuous use and 2 days on standby. Price: ĩ3 USD.

the proliferation of advanced technologies for the common citizen there may be more need for being sure that no listening devices are used at homes or workplaces, and in these situations is where there is a lack of tools. Although there are some cheap hardware detection devices available, there is an important lack of free software Software-Defined Radio (SDR) [7] tools available for the common user. To fill this gap and also to experiment with our own detection techniques we developed a proof of concept tool called Salamandra that uses a cheap SDR USB device to detect hidden microphones. Salamandra can be downloaded from its GitHub repository *https://github.com/eldraco/Salamandra*.

The goal of Salamandra is to **detect** and **locate** hidden microphones. To fulfill the goal of **detecting** microphones Salamandra uses the known technique of finding peaks in the power of electromagnetic transmissions. This technique is based on the fact that energy is needed to generate an electromagnetic signal in some frequency. Therefore, transmitting data in some frequency will generate a peak of power in the given frequency. This is a known and common technique used by most hardware detectors. The main problems with this technique are (1) that the origin of the frequency transmission in unknown and therefore is not known what is being detected; and (2) that there are microphones that do not transmit in this way, or do not transmit at all.

The second goal of Salamandra is to **locate** microphones. This is a much more difficult task and it is the core of Salamandra. The location technique used in Salamandra is based on the idea that the closer the receiver is to a signal power source, the more noise received, the more the frequencies overlap and the more the receiver can interact with them. The noise and overlapping always results in several simultaneous power peaks in neighborhood frequencies.

This overlapping and noise can be better be seen using a waterfall spectrogram. Figure 12 shows the frequency patterns of normal FM radio as seen by a waterfall spectrogram. The peaks are clear, well defined and do not overlap easily. In contrast, Figure 13 shows the frequency patterns of the microphone F-908 when receiving voice and somebody counting from one to ten.

Salamandra operates in two modes: **detection** and **location**. Although it is true that the location function also detects microphones, sometimes it is useful to have a clear detection

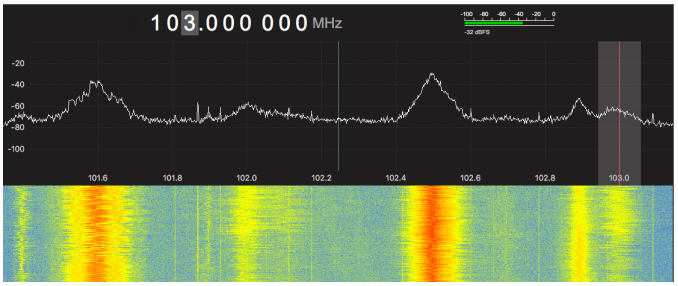


Fig. 12. Normal FM radio transmissions. The pattern of frequencies is clear and precise. There are no overlaps and the noise is minimum. This is in part because of the radio stations being far away.

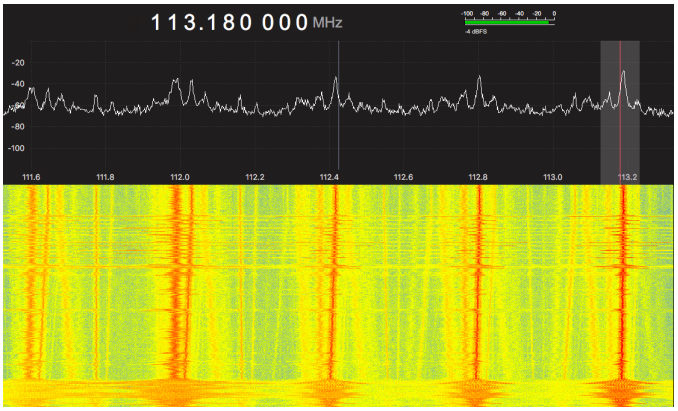


Fig. 13. Radio transmission of microphone F-908. The proximity to the mic makes the spikes more accentuated, the overlap with other frequencies larger and there is a small drift in the frequencies.

from Salamandra. One of such situations is when Salamandra reads signals from stored files.

The location function used in Salamandra is based on the notions of frequency overlapping and noise. For implementing the location function it is necessary to compute two values. First, it is necessary to find a threshold value for the power measurement that defines when a signal is considered *detected*. We call this value the Threshold 1. If any frequency overcomes this value, it is considered as part of the detection. The second value that Salamandra needs to compute for the location is the amount of different frequencies over the Threshold 1. Using this count it is possible to see how far away Salamandra is from the microphone.

The main features of Salamandra are:

- It is free-software, therefore adaptable.
- It can detect microphones transmitting in any frequency supported by the SDR device used.
- It was trained to detect microphones with maximum accuracy.
- It can detect microphones in real time.
- It can detect microphones offline from signals pre-captured and stored on hard-disk.
- It can locate microphones with good precision.
- It is highly configurable and adaptable to different situations.
- It can be tuned to a specific frequency for better results.
- It can optionally make a sound when a mic is detected.
- It can optionally make a sound when the receiver is getting close to a mic.

The following Subsections cover the operation of Salamandra, the source of signals, the training of its thresholds, the experiments where we compared it with a hardware detector and the final analysis of the results.

A. *Rtl_power Tool as Source of Data*

Salamandra receives as input data the CSV formatted lines from the output of the rtl_power tool [13]. The rtl_power tool is a simple FFT [14] logger for RTL2832 based DVB-T receivers [32]. It measures the differences in power levels on a given frequency range and produces a CSV file with the results of its measurements averaged over a time period. Each CSV output line has the following information:

- Date.
- Hour.
- Start frequency.
- End frequency.
- Frequency step in Hz (bins).
- Amount of samples in this line.
- For each frequency the value in dBm.

An example CSV line of rtl_power is:

```
2016-09-25, 17:40:32, 88000000,
90798210, 5465.26, 16, -37.1, -40.3, -39.8
```

The device selected for this experiment is the DVB-T+DAB+FM device, with the Realtek, RTL2838UHIDIR, chipset [32]. Figure 14 shows this device as it is advertised, its frequency range goes from 50Mhz to 1,760Mhz. We selected this cheap device to allow anyone to run Salamandra and find microphones in their houses.

