

Chapter 2

Intercepting Ambient Conversations

2.1 Introduction

Continuing from the previous introductory chapter regarding industrial espionage, in this chapter we will focus our attention on the technical means, methods, and equipment that “spies” use for intercepting ambient conversations from the room/place that the victim is located. In the next chapters we will continue the analysis with the interception of data and the interception of telecommunications.

2.2 Interception Devices

As we have previously mentioned, information isn’t stored only on computers, but it is also transmitted from individuals via conversations and phone calls. Thus, there is a series of different interception devices that aim to record audio and/or video and possibly transmit this information to a different location (these devices are collectively known as “bugs”). The rapid development of technology gives access to a plethora of electronic devices and parts used for interceptions, available in sizes small enough to make their visual trace almost impossible for the non-trained eye. Figure 2.1 depicts one of these devices.

Such devices, thanks to their small size, can be hidden in every possible location one can imagine. They can also be built-in or embedded in other objects or even “worn” on someone that was able to penetrate the area where the conversation to be intercepted takes place. Figure 2.2 shows a man’s belt that is equipped with a built-in microcamera. The very small hole that barely can be seen is the opening for the microcamera’s lens. There are also various different forms of cameras and microphones that are housed in sunglasses, ties, coat buttons, etc.

Fig. 2.1 Wireless setup for intercepting room conversations

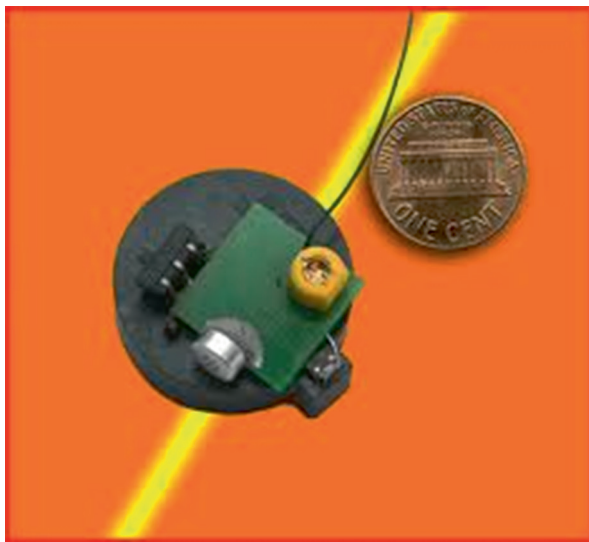


Fig. 2.2 Belt with built-in microcamera



“Bugs” can be used to monitor telephones, conference rooms, and every possible location company’s executives may be having a discussion. Such kinds of devices have been found even hidden in airplane seats of business class and also in fine dining restaurants where executives were discussing important deals during business lunches.

A fairly common practice also involves sending someone a gift. Like a modern “Trojan Horse,” the gift will be “bugged” with an interception device. There are dozens of such products as shown in Fig. 2.3 (desk clock, wall clock, calculator, etc.). A major limitation of “bugs” is the energy aspect. Battery-powered ones have certainly a limited operational time amount. Imagine, however, the case where the “Trojan Horse” gift itself is a mains-operated electronic device (e.g., a nice table lamp): the power source is now ensured, allowing the interception device to operate over a long period of time! In addition to that, the mains or telephony plug

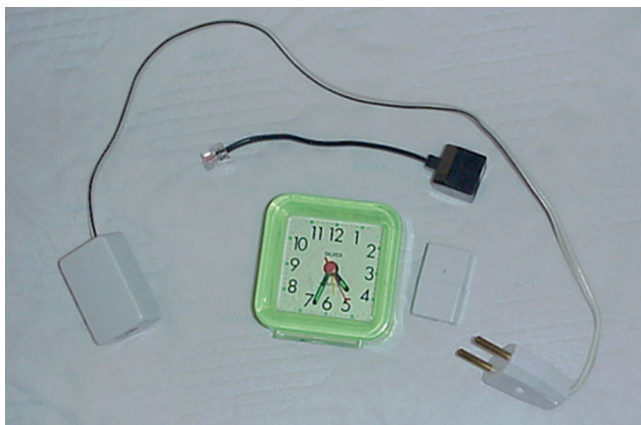


Fig. 2.3 Interception setups housed in various objects



Fig. 2.4 Digital voice micro-recorder

itself allows enough space to accommodate such a “guest” while at same time providing plenty of power.

