Spy Bugs: Definition, Classification and Types

Luigi Camporesi

Extra Large Srl, Via Costa del Bello 65, 47899, Serravalle, Republic of San Marino.

For correspondence: info@intercettazioni.biz

Drafted on 04/06/2022

The information in this document was found through research in publicly available documents or brought by author's observations and deductions. No proprietary information or technical data subject to non-disclosure restrictions by the respective owners has been reported or used as a starting point for deductions.

Abstract
In the world of surveillance there is a general lack of unified and standard terminology and definitions, probably also due to the secrecy imposed by those bodies that mostly push innovation: military and government agencies. This paper tries a minimal definition and classification for the so called spy bugs. A list of different types of spy bugs and an outline of future technologies for bugs and their power supply is also proposed.

1. Introduction
Bugs, spy bugs, hidden systems for viewing, listening and exfiltrating data, attack systems - there is no unique name for devices that can secretly collect and transmit conversations, images and data, just as there is no standard definition. To the best of our knowledge, there is also no single, standardized classification for these devices. In this document the following (arbitrary) definition and classification are used and are however sufficient to include (almost) all the devices described or only outlined below.

2. Definition
A definition for Bug (more properly for Hidden Audio, Video and Data Collection System) could be: "A *device or system installed in proximity of the target to be able to listen, photograph/film or steal data in a covert manner*". "Bug" refers to a small device, while this definition does not impose anything in this regard. In fact, sometimes the device for covert transmission can be large, under the eyes of everyone, without anyone thinking about the hidden function that it is actually carrying out.

3. Classification
A classification for these devices or systems - for capturing and transmitting audio, photo/video and data from targets at distance - could be one that considers the physical phenomena that can be used for the purpose: vibrations and electromagnetism. Vibrations need matter to be transmitted, while electromagnetic phenomena also move in empty space as well as through matter. Two main categories of devices or systems are therefore those that use for transmission:

Vibrations [1]

Electromagnetism [2]

These two categories can in turn be further subdivided. Vibrations travel through solid materials, for example concrete, iron, or through the air in the form of sounds, or through water and liquids in general. Infrasound and Ultrasound are the terms that define the vibrations in the air below and above the hearing threshold of the human ear respectively. Electromagnetism includes Magnetic Fields, Electric Fields, Electromagnetic Waves [3] for which the complete electromagnetic spectrum [4] and Electric Current should be considered.

Vibrations
- Vibrations (solid and liquid matter)
- Infrasound
- Sound
- Ultrasound [5]

Electromagnetism
- Magnetic Fields [6]
- Electric Fields
- Electromagnetic Waves
- Electric Current

Any device or system that, for the covert transmission of audio, images and data, uses any combination of the physical phenomena as above ordered, can be defined as Hybrid.

4. Micro Recorders
It should be noted that devices such as for example Micro Recorders - audio and video recorders of reduced dimensions - do not use any of the means of transmission listed above, since at a certain point they are physically removed for accessing the recordings and, however, can be considered as Bugs.

5. Commercial Devices and for Government Agencies
Another way for classifying bugs could be to set them into two main categories: those easily accessible on the open market and those reserved for government agencies. This classification often has a valid meaning but just as often it loses it. For example, although there are a number of devices reserved for government entities and are also

classified (on which government agencies impose confidentiality) and for which information is not publicly available, there is a number whose information is publicly accessible with some effort (for example by contacting the relevant manufacturers). Furthermore, a multitude of open-market devices can be used effectively - and they are - also by public institutions, thanks to the advancements of technological innovation in the commercial market.

To get an idea of what some of the technologies available to certain government agencies are, one can refer to the leaks of confidential data that have occurred in recent years. See for example the NSA TAO catalogs [7, 8]. Among the others, it is to be noted the use of "*radar illuminators*", systems emitting electromagnetic radiation that hit previously installed non-transmitting devices, or common devices such as printers and that, by processing the returning signal, are able to extract the audio in the vicinity of the radiated devices.

6. Types of Bugs
Below there is a list of bugs that includes types available on the open market, with some subject to commercial restrictions: in this case it is generally the manufacturer that restricts the dissemination of technical information by its own initiative and restricts the sale to government agencies. This list does not include some types of bugs that are normally available to government agencies or that are difficult to find.