Instead of accessing the SDR device directly, Salamandra uses the rtl_power tool to get the data because its quite difficult to read and interpret the electromagnetic signals. In that regard, rtl_power works very well and we have no intention of re-doing its work. This decision is important because it also means that users can store the readings of rtl_power for later analysis. A very important application of this separation is that it allows the creation of signal fingerprints files, that can be used to detect hidden microphones in the future. Their use may be as follows: First, the user makes sure that there are no mics on the room. Second, rtl_power is used to store the electromagnetic fingerprint on the room for several hours. Third, the file is stored. Fourth, when a check is needed, the user can re-take a fingerprint with rtl_power and compare it with the original one using Salamandra on both.

B. *Training the Thresholds of rtl_power*

Salamandra uses the rtl_power tool to obtain the signals, and it does it in two modes. In the first mode, Salamandra runs rtl_power internally and uses its output as values for the detection. In the second mode, Salamandra reads a CSV file from disk as it was created by rtl_tool. In both situations

Fig. 14. The USB device used in our experiments, a DVB-T+DAB+FM device, with the Realtek, RTL2838UHIDIR, chipset.

Fig. 15. The Ghost hardware microphone and camera detector. It was used to compare Salamandra against a known working bug detector.

Salamandra uses the data in the same way. However, it is important to find the best configuration of rtl_power in order to have consistent detections with maximum performance. This subsection shows how we trained the values used by rtl_power.

The capture of electromagnetic signals is a complex topic and it depends on several parameters. In order to train the thresholds of the rtl_power tool that maximizes the detection in Salamandra, we developed a group of experiments in different locations and conditions. The experiments consisted in running rtl_power with different configurations, and at the same time running the Ghost hardware detector [33] and Salamandra to see which combination of parameters generated the best results. The rlt_power commands run are variants of this example:

```
rtl_power -f50:1670M:4000Khz -g 25
          -i 1 -e 1h fmX.csv
```

The parameters that could be varied were: Start frequency, End frequency, Frequency step, Integration interval and Gain. The Start and End frequencies depend on which microphone needs tobe detected and most of the times they are fixed. After a large set of experiments for training rtl_power, we finally found the best set of parameters :

- Start Frequency: 50Mhz
- End Frequency: 1,760Mhz
- Step Frequency: 4,000Mhz
- Integration Interval: 1 second
- Gain: 25

The Start frequency, End frequency and Step frequency are intimately related and deserve a deeper study to find the best combination. They are related to the bin size for the Fast Fourier Transform and the optimal sampling frequency for that range.

C. Training Salamandra Thresholds for Detection

In the detection mode of Salamandra, the idea is to read the signal data and determine if there is a mic present or not. This type of work is called classification and in order to be precise, Salamandra should be trained carefully. Training Salamandra means to find the thresholds that offer the best performance, measured in the amount of mics detected and the amount of mics missed. The thresholds that can be tuned are two: First, the power level that the signals must overcome to be considered a mic, called Threshold 1. This threshold can be adjusted in Salamandra with the parameter -t. Second, the amount of frequencies that must overcome Threshold 1 in order to be considered a detection, called Threshold 2. This threshold can be adjusted in Salamandra with the parameter -F. A detection is made if the experiment overcame the Threshold 2. Only evaluating Threshold 2 is enough since it depends on Threshold 1.

The best way to know if Salamandra really works is to compare it, during the experiments, with other current solutions. For this purpose we compared Salamandra against a commercial hardware detector called Ghost [33]. Ghost is designed to detect any microphone or hidden camera in the frequency range 100Mhz-2,600Mhz. It includes two buttons, for detecting in different ranges of distances (up to 5m and 10m). The device alerts the presence of a microphone by a beeper and flashing led. The idea behind the hardware detection is to recognize any strong peak frequency inside a room. Figure 15 shows an image of the Ghost hardware detector.

The methodology to run the experiments for training Salamandra was:

1) Decide to put or not to put a mic.
2) Run Salamandra with different values for its Thresholds.
3) Use the Ghost hardware detector to see if it finds the mic.

The evaluation of the experiments was done as follows. When there was a mic present and it was not detected, we counted a False Negative (FN). When there was no mic and there was a detection, we counted a False Positive (FP). When there was a mic and there was a detection, we counted a True Positive (TP). When there was no mic and there was no detection, we counted a True Negative (TN). In this way, we can complete a confusion matrix and compute performance

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

TABLE II
SUMMARY OF THE EXPERIMENTS TO TRAIN THE THRESHOLDS OF SALAMANDRA. THE RESULTS COME FROM MORE THAN 85 EXPERIMENTS IN DIFFERENT LOCATIONS AND USING ALL THE MICROPHONES. SALAMANDRA WAS COMPARED WITH THE GHOST COMMERCIAL HARDWARE DETECTOR. THE BEST THRESHOLDS FOR SALAMANDRA IN A GENERAL WAY ARE THRESHOLD1 = 15.3 AND THRESHOLD2 = 2

metrics such as Accuracy, Precision, Recall, False Positive Rate and F-Measure1[1].

We run more than 85 experiments in different locations and using all the microphones. After all the experiments, we evaluated each threshold used by Salamandra and its performance. Table II shows the summary results for all the thresholds used. Essentially the best thresholds are Threshold1 = 15 and Threshold2 = 2, where Salamandra can get a False Positive count of 0 with a respectable True Positive Rate of 38%. Although the TPR seems low, it is still very good. This configuration of Salamandra is even better than the Ghost hardware detection.

According to the information in Table II, to run Salamandra similarly as the Ghost hardware detector the values of Threshold1 = 7 and Threshold2 = 3 should be used.

D. Salamandra Location Function

The most useful and novel feature of Salamandra is its location function. Locating microphones bugs can be very difficult, not only because they are hidden, but because the signal they generate can bounce in the objects of the room and causing interference. This is why the location function of Salamandra is a continuous process that shows an estimation of how close or far away the receiver is from the mic.

