HIDDEN ELECTRONICS DETECTION

Michael K. Ferrand

Microlab/FXR
Ten Microlab Rd.
Livingston, N.J. 07039

Abstract

The recent bugging of the U.S. embassy in Moscow has caused widespread attention to be focused on eavesdropping as a modern security threat. A brief history of electronic eavesdropping is given, and techniques used by persons wishing to gain confidential information are described. Various methods of detecting RF transmitting devices are explained and the limitations of conventional means for locating them. A device capable of transmitting an extremely pure fundamental signal and "listening" to harmonic signal reflected by semiconductor devices will be explained and demonstrated. The theory of operation is described and description of the electrical circuits will be given.

History of Electronic Eavesdropping

Electric eavesdropping was born with the first use of electricity for communication. The telegraph was the first device to be spied on. During the Civil War telegraph wires were tapped to obtain battle strategies. No doubt that soon after this discovery coded messages and countermeasures were in place. By the 1880's relatively sophisticated methods of protecting both telephone and telegraph conversations were in use. In the 1890's electric eavesdropping became a standard tool of booth law enforcement agencies and by persons whom today we would characterize as dishonest, but at the time did not violate any specific statutes. Throughout this century, vast improvements have been accomplished in electronic communication techniques. With the development of the transistor in the 1950's the high voltage power supplies needed to power vacuum tube were no longer needed. The development in the 1970's of the low-drain transistor, the long life battery, the micro-cassette, and the commercially available miniaturized voice actuator have given the eavesdropper another major step forward.

The Electronic Eavesdropping Detector

The problem of detecting electronic bugs has been of paramount concern to government agencies and law enforcement officials for many years. The device described, which we will call the "B1" uses the well known properties of semiconductors to locate listening devices whether or not they are in operation. It had been speculated for years that when a pure signal illuminated a semiconductor, harmonics or distortions of this pure signal would result. At that time, no one was able to confirm this speculation because all the available signal sources were so full of their own harmonics that the tiny harmonics that might result from an illuminated semiconductor were lost. Microlab/FXR investigated this problem in the late 1960's and then embarked on a research program that continues to this day. Using the technology we had developed in the microwave filter area, filters were developed to reduce the harmonic level of an output oscillator to 10-17 times the fundamental. Novel circuitry was developed to prevent harmonics from being developed inside the circuitry itself and to interpret the signals that might be returned from an illuminated area.

Bugging, Where, When and How

The RF transmitting bug is believed to be the most prevalent eavesdropping device by a wide margin. These are tiny devices that are reported as being placed inside the martini olive, inside fountain pens, walls, furniture, virtually anywhere the mind can imagine. The RF transmitter sends its signal to the eavesdropper's listening post where the information may be heard or recorded on tape.

In their most simple form, these bugs consist of the following:

1. a microphone
2. an oscillator to generate an RF signal that will serve as a carrier.
3. a means to modulate the output of the microphone onto the RF signal.
4. an antenna to radiate the modulated RF signal to a distant listening post.

0149-645X/88/0000-1035$01.00 © 1988 IEEE

5. a power supply to drive the oscillator and the modulator.

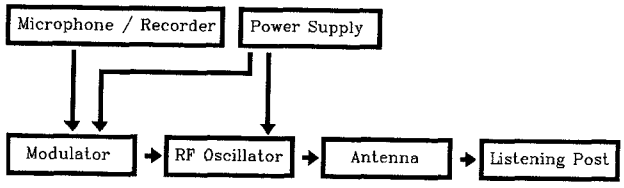


Figure I RF Transmitting Bug

At first glance the detection of an RF bug with a radio receiver appears simple. Indeed a number of companies advertise receivers that "light up" whenever they are in the same room as a bug. After all, even a tiny bug must generate a detectable signal when you're right on top of it.

As a practical matter, RF transmitters are very difficult to detect with RF receivers. First, the eavesdropper can select his operating frequency anywhere from below the AM broadcast band up through the short wave, TV, FM, VHF, UHF, and on to the microwave region. Many thousands of signals can be detected over these frequencies at any time. Each signal must be separately examined to assure that it is not a threat.