7. VHF-UHF-SHF Bugs
These are bugs that transmit signals in the frequency bands from 30 to 300 [MHz], from 300 [MHz] to 3 [GHz] and from 3 to 30 [GHz]. The signal can be analog or digital, in clear or encrypted and is collected by a generic or dedicated receiver.

8. Frequency Hopping - Spread Spectrum Bugs
These are Bugs that use the VHF-UHF frequency bands for transmission and that at the same time rapidly change the transmission frequency along a large portion of the spectrum [9], making them more difficult to detect and intercept. Also in this case the signal can be analog or digital, in clear or encrypted.

9. GSM/UMTS /LTE/5G Bugs
These are miniature mobile phones that transmit audio and/or video using GSM, UMTS, LTE and 5G (2G, 3G, 4G and 5G) technologies. In general they are relatively cheap.

10. Wi-Fi Bugs
These are often micro-cameras with the function for capturing ambient audio, but there are also simple microphones that transmit audio via Wi-Fi. The Wi-Fi signal has a relatively small transmission range, however with special antennas it can be picked up hundreds of meters away. Furthermore, there is always the possibility of collecting the signal in proximity, for example with a Wi-Fi-2G/3G/4G modem/router and re-transmitting it to its destination by Internet.

11. Bluetooth Bugs
Bluetooth bugs are normally reserved for government agencies due to their relatively high cost. However, it should be noted that even a simple pair of Bluetooth headsets connected to a nearby smartphone can be used as a bug.

12. Store & Forward Bugs
These are micro recorders that record audio and/or video locally and then transmit it when programmed or on demand. For the transmission they can use various technologies: VHF-UHF, 2G/3G/4G/5G, Wi-Fi, Bluetooth, etc.

13. Bugs for Powered Electric Cables
These are bugs powered by the electric current flowing in the cables and at the same time using the same cables for signal transmission. The cables can be for electricity supply, but also LAN, USB, telephone, alarm and video surveillance cables, cable TV, etc. The signal is superimposed on the flow of electric current.

14. Cable Bugs (Wired)
This type of bug has its own cable, powered autonomously and that carries the signal from the place where audio and/or video are picked up, to the place where the first step for usage is carried out, that could be recording or re-transmitting by a different method.

15. Optical Fiber Bugs
Optical fiber is used by these bugs for the transmission of the audio and/or video signal. In some case the optical fiber itself, properly displaced, also acts as a microphone as well as a means of transmission of the optical signal.

16. Fixed Telephone Bugs
These are bugs dedicated to capturing conversations along landline phones, both analogue and digital or VoIP. They make use of various technologies for signal transmission, or they may also consist of dedicated voice recorders.

17. Contact Microphones
Wall microphones are bugs that allow to capture the audio of a room by remaining outside, by placing, attaching or inserting a piezoelectric microphone in a wall. Once available, the signal can be recorded and transmitted in various ways.

18. Visible Light, Infrared and Ultraviolet Bugs
Visible light can be used to carry ambient audio for all to see without anyone noticing that the light is actually vibrating in a modulated way. This principle is used by visible light bugs which consist of special lamps and remote receivers to collect the signal. The infrared bugs instead transmit invisibly to the human eye as do the ultraviolet

light bugs.

Visible light bugs are destined to further development with the advent of Li-Fi [10], the optical correspondent of Wi-Fi. IP data in this case is transmitted by special lamps.

19. IP Bugs
IP bugs generally consist of microphones with an IP data transmitter integrated into devices such as modems and routers. In that case, they take advantage of the legitimate Internet connection to broadcast audio and video outside the target environments. Other IP bugs are instead dedicated to the theft of data and consist of devices that take care of making copies of the IP data stream and transmitting them through other channels, for example through an integrated 2G/3G/ 4G modem, thus escaping the controls on the internal network.

20. Software Modifications
Software modifications can be made to smartphones, PCs - especially if equipped with a microphone and camera - monitors and TVs, VoIP phones, Wi-Fi printers. They can be performed with physical access to the device or remotely, with different levels of installation difficulty. They allow to activate microphones and cameras remotely and to transmit audio, video and data.

21. Other Types of Bugs
For completeness, the following is a (partial) list of devices used by government agencies or that have passed into relative disuse. Their availability is limited and their existence can be deducted from leaks as in case [7], from the availability of historical data [11] or by the commercial availability of systems for their detection.