The technique used for location is based on the fact that when the receiver is close to a transmitting microphone, the strength of the signal overlaps with other frequencies and adds noise. By measuring this overlapping and noise it is possible to know how close the receiver is to the microphone. Technically, Salamandra counts the amount of frequencies that overcome the Threshold 1 and prints this information as a histogram in time. Thanks to this functionality, the receiver can moved around and the strength of the noise and overlaps can be observed.

An example command for locating a microphone can be done with the following command. It uses a Threshold 1 (-t) of 0 for great sensitivity, the location function is active (-s), and sound is active (-S).

[1]https://en.wikipedia.org/wiki/Precision_and_recall

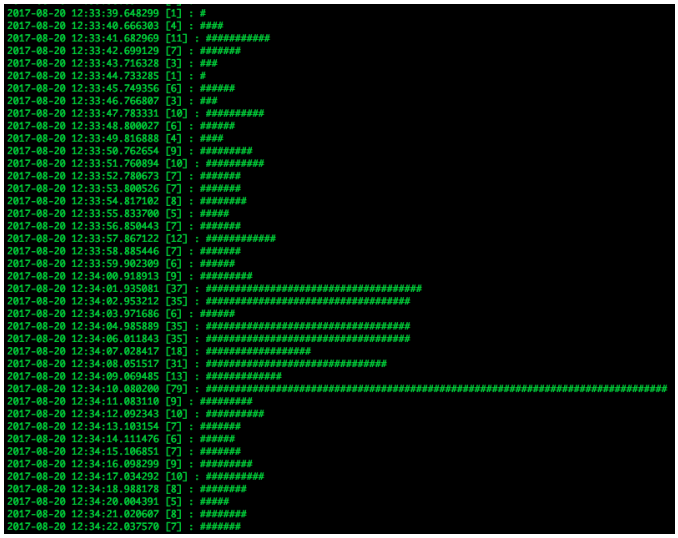


Fig. 16. Location function of Salamandra. It prints a histogram of the power levels received from the microphones. It can be seen as an estimation of the distance to the microphone and therefore used as a location feature.

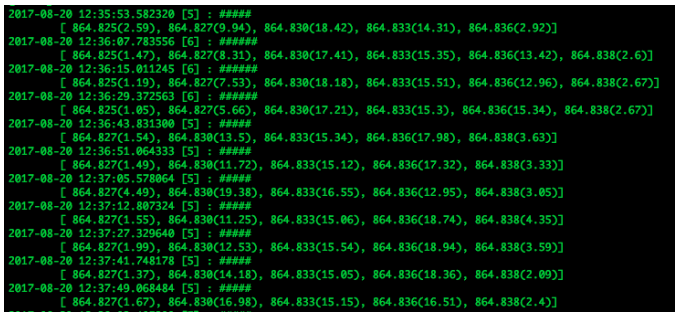


Fig. 17. Example of using verbosity >= 1 in Salamandra location mode. It can print the individual frequencies that trigger the detections. This is very important to find out if the detection is coming from a microphone, or radio station, or is an interference.

```
./salamandra.py -t 0 -s -S
```

Figure 16 shows an example run of Salamandra in location mode while finding the EAR-1 microphone (Figure 9). It can be seen that by moving away and closer to the mic the histogram changes.

Salamandra can be configured to have more verbosity in its output and this is important to obtain more information about the detection. If used with verbosity >= 1, Salamandra prints the frequency on which id did the detections. Figure 17 shows an example of using verbosity 1 while detecting the Baby Monitor (Figure 10) that it is known to transmit on the 800Mhz frequency range.

The most important feature of Salamandra on its location mode its the modification of the threshold to change the sensitivity of the detection. If a threshold (-t) of 0 is used, then any frequency over a dBm value of 0 will be counted for the histogram. In a normal home environment, the frequencies received from the outside are always below 0 dBm. A normal FM radio station, such as the ones received in a home, shows

power values up to -5.4 dBm. Therefore, a threshold value of 0 can be used as a minimum detection reference in a normal household. However, a -t threshold of 0 can be very noisy, so it is advisable to adjust it accordingly. Different thresholds will also vary the size of the histogram so it is more precise. A threshold from 5 to 10 would be more conservative.

E. Advantages and Disadvantages of Salamandra

To end up the Section about Salamandra we summarize the advantages and disadvantages of its usage compared with the common solutions in the market.

1) Salamandra is a tool designed to be adapted, modified and configured for each specific situation.
2) Salamandra can be used to locate microphones with good accuracy. Not only detect them.
3) It is possible to leave it running for long times (or continually) to monitor changes in the operation of the microphones.
4) It is possible to capture and store the signals with rtl_power and analyze them offline (or send to an expert analyst).
5) On location mode it is possible to walk around searching for mics. For monitoring a wide range of frequencies it is important to keep a slow pace.
6) The detection time is similar to the Ghost hardware detection.
7) The Ghost hardware detection runs out of battery and does not alert the user. In this situation, it will miss microphones and the user will remain unaware of this fact. This is a huge disadvantage, as there is not indication of this situation.
8) It is possible to modify the sensitivity of Salamandra to be more precise and fast, or to avoid frequencies that are know to not be microphones.
9) It is possible to obtain frequencies fingerprints of a place with rtl_power and store them for future comparisons.
10) Salamandra can be noiseless, allowing the user to detect a mic bug without alerting the attackers. This is in correspondence with an OPSEC practice[2]. Furthermore, this allows to perform counter-spy on the spies and record them when they collect the device.
11) Salamandra can find the exact frequency that is detected, giving more information to the analyst.
12) The Ghost hardware detector needs the constant input of the user to work, it cannot be used for continuous monitoring.
13) Given that Salamandra uses a computer, it is possible to listen to the suspicious frequencies to verify if they are a microphone or not. Using any spectrum analyzer tool, such as gqrx[3] it is possible to verify the detection. This is the ultimate detection: to tune the frequency and to listen to your own voice.

