

Telephone Threats

Introduction:

Due to their greater susceptibility to a variety of attacks, telephones probably pose the greatest single threat to audio security. Look around and you see them everywhere, with a growing number of attachments. Many of these attachments are capable of being utilized as installed, or modified with little effort to be used effectively as an aid to extracting audio from within an area.

Now, what are the ways in which information can be extracted from within an area? Basically, through the use of either a wiretap or a compromise (or bug).

If you remember from the introduction, we described a wiretap as an intercept of information while the telephone lines are in use, such as during a call. Bear in mind that any information appearing on the telephone lines is susceptible to intercept-data, fascimile, or any other form of intelligence. A tap can be made at almost any point between the transmitting and receiving telephone, but will most usually be between the transmitting phone and central office.

A tap can be affected without actually making direct contact with the lines involved. This is done through the use of induction coils, similar to those sold as accessories with most recorders. The results will not be as satisfactory as those obtained with a direct hookup, but they will be acceptable.

If a tap is properly installed, paying careful attention to impedance matching, it will be virtually impossible to detect-short of a physical examination of the telephone line pair involved. That means an examination from the instrument straight through to the central office, making a positive identification of every connection encountered.

During your training session on telephones, we will not be involved with taps to any extent. During your briefings, you will explain that you are checking the telephones and associated accessories only to the point where they enter the cable connection at the wall or floor. You cannot guard against what is said on the phone while it is being used legitimately.

Now, while most people are aware that a phone can be tapped, remarkably few are aware that it can also be turned into a very effective monitoring device, even while the handset is still on the cradle. Such an attack is usually called a compromise, but is better known as a "bug".

For the purpose of transferring audio, a compromise must have at least two things, and in some instances three.

- a. a transducer or microphone
- b. a vehicle (lines or a transmitter)
- c. power

In any telephone system, you have all three of these available.

There are generally three transducers available for use in every phone in use. These are the dynamic microphone known as the EARPIECE, the carbon microphone in the mouthpiece, and (is nothing any longer sacred) the RINGER. NO!! says you. YES!!!!!! says I.

"How can that be?" says you. "Simple" says I.

The "clapper" in most telephone are modulated by room audio and in certain instances, some telephones are resonant enough that this audio can be picked up by a high gain amplifier.

Don't relax yet. There are even more modern inventions to complicate an otherwise dull existence for the countermeasures person. In their infinite search for labor savings devices, an additional goodie was added--the speaker phone.

If you are like most other people involved in countermeasures or security, your next question was "WHY".

I wish I had a good answer for you, but I don't. In almost 100 % of the time, it is nothing more than a status symbol. When used as an amplifier for conference purposes, it is a very effective addition. But when used by most users, their conversations sound as if they were coming from the bottom of a deep barrel.

But this is no deterrent for an accomplished "spy". He will be eternally grateful for the constant search for "status symbol" attachments. Each one gives him an added opportunity to utilize an existing weakness of the system.

First, should a device installed in a telephone require power for operation, there is more than sufficient voltage available? When resting on-hook, there are 48 volts DC available. During a ring period, the voltage increases to approximately 100 VAC or pulsating DC. Upon lifting the receiver from the cradle, the voltage drops to approximately 7 VDC.

Next, let's begin looking at some of the ways in which a phone can be had. v First, is a simple drop in transmitter in which the mouthpiece is replaced with a look alike. The replacement mouthpiece has a built in transmitter which may be capable of transmitting an rf signal through free space or as a carrier current signal over existing lines. The "drop-in" can be installed in a matter of seconds and can be very difficult for the untrained person to detect.

Next, we will be exploring the use of wire and microphones, and considering the small size of microphones available, it shouldn't be too difficult to visualize how easy it would be to hide a microphone in almost any telephone and utilize the existing wiring to route the audio out of the area. Should you feel uncomfortable installing an additional microphone, go ahead and use the existing ones described above.

Progressing to the slightly less exotic, there are a number of things that can be done to the hook switch in order to get audio out of an area, to include rewiring the switch, installing a resistor, a capacitor, a neon bulb, a diode, a transmitter, bending and shorting the hook switch contacts, etc. All of these will allow conversations to be monitored while the phone is on hook and still permit incoming calls as normal.

The primary device which can be used that renders the phone inoperative from the point of incoming calls is the infinity transmitter. It is a device which is installed in the phone; the "bugger" dials the number, and prior to the phone ringing, he activates a tone device which in effect blocks the ringing voltage from the ringer and causes the phone to act as if it had been picked up. Conversations in the immediate area can then be monitored. If the phone is picked up to make an outgoing call, the infinity transmitter is immediately deactivated and the phone functions in a normal manner.