22. Passive Bugs
These are devices capable of capturing the ambient audio and transmitting it, even if not powered with electric current at all, when they are stimulated by suitable electromagnetic radiation. The best known historical case is that of "The Thing" [11]. For example, let's consider RFID tags that transmit information when illuminated with radio frequencies [12]. Some devices can also be powered, but in any case not transmitting, until they are stimulated by appropriate external radio frequencies [7].

23. TEMPEST
For the definition of the term see: "*TEMPEST is a U.S. National Security Agency specification and a NATO certification referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations. TEMPEST covers both methods to spy upon others and how to shield equipment against such spying.*" [13].

TEMPEST technology therefore refers to the possibility of leaking information from target environments by exploiting unintended emissions from the various systems. The classic example is the possibility of reproducing what the monitors display at a distance of tens of meters, exploiting their unintentional emissions [14]. Therefore, it is not literally a question of bugs, rather of systems for detecting, collecting and converting signals from the target devices and environments.

24. Ultrasound Bugs
The ultrasonic bugs convert the ambient audio into ultrasounds which are then transmitted using the surrounding atmosphere without anyone being able to hear anything.

25. VLF-HF Bugs
These are systems that transmit analog or digital signals in the frequency bands 3 to 30 [KHz] and 3 to 30 [MHz].

26. EHF-THF Bugs
Above 30 [GHz] electromagnetic waves can be used for data transmission (EHF - Extremely High Frequency [15], THF - Tremendously High Frequencies). See for example the frequency band between 24.25 and 52.6 [GHz] which has been identified for usage in 5G cellular telephone networks [16].

27. Magnetic Transmission Bugs
Magnetic fields can be used to transmit information a few meters away [6] and can only be detected with dedicated instruments, which are generally not very common. The existence of this type of devices is confirmed by the presence on the market of systems for their detection.

28. Hydrophones
Hydrophones are generally piezoelectric devices [17] capable of picking up sounds (vibrations) when immersed in liquids. They are used, among other things, to monitor the movements of submarines and to study marine fauna. They are also able to pick up sounds coming from the surface.

29. Laser Microphones
An entire category of laser microphones points an infrared (invisible) laser beam at a glass surface, using its vibrations to extract the sound from the indoor environment. A camera must collect the reflected laser beam. The laser beam generator and the camera must therefore "see" the glasses of the target room perpendicularly, or the two must be positioned appropriately, if perpendicular positioning is not possible.

A second type of laser microphones makes use of a different technology than the one described above. They are able to listen to targets in open spaces and also to pass through glass, strike and extract audio from objects of all kinds - better if they vibrate easily in response to the human voice - without the need to have the laser beam perpendicular to the target surfaces. In this case, a series of images in close sequence are converted into intelligible

audio.

30. Hardware Changes
Modifications to existing systems have been around for decades, especially for landline phones. A telephone modified in hardware can in fact remain with the handset in "open" mode even if it is lowered, allowing the capture of ambient audio and transmission along the telephone line.

31. Materials and Techniques
The sector of Hidden Audio Video and Data Collection Systems, *aka* Bugs, is partly inaccessible due to the secrecy operated by government agencies regarding the technologies, devices and systems at their disposal. The process for these technologies and systems for arriving on the open market often follows a standard path: to paraphrase Bruce Schneier on cyberattack systems: "*What is now classified as top-secret in the military/government sector, tomorrow will be the thesis of a Ph.D., then it will arrive on the open market*" [18]. For this reason, it can be a useful exercise trying to imagine some of the technologies that will be used in the future for bugs on open market and that probably already are used for systems reserved to government agencies. An important aspect is the power systems needed to supply electricity to hidden devices.

32. Piezoelectric Materials
"*Piezoelectricity is the property of some crystalline materials to polarize, generating a potential difference when they are subjected to mechanical deformation (direct piezoelectric effect) and at the same time to deform elastically when subjected to an electrical voltage (inverse piezoelectric effect or Lippmann effect). This piezoelectric effect occurs only along a certain direction and the deformations associated with it are of the order of the nanometer.* " [19]

Piezoelectric materials are used in many devices for listening, for example in contact microphones, capable of converting wall vibrations into electrical signals and then into audible and recordable sounds. Among the most advanced applications that can be imagined, the possibility must be considered that objects placed in proximity of the target environments are covered with piezoelectric material - for example cables inside walls - therefore capable of transmitting in an occult way the ambient audio.