[2]https://en.wikipedia.org/wiki/Operations_security
[3]http://gqrx.dk/

IV. Real Life Experiments on Mic Planting, Listening and Detection

To understand the types of commercially available microphones for spying, as well as the hardware solutions to detect them, is an important first step. However, more important is to know how they are used, which are their advantages, disadvantages and common limitations. Testing this type of real scenarios is what gives information about how often the battery should be changed, how far away the listeners may be, what type of noise is possible to encounter, the best places to hide them and the time required for detection. The best way to obtain this information is to conduct experiments.

The goal of the experiments is to understand the operational characteristics and limitations of the microphones, the Ghost hardware detector and the Salamandra tool. The experiments were designed to be as real as possible and they followed a methodology so they can be compared. The structure of the experiments was:

- One researcher (the Hider) has 10 minutes to place, or not, one or more mics in the place.
- The other researcher (the Seeker), that was waiting outside the premises, gets into the place and has to declare as soon as possible:
  - If there are mics.
  - How many.
  - Where is each of them, by finding them.
- During the search, the Seeker has to say aloud 10 or more secret passwords for the Hider to listen.
- The Hider should be listening and trying to catch the passwords.
- The results of the amount of mics and passwords are compared.

The experiments and their results are summarized in Table III. Each experiment is compared with the hardware detector Ghost as a reference. In all experiments, the Hider used a F-908 Receiver[24] for its peer F-908 mic bug transmitter, and a ICOM IC-R6 communications receiver[31], which was tuned every time according to each mic bug frequency. The IC-R6 receiver is able to cover a range wide range of frequencies, from 100kHz to 1309.995MHz.

A. Experiment 1

The Hider hid the microphone F-908 (Figure 8) in the living room of the premises. It was visible if a person look closely for it, but not visible if a person just walk by. The Seeker entered the apartment using the search mode of Salamandra (the mic was not findable from outside the premises). Three seconds after the Seeker entered, there was a clear detection in Salamandra, so it was possible to make an early detection without problems. The localization took much longer. At the beginning the Seeker had some good and constant detections in the lobby, approximately 6m away from the mic (the Seeker did not know the position). The Seeker searched the lobby without success for some minutes. Then the Seeker moved to the living room and kitchen, where there was a stronger

signal, but mostly erratic. The problem was that different positions of the antenna gave different readings. The readings on Salamandra suggested that this was the correct room, but is was difficult to pinpoint the exact location. We learned later that the electromagnetic signal bounces too much on the walls to recognize the exact place precisely. The Seeker determined the two more probable places in the living room and started to perform a physical search on them. It took the Seeker almost 40min to find the hidden microphone. In this experiment there were no passwords said aloud. Conclusion: the search function of Salamandra must be improved to be more precise. This function was helpful approximately 75% of the time.

B. Experiment 2

In this experiment the Hider placed the microphone MicroSpy (Figure 7) in the back of a couch between two cushions. This microphone emits a weak signal so it was very difficult to detect and find. Similarly, the listening range also suffers, as so does the quality. Therefore some of the passwords were not found at all (but we couldn't compute the recall). Most importantly, this microphone is quite unreliable and it stopped transmitting several times because the battery got lose. The disadvantage of the position of the microphone was that it is normally used by the people in the house and therefore it risks an early casual detection. For this experiment Salamandra was better trained and was ready for a good detection. However, it became important the ability to change the sensibility of the detection in order to accommodate to weaker microphones.

C. Experiment 3

In this experiment the Hider taped the F-908 microphone (Figure 8) under the dinning table. This was a good place to hide it because it is not common that the people look under the table. The time to detection was 10s, very fast, and it was detected from 15m away. This mic was detected fast because it transmits with a strong signal. The strong signal is good for good reception quality and distance, but it is clearly its main weakness. Despite the early detection, the Seeker took 25min to locate the mic, which speaks of the good quality of the hiding place. From the 16 passwords said aloud, only 3 were misinterpreted, giving a recall (or sensitivity) of 81%. In this experiment the Hider was listening 3m away from the mic. It was interesting to see how our methodologies for hiding and finding microphones evolved. The hiding become more sophisticated and the search become more methodological. For example, a good search methodology was to start with high sensitivity (-t 0) until some detection was achieved very quick. Then, the frequency was identified and Salamandra was adjusted to focus on that frequency and to be a little less sensitive (-t 3). With the adjustements it was possible to locate the microphone much more quickly.

D. Experiment 4

In this experiment the Hider placed the EAR-1 microphone (Figure 9) behind a large speaker. The hiding place was good but not totally invisible. From the start of the experiment we realized that there was a problem. The Hider stop listening audio in the receiver and the Seeker could not detect the microphone for 25min. Even though the Seeker could detect a microphone it was incapable of finding it. Upon later inspection we found that the hiding place was among other electrical cables and those induce some type of interference with the transmission. When moved to another position and with its antenna fully extended, the mic was functional again and the detection on Salamandra was clear. During this experiment the Hider found 0 out of 10 passwords, a total recall of 0%. During this experiment the Seeker also had the problem of a spurious frequency interference. The frequency was close to the 200MHz and it was intermittent. Fortunately Salamandra prints the frequency of each detection, making it possible to focus on the frequency that was believed belonged to the microphone.

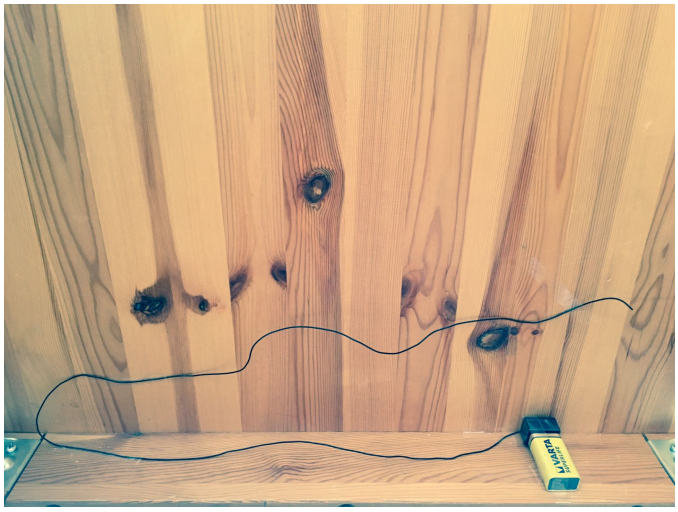


Fig. 18. Place where the mic F-908 was hidden during Experiment 3. The mic bug was tapped in one inner side of the table, making it hard to find. For experts performing physical searches, carefully trained for this activity, this place would not be a good choice, as the mic was visible in plain sight.

