

The Threat Explained

Introduction

A viable TSCM Program is equally interested in Denial as well as Detection. Within limits, however, you cannot separate physical security from technical security. The following guide is intended to assist you in making the initial determination concerning the current ability of the physical security systems ability to keep the would-be penetrator from gaining entry into the target area which would allow them to introduce a technical surveillance device.

The Threat

Clandestine surveillance is nothing new. During its evolution, it has progressed from the simple act of peering through bushes to the point where conversations were monitored from outside a building near a door or window or from hidden locations within a building.

With the further development of electricity and electronics, the tasks became simpler. The telephone permitted conversations over long distances to friends, neighbors and business acquaintances. It also permitted the monitoring of conversations by everyone on the party line. Although it was insinuated that "Gentlemen don't listen to other Gentlemen's conversations", clandestine monitoring was coming into vogue. Initially, it was simply the monitoring of telephone conversations, but rapidly evolves into the planting of microphones in selected locations. Monitoring by microphones remained the primary, but in no way the only, means until the miniaturization of the tube and later the introduction of the transistor. At this point, it became possible to build a transmitter capable of being hidden in extremely small locations or packages. Integrated circuits and chips have reduced the size even more drastically, even to the point that the microphone and power supply may be the bulkiest portion of a very powerful and sophisticated clandestine RF transmitter.

What Is the Threat?

The question you are probably asking is "What is the threat and how does it apply to me". You all have your own thoughts on how serious it is. By analyzing the different types of documented attacks initiated against governments, corporations and individuals in the past, you will see a pattern which indicates attacks come in one or a combination of the following basic methods:

- The wire and mic
- The RF transmitter
- The physical security weakness

Telephones and the Mic and Wire:

The ubiquitous telephone, like a waiter, is always there, but never really noticed. As long as you are able to get a dial tone and complete a call, you are happy and never question its loyalty. But, it IS always there. And it IS always capable of doing more than it was intended to do. Even coming from the manufacturer in its original box can't guarantee the instrument isn't defective and won't be passing audio while it is in the on-hook position.

Assuming your telephone is operating properly when installed, there are a number of things which can be done to it in a very short period of time, a matter of minutes in most instances. The hook switch, inside the instrument, can be attacked and bypassed through the simple task of bending the contacts so they are always making contact. Different types of electronic devices can be installed across the hook switch-resistors, diodes, capacitors, and neon bulbs, for instance. The transmitter (mouthpiece) can be replaced with one that is in fact a transmitter, operating only when you are conversing. A transmitter can be hidden within the telephone, with a hookup to either the transmitter or the receiver (earphone), and connected to the incoming lines for power. This type installation would be operating at all times, not just when you are talking on the phone. Should the phone be permanently mounted to a desk or the wall, an induction coil could be hidden under or behind it. Going a step further, an induction device can be utilized on the telephone pair at any location between the point where the phone enters the wall and closer control is established at the main telephone plant. In addition, anywhere the cable pair is accessible, a tap of one sort or another can be affected, monitoring your conversations any time the phone is in use. If the information is important enough to warrant the expenditure, you may be monitored by intercepting microwave signals or even satellite signals.

The mic and wire is nothing more than a variation of the telephone tap or monitor. The only difference is that the microphone and wire must be installed. HOWEVER, there may be instances in which existing wiring may be used and there may even be a suitable "microphone" already present. I'm talking about those instances where replaced wiring is not removed, only disconnected. The actual microphones may be as small as those used in hearing aids or as large as a wolfer type speaker. If it can be properly hidden, or it looks appropriate for the location, it is effective.

RF Devices:

Mention "bugs" and almost everyone instantly thinks of the olive in the martini or the device which can be hidden behind the lapel of a coat. Hollywood theatrics, perhaps, but definitely possible.

What Is a "Bug"?

Essentially, it is a device utilized to transfer intelligence from one point to another and is usually considered to be RF transmitters of one sort or another. They may be designed to operate at any frequency range, at any power setting and in any modulation mode, depending on the requirements of the opposition and the circumstances of the situation. What this means is that if a short distance has to be covered with an RF signal, the transmitter could be operating as a simple low wattage, clear text, AM (Amplitude Modulated), lower frequency unit, or as a sophisticated 1/2 watt, crystal controlled, FM, (Frequency Modulated), Sub-carrier, VHF (Very High Frequency), or UHF (Ultra High Frequency) unit. Simply stated, the opposition has the advantage in that he may choose any number of frequencies, modulation, and power. You, on the other hand, don't know what his operating characteristics will be, whether he will be operating when you perform your checks, or whether you are even in the area of a target. But, EVERY survey must be performed as if there IS an operating device in your area.

What will you be looking for in the way of a signal or signals.