Furthermore, piezoelectric materials could instead be used to extract energy from environmental vibrations, to supply power to low consumption listening devices, not connected to other power sources such as batteries or electrical power circuits [20].

33. Photoelectric Materials
The photoelectric materials [21] used in solar cells have an external appearance that is well present in popular mind. However, things could change and they have already done so at the research level with the arrival of photovoltaic coatings [22]. The possibility must be considered that common objects may contain microphones and transmitters powered by sunlight and ambient light thanks to the photoelectric coating.

34. Extraction of Energy from Radio Waves
These systems have already found commercial applications, see for example the Samsung remote control which does not require the replacement or recharging of the internal battery [23]. The history of the transmission and extraction of energy with radio waves dates back to over seventy years and scientific literature on the subject is available [24]. The existence of devices that are powered by extracting energy from the electromagnetic emissions present in the target environments is therefore to be taken into consideration.

35. Conclusions
The problem of a unique name for spy bugs reflects the fact that their functions can be fulfilled by so different devices and systems, from miniature to big one, from hidden to visible, from strictly close to target to hundreds meters away. This can be solved by using a quite long definition such as "*Hidden Audio, Video and Data Collection System*" that, although substantially correct is probably not that convenient to be used in common talks and writings.

The classification of spy bugs and systems made by the physical phenomena in use for transmission should work for every spy bug that is and will be in use. Just adding the category "physical move" for considering micro recorders seems to catch all the possible devices.

References

[1] https://it.wikipedia.org/wiki/Vibrazione

[2] https://it.wikipedia.org/wiki/Interazione_elettromagnetica

[3] https://it.wikipedia.org/wiki/Electromagnetic_Radiation

[4] https://it.wikipedia.org/wiki/Spettro_elettromagnetico

[5] https://it.wikipedia.org/wiki/Ultrasuoni

[6] https://www.researchgate.net/publication/224566802_A_communication_system_using_magnetic_fields

[7] https://nsa.gov1.info/dni/nsa-ant-catalog/index.html (parody site for the NSA)

[8] https://en.wikipedia.org/wiki/NSA_ANT_catalog

[9] https://en.wikipedia.org/wiki/Frequency-hopping_spread_spectrum#:~:text=Frequency%2Dhopping%20spread%20spectrum%20(FHSS,to%20both%20transmitter%20and%20receiver

[10] https://it.wikipedia.org/wiki/Li-Fi

[11] https://en.wikipedia.org/wiki/The_Thing_(listening_device)

[12] https://it.wikipedia.org/wiki/Identificazione_a_radiofrequenza

[13] https://en.wikipedia.org/wiki/Tempest_(codename)

[14] https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-577.pdf

[15] https://it.wikipedia.org/wiki/Extremely_high_frequency

[16] https://en.wikipedia.org/wiki/5G_NR_frequency_bands

[17] https://en.wikipedia.org/wiki/Hydrophone

[18]
https://www.schneier.com/blog/archives/2015/02/the_equation_gr.html

[19] https://it.wikipedia.org/wiki/Piezoelettricit%C3%A0

[20]
https://www.researchgate.net/publication/342354566_Piezoelectric_Energy_Harvesting_Solutions_A_Review

[21] https://it.wikipedia.org/wiki/Cella_solare

[22]
www.researchgate.net/publication/332762858_The_efficiency_of_thin_film_photovoltaic_paint_A_brief_review

[23] https://www.wired.it/article/eco-remote-telecomando-samsung/

[24]
https://www.researchgate.net/publication/314126417_RF_power_harvesting_a_review_on_designing_methodologies_and_applications
[21] https://it.wikipedia.org/wiki/Cella_solare

[22]
www.researchgate.net/publication/332762858_The_efficiency_of_thin_film_photovoltaic_paint_A_brief_review

[23] https://www.wired.it/article/eco-remote-telecomando-samsung/

[24]
https://www.researchgate.net/publication/314126417_RF_power_harvesting_a_review_on_designing_methodologies_and_applications