E. Experiment 5

In this experiment the Hider placed the microphone F-908 (Figure 8) in a very difficult place to find. The Hider was listening from 6m away and it was possible to perfectly listen to all the conversations in this large room. The detection of the microphone was done after 3min, which is still fast, but to pin point the physical location was much harder. Even though the Seeker could narrow down the position of the microphone with a 20cm precision, it was not possible to find it until 20min later. Figure 19 shows the place where it was hidden as it is normally seen by the inhabitants of the house, and Figure 20 shows the same place but now the microphone is visible. During this experiment the Hider found 5 out of 10 passwords, reaching a recall of 50%.

The quality of the audio of the microphone F-908 is so good that it was even painful to listen to the audio when

Exp. Id	# Mics Hidden	# Mics found	TTD	TTF	Passwords spoken	Passwords listened	Distance of the Hider	Ghost
1	1	1	3s	40min	10	10	5m	Yes
2	1	1	7s	40min	-	-	4m	Yes
3	1	1	10s	25min	16	13	2m	Yes
4	1	1	25min	-	10	0	4m	No
5	1	1	3min	20min	10	5	6m	Yes

TABLE III
COMPARATIVE OF REAL LIFE EXPERIMENTS OF HIDING A MIC AND FINDING IT USING THE SALAMANDRA DETECTION TOOL. DETECTIONS ARE COMPARED WITH THE HARDWARE DETECTOR GHOST. (TTD = TIME TO DETECT, TTF = TIME TO FIND)

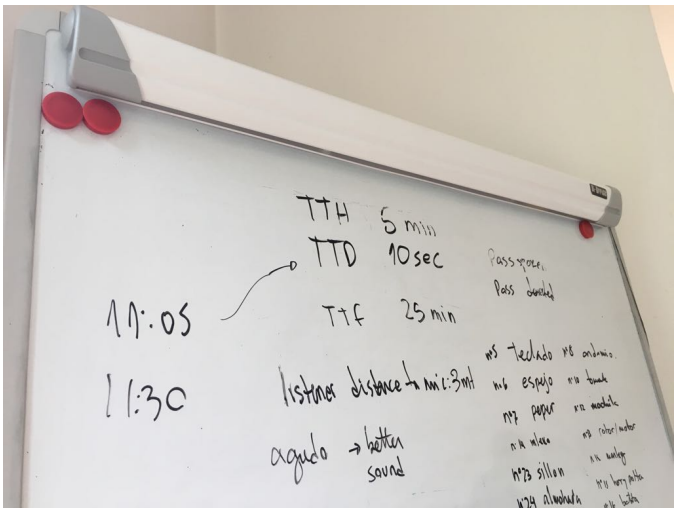


Fig. 19. Place where the mic F-908 was hidden during Experiment 4. The mic can not be seen in this picture, to show what people normally sees on the whiteboard. It is an example of a very good place to hide the mic, that even when it was detected it took a long time to find. The whiteboard was a good choice since interesting conversations take place around it.

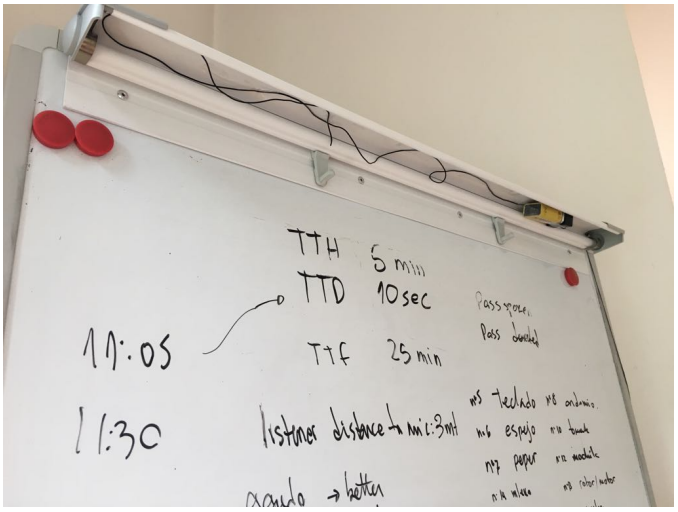


Fig. 20. Place where the mic F-908 was hidden during Experiment 4. The lid of the whiteboard is open to see the mic. During Experiment 4 the Seeker took 20min to find the mic.

people spoke close to it, or when there were loud noises in the room. A normal conversation at one meter from the microphone could be barely tolerable for the Hider. A sharp object falling to the floor made the Hider jump. Despite the humor in the situation, this is a real problem if humans are listening in real time to the microphone, and it could provide an opportunity for amusement[4].

In order to understand the good quality of the audio produced by the F-908, a test recording of the microphone output used in a real environment can be found in the following site: https://vocaroo.com/i/s0zCDvFjQfso .

F. Lessons Learned on Real Life Experiments

The different experiments placing and finding mic provided a lot of field experience. It is possible then to highlight the following key findings.

