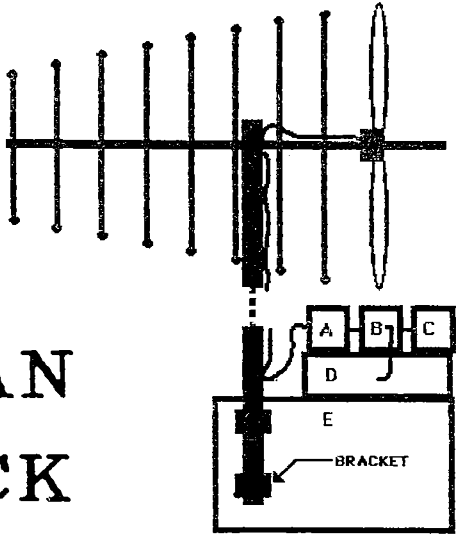
BEYOND



VAN ECK PHREAKING

BEYOND VAN ECK PHREAKING

CONSUMERTRONICS, 2011 Crescent Dr., P.O. Drawer 537, Alamogordo, NM 88310.

INTRODUCTION

It has been clear for decades that, at least in theory, that the reception of **Video Display Terminal (VDT) Electromagnetic Interference (EMI)** could be remotely intercepted and reproduced – regardless of the type or make of the VDT used. In 1985, **Wim Van Eck**, doing security research for his employer (**Dr. Neher Laboratories PTT**, Leidschendam, Netherlands), experimentally proved that such eavesdroppings could be made practically by anyone with a minimal investment in equipment and technical expertise. And that successful eavesdropping can occur at ranges beyond 1 km using an ordinary TV (ie: TV receiver), an external sync. generator and a directional antenna.

The methods developed by Van Eck are described and amplified herein, as well as countermeasures. This information is provided for educational purposes only. We do not suggest that any illegal use of it whatsoever be made. If you have any additional information on these methods and countermeasures, please send it to us at the above address.

Although Van Eck eavesdropping is misbelieved to be only a form of passive tapping – that is, the eavesdropper cannot affect what is being displayed on the VDT or processed by its computer – there are exceptions. For example, if some of what is being displayed/processed can be controlled by the phreaker (ex: thru an active phone line tap), he can prompt responses from the VDT operator/computer and provide him/it misinformation, based upon all of the displayed info. all of which may not be available from the phone tap alone. It is also possible for a phreaker to gain control of the computer itself, and thru an unmanned but live VDT, get it to divulge info. that it refuses to transmit by phone, by having it display the info. on the VDT instead. Secure computer systems closely monitor what info. is transmitted by phone. Since none would be in this case, no security alarm would be activated. Some of this divulged info. (ex: passwords, keys, PINs) can be used for subsequent non-Van Eck attacks. The phreaker can also save himself considerable cryptanalysis efforts if he can correlate a plaintext display with its transmitted ciphertext.

Although it is widely misbelieved that Van Eck's discoveries have only illegal applications, this is NOT true! A Van Eck set-up is a cheap and versatile way of obtaining additional computer monitors without the need of making hardwired connections, board insertions, monitor purchases, etc., and to enjoy computer games designed for TV displays. Van Eck can also be used in cases where more than one TV is tuned to a certain channel, without the need of additional cabling or antennas.

For additional info. on Van Eck methods, see the prestigious: **COMPUTERS & SECURITY**, Vol. 4, Dec. 1985, ATTN: **DR. HAROLD JOSEPH HIGHLAND**, Distinguished Professor Emeritus, **SUNY**, 562 Croydon Rd., Elmont, NY 11003.

BEYOND VAN ECK PHREAKING is published by:

CONSUMERTRONICS
2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310

ELECTROMAGNETIC INTERFERENCE (EMI)

From **Maxwell's Equations**, the strength of an electromagnetic field is directly related to the acceleration of electric charges. Consider:

(1) Whenever fast-rise square waves and pulse trains are applied to non-linear junctions, characteristic of semiconductors, radiation of harmonics of the them occur. In fact, a common security practice to find electronic bugs and taperecorders (active or dormant), hidden in a room is to swamp the room with microwaves and observe the return of first harmonics that result from non-linear junction action. In fact, it is this reason why the Soviets buried thousands of cheap diodes in the walls of the new U.S. Embassy in Moscow. By swamping the Embassy with non-linear junctions, they could conceal actual bugs. For pulse frequencies (freqs.) in the 1-20 MHz range common to modern computers and terminals, significant radiated harmonics extend into the UHF region.

(2) The strength of EMI is much more affected by the rate of change of an electric current than by the magnitude of the current itself. Since computers use digital switching with extremely fast rise and fall times, they produce far more EMI than do analog devices.

(3) The spectral density of any waveform can be defined using Fourier Analysis. Square waves and pulse trains are rich in freq. content. The freq. contents of any digital pulse train depends upon its fundamental freq. (if any), pulse width, duty cycle, rise and fall times, etc., and can vary considerably between different types of pulse trains. Thus, the EMI they produce is also rich in freq. content – broadband EMI. Broadband EMI is harder and more costly to eliminate than narrowband

(4) The spectral density for typical digital waveforms decreases with freq. This is compensated for in the radiated field because higher freqs. radiate more efficiently than do lower freqs. by conductors due to antenna and field considerations. As it turns out, the received spectral density is roughly constant thru the entire band of radiated harmonics. Since VDTs are mostly constructed of digital circuits, its cir-

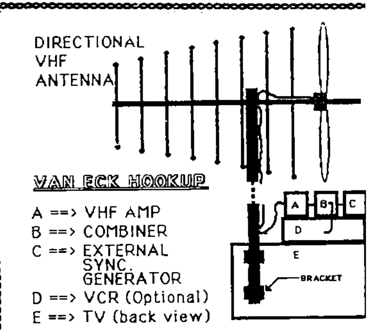


FIGURE 1: ACTUAL HOOKUP OF THE VAN ECK PHREAK STATION.

cuits radiate just as those of the keyboard, expansion interface, etc., with the exception that much added EMI comes from the VDT's Cathode Ray Tube (CRT) itself. A phreaker can pick a quiescent between-station VHF-band setting with his TV to monitor a VDT signal hundreds of yards away.

(5) Any conductor that carries an electric current acts as an antenna and radiates a field produced by that current. Computers typically contain thousands of conductors (PC board traces, wires, etc.) varying from a few millimeters to hundreds of centimeters long. And broadband signals have high probability that one or more freq. components will resonate with any circuit conductor, resulting in an efficient signal-to-antenna coupling. Thus, computers act as nearly ideal antenna fields for the broadband EMI they produce in abundance.

(6) The amount of escaped EMI largely depends upon the shielding used. Modern computers are shielded to fairly stiff FCC regulations. The old TRS-80 Model I produces such a high EMI that you could troubleshoot it using an AM radio! It is such a good noise radiator that I was tempted to include it in our Jammer section in our HIGH VOLTAGE DEVICES ($20) manual. Still, modern computers radiate more than enough to be eavesdropped upon. For example, with the IBM-PC, we got excellent reception at 10 yards when tuned at 95.4 MHz (apparently the 20th. harmonic) on an FM radio with an ordinary whip antenna that we bought at a garage sale for $1. We recorded the results on an el cheapo cassette recorder. Viewing the played-back signal on the oscilloscope revealed that each key had it's own characteristic signature that could be digitized, analyzed and reproduced! In other words, a phreaker with an el cheapo FM radio and cassette recorder can eavesdrop on modern, FCC-approved IBM-PCs and compatibles. One doesn't even need a Van Eck set-up!

MORE ON VDT EMI

The actual field radiated by the VDT consists of a linear combination of low-level narrowband harmonics radiated by the clock circuitry, broadband harmonics radiated by the mixture of various other square wave and pulse train circuitry, including the video signal. The video signal is amplified by the video signal processing circuitry from the TTL level to hundreds of volts to drive the electron beam of the CRT.

For example, if the VDT's system clock freq. is 1.6 MHz and its video dot clock is 12.0 MHz, you will find narrowband noise harmonics spaced 1.6 MHz apart. The level of broadband EMI largely depends upon screen density (ie: the number of displayed chars., proportional to the level of the video signal component). The level of narrowband EMI does not depend upon screen density but upon the VDT's system and video dot clocks. From experiments, it is concluded that the video signal is the most powerful source of broadband EMI while the clocks are the most powerful sources of narrowband EMI.

Except in cases of localized electromagnetic eavesdropping, it is the radiated video signal that is of most interest to the phreaker. Each radiated harmonic of the video signal is remarkably close to that of a typical broadcast TV signal except that it usually does not conveniently occur at a standard broadcast station.

However, the received signal does not contain the Vertical Synchronization (VS) and Horizontal Synchronization (HS) components. This is because synchronization (sync.) freqs. are so low that they transmit very poorly. To receive the video signal on a TV without the syncs. gives the appearance of a scrambled TV signal. In fact, the techniques used to recreate the syncs. are similar and also applicable to those used to unscramble some types of scrambled TV and to record VHS tapes protected with Copy Guard.

Many urban dwellers who use external, directional TV antennas, are now annoyed by VDT EMI without even being aware of it. These signals may give the appearance of an unknown scrambled station superimposed upon an existing station, or patterns consisting of herringbones, diagonal lines or bars, or a windshield wiper effect (radio EMI will also cause some of these effects). And these people can receive more VDTs (and more clearly) simply by using and pointing directional antennas in the direction of where VDTs get their heaviest uses - professional and financial offices - and tuning between stations using their VHF fine-tuning knobs. Van Eck performed his experiments in a roving vehicle. Although a mobile receiver can cover a much greater area than a stationary receiver, roaming around with a 30-foot directional antenna could prove embarassing - especially with the increased awareness of Van Eck phreaking.

With the increasing advent of home and office personal computers, telebanking, viewer-response TVs, VCRs, etc., neighbors can eavesdrop on each other using Van Eck methods. Several years ago, a young couple living in a condo were fond of taking home movies of their sexual activities. Then, they would play them back on their VCR late at night. Unfortunately, they had left a roof-top antenna hooked up to their TV's VHF antenna screws, which also served as the input from their VCR. Needless to say, much of their neighborhood shared in their enjoyment. Only after receiving weird stares and obscene phone calls did they finally discover the embarassing truth. Even without an antenna hookup, they would have been at risk to the Van Eck phreaker who could eavesdrop on the EMI of their TV's CRT blocks away!

HOW TVS WORK

Figure 4 is a simplified block diagram of a TV. Note that the VS and HS signals are broken out by the Video Separator. Most TVs are equipped with a VSB demodulator and a detection BW of 4.5 MHz. This is equivalent to an AM detector with an 8 MHz detection BW. This means that the TV can look at only a small slice of a signal lobe (20-50 MHz wide) of the VDT, thus inter-channel VHF fine-tuning is important, and the reconstructed image suffers directly from whatever portion of the BW that is either missed or not detectable.

CONSUMERTRONICS
2011 Crescent Dr., P.O. Drawer 537
ALAMOGORDO, NM 88310
(505)-434-0234

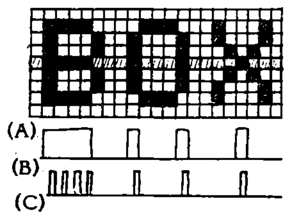


Figure 2: Display of a video signal by a VDT. (A) shows how a CRT image (BOX) is created from pixels. (B) is a typical initial video signal, and also the observed optical display. (C) is a typical final video signal that controls the electron beam intensity. This signal is derived from the (B) signal by ANDing the (B) signal with a square wave whose *period* is about equal to the *duration* of the minimal (pixel-length) (B) pulse width. The reason why (C) and not (B) is used to control the electron beam is because the beam produces some smearing so (C) is required to produce the sharpest images. The CRT's Brightness Control dictates the width of (C)'s pulses. The brighter the setting, the wider the pulses. For very bright settings, narrow pulses begin to appear at the zero points, which result in a brightening of the CRT's background. That's why a bright screen produces smeared images. The (C) pulse amplitude are set by the CRT's Contrast Control. The greater the amplification of the pulse, the greater the image contrast, and the sharper the pulse skirts are.