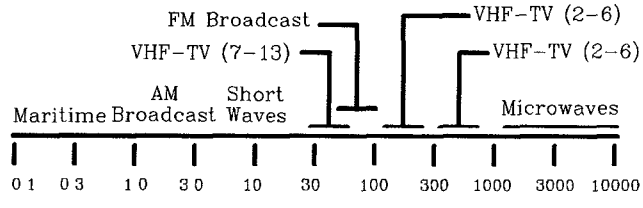
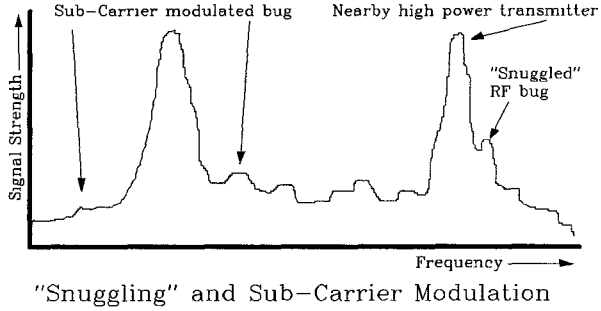


Figure II Eavesdropping Frequencies

The eavesdropper can further conceal his presence by selecting his operating frequency so as to "snuggle". In this case the bug frequency is placed as close as possible to that of a nearby high-power commercial transmitter. The associated listening post uses a highly selective narrow band receiver to separate the bug's signal from that of the transmitter. Countermeasures receiver must cover wide frequency ranges and generally cannot be made so selective.



"Snuggling" and Sub-Carrier Modulation

Figure III

The eavesdropper can also minimize detection by using one or more techniques of RF switching to activate and deactivate the bug. These techniques keep the bug from generating unnecessary RF radiation which could lead to its detection. They also extend the life of the batteries in the bug. One such method is called voice actuation. This method automatically turns the bug on when there is a nearby conversation. When there is no conversation, the bug simply does not transmit and thus cannot be detected by a conventional "listening" device.

Remote switching is another method of RF switching. These bugs may remain absolutely silent for months or years, until the eavesdropper determines that he wants to listen in. Then the bug is remotely or electronically switched to it's "on" position and begins to transmit. The eavesdropper later turns the bug off when he has accomplished his mission. Remote switching makes it much more difficult to detect bugs by conventional receiver means. Storage and burst represents a third type of RF switching. An entire conversation is stored onto a tape recorder using a voice actuator to conserve tape. At a safe time the eavesdropper turns on the RF bug which transmits a playback of the tape to the listening post. This playback can even be accomplished at high speed so as to minimize the broadcast time required.

The eavesdropper can alternately employ timers to limit his RF transmission to preselected hours. A transmitter can also be triggered to transmit only when the lights are on and the room is occupied. Some of the foregoing methods of RF switching are totally beyond the control of a sweep team using a countermeasures receiver, such as storage, burst, timers and remote switching. Others, such as voice actuation and light switching, may be somewhat controlled by a sweep team but only at the expense of alerting the eavesdropper.

Numerous methods of modulation are available to the eavesdropper, ranging from very simple to rather complex. The variety of these modulation methods assists the eavesdropper in his attempts to avoid detection by a countermeasures receiver. Some of these modulation methods are noted:

Amplitude modulation (Conventional or Single Sideband)
Frequency Modulation
Angle Modulation
Phase Modulation
Subcarrier modulation (including pulse-position, pulse-width pulse-frequency, pulse-amplitude, and various pulse-code modulations)
Translated modulation

No countermeasures receiver is capable of verifying bugs using all of the available methods of modulation.

The microphone greatly influences the performance of any bug. More sensitive microphones with wider frequency response pick up more distant conversations. Directional microphones exclude sounds from unwanted directions.

Audio filters exclude specific unwanted sounds. Microphone miniaturization makes visual detection more difficult.

All electronic eavesdropping devices require some form of power supply. The miniaturized long-life battery is by far the most widely used power supply because it is so small, readily obtained, and easily deployed. But the life of a battery is limited so other power supplies are also used.

Ordinary house current is convenient for the eavesdropper to power his bug. Thus bugs are often located in wall receptacles, light fixtures and the like because the eavesdropper there finds a reliable and unlimited source of power. He may also place a bug inside a wall and draw his voltage from any nearby power cable. Telephone wires also provide a reliable source of voltage for the bug. Thus RF and other types of bugs are often located inside telephone instruments, telephone wall boxes, telephone switching circuits, or along telephone wires. These bugs may or may not pick up the conversations on the telephone lines. They are primarily intended to use the drive power provided by the telephone. Other power supplies include solar batteries, acoustic or barometric batteries, and other sophisticated sources of energy. These supplies are not believed to be in common use at the present time. Every transmitting bug requires some form of antenna. Long antenna wires of several inches or longer are commonly used and often lead to the discovery of the bug. Smaller ferrite loaded antennas are also used, as are clips that attach to and use existing wires in a building.