1) That the hiding location strongly depends on the type of device and the power autonomy. These aspects will determine, for instance, how often the Hider would have to return to the location to change the device batteries. An important consideration are the mics antennas, which are long and should be properly extended for a better performance.
2) A good hiding location will depend on the behavioral patterns of the target. In some environments, there are locations that are barely examined by the victims, making them ideal places. In other situations, when victims maintain a clean and very well ordered place, finding a good hiding location may prove extremely difficult.
3) As observed with the case of The Great Seal bug or the Experiment 5, the best place to hide a mic is often just in front of the victim's eyes. Fourth,
4) Upon hiding a mic, it is paramount to make test of hearing to be sure the mic is well placed.
5) The time to find a microphone is quite fast, with some cases of immediate detection upon entering the place.
6) The time to locate a microphone is much larger, with an average time of 20min and up to 40min.
7) The hardware detectors can run out of battery without indicating it, and therefore they may miss the detection of a mic.
8) The location function of Salamandra was very useful. It helped develop a search methodology.
9) The experience in locating bugs and the knowledge of the tools are very important to successfully locate mics.

[4]https://www.instagram.com/p/8ZsZy0qDz0/

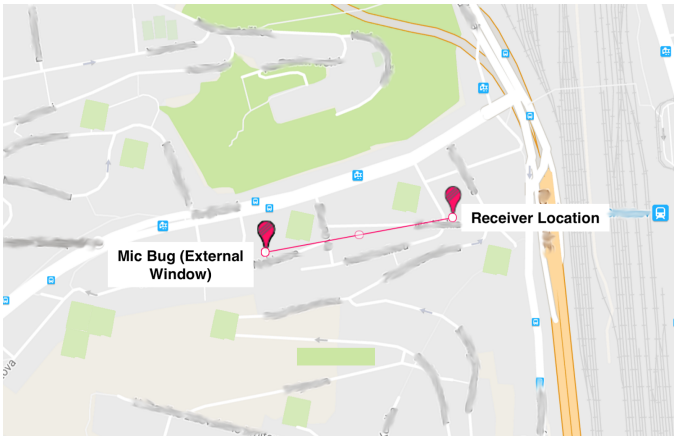


Fig. 21. Example of Mic Bug location and Receiver location in one of the field experiments using a F-908 device.

Mic Bug Location	Receiver Location	Distance	Quality	Target
T_1	R_1	0,16Km	2/5	10cm from mic bug
T_2	R_2	0.13Km	5/5	10cm from mic bug
T_3	R_2	0.14Km	3/5	10cm from mic bug
T_4	R_2	0.21Km	4/5	10cm from mic bug
T_5	R_2	0.24Km	2/5	10cm from mic bug
T_6	R_2	0.30Km	4/5	20cm from mic bug

TABLE IV
PERFORMANCE EXPERIMENT WITH F-908 MIC BUG, NON STATIONARY. THE RECEIVER WAS PARTIALLY STATIONARY.

V. ANALYSIS OF MICROPHONE BUGS LISTENING RANGES

In this section we present our field experiments on range performance of mic bugs. From the four devices available for testing the performance, we chose the F-908 device. The F-908 audio quality is extremely good compared to EAR-1 and MicroSpy, and is the smallest in size. The experiments performed covered different setups and locations in order to provide a more comprehensive and unbiased documentation on range performance. Figure 21 shows an example of an experiment testing the performance of the F-908 device in the wild.

A. Device: F-908 - Location: Non stationary

The first experiment of performance was with a non stationary F-908. The victim, or target, was moving through city streets, with old five storey buildings and non square blocks layouts, as shown in Figure 21. The receiver was moving and then stationary, with an increasing distance to the victim ranging between 100 and 300 meters. The performance of the F-908 was not stable. The listening quality was negatively affected when close to certain buildings, in some cases the listener could barely understand what the target was saying. As expected, when there was a clear path or less buildings between the target and the listener, the quality of the audio improved considerably. Details of this experiment are summarized in Table IV.

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

TABLE V
PERFORMANCE EXPERIMENT WITH F-908 MIC BUG, STATIONARY. THE RECEIVER WAS MOVING, GETTING CLOSER TO THE TARGET.

Mic Bug Location	Receiver Location	Distance	Quality	Target
T_1	R_1	0.30Km	4/5	20cm from mic bug
T_1	R_2	0.23Km	5/5	20cm from mic bug
T_1	R_3	0.00Km	4/5	5cm from mic bug

TABLE VI
PERFORMANCE EXPERIMENT WITH F-908 MIC BUG, STATIONARY, INSIDE A RESIDENTIAL OPEN SPACE. THE RECEIVER WAS MOVING CLOSER TO THE TARGET BUT LOCATED IN THE SAME BUILDING THAN THE TARGET.

B. Device: F-908 - Location: External Window, Stationary

The second experiment to measure performance was carried out with the F-908 in a stationary position. For this experiment, the F-908 was placed in an external facing open window. The receiver was moving, getting closer to the target, then farther and closer again. The listening quality was in most of the measured points far better than in the previous set up, even in farther distances reaching the 300 meters. Details of this experiment are summarized in Table V.

C. Device: F-908 - Location: Inside Open Space, Stationary

The third experiment to measure performance was carried out with the F-908 in a stationary position, indoors of a residential location. The receiver was located inside the building, moving closer in terms of vertical distance. The listening quality, even in an enclosed environment, was very good. Details of this experiment are summarized in Table VI.

VI. EXPERIMENTS ON IMPROVING THE AUDIO QUALITY OF MIC BUGS

One of the most important limitations of using spy mics is that attackers are usually forced to put them in places without access to good quality audio. It is common, then, to lose conversations or to miss some important information. Our experiments of Section IV show that in the worst cases, the recall of information (amount of information really retrieved from all the information wanted to be retrieved) can be as low as 50%, with some experiments getting up to 81%. Therefore, we conducted some experiments on trying to improve the quality of the audio received by the listener while using spy phones. For this task we asked the expert 3D animator Fermin Valeros to help us with the noise reduction software (https://ferminvaleros.com/).

We conducted three experiments. First a normal conversation, second a normal conversation with instrumental music and third a normal conversation with music with lyrics. In the three experiments we recorded with the mic F-908 (Figure 8).

The original audio of Experiment 1 can be listened here *https://vocaroo.com/i/s1TgZhXjEcLu*. It can be listened that there is a loud background noise and the sounds are saturated. It is possible to hear the conversation but it can be easy to miss parts. After an offline processing the audio Fermin was able to reduce most of the noise and improve the quality of the sound. The processed audio of Experiment 1 can be listened here https://vocaroo.com/i/s0TPZl4cmsFK.