You can verify these things by playing around with your TV or computer monitor Brightness and Contrast controls. At that time, temporarily set the Brightness Control low. By doing this, you can easily see how the individual pixels are formed. Then, temporarily set the Brightness Control to full bright. When you do this on some monitors, the vertical retrace is revealed. As you can see, vertical retrace occurs in steps that progressively compress at the top of the screen due to manner that the vertical voltage falls. You can also count the number of horizontal trace lines per display line or per inch.

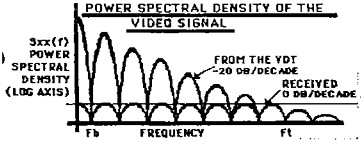


Figure 3: POWER SPECTRAL DENSITY (PSD) OF THE VIDEO SIGNAL. As you can see, in theory, the received signal has a flat PSD upto about 9 harmonic lobes, then it decreases by about 20 DB per decade.

VIDEO SIGNAL COMPONENT

VDT screens are composed of pixels (small dots), of which all alphanumeric and graphical images are composed. The pixels are laid out in horizontal lines that are scanned by the CRT's electron beam, similar to TV ("composite color" computer monitors are basically color TVs). To create pixels, the electron beam is switched ON and OFF (ie: modulated) as it horizontally scans. The video signal is a digital signal in which a logical zero turns-OFF the beam (ie: inhibits the spot), whereas a logical one turns-ON the beam (ie: creates a spot). Therefore, there is a direct and predictable relationship between the video signal modulation and the resultant image.

PHREAKING "BENEFITS"

The many "benefits" derived by phreakers to eavesdrop on private, commercial and government VDTs are:

(1) To learn access codes, passwords, PINs and keys to later penetrate the system or defraud it or its subjects (ie: clients, employees, patients, etc.) in some other manner.

(2) To learn personal information about subjects for its intrinsic (ie: gossip) value.

(3) To learn more on how systems work; to satisfy curiosity; for the sheer joy of hacking. There is now a small but growing number of "Van Eck Listeners" (VELs) pioneering these techniques in the traditions of SWLs and scanner listeners.

(4) To obtain government, trade or business secrets (ex: client lists, price lists, supplier lists, product designs, publications, etc.). Such knowledge can be worth $ Millions! And such practice is most probably illegal!

(5) To obtain knowledge on subjects of interest (ex: medicine, law, government).

(6) To obtain news and announcements before they are publicly known and before they are heavily censored.

(7) To investigate a person, business or association.

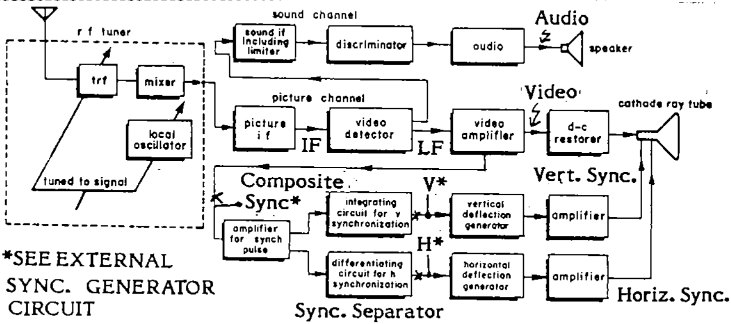
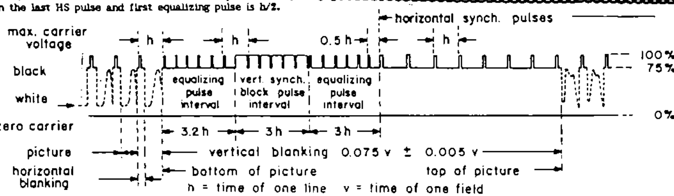


Figure 4: Block diagram of a TV (derived from **Cleveland Institute of Electronics (CIE), "Monochrome and Color Television"**, 1960, P. 21). Notice insertion points for the composite sync., and for the HS and VS (generated by the External Sync. Generator).

Figure 5: U.S. Standard Envelope for Monochrome Modulated Carrier, First Field (derived from CIE, **"Monochrome and Color Television"**, 1960, P. 17). The Second Field looks identical except that the spacing between the last HS pulse and first equalizing pulse is h/2.



The power spectral density of the video signal can best be described by the formula shown:

$$S_{XX}(F) = A\left(\frac{\sin \pi F T_b}{\pi F T_b}\right)^2 \left(\frac{1}{\pi F T_T + 1}\right)$$

Where Tb is the duration of one bit in the final video signal (Figure 2 C)), Tt is the finite transition time of the beam and A is a function of the amount of displayed pixels and the signal amplitude in volts. The last factor is the filter characteristic equation of a low-pass filter with cutoff freq. of: $1/T_T$. The power spectral density of the signal is fairly constant upto the fundamental freq. of: $1/T_b$. Beyond Fb (1\Tb), it then, in theory, decreases by a rate of 20 DB per decade until it reaches Ft (1\Tt). Beyond Ft, the low pass filter cut-off freq., it decreases by a rate of 40 DB per decade.

In most practical cases, Fb is in the 20-50 MHz range, while Ft is in the 200-500 MHz range (depending upon the computer and monitor used). Thus, the radiated signal consists of the fundamental plus about 9 usable harmonics - spanning the entire VHF band (30-300 MHz), and the lower part of the UHF band (300-3000 MHz).

The video signal is radiated by the electron beam within the CRT, and by the video processing circuitry and cabling. In the range 20-500 MHz, in theory, EMI efficiency monotoneously increases with freq. at a rate of about 20 DB per decade. The actual rate is largely determined by the physical sizes of the VDT's electronic components radiating the signal (ie: antenna effect). In theory, this increase almost exactly compensates for the 20 DB decrease in the power spectral density of the video signal, thus producing, upto about Ft, received signal lobes of uniform strength spaced uniformly apart along the spectrum well within the VHF receiving range of even the cheapest TVs. The term, "in theory" is used because, in reality, some radiated lobes may be as high as 20 DB higher than expected from the theory due to the extremely complex interrelations of numerous factors.

Because each signal lobe is an AM version of the Line Feed (LF) signal upto the Nyquist freq. $1/2T_b$, any one lobe will reproduce the entire information found on the VDT CRT.

SUITABLE TV RECEIVERS

For Van Eck purposes, best results are provided by a black and white TV. The TV need not be expensive as long as it produces clear and undistorted images, has excellent sensitivity, has proper brightness and contrast control, and has accessible vertical and horizontal adjustments. VHF fine-tuning (standard) and a 75 ohm (cable) VHF input are also preferred. For mobile use, it should also use batteries or operate from a vehicle's cigarette lighter. If the TV is 120 VAC operated, it should have transformer isolation of the 120 VAC line from the TV circuits (cheaper models don't have this isolation) - very important if you do any kind of internal connection or modification of the TV.

OBSTACLES TO TV RECEPTION

The two major obstacles to good Van Eck TV reception are:
(1) TV RECEIVER TUNING
(2) REPLACING SYNC

(1) TV RECEIVER TUNING

Since the placement of the optimum video signal lobe to attack will likely occur between VHF channels, to minimize interference between two powerful adjacent TV stations, the need to fine-tune between stations is important. Most TVs have this feature (those with synthesized tuning don't). But the best way is to use a VCR. First, recording signals is a virtual necessity for the serious phreaker. Second, almost all VCRs come with the capability to fine-tune 12 or 14 VHF stations thru the bank of small pot and selector switch pairs under a removable cover. One or more of these settings can be set aside for VDT "phun" and games without disturbing the tuning of the other stations. One can hook up a VCR's VHF input to an external VHF directional antenna thru a 75 ohm-to-300 ohm transformer (cable is 75 ohm, split-pair is 300 ohm). The VCR's VHF output is then hooked up to the TV.

(2) REPLACING SYNC

In review, the sync. signals are separated from the video signal by the video separator in the TV. For normal TV signals (cable or antenna-received), the sync. signals are an integral part of the input signal. For VDT video signals, the sync. signals must be added to produce a readable CRT.

Many VDTs are based upon the same principle as European black-and-white TVs (not commonly available in the U.S.) - these TVs can sometimes be tuned to generate nearly the same freq. with their internal free-running sync. oscillators as the VDT being monitored. Also, we understand that RGB (computer) monitors can be similarly tuned for Van Eck purposes. Using TVs of this type can make remote eavesdropping on VDTs a virtual breeze! Even if VDTs with abnormal sync. freqs. are used, security is not guaranteed because the phreaker can access this oscillator and adjust the syncs. accordingly.

If you can't obtain this kind of TV, the syncs. must be either externally provided or recovered from the received signal:

EXTERNALLY SUPPLIED SYNC:

Van Eck suggests external syncs. can be provided by building a device consisting of a 15-50 KHz oscillator (multiscan monitors currently go up to 35 KHz) and a divide-by-N circuit. The purpose of the divide-by-N is to provide the proper VS freq., which is related to the HS freq. by:

FREQUENCY (Horizontal) = N x FREQUENCY (Vertical)

Where N is equal to the number of horizontal lines (see TABLE). Once the number of horizontal lines are determined or guessed, according to Van Eck, the HS freq. can be divided by that number to produce the VS freq., and only the HS freq. need be adjusted.

Since there are several different HS freq. and N combinations available in modern computer monitors, a selector switch must be provided to select the appropriate HS freq. A second selector switch must be provided that selects the N value from those most popular (or the two switches can be combined).

Here is where it appears that Van Eck made a serious error. For example, if you divide the number of visible lines into the HS freqs. rated for various monitors, you will come up with odd N values for the VS freqs. The truth is, there are only two widely known VS freqs. - 60 Hz (most common) and 50 Hz. So, why not just generate 60 Hz and 50 Hz VS signals as shown in Figure 6? TV circuits don't derive the VS freq. (60 Hz) from the HS freq. (15.75 KHz), they derive it from the 60 Hz AC line freq., or generate it using a Motorola MM5369 (or similar IC) and a 3.57954 MHz color TV crystal. Where Van Eck's error lies is that he implies that you use the published VISIBLE number of lines displayed by the VDT - not the unknown total number of lines. For example, for TVs, 16 horizontal lines are invisible because they occur during the 1.25 msec blanking pulse. VDT monitors are rated by the number of visible or displayable lines (ex: 200, 350). The total number of lines are not published and may, in fact, vary between same-type monitors.

The HS freq. can easily be generated using the very common 555 multivibrator/timer chip. Or a programmable divide-by-N CMOS chip can be used in conjunction with crystals. One such chip is the CD4059A, which can be programmed to divide any freq. (upto the UHF band) by any number from 3 to 15,999! The highly directional VHF antenna is first fed to a VHF amplifier (after transformer matching to 75 ohm lines, if required), such as the 10 DB SIGNAL AMPLIFIER (50-500 Mhz), Radio Shack #15-1118. The output of this amp and the external sync. generator are combined using the 75-OHM, 2-WAY COAXIAL COUPLER/COMBINER, Radio Shack #15-1141C, in the combiner mode. The output of the Combiner is then fed into the VHF antenna port of the TV. The signal level of the external sync. generator is then adjusted until the TV responds to the sync.