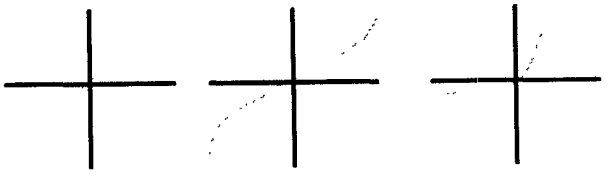
Several methods of packaging the bug are available to the eavesdropper. Generally the electronic components are mounted on a small circuit board which may be unprotected, wrapped in tape, contained within a metal, wooden, or plastic enclosure, or sealed in epoxy. Metal boxes are usually avoided because the eavesdropper wants to escape detection by a metal detector. Epoxy encapsulation is attractive because the bug may not be identified even if it is discovered.

Simple RF bugging transmitters are commercially available and sold under such names as "wireless microphones" and "baby sitters". The most sophisticated transmitting bugs are readily constructed by people with minimal electronic background. The seemingly high technology required and the illegality of the RF bug does not prevent it's wide deployment. The technology that is used in the B1 unit does not rely in any way on the RF transmission coming from the bug.

Theory of Operation

The B1 unit uses an electronic detection system that illuminates a suspected area with a low power UHF signal. The reflected signal is examined for harmonic content. All transistors and other modern solid state devices produce a positive response from the device. Normally only these devices product this positive response. The magnitude of this positive response increases as the electronics detector is moved closer to the solid-state device even when the device is completely hidden from vision and whether or not such a device is operating.

Corroded metal parts in loose contact with each other produce a negative response from the B1 unit. This non-linear phenomenon has been termed the "rusty bolt" effect and is a source of electromagnetic interference. Only such corroded parts can produce this negative response, the amplitude of which generally varies rapidly with time. All other objects such as wall, ceilings, furniture, fixtures and personnel produce no returned harmonic signal.



Most substances have linear current-voltage curves and generate no harmonics

Loose metal junctions have non-linear symmetrical curves and generate odd harmonics

Semiconductors have non-linear assymetric curves and generate even harmonics

Current-Voltage curves for various materials

Figure IV

The B1 evaluates the returned signal from the returned area and determines if any solid-state devices or corroded metal parts are in the suspected area. The appropriate readout is employed to display the desired information. Typically, a device containing transistors can be detected at a range of 5 to 10 feet and corroded metal parts detected at a range of 3 to 5 feet. The B1 electronic detection system can be broken down into the following sub-systems:

a. A solid-state microwave transmitter
b. Antenna assembly
c. A microwave receiver
d. IF Amplifier circuits
e. Processing circuits
f. An AC-DC power supply

The Microwave Transmitter

The fundamental transmitter power is generated by a transistor oscillator operating at a nominal frequency of 915 MHz. It produces a CW power output of 500 mW. The output of the oscillator is fed through a 15 dB. Directional coupler to a ferrite isolator, which prevents frequency pulling caused by large impedance mismatches at the face of the antenna. The side arm of the coupler provides a reference signal for a phase locked loop (PLL) from which the receiver local oscillator power is derived.

Antenna Assembly

The output of the transmitter module is fed to the transmit port of the boom antenna assembly. This assembly contains a resonant slot antenna for transmitting and a separate slot for each of the second and third harmonic receive frequencies. The transmit signal is fed through a pair of band-reject filters to a balun where the unbalanced impedance of the input coaxial line is transformed to a balanced impedance at the slot.

Microwave Receiver

The receiver input of the B1 unit is connected to a diplexer which splits the input into two bands. One is at the second harmonic and the other is at the third harmonic of the transmitted signal. Bandpass filters in the diplexer are tuned to each harmonic and provide further rejection of the transmitted signal. The output of each filter is fed to the signal input port of a balanced mixer circuit which provides over 15 dB. Rejection of local oscillator signals at the receiver input port and also very high attenuation at the IF port to AM signals which may be present at the local oscillator port.

IF Amplifier Circuits

The output of the second harmonic mixer is a signal at 1 MHz. (2 times the transmitter-VCO offset frequency). This signal is fed through a mixer bias circuit and an IF pre-amplifier. The level at the output of this preamp is sufficiently high so that further noise contributions are negligible and the receiver noise figure is established.

Processing Circuits

The outputs of the amplitude detectors of the two channels are combined in a difference comparator circuit. If the amplitude of the second harmonic channel is larger then the third harmonic channel a positive output results from the comparator. If the third harmonic output is larger, the comparator output is negative. This output signal is fed to three indicator circuits.

AC-DC Power Supply

A conventional AC-DC power supply provides -34V and +/- 17V unregulated to the B1 unit.

Conclusion

A novel approach for detecting electronic eavesdropping devices has been described. The increasing sophistication of the devices used for bugging has spurned new methods for protecting confidential information. Based on a relatively simple phenomenon exhibited by all semiconductor devices, this device has overcome some basic problems associated with traditional methods of electronic eavesdropping detection.