In Experiment 2 we recorded a normal conversation with instrumental music. The original audio can be found here https://vocaroo.com/i/s1hFlqzpOz8c. After the processing of the audio, it ws possible to obtain a clearer sound. The post processed audio can be listend here https://vocaroo.com/i/s0SvjnYP5OlS. In this experiment there was not too much change from the original.

In Experiment 3 we recorded a normal conversation with music with lyrics. This was the most difficult work since there were multiple voices simultaneously. The original audio can be found here https://vocaroo.com/i/s1lcnlu88Utf. After processing the audio it was very impressive how the music was taken out and it is possible to listen to the conversation much better. This was a huge audio improvement. The processed audio can be listened here https://vocaroo.com/i/s1THE95wCyzS. This last experiment debunked the myth that playing music while talking is a good countermeasure for impairing the listening.

These simple experiments show that of-the-shell software can be used to dramatically improve the quality of the spy microphones, and it is expected that much more can be done in real time with the appropriate equipment.

VII. Notes on Battery Usage

One common and often overlooked factor of microphone bugs is the power source. Typical microphone bugs used for long term covert listening operations need a long lasting power source. Is for this reason that they are commonly placed in electrical sockets, where they may remain hidden for long periods of time without need of periodic maintenance by the eavesdroppers. Commercial microphone bugs use removable batteries. This type of power source introduces strong limitations for the eavesdroppers in terms of hiding locations of the mic bugs and the routine access to the target location.

During our experiments, we compared the advertised battery autonomy of the devices with the real autonomy we encountered. Three of the selected microphones, F-908, MicroSpy and EAR-1, use a typical 9v battery. They are advertised to last around 100 and 168 hours. Only in the case of the EAR-1 we found this autonomy was accurate when compared to the advertised. The MicroSpy lasted around 72 hours, while the F-908 lasted less than 12 hours of continuous usage. The advertised autonomy of the Beurer BY 84 model was far lower than advertised, lasting only 5:40 hours of continuous usage. The MiniA8 advertised autonomy was very accurate. When it comes to 9v or AAA removable batteries, the model of the batteries can influence these results. In all our cases the same battery manufacturer was selected: Varta.

Device	Advertised Battery Autonomy	Autonomy Validation
MicroSpy	168 hours	Lower than advertised
F-908	-	Lower than the rest
EAR-1	100 hours	Accurate
Beurer BY 84	22 hours	Lower than advertised
MiniA8	2 hours	Accurate

TABLE VII
IN MOST CASES, THE ADVERTISED BATTERY AUTONOMY TURNED OUT TO BE ACCURATE, WITH TWO EXPECTIONS IN WHICH THE BATTERY LASTED LESS THAN EXPECTED.

VIII. Future Work

The field of audio listening devices has proved to be extensive, and in this research we have just grasped the surface. Our future work includes the following areas:

- **Using every-day listening devices as camouflage: the baby-monitor case.** Baby monitors are widely used nowadays. While we did some initial tests with these devices, we plan to perform more thorough experiments to find how well these devices do in comparison with more standard mic bugs. Also, to know how these devices can be used in special situations to hide in plain sight.
- **Detection of alternative devices: the GPS tracker case.** GPS trackers are an interesting piece in a surveillance kit. We will study these devices and evaluate ways of detecting them with our current software.
- **GSM Listening devices.** There is a wide variety of listening devices using GSM technology. While we tested one model, we plan on experimenting with more of them, testing places to hide them, possible interference, and how to overcome the limited battery autonomy.
- **Improve Salamandra** to use a better interface and to have more novel detection methods.

IX. Conclusion

Microphones bugs are a well known mechanism to spy on people. A mechanism that has been updated with new technology in the last years. However, the security community has a deep misunderstanding of how the technology works and how to detect them, despite the known cases of spied citizens. This is an important concern to address, and it was necessary to gain control over this technology to understand it. We performed a large amount of experiments with real microphones bugs and we created our own SDR detection tool in order to find out the reality of using microphones to spy. Our research showed that placing microphones is very difficult because of the power supply needed, the characteristics of the mics and the difficulty to listen to conversations with accuracy. A large amount of resources are needed to perform this activity correctly. In contrast, our novel detection tool, called Salamandra, was capable not only of detecting mics, but also to locate them with great accuracy. We performed more than 120 experiments to find microphones in real houses, to

train our tools, to know how far the microphones can transmit, and to see how the quality of audio can be improved by software.

Microphones are still used to listen others. This technology advances quickly and the detection tools must follow. Placing microphones is hard and costly, but it can give a large amount of information to the attackers, specially if the victim does not expect this type of attack. Finding microphones is easier for most of them, except for the GSM types which are still difficult to find.

ACKNOWLEDGMENT

The authors would like to thank Fermin Valeros (**https://ferminvaleros.com**) for his contributions on processing, and cleaning the audio recordings of mic bug listening experiments. Thanks to him, we could debunk the myth of using a radio for making the listening more difficult. Do not use a radio, it doesn't work.

REFERENCES

[1] Weiwei, A [aiww]. (2015, October 4).[Video of microphone bug and response from Ai Weiwei to his listeners by Ai Weiwei]. Retrieved August 06, 2017, from: https://www.instagram.com/p/8ZfCgkqD7A/.

[2] Weiwei, A [aiww]. (2015, October 4).[Photograph of microphone bug extracted from his study by Ai Weiwei]. Retrieved August 06, 2017, from: https://www.instagram.com/p/8ZfCgkqD7A/.

[3] Weiwei, A [aiww]. (2015, October 4).[Photograph of microphone bug as found in his study by Ai Weiwei]. Retrieved August 06, 2017, from: https://www.instagram.com/p/8Ze17BqD6h/.