The video signal without either HS or VS, or a proper relationship between them, is one that has both severe rolling (no VS) and horizontal tear (no HS). As the syncs. take effect, first one and then the other of these conditions are corrected. Combining adjustments between the external sync.'s tweekers and the vertical roll and horizontal tear adjustments on the TV usually produce the best results.

The preferred method of mixing the video signal and sync. signals is by feeding the video signal thru an antenna pre-amplifier, then mixing the two at the output of the preamp (input of the TV or VCR).

Another easier way to generate external syncs. is to use what's called a "Video Stabilizer." This device, advertised in video magazines, removes the syncs. from incoming signals, then superimposes its own syncs. on the signal. Video Stabilizers are most commonly used to de-

Figure 6: Very versatile, **External Sync. Generator** circuit. Ideal for **Van Eck applications.** One rotary switch selects **MDA, CGA, EGA, PGC and MULTISCAN.** The selected crystals are commonly available from either **DIGI-KEY** (800-344-4539, 701 Brooks Ave. South, Thief River Falls, MN 56701) or **JAMECO** (415-592-8097, 1355 Shoreway Rd., Belmont, CA 94002). There are other commonly available crystals whose freqs. are evenly- or almost-evenly-divisible by an integer number, N. Division-by-any-N can be done using the **CD4059A Divide-By-N-Counter.** See the **RCA Data Book** for details of the CD4059A, particularly its Modes 8 and 10.

Note that although this design includes all major monitor types, almost all of the high-end monitors are used for intensive graphics applications, such as CAD and CAE workstations, and their displays are of little value except perhaps to industrial and Government spies. Eavesdropping on high-density displays requires a more sophisticated Van Eck set-up that uses a comparable monitor (NOTE: **We are very interested in this implementation for future editions of** BEYOND VAN ECK PHREAKING). **Knowledge of the types of VDTs used by the target is helpful but not essential.**

To compute your (Jn) JAM inputs to the CD4059A, Mode 8, use this formula for any N (upto 15999):

N = 8*(1000*J4+100*N1+10*N2+N3)+N4

Where: N1 = Value of J13-J16, N2 = Value of J9-J12
N3 = Value of J5-J8, N4 = Value of J1-J3

To compute your JAM inputs, Mode 10, use this formula for any N (upto 9999):

N = 1000*N1+100*N2+10*N3+N4

Where: N1 = Value of J13-J16, N2 = Value of J9-J12
N3 = Value of J5-J8, N4 = Value of J1-J4

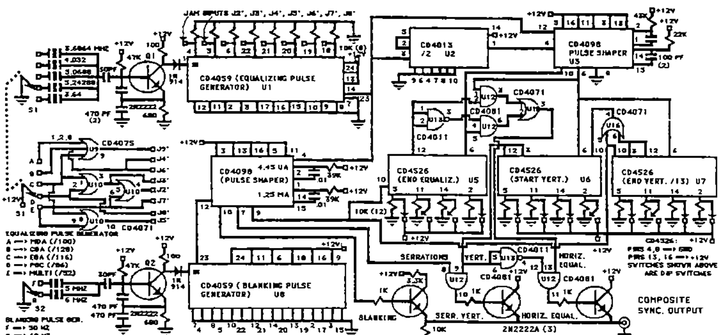
This circuit can be wired one of two ways to the TV. The Composite Output can be combined with the amplified video signal using a #15-1141C **Radio Shack Combiner** (prior mixing may be required). Or it can be wired directly to the input of the Sync. Separator within the TV (isolation can be performed thru optical coupling). In the first case, the **External Sync. Generator**'s ground is isolated from the TV's ground. In the second case, disconnect the output from the previous (Video Amplifier) stage that serves as the Sync. Separator input.

A third method is also possible. This requires wiring the modified **External Sync. Generator's** HS and VS (see **Figure 7**) outputs to the TV's HS and VS inputs, respectively. This would require disconnecting the TV's Sync. Separator, which could cause problems because most TVs feedback their HS outputs to the Sync. Separator for PLL purposes.

This circuit not only provides the HS and VS, but all equalizing and blanking pulses (see **Figure 5**; not absolutely essential but they increase readability). Vertical retrace lines will appear on the TV if the blanking pulses are excluded. Some horizontal picture jitter will occur if the equalizing pulses (at twice the HS freq.) are excluded with the blanking pulses.

Starting from the top: Q1 generates the crystal freq. selected by the ganged selector switch, S1. This freq. is divided down by U1, a programmable divide-by-N counter. The N is determined by SW1b and U9/U10 logic. The output of U1 is the equalizing pulse freq. required by the selected VDT. U2 is a divide-by-2 that converts this freq. into the HS freq. U3 is a dual pulse shaper.

To conform with standard TV design, U3's first section shapes the HS pulses to 5.08 μsec wide; its second section shapes the equalizing pulses to 2.54 μsec wide. Although pulse width is not critical, the RC networks can be adjusted if desired. The outputs of U3 are the HS and equalizing pulse trains. Note that although sync. and blanking timing must conform with the VDT's (else tear occurs), for best results, sync. pulse widths should conform to the TV.



Q2 (bottom) generates the identical blanking and VS freqs. S2 selects between the two standard values of 60 Hz (most common) and 50 Hz. Similar to U1, U8 divides the crystal freqs. down to their correct 50 Hz and 60 Hz values. TVs commonly use the 60 Hz AC line freq., but rock-solid 60 Hz line freq. is not available to the mobile Van Eck unit, and crystal freq. is far more precise. U4 is another pulse shaper.

U4's first section produces the serrated pulse train, with 4.45 usec pulses, that occurs only during the VS pulse. Since the serrated pulses are negative, the inverse output is taken. The second section produces the 1.25 msec blanking pulse. This pulse may vary between 0.83 and 1.33 msec in TVs, but it's usually 1.00–1.25 msec wide. However, for best results, blanking pulse width may have to be adjusted for a trade-off between what's acceptable to the TV and what's produced by the VDT. Although most TVs have a fairly broad tolerance for the blanking pulse width, for best results, try out different TVs. The compromised adjustment may sacrifice a few lines at the top or bottom, or add extra lines. Remember that CGA monitors use 8 trace lines per char. line, while MDA and EGA use 14, so the sacrifice of a few lines shouldn't adversely affect readability.

The purpose of U5 (divide-by-18) is to trigger ON at the onset of the blanking pulse and to gate 18 equalizing pulses to the output before shutting down. This gating action occurs thru the U11–U13 logic. When U5's output is low (before and after the 18 count), the HS is gated to the output. Actually, U5 is wired as a divide-by-9, but, because it counts HS pulses – not equalizing pulses – it actually performs a divide-by-18 on the equalizing pulse freq.

The purpose of U6 and U7 is to provide the location and duration of the VS during the blanking pulse. Both are enabled by the blanking pulse and are initially low. At the count of 7, U6's output goes high and it stays high until the count of 13, when U7's output goes high. U6 is switched low when U7's output is gated to U6's master reset thru U11b.

This circuit is very versatile because the U5–U7 divide circuits are programmable thru their dip switches. Any of which can be programmed to divide by any integer N from 1 to 16. Thus, the total number of equalizing pulses, and the width and location of VS within the blanking pulse are all programmable. Once a TV reception is made of a VDT signal, jitter, blanking and vertical retrace can be optimized, if necessary, by changing dip switch settings.

Q3–Q5 provide the composite sync. output. Q5 (HS/equalizing) is ON during the entire display cycle. Q3 (blanking) is ON only during the blanking phase of the display cycle. Q4 (serrated vertical) is ON only during a small portion of the blanking phase.

Once this circuit is built, set up a Van Eck system to eavesdrop on the type of VDTs of interest to you. Then make and record adjustments that optimize the TV display.

scramble satellite TV and copy VHS tapes with Copy Guard protection. For Van Eck purposes, it essentially adds syncs. to where none existed before. Note that the term, "stabilizer" is a generic term. Not all "video stabilizers" provide for a missing sync., so if your application is Van Eck-related, be sure obtain that feature with your stabilizer. Also note that the syncs. provided are for TVs and will not match what's needed to replicate VDT signals, so modification of its syncs. generators will be required. Texas Instruments, Standard Microsystems and Motorola produce video processing chips applicable to Van Eck designs.

VIDEO–BASED SYNC:

The spectrum of the video signal gives away the relative locations of the HS and VS. Simply, the video signal is made to equal zero during horizontal and vertical flybacks of the CRT's electron beam. Thus, although the syncs. themselves are not present in the video signal, their footprints are. The two null areas differ from each other by size. The null produced by the blanking pulse (which contains hidden in it the VS) is about 80 times wider than the HS null.

A circuit is then designed to reproduce the syncs. by synchronizing with these nulls. To do this, either the received signal-to-noise ratio must be high or the HS signal must be extracted from the LF signal using a tunable narrow bandpass filter. The resultant signal is a 15–35 KHz sinewave, sometimes with considerable phase noise. A slow Phase-Lock Loop (PLL) circuit can be used to further filter out this noise. Then a pulse-shaper is used to contour the sinewave into the appropriate pulse-type syncs. Again, the VS freq. is obtained by dividing the resultant HS freq. by the number of screen lines.

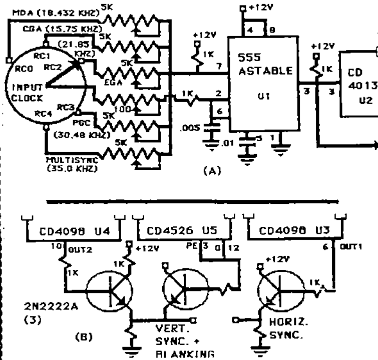


Figure 7: (A) is an alternative to the Equalizing Pulse Generator stage used in the **External Sync. Generator** circuit. It replaces the top crystal bank, Q1, U1, U9 and U10. It may drift a little, but it's much simpler to build. The five 5K cermet pots (20-turn preferred) are individually tuned for TWICE the shown HS freqs. (in KHz), with the optional external linear 100 ohm single-turn pot tuned mid-way. The 100 ohm pot is used to fine tune the display.

(B) is an alternative to the Composite Sync. Output used in the **External Sync. Generator** circuit. One output is for VS plus blanking, the other for HS.

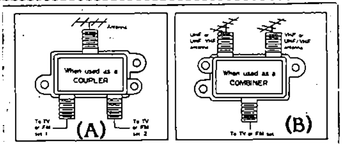


Figure 8: RS 15-1141C 75-OHM, 2-WAY, COAXIAL COUPLER/COMBINER can be used as shown in (B) to combine an external syncs. to the amplified video signal.

VAN ECK DISPLAYS

Van Eck TV displays at best closely resemble the VDT display monitored. But consider:

(1) Of course, a B&W TV cannot reproduce the colors used on color VDT displays.

(2) VDT lines will be displayed as dots on the TV because the strength of the video signal is proportional to the CHANGE in the pixels in the VDT. Thus, a VDT dot will look like a dot on the TV, but a VDT line will be displayed as a dot on each end where the rise and fall edges of the line occur. There may be some comet-trailing, depending upon brightness and contrast settings and other factors.