Regarding their operation, these setups may either transmit or store the intercepted data. A simple digital voice recorder (or specialized devices as the ones shown in Fig. 2.4) can record dozens of hours of conversations. Furthermore, it can even be activated upon voice detection in order to serve the spy for many days before eventually running out of battery power. Of course, it is imperative to ensure the removal of the device from the room it is located in order to retrieve the data recorded. Thus, usage of a digital voice recorder requires a second or even more “visits” to the room to be “bugged,” and this can prove to be difficult. Transmitting devices that will be analyzed shortly below overcome this limitation.

It is also possible to intercept wireless transmissions (from Wi-Fi networks but also from cellphones and cordless phones). We will refer to both Wi-Fi and cellphone and cordless phone interceptions in the following chapters.

2.3 Transmitting Setups

Video and audio recorders are “passive” in nature, in the sense that they do not transmit any information. Therefore, it can be more difficult to be located. Transmitting devices, however, have an important advantage. The intercepted information is immediately available and does not require any second visit to the area in order to retrieve the bugging device. This is especially important in cases where rapid decisions must be made and the information must be available in real time. On the other hand, given their limited size and the energy efficiency required, their range is limited. This is why there often exists a repeater (or a monitoring station) in an office close by to the intercepted one or in a car parked outside the area that the interception is conducted. The repeater, hosted in a place where more room available receives the initial transmission, amplifies it and retransmits it in a great distance, so that the spy can get access. Indeed, the original minitransmitter might be hidden in the desk of the CEO, while a bigger size, mains-operated repeater can be placed in an adjacent office (even in another floor).

A very effective way to extend the transmission range is by using a modified cellphone that the spy has carefully hidden in the room. In this case, the cellphone automatically and silently answers a predetermined phone call, and it transmits the conversations to the other end. Therefore, there is no need to use a repeater anymore, since the intercepted material can be received even from another country, thousands of miles away. This practice has the disadvantage of the relatively bigger size of the cellphone, but even so, the cellphone may be deceitfully hidden inside a larger “innocent” device. Of course, there already exist specific devices available in the market to be exclusively used for such cases with a significantly smaller footprint. Figure 2.5 depicts such a device, equipped with a SIM card. These devices are essentially a micro-cellphone (without a screen and keyboard) with a powerful microphone. They require a plain mobile telephony SIM card, and they can be called as a normal telephone. As already mentioned, when called, they silently take

Fig. 2.5 Interception device transmitting via the cellular network



the call and switch the microphone on, so that the spy can listen to the ambient sounds. The major disadvantage of such an implementation is the very limited operating time (a few hours). Should, however, an external energy source be provided, then they can operate for much more time.

As already mentioned, transmitting devices can be detected since they are “active” in nature. Their transmission (and therefore their location) can be detected by using specialized equipment (such as spectrum analyzers or field meters) as we will be discussing in the respective chapter. This is why a more elaborate (and expensive) alternative exists. This device records conversations similarly to a digital voice recorder but does not transmit them immediately. Instead, after collecting enough data, it converts them to a digital signal, then compresses it, and transmits it, possibly encrypted. This way, the signal transmission is not constant (as is the case with normal transmitters), making the detection incredibly difficult (it is required to keep using a detector in the room for many hours). An equally difficult to detect device uses a spread spectrum transmitter that uses the direct-sequence spread spectrum (DSSS) or the frequency hopping spread spectrum (FHSS) technology. In both cases it is very hard to detect such transmissions. In the first case, the difficulty derives from the fact that the transmission is low power but in wide frequency spectrum so it is not easily distinguished from the electromagnetic noise of the environment, whereas in the second case, the transmission rapidly switches between different frequencies.

2.4 Microphones

Microphones are the core elements of every ambient audio-intercepting device. Apart from their use in devices, they can also be used standalone. Installing a high-sensitivity microphone (Fig. 2.6) and wiring it to an adjoining office is a simple solution. Of course, the wiring part is the most revealing one and can be spotted. The usage of a conductive pen (or conductive paint) is impressive.