Everything!!!! You could be targeted by a signal which is AM amplitude modulation, FM frequency modulation, PAM pulse amplitude modulation, PPM pulse position modulation, spread spectrum, etc., and may be operating with signals that are composed of Sub-carrier modulation, Single side-band modulation, Double side-band modulation, etc.

They may be operating almost anywhere in the frequency spectrum VLF very low frequency, LF low frequency, HF high frequency, VHF very high frequency, UHF ultra high frequency, Light spectrum, etc.

Their intelligence might consist of Audio, Video, Data, etc.

They may be hidden in Offices, Homes, Apartments, Vehicles, Aircraft, Public areas, etc.

Information targeted may be Personal, Business, Travel, Meetings, R&D, etc.

Although the information provided above may look overwhelming, the task can be handled if approached a signal at a time.

Physical Security Weaknesses:

Where do you start and where do you stop. There is no clearly defined line. When evaluating an area during a survey, you will be interested in how the opposition could enter if they aren't approved personnel. Look at the doors and windows. Ask about personnel access restrictions. Are the locks and alarms acceptable? Specifically, when you are evaluating an area, you are interested in how someone may gain entry to a secured area or extract information from such an area. What you will be doing is performing an acoustical evaluation of the area to insure that conversations taking place within cannot be overheard from outside. Insure that the doors are flush with the facing at the top, bottom and sides. Walls should be solid all the way to the true ceiling-not stopping at, or above the false ceiling. All holes and openings in the walls should be sealed. All excess and unused wiring removed from the walls and the overhead. Remove speakers from the area, or make sure there is a positive means of insuring they are disconnected. Remove or disconnect phones. Is there an alarm system and is it working properly for secured areas?

What Are the Most Likely Target Areas?

Determining what areas are most likely to be "hit" will be decided by talking with security personnel as well as the manager or vice president in charge of operations. They may have decided the whole facility requires a TSCM survey when in fact only a few select areas need be examined. Primary interest should be those places where the information comes together-the executive areas, program managers, conference rooms, etc. We are looking for the apexes, because obviously, it is impossible to "bug" every room and phone in a large complex. In addition, management should be concerned with such areas as contract negotiations, executive personnel records areas and so on. In determining when the best time for a survey might be, consider immediately prior to any important happening, such as contract negotiations, product development or release, major financial happenings, anything that could have a strong bearing on the company's well being and continued success. That is not to say that intelligence is not gathered at times other than during those periods. Larger organizations may require a survey on a monthly basis or no more often than quarterly or semi-annually. If it is done on a recurring basis, the service should not be performed on a clockwork basis, but on a more random basis. A pattern should be avoided.

Limited Surveys and Monitors:

Limited surveys are those actions performed covering limited areas and/or time. Normally a limited survey would be performed on an area such as a conference room in which a sensitive meeting is to be performed. The meeting is generally scheduled to begin at a certain time and the TSCM technician may have only an hour or so to perform the major aspects of a physical examination with an in-place monitor to be conducted during the course of the conference. If that is the situation, one person should begin an RF examination while the other performs the physical portion.

Under these conditions, nothing can be guaranteed, but an effort must be made to check ALL the obvious places first and work back to the less obvious. An hour is quite a bit of time when nothing more than a good physical is performed. You will be removing plug coverings and checking wall hangings. Furniture is examined to insure there are no added pieces of wood, insure that the seat bottoms have not been cut or ripped in such a manner as to permit the introduction of a recorder or a transmitter. Check the overheads for anything that appears unusual--extra wiring, boxes or packages, wood or concrete chippings, even pieces of wood or concrete which could be hiding a monitoring device. If possible, check the adjacent areas and the outside walls for similar items located near the walls of the secured area.

When performing a monitor or an RF examination, write down all suspect signals and come back to them after you have completed a thorough examination of the spectrum. Unless something is not right, you shouldn't spend too much time on any one particular signal during the initial phase. If something is found, notify the proper person immediately. BUT, don't assume that is the only device that has been installed. There very well could be several more.

Who the Customer Should Suspect:

Anyone associated with the activity could be a suspect. It may be a disgruntled employee "getting back at you", or outside elements, such as the opposition. It could be friendly or hostile governments, or terrorists. Don't disregard the criminal element planning a kidnapping or robbery. Anything and everything is possible.

How Access Can Be Gained:

That may be the simplest part of the whole operation. Who really looks at a maintenance delivery person? How about the building custodians and repairmen? The char force has more opportunity than anyone else, with the possible exception of the night and weekend security force. Seduction may be the best way--we then have as suspects a spouse, secretary, or lover. The list can go on and on, but I'm sure you're getting the drift of the discussion.

We have little control over these things; we MUST be aware that they are possible when evaluating an area. As you gain experience, you will get a feeling about what the potential problem may be and key on those areas.