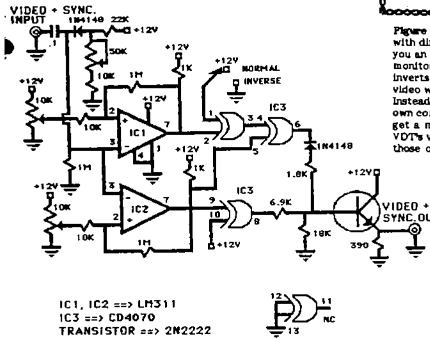


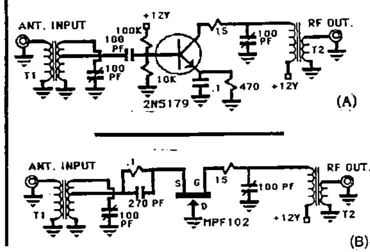
Figure 9: Do-it-yourself **Video Stabilizer.** Usable with VCRs and TVs with direct video inputs. The nominal use of this circuit is to provide you an inverse video option for coupling color computer monochrome monitors. It clamps the input voltage level, separates the sync. pulses, inverts the video (if that be your choice), then recombines the new video with the old sync. pulses. The application to Van Eck is obvious. Instead of recombining the old sync. with the new video, produce your own composite sync., and combine it with the new video. Thus, you can get a more readable (inverted or non-inverted) reconstruction of the VDT's video signal being monitored while changing the syncs. to match those of the VDT.

The input clamp circuit is used to clamp the sync. level to eliminate constant adjustments to the inputs of the LM311 comparators. IC1 passes both the sync. and video signals. IC3a allows for the selection of normal or inverse video. IC3b cancels out the old sync. IC2 is set to separate out only the old sync. Its output goes to IC3b to cancel out the old sync. Its output also goes to IC3c, which re-inverts the sync. Q1 recombines the new video with the old sync. For Van Eck uses, IC3c serves no purpose. Instead, it is substituted with the composite sync. output from the **External Sync. Generator,** described herein, or similar.

Figure 10: Two general-purpose RF amps. good to about 1200 MHz. For much more info. on RF circuits and methods, see our **SECRET & SURVIVAL RADIO** ($20) Manual.

(A) 15-18 DB GAIN RF AMP: Amidon T50-6 (yellow) toroid cores are best for optimum Q for T1 and T2 (T2 duplicates T1 but with no tap). The core is wrapped with a maximum number of turns (evenly spaced single layer) using 28-30 guage magnet wire for the T1 secondary. Its tap point is set at about 600 ohms. Location is at 25%-33% of the total turns. T1 primary windings are about 10% of its secondary windings, and are wrapped evenly spaced on top of the secondary. Because this is a high gain RF amp., self-oscillations can be a problem. Use good wiring techniques. To cure low freq. oscillations, parallel the primary of T2 with a 1K-10K resistor. However, this will lower Q and selectivity, so pick the highest resistance that stabilizes the amp. This resistor can also be used to optimize the received video signal BW.

(B) 12-15 DB GAIN RF AMP: This amp uses the same T1 and T2 RF transformers described above. And the same techniques are used minimize self-oscillations (minimum G connection to ground). The primary virtue of a grounded-gate RF amp. is its enhanced stability. Two of these amps. can be cascaded for greater gain (not usually advised because too much gain prior to a mixer stage can impair dynamic range).



(3) Because the VDT and TV will be using different blanking freq. sources, the two will be out of phase with each other. The TV display will then have "hum bars," which consist of broad, horizontal shading bars that roll thru the display. They are usually not serious but they can be tuned out by manually synchronizing the blanking freq. generator of the external sync. generator, by using a PLL to lock this generator to the video signal nulls that represent video signal blanking, or by using a TV that has this capability.

(4) The TV's reconstruction of the VDT image may not start on line #1 nor end on line #262 because the TV is forced to obey the sync. freq. rules of the VDT (else you get tear). Where the TV's display starts and ends depends upon the effect of the VDT's syncs. have upon the vertical ramp voltage waveform. See **Figure 12.** The ramp voltage waveform can be adjusted by using the vertical height adjustment on the TV.

(5) Because CRTs used with TVs don't have nearly the resolution as those used on VDTs, reconstructed graphics images will look a lot fuzzier. Further, since TVs are good for wordprocessing to an extent not exceeding 64 chars./line, reading 80 chars./line, although possible for eavesdropping purposes, is far from ideal. To overcome this problem requires adapting Van Eck methods to computer monitors of sufficient resolution (ex: EGA).

TABLE OF DISPLAY INFORMATION RELEVANT TO VAN ECK:

Display Type	*# Vert. Lines*	*# Horiz. Lines-N*	*Horiz Sync Freq. (KHz)*	*Vert Sync Freq. (Hz)*	*Video BW (MHZ)*
TV		262.5	15.75	60	
MDA	720	350	18.432	50	16.257
CGA	320, 640	200	15.75	60	14.318
EGA	640	350	21.85	60	16.257
PGC	640	480	30.48	60	30
MULTI.	800, 900	560, 600	to 35.00	50, 60	30-35

Note: These are values for popular models. However, there are many exceptions, particularly with multiscan displays. Under *# Horiz. Lines (N), N* is the value that the *Horiz. Sync. Freq.* is divided by to obtain the *Vert. Sync. Freq.* Note how the Video BW compares to the 8 MHz AM detection BW (4.5 MHz VSB BW) of TVs.

CONSUMERTRONICS
2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310

FIND-THE-RIGHT-CRYSTAL FOR VDT MONITORS USING CRYSTALS SOLD BY JAMECO & DIGI-KEY

XTAL FREQ. (MHZ)	FACTORS (N) TO DIVIDE XTAL FREQS. BY TO GET VDT HORIZ. FREQS. CGA 15.75 KHZ	MDA 18.432 KHZ	EGA 21.85 KHZ	PGC 30.48 KHZ	MULTISCAN 35.00 KHZ
1	----------	----------	----------	----------	----------
1.8432	----------	100	----------	----------	----------
2	126.984126	----------	----------	----------	----------
2.2163	----------	----------	----------	----------	----------
2.304	----------	125	----------	----------	----------
2.4576	----------	----------	----------	----------	----------
2.5	----------	----------	----------	----------	----------
2.56	----------	----------	----------	83.989501	----------
2.6	----------	----------	118.993135	----------	----------
2.94912	----------	160	----------	----------	----------
3	----------	----------	----------	----------	----------
3.145	----------	----------	----------	----------	----------
3.2768	----------	----------	----------	----------	----------
3.57954	----------	----------	----------	----------	----------
3.57561	----------	193.989257	----------	----------	----------
3.64	----------	----------	----------	----------	104
3.6864	----------	200	----------	----------	----------
3.7	----------	----------	----------	----------	----------
3.859	245.015873	----------	----------	----------	----------
4	----------	217.013888	----------	----------	----------
4.032	256	----------	----------	----------	----------
4.1943	----------	----------	----------	----------	----------
4.433	----------	----------	----------	----------	----------
4.9152	----------	----------	----------	----------	----------
5	----------	----------	----------	----------	----------
5.0688	----------	275	231.981693	----------	----------
5.185	----------	----------	----------	----------	----------
5.24288	----------	----------	----------	172.010498	----------
5.9904	----------	325	----------	----------	----------
6	----------	----------	----------	----------	----------
6.144	----------	----------	----------	----------	----------
6.5536	----------	----------	----------	215.013123	----------
7.3728	----------	400	----------	----------	----------
8	----------	----------	----------	----------	----------
9.216	----------	500	----------	----------	----------
10	----------	----------	----------	----------	----------
11.0592	----------	600	----------	----------	----------
11.9813	----------	----------	----------	----------	----------
12	----------	----------	----------	----------	----------
14.3181	----------	----------	----------	----------	----------
15	----------	----------	----------	----------	----------
16	----------	----------	----------	----------	----------
18	----------	----------	----------	----------	----------
18.432	----------	1000	----------	----------	----------
19.6608	----------	----------	----------	----------	----------
20	----------	----------	----------	----------	----------
22.1184	----------	1200	----------	----------	----------
23.4	----------	----------	----------	----------	----------
32	----------	----------	----------	----------	----------
32.768	----------	----------	----------	----------	----------
36	----------	----------	----------	----------	----------

CRYSTAL SELECT TABLE: This table shows which commonly-available crystals (from **JAMECO** and **DIGI-KEY**) can be divided down to a VDT monitor freq. or closely to it. This makes selection of usable crystals much easier.

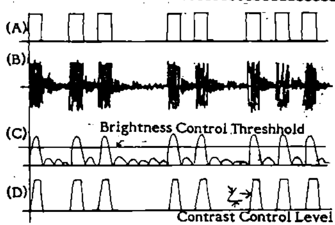


Figure 11: The signal processing in a TV of the received video signal from a monitored VDT. (A) shows the input video signal. (B) shows the IF signal generated by the TV in response to (A). (C) shows the resulting LF signal. Because of the AM detection, this results in the envelope of the IF signal. (D) shows the reconstructed video signal in the TV after optimal adjustment of brightness and contrast levels. Notice how closely it resembles the video input signal. The signal threshold is adjusted by the Brightness Control to select pulse width. The amplification of the signal selected by the Brightness Control – thus the shape of the pulse skirt – is controlled by the Contrast Control. Note that the reproduced image of the VDT on the TV is like a negative photo. For TV's, the height of the pulse defines the black level while the white level is defined by the pulse's baseline.

```
00010 CLS:DEFSTR A,B:DEFDBL S-Z:K=0:DIM S(9),A(9),T(500):
PRINT"'CRYSTAL' PROGRAM FINDS THE NEAREST COMMONLY
AVAILABLE CRYSTALS WHOSE FREQS. ARE OR ARE NEARLY
EVENLY DIVISIBLE BY AN INTEGER TO OBTAIN VDT HORIZONTAL
FREQS.":PRINT
00020 PRINT"'CRYSTAL' CAN BE ADAPTED FOR ANY OTHER
APPLICATION IN WHICH EVEN DIVISIBILITY IS IMPORTANT. DATA
STATEMENTS, TOLERANCES, ETC. CAN BE CHANGED
ACCORDINGLY.":PRINT
00030 PRINT"'CRYSTAL' IS COPYRIGHTED 1988 BY JOHN J.
WILLIAMS, 2011 CRESCENT DR., PO DRAWER 537, ALAMOGORDO,
NM 88310. ABSOLUTELY ALL RIGHTS RESERVED. FOR A COPY OF
THIS PROGRAM ON AN MSDOS OR PS/2 DISK, PLEASE SEND $20 TO
ABOVE ADDRESS. THANX.":PRINT
00040 TT=0:DO:TT=TT+1:READ T(TT):IF T(TT)<0 THEN TT=TT-1:
GOTO60
00050 UNTIL TT>500
00060 INPUT"'ENTER'=PRINTER IS READY, ELSE 'E'=END
PROGRAM: ";A:PRINT:IF A>"" END
00070 PRINT"FIND-THE-RIGHT-CRYSTAL FOR VDT MONITORS
USING CRYSTALS SOLD BY JAMECO & DIGI-KEY":PRINT:IF K=0
THEN K=1:ROUTE128:GOTO70 ELSE ROUTE0
00080 LPRINTTAB(16);"FACTORS (N) TO DIVIDE XTAL FREQS. BY
TO GET VDT HORIZ. FREQS.":LPRINT"XTAL FREQ.";TAB(16);"CGA";
TAB(31);"MDA";TAB(46);"EGA";TAB(61);"PGC";TAB(76);
"MULTISCAN"
00090 LPRINT"(MHZ)";TAB(16);"15.75 KHZ";TAB(31);"18.432 KHZ";
TAB(46);"21.85 KHZ";TAB(61);"30.48 KHZ";TAB(76);"35.00 KHZ":
LPRINT
00100 S(1)=15.75:S(2)=18.432:S(3)=21.85:S(4)=30.48:S(5)=35.00
00110 Q=1:DO
00120 P=1:DO:SS=1000*T(Q)/S(P):A=STR$(SS):K=INSTR(1,A,"."):IF
K=0 GOTO150
00130 L=LEN(A):M=K+6:IF M<L THEN A=LEFT$(A,M)
00140 K=K+1:IF INSTR(K,A,"00")=K OR INSTR(K,A,"01")=K OR
INSTR(K,A,"98")=K OR INSTR(K,A,"99")=K GOTO150 ELSE A="
"+STRING$(10,"-")
00150 A(P)=A:P=P+1:UNTIL P>5
00160 LPRINT T(Q);TAB(15);A(1);TAB(30);A(2);TAB(45);A(3);TAB(60);
A(4);TAB(75);A(5)
00170 Q=Q+1:UNTIL Q>TT:END
00180 DATA 1,1.8432,2,2.2163,2.304,2.4576,2.5,2.56,2.6,2.94912,3,
3.145,3.2768,3.57954,3.57561,3.64,3.6864,3.7,3.859
00190 DATA 4,4.032,4.1943,4.433,4.9152,5,5.0688,5.185,5.24288,
5.9904,6,6.144,6.5536,7.3728,8,9.216
00200 DATA 10,11.0592,11.9813,12,14.3181,15,16,18,18.432,19.6608,
20,22.1184,23.4,32,32.768,36,48,49.435,49.88,-1
32767 END
```

