Who's Listening?

About the author: Ian Murphy, aka Captain Zap, is the President and CEO of IAM/Secure Data Systems. He can be reached via email at ravensceo@ravenswoodinc.com

Satellite Jamming Devices And Interception Of Data!

By Ian A Murphy

Could someone with off the shelf parts inflict damage and harm by jamming satellites? According to this columnists research, it would be possible as discussed in the August 2002 installment of Who's Listening. Now we learn more on how this could happen.

You don't need large dishes with great amounts of power to do this. All that is needed is a moderate size dish, a few tens of watts at microwave frequencies, and Bingo! You've got an effective satellite jamming station! And then you have to address the issue of the telemetry channel. They may not be able to overtake the signal, but if jam the signal with another, it may be possible to affect the operation, stability or orbit of the target. Frequencies for such channels are available from a number of sources and for as little as $2.50 per frequency.

Now these examples and the reported stories dealing with television stations interruption's are fast becoming one of the most feared aspect of open air transmissions. Such transmitter frequencies are no longer the domain of commercial radio and television stations. Transmissions on any frequency are just a phone call away from suppliers who provide common or business radio transmission technology.

So if satellite and television stations can be interrupted by such forces, six million dollar helicopters are taken down because of CB radios, and automobiles cease to operate due to a wide spectrum of emitted signals, then the possibility to intercept and harvest vast amounts of knowledge is available to those who wish to gather such. Now to explain such basic interceptions are now commonplace with horrific results to those who do not believe that such things can happen. For a simplistic view of such emitted signals, take a standard "Walkman" type of radio and visit one of the many locations of ATM's or better known as "money machines". (This exercise may also be performed near any standard personal computer if ATM's are not available.) and tune through the FM band. With careful tuning, one will be able to "hear" machine functions occurring. Taking basic simple electronics, one may have the ability to receive and reconstruct such impulses to a readable form.

Or an example of larger scale and better know, would be with the use of back-yard home satellite dishes. Dishes range from 6 to 12 feet wide. Signals available include music, sports, news, movies, stock and commodity trading quotes, weather, education and other such information services. In addition to these services, a number of different multi-site conference services are available from a host of major hotel chains as well as privately organized meetings held for specific time periods and dates.

All may be tuned through the use of a dish and sensitive information that may not be available to someone, is then made available and no one is the wiser! Transponders are not private, and are rented out for only the time used. And one other thing that might bring you to your senses about such signals, is that the signals are transmitted by the satellite over a wide area to anyone who can receive such signals.

One other development is the small Micro-Sat by Norsat. This complete system offers both satellite bands coverage, Ku and C, a small dish and circuit board that fits inside an IBM PC. The unit downblocks 950 MHz to 1.45 Ghz, offers a maximum baud rate of 9600 BPS, frequency, bandwidth, video and audio selectable formats and may be connected to the VideoCipher II, B-Mac and Oak Orion descrambling systems.

Some other such signal reconstruction devices are now also available through the mails. One such device is available in plan form from Don Britton Enterprises and is called the Re-Process Sync Amplifier. The device was

developed to receive signals emanated from cable television systems. What the device does in essence, is to take a signal that "leaks" from cable TV systems and receives such, adds a sync signal needed by the television set to display the received signals and then sends the signal to the antenna input of the set so that display may happen. Now if weak signal reception is available from leaking cable systems, then the ability to receive weak signals from logical devices is also possible.

Interception and Weapons Possibilities

Think about possible interception points pertaining to logical security methods. Communications may be encrypted, data may be stored in an in-active form and access is only a matter of time while the interceptee is waiting for the dispersal. The next security concerned area covered would be for the encryption of the information in its stored and transmitted form. The encryption is all wonderful and good for the transmission and storage, but does nothing for the information as it is in its final stage to the human eyes!

And you only have two ways to get it to the eyes, in hard copy or by a video screen. Now you think that interception is not possible since the information is encrypted, but the data must be decrypted so that the human connection may use the information. The human connection allows for the reception of said information by the afore mentioned devices and lets interception to happen through the clear or decryption points of the attacked devices.

One other point to mention; other possible effects of reception / transmission to security in general, could affect other controls ranging from building energy management to security access and monitoring controls. To give a better understanding of such equipment, we will discuss some of the devices known. One such device known as the Van Eck device and the other is called the Re-Process Sync Amplifier. Some may feel that there are two different systems involved in this discussion, but the author finds no major difference between the two, with the exception of the Van Eck device is built for operation on European voltages and has a built-in digital frequency meter. The one major difference found is with the dates of copyrights for the two devices.

The Don Britton device is dated 1979, while the Van Eck unit is dated October,1985. Note: Another unit, with plans for such devices, are available from Consumertronics, located in Alamogordo, New Mexico. Besides the plans for a Van Eck type reader, one book offers information in reference to computer crime and countermeasures, how systems are penetrated, BBS advice, Password defeats, TEMPEST, crosstalk amplifiers and a 200 word phreaking terms glossary. All for only $15.00 We will begin with a basic understanding of the inner workings of the device.

The one other major basic difference with the two reader boxes is that the Van Eck box is designed for use with TV's and VDT's used in Europe as compared with the Britton box built for use in the United States. This device in general, is designed to restore and regenerate the sync and colorburst signals and ignores all information appearing during either the vertical or horizontal blanking.

Its basic result is reconfigure through the use of supplying artificial external signals inputted directly to any video monitor through a simple 10-50 dollar modification of the TV or video monitor, or in simple english, takes a weak video signal and tries to shape or match it and then boost its output to a normal television screen.

One other interesting thought comes to mind with the use of video tape copy protection methods. Since these methods use a means that makes it tough on the VCR not the TV from generating signals for tape duplication, there have been a number of devices that assist in the restoring and re-structure of the picture and sound. One device is known as the "Line Zapper". The device helps to adjust the brightness changes, vertical jumping and jittering, and video noise. It is available in kit or complete form.

Pricing starts at $69.95 and complete tested units cost $124.95. Now if this unit can assist in the filtering and structuring of commercially induced weak signals, then it should be able to take a boosted signal presented to it and clean the picture to something of useable form. Some may see this only as a filter for video processing with a focal point on the actual copy-guard techniques, but such a device incorporated into the Van Eck type of gear should assist in the overall signal restructuring.

Now one other interesting point about possible video signaling re-construction methods was addressed in a multi-part series published in Radio-Electronics based on the methodology used for the construction of video signals scrambled by different vendors of cable and over-the air pay television. The series dealt with all aspects and methods of video and audio, (complete with discussions on the DES methods used for the VideoCipher units and the like,) used in commercial systems in use. One other thought comes to mind of an experimental nature.

Since the screen of a computer is not always changing and for the most part stable in its display, why not take the received signal and digitize it! You could filter out signal noise clean up any true video signal present. This is no great techno-wonder, the basic gear could be put together with Radio Shack or the like types of equipment. And the cost is still most reasonable. If not available there, costs for home-brew gear would not be that high. The simple electronics blocks would consist of comparators, video detectors, data seperator gates, a to d - d to a converters, data amp and a signal level converter.

(**Next Month:** *How to make a simple and cheap transportable reception device made with easy to buy Radio Shack parts!)*