

Selecting the Device

In Section I, an Option Sequence was set forth leading us to the point where, based upon the intelligence gathered during the Target Analysis, we must now commit ourselves to the selection of the device(s) upon which we must depend. Within this Section we are going to look at various methods of attack, that is, the device. We will not, at this time, begin to explore the esoteric electronics of the various devices. We will, however, examine the pros and cons involved with each selection. We will attempt to discuss these methods of attack in a broad way, weighing the advantages against the disadvantages.

Early in this text it was said that the ideal method of eavesdropping was to be physically present during the discussion of interest. And still, we did not want to be detected; therefore our physical presence was ruled out. That is, unless we could somehow share the secret of Lamont Cranston (The Shadow). Well, lacking that talent, the next best thing to being there is to have placed the most basic of eavesdropping tools...the mic and wire run.

The Mic & Wire Run

Advances in technology have greatly altered this simple approach. Not only are microphones available today that are unbelievably small, but transmitting wire as thin as a single strand of hair from your head is available. It is virtually invisible to the eye and can be concealed in the cracks between the boards or tile on a floor or can disappear into the minute crack existing between the baseboard and the wall.

Microphones, either directional or non-directional, are no longer cluges...extremely high fidelity microphones smaller in diameter than a pencil eraser are commonplace.

So what are the disadvantages? Many! Microphone installations are not overly popular in that they require extensive access to the target area. It takes a great deal of time to properly install and conceal any microphone and, if one chooses to install the fine wire runs, great care must be exercised to avoid breaking the wires during the concealment process. Another disadvantage is that, unless one wants to run the transmission line into an RF Transmitter, install one or more line boosters, etc., the listening post must be relatively close by.

There are other methods to employ the microphone as your eavesdropping choice, among these would be tying the transmission line from the microphone to some fortuitous path, perhaps excess wiring among the utility lines or, more commonly found, excessive and unused telephone wiring. Still, unless the listening post is nearby you will be forced to employ line amplifiers along the path.

R.F. Transmitters

By far the most popular choice of "bugging" is the RF transmitter. There is any number of potential frequencies available. The signal may be modulated in many ways and combinations. Various esoteric techniques are possible, ranging from burst transmissions, to spread spectrum signals or swept frequencies. Simple frequency modulated or amplitude modulated signals might be "snuggled" with legitimate commercial signals; that is, transmitted at a frequency extremely close to the legitimate broadcast and at a signal level so weak in comparison that it is easily

missed during any countermeasures effort. The transmitting devices available today can be easily acquired, simple devices such as "Wireless FM Microphones" or "Baby Sitters", both of which are legally sold over the counter in many electronics stores. They can also be extremely complex and easily concealable because of their small size. The device can be hidden in the barrel of a fountain pen, in some office artifact, within a block of wood made to appear as a part of the furniture. The ways in which to hide an RF Transmitter are virtually limitless.

As I said, this is the conventional first choice. Still, they are not without problems. First, there is the need to limit the output of the device in order to make its detection as difficult as possible. When one reduces the output, the signal must still be strong enough to be received at the selected listening post. This means that one must carefully evaluate free space loss, building construction, atmospheric, etc. The necessary power to drive the device must be determined. Do you utilize batteries and have to service the device, or do you steal existing power?

Carrier Current

Again, this attack has certain advantages. You do not have to worry about providing power for your device since you will be employing the existing AC power lines within the target area. This approach has been used successfully in the past but is not frequently employed today. It is a rather easily detected attack, requires time to install and, of greatest concern, you must have your listening post very close by. The signal imposed on the house wiring will not easily couple across a transformer, requiring the listening post be set up on the same side of the transformer, usually within the building.

Telephone Compromise

Without doubt, the telephone represents the greatest threat to security (in terms of audio security) there is. To begin with, a telephone is generally found at or near the conversational center of the target area. It provides the would-be eavesdropper with all the necessary components (mic, power, transmission path, etc). One has the choice of performing any number of modifications to the instrument or tapping the lines. The difference being, of course, that if you elect to "tap", you are going to limit yourself to eavesdropping on on-going telephone conversations. By modifying the instrument you will be able to pick up in house conversations while the instrument is in an "on-hook" condition. The only disadvantages are that you must be able to establish access to the instrument and/or frame room.

Other Attacks

Let your imagination run wild...Laser attack? Light attack? The use of these will depend upon the Target Analysis you have accomplished. And, frankly, many of these attack methods, while technically possible, are not practical and/or give less than desirable results.