CRYSTAL SELECT PROGRAM "CRYSTAL": "CRYSTAL" produces the Crystal Select Table shown. Line #120 should be changed to read: ***SS=500*T(Q)/S(p)*** if crystal selection is based upon the equalizing pulse freq. and not the HS freq. **CRYSTAL** can also be easily modified to serve any need in which even divisibility by an integer is important, including analysis of public key ciphers. Data statements, S(n) values, tolerances, etc. can be changed accordingly. BASIC source code and compiled .COM file are available (MSDOS, PS/2) are available from **CONSUMERTRONICS** (P.O. Drawer 537, Alamogordo, NM 88310), $20.

COUNTERMEASURES

Because of the great value placed upon word and data information displayed (and radiated) by VDTs and the ease and simplicity of phreaking this information, countermeasures are usually required. Note that these countermeasures can double or triple system cost. They should consist of:

(1) Use computer equipment that is **TEMPEST**-rated for highly sensitive uses, if available to you. To obtain **TEMPEST** rating, the equipment must be stringently tested and approved by a special Government committee (**TQSC**) based upon still-classified standards. Approved equipment is placed on the, "**TEMPEST Preferred Product List**" (PPL). Once listed, the equipment cannot be exported or sold to the public without prior U.S. Government approval.

There are apparently two **TEMPEST** standards. The U.S.A. standard is the **NACSIM5100A**, while the **NATO** standard, apparently heavily derived from the **NACSIM5100A**, is the **AMSG720B** standard. Both standards apply to all types of equipment, and are not restricted to electronic equipment. Because of the security of **TEMPEST**, such equipment may not be available even for high-security commercial needs. And where available for low and medium security needs, it may be so expensive as to be uneconomical to use. Your best chance of obtaining **TEMPEST** expertise is to join a Government program where **TEMPEST** security is applied.

(2) Surround the computer station or VDT with a metal cage. The degree of protection is roughly proportional to the thickness of the cage (from several hundred KHz to several hundred MHz), and leak points (ex: CRT, keyboard, cables, air vents, cage joints). Cables should all be shielded (including power, but particularly the cable between the VDT and keyboard or expansion interface). Power and other non-signal cables must also be shielded because they can resonate with the video signal and re-radiate that signal along their lengths. Air vents can be baffled/honey-combed/screened. Exposed CRTs can be of the gold-coated type, and-or shielded with a grounded screen. And special materials can be used when assembling metal cages to minimize leakage thru cage joints.

(3) Choose properly designed computer equipment. Electronic parts should only be as fast as what's necessary for system speed, to cut down on the harmonic Bandwidth (BW). In other words, don't use 80 ns chips on a 4.77 MHz system because the 2nd. and 3rd. harmonics will also be switched at almost full-strength. Electronic filters and decoupling capacitors should be amply used to reduce EMI. Return paths should be as close to and as parallel to signal paths as possible. Signal wire lengths should be minimal. The VDT should be properly grounded.

(4) Avoid mounting VDTs near reflective surfaces and ground planes as they increase the range of radiated signals. For example, metal tables should be avoided because they act as a ground plane for vertical conductors (ie: antennas) and as reflector for horizontal ones inside the computer, keyboard and VDT, thus inncreasing transmitted power by as much as 3 DB. Also avoid nearby metal doors, partitions and heavy equipment for the same reasons.

(5) Subject the CRT's scanning to a cryptographic algorithm. The standard scanning method is to scan from the top of the screen to the bottom in a 1,2,3... order. By subjecting the scan order to a password and transposition algorithm that controls the vertical voltage ramp, the CRT can be scanned in a random-like order, making reconstruction almost impossible (N! possible combinations, where N equals # of scan lines). See Figure 13. Unless carefully observed, such a received signal appears much like raster and can be easily overlooked. This implementation can cost as little as $100 extra per VDT.

(6) Display only the absolute minimal amount of sensitive info. on the VDT. Seldomly or never display passwords, access codes, PINs and other critical data that can be used to phreak the system.

(7) Use the highest level of VDT resolution that you can. For example, 132 chars. across (typical of most spreadsheets) is much preferred over 80 chars. Since TV resolution is poor compared to computer-grade monitors, high density VDT text is not readable on a TV. High density modes eliminate the "*$99 Phreaker*," but more sophisticated eavesdroppers no doubt have adapted multiscan monitors to their systems.

(8) Operate the VDT at its minimum comfortable contrast and maximum comfortable brightness levels. High contrast levels coupled with low brightness levels produce much stronger video signals, and thus substantially increase the eavesdropping range over the opposite condition. Further, since the phreaker will tend to tune his Van Eck set-up based upon expected normal levels of contrast and brightness, he will likely misjudge the distance (and perhaps direction) of an abnormal video signal, thus mis-identifying its source, and perhaps dismissing the signal as too weak or too noisy to bother with.

(9) If all other countermeasures fail, VDT EMI can be jammed using high energy noise fields in the VHF and low-UHF bands. However, this is not advised because it will cause great interference with nearby TV and FM broadcasts, would certainly provoke FCC action, and would endanger the health of workers in the area. Jamming can also be accomplished to a degree by operating near the VDTs powerful color TVs continuously randomly tuned between the VHF stations. And by operating all VDTs as closely as possible to each other, especially if the VDTs are of the same type. However, jamming countermeasures are often unpredictable and can provide a false sense of security because, even among idential VDTs, the produced EMIs can be substantially different in freq., content allowing for eavesdroppers to zero-in on specific VDTs in a bunch. Before relying upon jamming techniques, your set-up should be thoroughly analyzed from a devil's advocate point of view to determine whether or not the jamming adds significantly to your security.

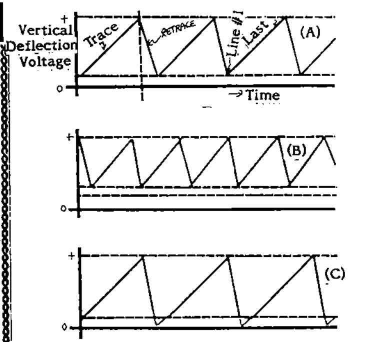


Figure 12: Typical TV Vertical Deflection Voltages. (A) is the normal waveform. Note that the retrace ramp is much sharper than the trace ramp. Even so, for TVs, 16 horizontal lines are wasted during blanking and vertical retrace. (B) and (C) are waveforms that might result from Van Eck uses, either from reconstructing the VDT's syncs. or in maladjustment of an external sync. generator. In (B), the retrace is ended before the beam can return to line #1, resulting in a clamped voltage and a vertically-squeezed display. In (C), the TV's retrace is faster than the VDT's, so there is a dead spot at the top lines where the TV's beam idles, resulting in a thin bright band at the display's top. A variation (not shown) is where the TV's voltage saturates at the top where it waits for a slower VS pulse. This results in a clipped (flat-top) voltage and a thin bright band at the bottom.

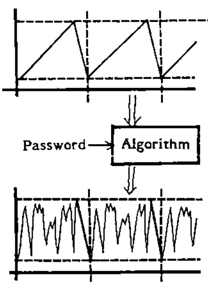


Figure 13: Van Eck countermeasure in which a password and a transposition algorithm is used to transform a normal VDT beam trace sequence into one using an encrypted order of lines. Note, this method is more complex to implement if the first and last lines are changed.

CONSUMERTRONICS
2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310

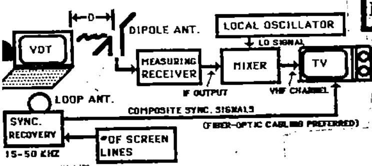


Figure 14: Block diagram of a measuring set-up used to determine the eavesdropping ranges (D) and directions of VDTs. The objective of this set-up is to measure the vulnerability of VDTs to Van Eck eavesdropping. Since there are several sources of VDT EMI, it is not enough to measure the strength and freq. distribution of the combined EMIs. Therefore, this test set-up simulates an actual eavesdropping and is a much better indicator of system vulnerability than field strength meter and signal analyzer testing alone.

The loop antenna is placed near the VDT's high voltage transformer to pick up the magnetic component of the radiated HS signal from it (most VDTs). This signal is then filtered and stabilized with a PLL circuit. The VS is obtained from the HS by division with the number of screen lines. Both syncs. are combined into a composite sync., and then fed into the input of the sync. separator circuit of the TV. It is preferred to connect the sync. recovery circuit to the TV thru an optical link as their distances may be exceed 1,000 yards (although under 100 yards is more common for unshielded VDTs and 20 yards for shielded VDTs), and optical cabling reduces losses and eliminates video signal interference with the composite sync. An alternative to this sync. restoration set-up is to artificially generate the sync. as a phreaker would actually be forced to do (as described herein).

There are two test philosophies:

(1) From the OEM's point of view, the test must be standard. In this case, the VDT under test is placed one meter above the earth conductive plane at the measuring site. The test equipment is more-or-less a permanent set-up with standard distances between VDTs and the dipole antenna. And a specific display pattern, contrast and brightness are used. And reflective objects, partitions, etc. are minimal or at least standardized.

(2) From the VDT user's point of view, each VDT is tested under its actual use conditions with no special efforts made to increase or decrease the EMI for the first test to establish baseline. Subsequent tests can be made to minimize eavesdropping by determining what countermeasures work best.

A dipole antenna is used to pick-up the EMI, which is then measured by a calibrated Measuring Receiver of the 30-1000 MHz range. Because the IF signal produced by the Measuring Receiver is filtered at its detection BW, a detection BW of at least 1 MHz must be selected. At 1 MHz, the presence of a page of text is discernable but the text itself is not readable. For minimal readability from CGA VDTs, the detection BW must be at least 4.5 MHz. Optimum results for TVs are obtained at 8 MHz, particularly for EGA, VGA and multisync monitors. The IF from the Measuring Receiver is beat against another (LO) frequency in a mixer to produce a sum freq. equal to a standard VHF channel if the IF freq. itself lies above or below the VHF band. However, in most cases, the IF lies between VHF channels, where VHF fine-tuning is all that's required.