[4] Bangkok Post [BangkokPostNews].(2015, October 5). Chinese artist Ai Weiwei shows government bugs. Retrieved August 06, 2017, from: https://twitter.com/BangkokPostNews/status/651115559724019712

[5] Dunne, C. (2015, October 05). Big Brother Is Bugging Ai Weiwei. Retrieved August 06, 2017, from http://hyperallergic.com/242008/big-brother-is-bugging-ai-weiwei/

[6] PINow. (n.d.). Bug Sweep, Bug Detection, TSCM. Retrieved August 06, 2017, from https://www.pinow.com/investigations/bug-sweep-tscm

[7] Software-defined radio. (2017, August 16). Retrieved August 19, 2017, from https://en.wikipedia.org/wiki/Software-defined_radio

[8] How can you find a bug (listening or video device) in your house? What are some cheap ways to debug? (n.d.). Retrieved August 06, 2017, from https://www.quora.com/Surveillance-How-can-you-find-a-bug-listening-or-video-device-in-your-house

[9] Hubest, A. (2011, August 04). Audiosurveillance. Retrieved August 19, 2017, from https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol4no3/html/v04i3a04p_0001.htm

[10] Aldrich, R. J. (n.d.). GCHQ: The Uncensored Story of Britains Most Secret Intelligence Agency. Retrieved August 19, 2017, from https://www.amazon.com/Gchq-Richard-Aldrich/dp/0007312660

[11] Kipling, R. (2017, August 20). "Wireless" . Retrieved August 19, 2017, from http://www.unz.org/Pub/Scribners-1902aug-00129 Originally published in August 1902

[12] Stenice. (n.d.). Retrieved August 19, 2017, from http://www.cryptomuseum.com/covert/bugs/stenice/index.htm

[13] Rtl Power. (n.d.). Retrieved August 06, 2017, from http://kmkeen.com/rtl-power/

[14] Fast Fourier transform. (2017, August 11). Retrieved August 19, 2017, from https://en.wikipedia.org/wiki/Fast_Fourier_transform

[15] The Great Seal Bug. (n.d.). Retrieved August 19, 2017, from http://www.cryptomuseum.com/covert/bugs/thing/index.htm

[16] Satyr. (n.d.). Retrieved August 20, 2017, from http://www.cryptomuseum.com/covert/bugs/satyr/index.htm

[17] Transistor. (2017, August 19). Retrieved August 19, 2017, from https://en.wikipedia.org/wiki/Transistor

[18] KGB Bug. (n.d.). Retrieved August 19, 2017, from http://www.cryptomuseum.com/covert/bugs/kgb/index.htm

[19] OPEC Bug. (n.d.). Retrieved August 19, 2017, from http://www.cryptomuseum.com/covert/bugs/opec/index.htm

[20] Ebay. (n.d.). Retrieved August 19, 2017, from https://www.ebay.co.uk/

[21] Amazon. (n.d.). Retrieved August 19, 2017, from https://www.amazon.com/

[22] Micro Mobility Systems Mini Micro FM Spy Bug Audio Surveillance Transmitter. (n.d.). Retrieved August 19, 2017, from https://www.ebay.co.uk/p/Micro-Mobility-Systems-Mini-Micro-Fm-Spy-Bug-Audio-Surveillance-Transmitter-Transmits-14-Days/132610129?_trksid=p2047675.m4096.l9057

[23] Professional FM Spy Bug Transmitter. (n.d.). Retrieved August 19, 2017, from http://www.ebay.co.uk/itm/PROFESSIONAL-FM-SPY-BUG-TRANSMITTER-/172267729268?hash=item281bf4f174%3Ag%3ALs4AAOSwdrRXG4m2

[24] F908 Wireless transmitter receiver mini Covert FM Audio Listening Device Ear spy. (n.d.). Retrieved August 19, 2017, from http://www.ebay.co.uk/itm/F908-Wireless-transmitter-receiver-mini-Covert-FM-Audio-Listening-Device-Ear-spy-/191912821464?hash=item2caee542d8%3Ag%3ADQIAAOSwp5JWXvPW

[25] Beurer BY 84. (n.d.). Retrieved August 18, 2017, from https://www.alza.cz/maxi/beurer-jby-84-d2705172.htm

[26] Wireless Hidden Spy listening Device Tracker Room Bug Remote Audio Surveillance. (n.d.). Retrieved August 19, 2017, from http://www.ebay.co.uk/itm/Wireless-Hidden-Spy-listening-Device-Tracker-Room-Bug-Remote-Audio-Surveillance-/252364469752#shpCntId

[27] Spy Audio Devices. (n.d.). Retrieved August 19, 2017, from https://www.indiamart.com/ams-security/spy-audio-devices.html

[28] Voice Activated Wireless GSM Spy Bug SIM Mains Adapter Plug Surveillance Adaptor. (n.d.). Retrieved August 19, 2017, from https://www.ebay.co.uk/p/Voice-Activated-Wireless-GSM-Spy-Bug-SIM-Mains-Adapter-Plug-Surveillance-Adaptor/748264310?iid=272793750899

[29] Kirn, P. (2017, March 14). Could you spy on someone using a microwave oven as a mic? Retrieved August 19, 2017, from http://cdm.link/2017/03/theory-spy-someone-using-microwave-oven/

[30] Newman, L. H. (2017, March 13). Kellyanne Conway Wonders If a Microwave Can Spy On You. Spoiler: It Can't. Retrieved August 19, 2017, from https://www.wired.com/2017/03/kellyanne-conway-microwave-spying/

[31] IC-R6. (n.d.). Retrieved August 19, 2017, from http://www.icomamerica.com/en/products/receivers/handheld/r6/default.aspx

[32] RTL2832U FC0012 Mini DVB-T DAB FM USB Digital TV Dongle - Black. (n.d.). Retrieved August 20, 2017, from http://www.dx.com/p/rtl2832u-r820t-mini-dvb-t-dab-fm-usb-digital-tv-dongle-black-170541

[33] Ghost Detector. (n.d.). Retrieved August 20, 2017, from https://www.alibaba.com/product-detail/YZ069-Ghost-Detector-RF-Hidden-Camera_60080712109.html?spm=a2700.7724838.2017115.1.3c93b095BkVL9x