Fig. 2.6 High-sensitivity microphone



Fig. 2.7 Wall microphone**Fig. 2.8** Parabolic microphone

This paint (usually based on silver) is commonly used to repair broken car rear window heating elements. The trail of the pen creates a conductive film as in an electrical conductor of practically zero thickness. It therefore allows connecting a microphone, across the length of a wall. Repainting the wall to cover the trail of the pen, one ends up with a completely stealth interconnection. Interception from an adjoining room sharing a common wall is equally effective using a stethoscope or a simple water glass. For professionals, there are in fact advanced electronic “stethoscopes” (wall microphones) to be used for such purposes (Fig. 2.7).

Another category of microphones is directional microphones, usually parabolic ones (Fig. 2.8). These microphones can pick up sounds from a great distance. However, when operated in high-level noise environments such as cities, their effectiveness is limited. On the contrary, they are quite popular among nature lovers who are able to hear various birds and animals from a distance in quite places such as forests.

Finally, sound can propagate in a natural way to nearby areas, without the use of equipment or microphones, through a hole on the wall, air-conditioning ducts, chimneys, heating pipes, etc. It is indeed remarkable how we focus our attention on high-tech electronics, while construction flaws such as thin walls or lack of audio insulation are more than enough for a “leakage.”

2.5 Exotic Tools

More advanced “tools” include a modified incandescent light bulb whose lighting intensity is modulated by the sounds of the environment, producing an unnoticeable to the human eye flickering. With the appropriate equipment, these minor changes in the light intensity are converted back to audio. A similar real-world analogy is that of the disco lights that light according to the music. In that case, the effect of course is visible to the naked eye. Needless to mention that there must be a line of sight connection between the target and the spy.

Another line of sight technique can be described from the espionage case in the US Ambassador’s office in Moscow, in 1945. Back then, the Soviets gave the US Ambassador a carved wood plaque of the Great Seal of the United States as a gift and a “gesture of friendship.” However, this gift was nothing more but a covert listening device. The most impressive aspect of the case is the bug’s design. Designed by Leon Theremin, the device was passive and only activated when it was radiated by a signal at a precise frequency (it is therefore considered as a predecessor to RFID). That could also be done from a distance, making it perfect for that use.

The device was equipped with a membrane in a cavity that resonated at the frequency of the beamed signal. When that signal was transmitted, the device would be modulating the sound it received through the wood panel in front of it and would transmit it at a different and higher frequency than the beam used to activate it. The bug’s transmitting signal could then be picked up and demodulated to reveal the context of conversations taking place in the Ambassador’s residential study.

Even though it had an antenna to transmit the intercepted conversations, its design made it very difficult to be discovered. Being completely passive, it had to power source, and it was only transmitting signals when it was resonated by the beaming signal at 330 MHz as it is said.

It took quite a while till the device was discovered by accident in 1952. A British radio operator picked up American conversations on an open radio channel, obviously at the same time as the Soviets were beaming signal to activate the device.

Another technique, usually portrayed in movies, is to intercept sound from the subtle vibrations on window glasses. This movement, measured in microns of a meter, changes the reflection angle of an invisible infrared laser beam whose beam can in turn be demodulated into sound. Again, in this case, every noise, such as vehicles passing by, dramatically decreases the system’s efficiency.

Since we mentioned vehicles, even a car can possibly be “bugged,” both for intercepting sound as well as tracking its’ position with a GPS-based device. The list of “exotic” devices also includes devices used to intercept fax messages.

It is also possible to conduct a passive interception without any kind of intervention. In (forgotten by now) cathode-ray tube (CRT) monitors it was possible to remotely reconstruct the signal due to electromagnetic transmissions (Van Eck-TEMPEST effect). Based on the same principle, signal interception from wires is possible, through induction. In Fig. 2.9 a special inductive coil is shown which intercepts telephone signals without breaking the circuit, just by picking up the electromagnetic fluctuations. The basic principle here is that according to

Fig. 2.9 Inductive coil for intercepting telephone signals



Maxwell's equations, a varying electric field produces a magnetic field and vice versa. Physical audio in electronic devices is transformed to a varying electrical current that produces a magnetic field. So, the induction coil picks the magnetic field, transforms it back to current, and drives an amplifier to allowing overhearing the initial audio.