For a closer simulation to actual eavesdropping, a directional antenna should be used instead of the shown dipole antenna. Directional antennas provide at least an additional 10 DB of gain.

The advantage of this method over a straight Van Eck set-up are:

(1) It allows field strength measurements in the 30-1000 MHz range.

(2) Since Measuring Receivers are designed to be far more sensitive than ordinary TVs, it more closely simulates the danger zone of reception by highly sophisticated Van Eck phreakers than does a straight Van Eck set-up.

(3) Correlations can be made between ease of reception an actual EMI levels and freq. distributions (PSD). This provides more information for minimizing VDT susceptibility and for generating effective countermeasures.

THE REAL THING!!

If you've purchased a previous edition of BEYOND VAN ECK PHREAKING, you will be very pleased with this new edition, for two reasons:

(1) In the first edition, all of the drawings were made by hand. Altho they were legible, it is always better and neater to use machine-made drawings. As we have done here, we are progressively updating our popular manuals with machine-made drawings plus loads of new, useful information.

The "machine" used here is the MACINTOSH 512Ke, using SUPERPAINT on an IMAGEWRITER I printer. Altho we generally perfer to use PCs, I found that this handy-combination is easy to use while producing impressive and very readable artwork. (I am looking for MAC fonts - particularly the larger sizes and all Chicago sizes. If you have them, please write me or just send them. I am also looking for a MAC SE or MAC PLUS in very good condition and at a bargain price).

(2) Because of my fortuitous association with one of the hacker legends (I just can't remember who), I have been able to obtain, what has been represented to me, a block diagram and actual set of plans of the SYNREST (SYNC RESTORER) actually used by WIM VAN ECK in his famous (or infamous) work!!!

When I received this package, at first I scoffed at the idea that the mussed-up and messed-up pile of loose-leaf notes in my hot, sweaty hands were really THE TOP SECRET WIM VAN ECK SYNC RESTORER plans. But after reading thru them, and actually constructing and testing the device, I was (and am) absolutely convinced that they are indeed the real thing.

As I have repeatedly stated, your contributions to CONSUMERTRONICS are vitally important. This is a classic example of how vital they are. So, please keep up the good work. And of course the more business we do, the better we can afford to properly compensate information sources for hard-to-get, dyn-o-mite information. If you can improve upon this very useful device, please provide CONSUMERTRONICS your improvements.

The plans shown herein can be used, in conjunction with a slightly modified TV (ie: TV receiver), to eavesdrop on VDTs (Video Display Terminals, called VDUs in Europe). Maximum reception distance is typically about 1 KM, but depends mostly upon the VDT used, its position and orientation from the TV antenna, and the presence of shielding and other absorbers and reflectors between and-or around the VDT, TV or both.

The purpose of SYNREST is to reconstruct the VDT's horizontal and vertical sync signals by tuning the device accordingly, as it is usually not possible to get physically close enough to the VDT's high voltage transformer to couple off of its magnetic field.

HOW THE SYNREST WORKS

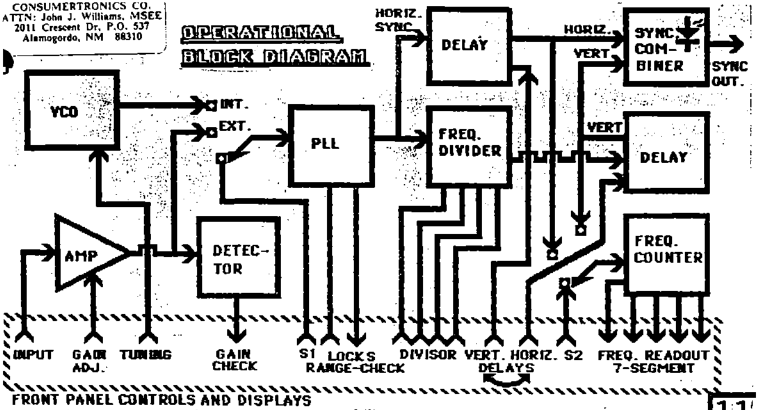
All pots, switches and displays are accessed from the SYNREST's front panel. The power supply used is of a standard design for producing +12V, +5V and -12V, as required by the circuitry.

The VFO (Variable Frequency Oscillator) is used to produce the horizontal sync. It is a simple 555-type oscillator. It can't be practically substituted for a crystal-controlled oscillator, because you must be able to vary it. Use high quality components only. The two pots used to control its frequency allow for gross and fine tuning. The VFO will produce outputs of 15-22 KHz.

The PLL (Phase-Locked Loop) is used to stabilize the VFO's output. Else you usually end up often manually adjusting these pots. PLL time-constant is about 0.29 seconds. The PLL's VCO operates at 2x the VFO frequency. The PLL can be adjusted to increase/decrease its locking range thru its 47K pot. The LED indicates when the PLL is in lock.

CONSUMERTRONICS CO.
ATTN: John J. Williams, MSEE
2011 Crescent Dr, P.O. 537
Alamogordo, NM 88310

OPERATIONAL BLOCK DIAGRAM



The output signal of the PLL (after division by two) is used as the horizontal sync signal. The PLL VCO's signal is fed into the FREQUENCY DIVIDER. Its divisor is set by a series of front-panel rotary or thumbwheel switches. When doing your "wild thing" with your Van Eck device, you set the divisor to either TWICE the number of screen lines the VDT has or to its exact number of screen lines:

(1) TWICE THE # OF LINES: The black-and-white TV you use interlaces the screen lines. For those VDTs that use half lines (most).

(2) SAME # OF LINES: For those VDTs (ie: color TV and composite monitors) that use interlacing.

The signal outputted by the FREQUENCY DIVIDER (usually 60 Hz US, 50 Hz elsewhere) is the vertical sync signal.

The delay times and pulse widths of both the horizontal and vertical sync signals are set by their appropriate 74LS123 double-monostables. The vertical and horizontal DELAY pots are used to set the delay times to adjust the physical position of the received VDT signal on the TV.

Depending upon the position of S2, either the horizontal or vertical frequency is displayed. Thus, you can immediately identify and record the correct sync values and settings for most VDTs encountered (except PGC and Multisync). If the displayed signal is greater than 21.85 KHz, you are probably locked onto the VFO's second harmonic. If so, adjust the PLL's lock pot so that it locks onto the VFO's fundamental frequency.

Both sync signals are logically ANDed, and are then buffered and fed into the OT (OPTICAL TRANSMITTER) LED. So that you don't have wires connecting the SYNREST to the TV's innards, optical coupling is provided. A pot is provided to adjust the OT LED's intensity, and should be adjusted high enough for reliable reception by the OR (OPTICAL RECEIVER), yet low enough so that the TV responds to VFO frequency adjustments.

If you are able to access enough of the VDT's high voltage transformer's magnetic field, you can plug in a magnetic probe into the SYNREST's INPUT and switch S1 to the narrowband AMPLIFIER (instead of the VFO), set for the horizontal sync frequency (as the high voltage transformer is usually operated at this frequency). Amplifier sensitivity (ie: gain) is adjustable by means of a 10K pot. The amplifier's LED will light when the pick-up signal is strong enough to be usable by the SYNREST.

Any suitable coil can be used as the pick-up. What you use largely depends upon your particular set of circumstances. If you have access to a location inside of or very near the VDT, a small, hidden pickup coil will usually work (pre-amplification) may be required. However, if you are some distance from the VDT, a much large coil would be required.

The function of the INPUT can be verified by hooking up a second, unmodified TV. This TV is turned ON and tuned for a strong broadcast station signal. The magnetic probe is then moved near and around this TV until the amplifier's LED is ON, indicating a satisfactory pick-up.

The INPUT can also be connected up to any appropriate function generator output. I would recommend that you select the generator frequency at 512 times the horizontal sync frequency and divide it down, because a signal stability of at least 0.005 Hz is required to obtain a reasonably stable (ie: non-moving) display on the TV.

The OT is snapped on to the TV's case (usually rear) wherever you have placed the OR. We embedded our OT in a 25-cent Radio Shack donut magnet. We then glued a steel plate (with a hole punched into it) onto the back of the TV over the OR's position. This provides a firm seating, yet one that we can easily adjust for optimum signal reception.

One output of your TV's Video Amplifier is fed into its Sync Amplifier (see Figure 4). This connection is broken; one end is hooked-up to Pin #1 of OR connector X1, and the other to Pin #3 (any suitable connector can be used). All OR grounds shown are of course the sync circuit ground.

When the OT is connected and transmitting the composite sync to the OR, the sync signals are buffered and rectified to activate RELAY K1. K1 then switches from the composite sync signal emanating from the Video Amp to that emanating from the SYNREST. The moment that you either remove the OT or turn OFF the SYNREST, its signal is lost and K1 drops out and reconnects up the Video Amp.

Consult your TV manual on how to operate your TV. Some TVs have a front-panel LED indicator that indirectly indicates when your TV is locked into the received sync signal. (This LED is usually driven by the TV's mute circuit, and really directly indicates the reception of the audio signal.)

Each TV has a very narrow lock range for its horizontal sync. The center frequency of the TV's lock range is adjusted by an INTERNAL pot. Since the SYNREST produces frequencies out of the normal lock range (14-21 KHz), to get the SYNREST to function on a practical basis requires moving the TV's lock pot to its front panel or other accessible external point.

If you don't know much about your TV circuitry and function, you usually can get a SAMS that describes it. And some TVs have the schematic glued to the inside of the back cover or case.

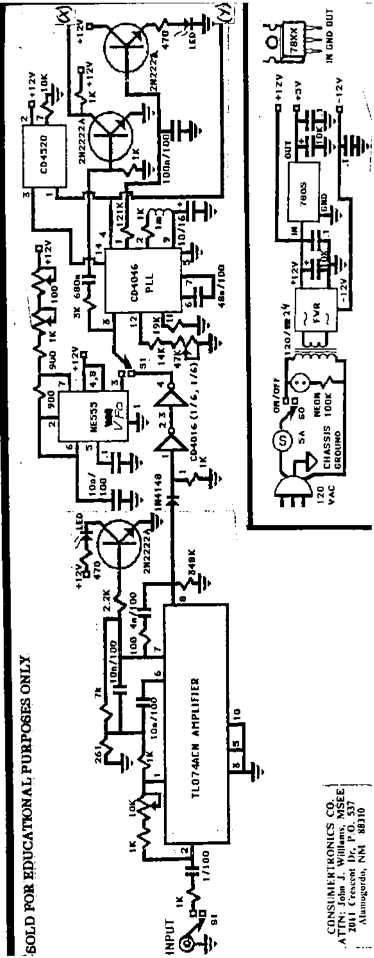
When you use your TV as both a VDT receiver and as a normal TV receiver, you will have to re-adjust its lock range pot as you go back and forth between uses and as you go between different types of VDTs. The lock range pot is adjusted so that the TV's front-panel LED is strongest.

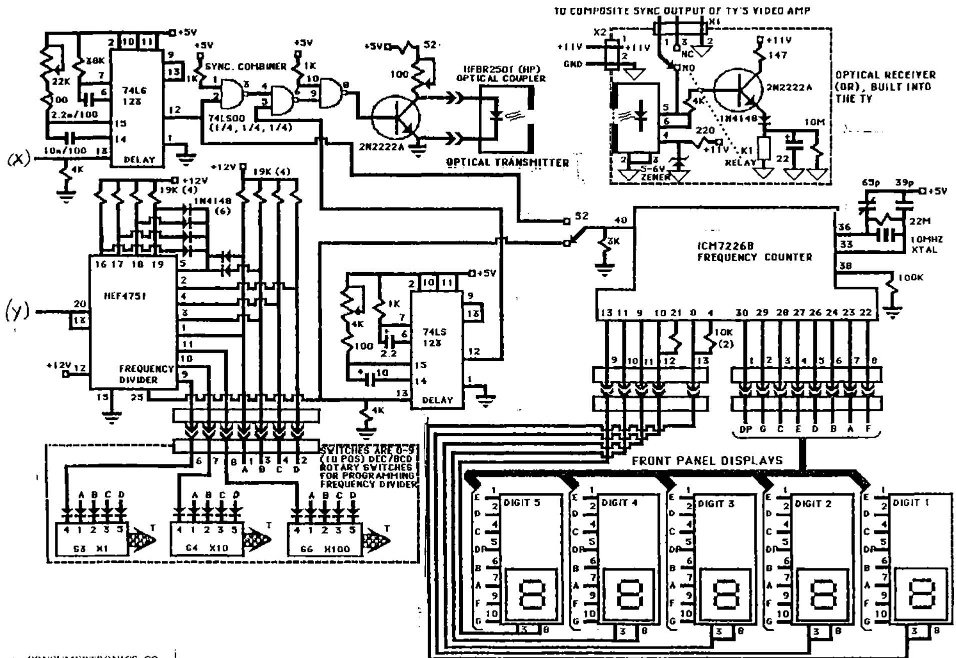
Because the SYNREST's signal generating capability, it should not be turned ON when you are using your TV to receive broadcast stations as it may cause interference. Of course if your rude neighbor leaves his TV ON loud all night long, it's a neat way to scramble his reception to cause him to turn his set OFF - maybe even to throw it out!

NOTE: As part of CONSUMERTRONICS SPECIAL PROJECTS offer, we will provide you a completed and tested SYNREST and modified quality Black & White TV for only $995 (+$25 shipping/handling), prepaid. Allow six weeks. If you want us to include a broadband TV antenna (commonly available from Radio Shack), add $100. If you want us to include an electromagnetic output (along with the standard OT) to study its capability to scramble nearby TV reception, add $25.

Because a TV receiver cannot produce as sharp of an image as that produced by a VDT, CONSUMERTRONICS is in the process of developing a Van Eck device that will work using an EGA or Multisync monitor instead of a TV. However, because of the difficulty in obtaining a schematic for any of the popular EGA and Multisync monitors and a shortage of manpower, we have yet to complete this project. Any assistance or information contribution you can provide us would be helpful. If you require compensation, please notify us accordingly, prior to providing us your help.

Please send $2 for our most recent TECHNOLOGY SURVIVAL CATALOG. The best of successes in all that you do.





CONSUMERTRONICS CO.
ATTN: John J. Williams, MSEE
2011 Crescent Dr, P.O. 537
Alamogordo, NM 88310

JOHN J. WILLIAMS

2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310
(505)-434-0234

03/28/88 - 11:08:20

DR. NEHER LABORATORIES PTT
ATTN: DR. WIM VAN ECK
LEIDSCHENDAM, NETHERLANDS

DR. WIM VAN ECK:

How are you? I hope fine.

We are doing research into your method of eavesdropping on VDUs (VDTs) using ordinary black and white TV receivers, directional antennas, and external sync. generators.

The articles you have published on the subject are most interesting and informative. However, they are also incomplete and misleading. For example, you don't specify the design of the external sync. used or its exact method of insertion into the TV. For example, is it combined to the incoming video signal using a combiner circuit, inserted directly into the sync. separator within the TV as a composite sync. (the method we found to be best), or inserted into the horizontal and vertical sync. amp. circuits as individual syncs. Please explain.

Also, your dissertation into deriving the vertical sync. by dividing the horizontal sync. by an integer equal to the number of horizontal lines is misleading at best and wrong at worse. Modern VDTs, at least in the U.S. have one of two vertical syncs. only: 60 Hz or 50 Hz. If you divide the number of visible video lines into the horizontal sync. freq., as your articles imply, you get an odd ball number for the vertical sync. that is WRONG because it does NOT consider non-displayed horizontal lines that occur during the blanking phase. In fact, you don't give any details about blanking or providing the equalizing pulses. Without blanking, vertical retrace is displayed. And without equalizing pulses, more jitter is created as the TV's CRT interlaces fields 1 and 2. Both of these adversely affect the readability of the reconstructed VDT image.

You also don't provide information on the ability of the TV to clearly ~~display~~ the standard 80 char./line text and graphics, nor how to design the external sync. to accommodate HDA, CGA, PGA, VGA, EGA and Multisync monitors and their various horizontal sync. freqs.

What are the reasons for the errors and vaguities? Please provide us any additional specific and detailed information on designing, calibrating, testing and applying your methods.

We have designed several Van Eck systems so far, and have also enjoyed very good results. If the information you provide us is specific, detailed and substantial, we will provide you with specific, detailed and substantial information about our designs, results and countermeasures immediately upon receipt of your information.

Hopefully, by cross-pollinating, we can mutually increase our levels of expertise both in the Van Eck methods of eavesdropping and the countermeasures used to thwart them.

Best Regards

John J. Williams
JOHN J. WILLIAMS

St. Paulusstraat 4
2264 KZ Leidschendam
Telephone + 31 70 43 66 02
Telex 31238 drd nl
Postal giro 2445
Telefax + 31 70 43 64 77

Mailing address:
PTT Dr. Neher Laboratories
P.O. Box 421
2260 AK Leidschendam
The Netherlands

ptt dr neher laboratories

Consumertronics Co.
Attn. Mr. John J. Williams
P.O. Drawer 537
Alamogordo, NM 88310
U.S.A.

Your reference	Letter of date	PTT reference	Telephone
	March 28 1988	694/RE/174	+31 70 43 55 91

Enclosures

Date
April 8, 1988

Re Compromising emanation from VDTs

Dear Sir,

Thank you for your comments on my work on compromising emanations. Due to your work in this area you have found out some of the intentional incompleteness in my publications. As you will understand publication of the work carried out at the laboratories on this topic is intended to make people aware of the problems and state ideas on the ways to solve these, rather than to provide a receipe to obtain information from compromising emanations.

I do not agree with your qualification of my publication as 'misleading'. It is common practice not to give full designs of equipment in scientific papers, especially in this case, where people may be interested in obtaining data on 'how to do it'.
Of course half the information on the screen may be lost during reconstruction of the data due to the interlaced TV screen build up. It does affect the readability of the screen, but does not affect the results of the test on whether or not the data may be reconstructed.

You are right in your conclusion regarding the ability of a TV receiver to clearly display the signals from monitors with a higher resolution. Our interest though was mainly focused on simple means to obtain data from emanations from equipment. Of course we have looked into the possibility of also reading information from other sources at a later stage, using more sophisticated equipment, aiming for a measurement method, not aiming for data-reconstruction itself. Struck by the effect of the first publications PTT management has classified all information on these further developments and therefore I am not in the position to give you further details.

The methods we use for the testing of VDTs are internal PTT measuring methods and are not for publication. In my view you can easily develop your own methods based on your own experiences. The only thing a measuring procedure should be based upon is giving the user of the tested equipment an idea of the vulnerability to eavesdropping of this kind (as you know there are many other ways to obtain information besides this specific kind of eavesdropping).

I hope I have informed you sufficiently,

With regards,

Wim van Eck

monitoring with TVRO

This is a public domain file that has been reprinted with permission from an article that appeared in the Spring 1988 issue of **2600 (2600 MAGAZINE, P.O. Box 752, Middle Island, NY 11953, (516)-751-2600). 2600** is the Number One hacker's manual for phone and computer systems. Subscriptions are $15 for individuals and $40 corporate. Back issues are available for $25 per year, from 1984 thru 1987.

Although this article does not directly relate to Van Eck phreaking, the topic is a sister subject since much phone traffic is computer data, and it is another state-of-the-art method used to remotely eavesdrop on computers.

CONSUMERTRONICS
2011 Crescent Dr., P.O. Drawer 537
Alamogordo, NM 88310

This public domain article, written a couple of years back, was obtained from ARPANET. It goes into technical detail on receiving microwave linked telephone conversations using conventional and widely available ham satellite equipment and/or plain satellite TV receiving equipment. Our thanks to the subscriber who sent it in. Regretfully, we don't know who originally wrote the article.

Now that Congress has chosen to attempt to patch a massive hole in the security of communications in the U.S. with a badly drafted law that does not require or even encourage carriers to implement solutions that actually increase real security, I thought I would repost an article I wrote a year ago about a major aspect of the real problem. I hope by so doing to remind everyone that even with a draconian law in place it is still very easy to intercept many regular telephone calls and data circuits.

Nothing in the Electronic Communications Privacy Act of 1986 requires or even particularly encourages carriers to increase the security of radio or satellite links. Listeners who get caught can be punished, but nothing has been done to make listening harder.

The kinds of interception I describe are now highly illegal under the new law, but the equipment required is very widely available (and has important legitimate uses that make a ban on sale or possession very unlikely) and the act of interception can be carried out in total secrecy and is nearly impossible to detect from a distance. The justice department has stated that they do not intend to seriously enforce the radio portions of the law which have been generally recognized to be unenforceable even by the bill's sponsors. So the law, while draconian, really won't have much of a deterrent effect even as respects casual listeners. And casual listeners are not the real problem.

Yes, it is possible, and not even very difficult.

Some years ago it was pointed out that 66 percent of long distance telephone trunks went by ground based microwave. And while the long distance carriers have been working (under some pressure from the NSA and White House) to convert these circuits to optical fibers or at least coaxial cable there are still many routes that use microwave or satellite hops. I don't know an exact figure but I think it would be reasonable to guess that at least 40-50 percent of long distance trunks include a microwave or satellite hop. And some 75 percent (approximately) of long haul microwave relays use the 3.7-4.2 Ghz band which is readily receivable by a TVRO.

Most long haul microwave systems use FM modulation and frequency division multiplexing (FDM) of single sideband suppressed carrier voice channels. Some satellite systems also use this modulation. Unfortunately, FM-FDM-SSB modulation is quite easy to receive with simple and widely available equipment. Recovering the contents of a specific channel is very easy, which opens up the possibility of monitoring random phone calls to a specific group of destinations or monitoring specific private line data or voice circuits (which are assigned to a multiplex slot for long periods of time).

The question of whether a TVRO could be used to monitor phone conversations has been raised on the net. The answer is that with the addition of a stable general coverage single sideband receiver (such as an ICOM R-71 or a Kenwood R-2000 or the receiver section of a modern transceiver) connected to the unfiltered and unclamped video output (provided for connecting stereo adapters and descramblers), a TVRO can be used to listen to FM-FDM multiplexed telephone signals from both celestial and ground-based sources.

Further, with a stable down block down converter that converts to the UHF TV band and one of the scanner type receivers designed to cover this band, one can also receive some of the single channel per carrier (SCPC) signals that carry telephone circuits to more remote places (along with network radio feeds, Muzak, and various broadcast data services such as the AP and UPI news services). (Some signals are dithered and require some form of closed loop AFC to receive them.)