2.6 Systems for Enforcing Secrecy of Communications

Having described various interception and bugging devices, we will describe some devices that aim to “neutralize” their presence. A conference room or an office can be equipped with the systems described in the following paragraphs to avoid the interception of confidential information during meetings.

A cellphone jammer (Fig. 2.10) covers all cellular bands to protect against hidden cellphones that act as interception devices. This tool is simply a transmitter that transmits along the whole frequency band mobile phones operate in. By masking the legitimate mobile telephony signals, this device renders mobile phone service inoperable in the nearby area. Depending on the power of the device, the jamming area can be extended to miles around it. It must be noted that in most places the use of cellphone jammers is illegal, because apart from the fact that interfere with the provider's network, they can also prohibit an emergency call from being placed.

Wireless camera and Wi-Fi network jammers (most wireless cameras operate on the same 2.4 GHz band as Wi-Fi networks do). Employing the same technique as the cellphone jammer, they operate in the frequency band where most wireless cameras operate, effectively blocking their transmission.

Fig. 2.10 Cellphone jammer



Analog and digital recorder jammers involve a device that prevents recording of conversations in a specific room, neutralizing the microphones of recorders present there. There are two basic categories of such devices. The simpler form looks like the one shown in Fig. 2.11 and creates white noise (random frequency and amplitude sound similar to the noise that an analog TV makes when is not tuned on a channel). This noise gets superimposed to the normal conversation. The combined sound recorded by the intercepting setup is very difficult to understand. Apparently, this sound is also audible from the participants, thus making it a quite annoying solution. More advanced devices like the one shown in Fig. 2.12 produce inaudible frequencies in the ultrasound band that have the same result. Although not necessary per se, in order to be unnoticeable, they can be housed inside an “innocent” device such as a clock.

Excellent audio interception security is provided using a special intercom system. The simplest form of consists of a helmet with a microphone and headphones that is connected to a same one used by the other participant. Voice is amplified from the microphone and transmitted to the headphones of the other participant,

Fig. 2.11 White noise jammer

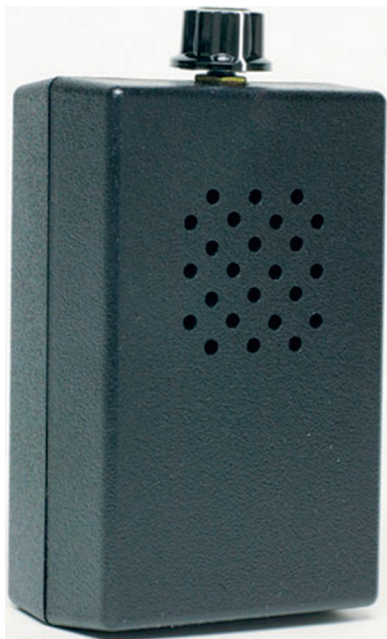


Fig. 2.12 Ultrasound jammers



while the helmet itself does not allow sound to be audible outside of it. Needless to say that it is not very practical and not many executives would like wearing it.

Having already secured that there are no interception devices present in the room, then telephone communications need to be protected as well. This can be made possible by using crypto devices (both for cellphones and landlines) that, as the name suggests, encrypt the telephone calls.

2.7 Summary

It is obvious that the devices portrayed in spy movies that were merely beyond imagination a few decades ago (James Bond, Mission Impossible, etc.) have become a reality. The most worrying fact is that nowadays their cost is very low (even 20€ are enough for a fully functional device), and they are relatively easy to find in the market. Detection on the other hand requires much more expensive equipment and expertise as we will discuss in the corresponding chapter, especially in the presence of professional and advanced interception devices. Continuing on to the next chapter, we will examine interception of computer data.

Industrial Espionage and Technical Surveillance
Counter Measurers

Androulidakis, I.I.; Kioupakis, F.-E.

2016, XIII, 126 p. 74 illus., 65 illus. in color., Hardcover

ISBN: 978-3-319-28665-5