This vulnerability has been well known in security circles for many years, but as the number of TVRO systems has increased to over a million, the problem assumes a somewhat different perspective. In 1976 Mitre estimated that it would cost $50,000+ to intercept microwave telephone calls, and would require a 10 foot dish. In that era a 10 foot dish would attract much attention. Today one can buy a TVRO system with a 75k LNA and an 6-12 foot dish for $1000-$1500, and almost nobody will give the system a second glance as TVRO's are commonplace. A 75k LNA beats the 10-12 db noise figure receiver that Mitre based its calculations on by a very substantial amount. And the current generation of computer controllable general coverage SSB receivers are much cheaper demultiplexing devices than the synthesizer and selective voltmeter that seemed necessary in 1976.

"One should not presume that a long distance telephone call is private."

The existence of all these millions of receivers that can pick up both celestial and ground-based telephone circuits means that one should not presume that a long distance telephone call is private. And more important (because they are much easier to find in FDM complexes), nobody should assume that a private leased line is secure (unless the long distance carrier has specially routed it via lightwave (much more secure) or coaxial cable (somewhat more secure) for its entire path. (Obviously conventional wiretaps also have to be considered if there is some reason to believe that some individual or organization has a strong enough reason to be interested in your communications to face the risks involved in actually physically tapping your lines.)

Background

Communications satellites carry telephone traffic in several formats. The principle formats are:

Multi Channel Systems

1. FDMA-PSK-TDM-PCM.

Used on a number of transponders on 4 and 12 Ghz satellites. Heavily used by private business for tie lines and other leased line services. Sometimes mixed with data. Quite secure if encrypted. Not easily intercepted by private individuals.

2. TDMA-PSK-TDM-PCM.

Used on SBS (12 Ghz) satellites as the principle access technique. Therefore SBS Skyline service and some MCI service (they are now both owned by IBM) is protected this way. Used also on some 4 Ghz transponders. Very difficult for private individuals to intercept even if not encrypted. Some circuits are encrypted, some not. TDMA is felt to be the heavy use satellite access technique of the future as it offers very efficient use of transponder power and dynamic allocation of system capacity to those links which are currently active. When combined with encryption it is quite secure.

3. FDMA-FM-FDM-SSB.

Standard modulation used on almost all terrestrial long haul telephone microwave circuits. Used on several 4 Ghz domestic transponders and most older multi channel Intelsat links. Wideband FM-FDM signals can be readily received by standard TVRO receivers, and an individual channel can be easily picked out of the multiplex signal with a garden variety general coverage SSB communications receiver. Very easy for private individuals to intercept.

4. CDMA-TDM-PCM, otherwise known as spread spectrum.

CDMA or spread spectrum techniques are widely used on military satcom links because of their security and resistance to jamming. Intercepting and decoding well designed secure spread spectrum signals is difficult even for large well equipped intelligence agencies. Decoding some of the commercial spread spectrum data signals can be accomplished by a private individual with the right equipment, but is moderately difficult.

Single channel systems

5. FDMA-FM, otherwise known as SCPC-FM.

Single Channel Per Carrier is used to transmit one single noFM telephone channel between two points. A transponder carries many such FM carriers at one time. Frequencies used are often coordinated by a central station when the call is set up, and may only be used for the duration of the call. This technique is used for communications with remote places that rarely need more than a few circuits at once. Can be relatively easily intercepted by a wide band scanner connected to a very stable block down converter. Easy for private individuals to intercept.

6. FDMA-PCM, otherwise known as SCPC-PCM or SPADE.

This technique is the international standard Intelsat method of establishing telephone connections between places that don't have enough traffic to warrant permanently assigned FDM trunks. Each direction of each telephone call is assigned a channel by the central control station. Stations transmit a PSK keyed carrier on that channel for the duration of the call. Each carrier contains one 8 Khz sampled PCM bitstream along with some error correction and synchronizing bits. As far as I know encryption is not used. The signal can be intercepted by a sophisticated individual but intercepting it requires a rather large dish as the effective radiated power per carrier is very much less than for most SCPC carriers use. A few domestic satcom SCPC users use PCM, probably with some form of encryption. Hard for a private individual to intercept.

7. FM-FDM-FM (Subcarriers on Video feeds).

As most TVRO owners discover, many of the video feeds contain additional subcarriers that carry unrelated or tangentially related material. Included among these are cue and coordination channels that may occasionally carry telephone-like conversations. There are no regular telephone circuits on video subcarriers however. These subcarriers are trivially easy to intercept as most TVRO's have tunable audio demodulation.

On FM-FDM-SSB

All it takes to recover FM-FDM-SSB signals is a suitable wideband FM receiver connected to a stable general coverage SSB receiver that tunes the frequency range used for the baseband. TVRO receivers have the correct bandwidth for many such signals and often incorporate provisions for IF filters that can be used to better adapt the receiver to the narrow band signals found on some transponders. And modern general coverage SSB receivers and transceiver receiver sections with synthesized tuning, digital frequency display, and narrow IF filters are well suited to recovering the audio on a particular channel.

Listening to FM-FDM-SSB signals can be accomplished by tuning the TVRO receiver to either a satellite transponder carrying an FM-FDM-SSB signal (this may involve restricting the IF bandwidth with a filter as some transponders carry more than one FDM-FM signal), or pointing the antenna at a nearby terrestrial microwave transmitter and tuning the receiver for maximum signal.

Once the FDM-FM signal has been tuned in, the single sideband receiver can be used to search the baseband (typically .3 Mhz to 6 or 8 Mhz) for telephone conversations, data transmissions, and other private line circuits. Individual channels will appear as USB or LSB signals at precise 4 Khz intervals. In fact, the whole baseband is organized into 12 channel groups, 60 channel supergroups, and 600 channel mastergroups according to a standard frequency plan (the AT&T plan as usual is different from the CCITT one used internationally).

"Nothing in the Electronic Communications Privacy Act of 1986 requires carriers to increase the security of radio or satellite links."

Most channels have completely suppressed carriers, although certain channels will seem to have a carrier in them (but slightly off frequency) which is something called a pilot tone, used to monitor circuit continuity and control overall gain. Depending on how archaic the telephone trunk equipment is on a particular trunk, it may have a 2600 hz SF signalling tone in it when it is idle which is dropped when the channel is in use for a call. Trunks which use SF signalling also often use MFKP (multi-frequency key-pulsing—the famous blue box version of tone dialing) to pass telephone numbers on to the destination switch. More modern trunks use CCIS (common control interoffice signalling) which is a packet network replacement for the earlier and less secure in band signalling that uses separate signalling channels to carry all the signalling for all the trunks in a trunk route.

Obviously, a single signal usually carries only half a telephone conversation so it is necessary to use two receivers and TVRO's to pick up both sides of the call clearly. Receiving both sides of a terrestrial circuit requires a suitable location where both directions of transmission can be picked up, which usually means a site in line with the microwave path. Sometimes both directions of transmission from a single repeater site can be monitored by a very nearby (less than a couple of miles) receiver. Many telephone trunks have low enough echo return loss so that both parties can be heard even when monitoring only one direction of transmission, so it is quite possible to listen to both sides of some conversations with only one receiver. Both sides of a satellite FDM circuit can usually be found on the same bird but are sometimes not, and sometimes not even on FDM satcom at all.

In general, particularly on terrestrial signals, all the channels in a 12 channel group originate and terminate at the same place. The groups and supergroups that make up a mastergroup however often originate from several different places. Demodulation to baseband audio is generally done as few times as possible on a trunk or private line circuit that connects two places, the 12 channels of its group are shifted to various frequencies within the baseband of the different satellite, microwave, or coaxial cable FDM signals that carry it to its destination. But at least with older multiplexing equipment the granularity of routing resolution is usually a group (occasionally half a group), and all 12 of the channels in a group usually end up demodulated to audio at the same place.

Channels within a group are assigned to various purposes. Some may carry telephone trunks, some may carry private line data, some may carry private trunks that belong to large companies, and a certain percentage are reserved for use as spares. It has long been telephone company practice to route the telephone trunks between two switching centers over several different paths to supply redundancy in the event one path fails (and also to make it harder to intercept a particular call between the two switches). This means that any given FDM group may contain trunks from several different trunk groups rather than containing all the trunks from, for example, Chicago to West Bend.

On PSK TDM

The most secure technique in commercial service, and probably the technique that will predominate on satellite links in the future, is TDM-PCM (time division multiplexed pulse code modulation) either phase shift keying (usually QPSK) a continuous carrier on a transponder that may have several such carriers on it (FDMA—frequency division multiple access) or keying a single carrier that occupies the whole transponder in bursts precisely timed so as to not overlap other carriers from other stations that it shares a transponder with (TDMA—time division multiple access).

Telephone traffic on TDM-PCM links is sampled 8000 times a second and converted into 8 bit binary values (in a sort of floating point format called A-law or U-law companding that greatly expands the dynamic range from softest to loudest that the channel will handle). (There are other digitizing standards used on satellite phone links but the standard T carrier—D channel bank is widely used.) Some number of these channels (often 24) are combined into a high speed serial bit stream (often 1.544 mb/s) by sending one sample from each channel in serial form as a string of 8 bits followed by a sample from the next channel and so forth. Sometimes this composite bit stream or the bit stream from individual is encrypted with a DES chip. Error correction and framing bits and sometimes special control channel bits are added. This digital bit stream is then scrambled (so it has more predictable transition statistics and little or no DC component) by a linear feedback shift register sequence. The resultant bit stream is used to PSK modulate a carrier which is uplinked to the satellite.

Receiving these FDMA-PSK-TDM-PCM digital transmissions requires complex RF modems, a large enough dish to get an acceptable signal to noise ratio (and BER), and often requires knowledge of DES encryption keys used (unless you are a major intelligence agency and can break DES). While some such transmissions that aren't encrypted could be intercepted by a sophisticated individual, particularly one who had access to the RF modem and multiplexing hardware used by the subscribers, the required expense is orders of magnitude greater than that required to intercept FM-FMD-SSB signals and the equipment required is specialized and not widely available. (Decoders for TDM-PCM bit streams could be built by a skilled person from available chips relatively easily, but the PSK high speed RF modem technology used would not be easy for even a skilled person to duplicate without substantial resources.) Presumably few if any casual listeners intercept TDM-PCM radio circuits; the only listeners to such transmissions are the intelligence agencies and perhaps industrial spies who can afford to buy the necessary hardware to listen to their competitors' private circuits. And more and more users of such links are encrypting them with DES (which is relatively easy as the information is already in a digital format).

TDMA-PSK-TDM-PCM signals are much more complex than most FDMA-PSK-TDM-PCM signals. This is natural since all traffic is transmitted by having each station on the network transmit a burst of very high speed (tens of mb/s) data in an assigned time slot round robin fashion. Included in the burst is all of the traffic that station has with every other station on the network. Every other station monitors all the bursts from stations it is in communication with and picks out the channels that correspond to its incoming traffic. In many such systems, burst lengths and time slots are dynamically assigned by a master ground station computer as calls are set up and terminated. Each station is capable of receiving and decoding the bursts transmitted by every other station it talks to, so if the channels are not encrypted it could monitor much of or all the traffic going through the transponder.

The burst formats are complex and contain error correction, status and control channels, call setup channels, and so forth. And the bursts are scrambled just as in the continuous carrier FDM case. Intercepting and demodulating such a signal would be a major task and is probably something that has only been done (by intelligence agencies) by using perverted versions of the ground station hardware and firmware used by the system. In addition to the complexity of the task of sorting out the digital information and finding the right time slot from the right burst to retrieve the channel of interest, the very high speed fast lock-on RF modems used to demodulate the bursts are themselves non-trivial devices. I suspect that even perverting the firmware in a legitimate ground terminal is complex enough so that no private individual could easily accomplish it without access to a lot of detailed non-documented information (such as source of the firmware and precise details of the protocol and burst formats).