BEYOND

VAN ECK PHREAKING
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. Neber Laboratorium 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 with 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 thus an unmonitored live VDT, get it to change 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 cryptography 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. 6, Dec. 1985, ATTN: DR. HAROLD JOSEPH HOLLAND, 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

CONSUMERTRONICS publishes over 100 manuals and software packages, and offers various services. Related CONSUMERTRONICS publications include: COMPUTER PERFORATING (1975), PHONE COLOR BOX (1980), AUTOMATIC TELLER MACHINES (1981), ATM ADDENDUM (1982), SECRET & SURVIVAL RADIO (1982), ABSOLUTE COMPUTER SECURITY (1982) and CRYP TANOLOGY TECHNIQUES (1984). The latter two manuals are also available with diskettes (922 each total: we fully support PCDOS, MSDOS and PS/2). Two catalogs are available. OUR TECHNOLOGY SURVIVAL CATALOG is mostly devoted to computing equipment and electronics. OUR SUPER-SURVIVAL CATALOG is mostly devoted to physical means of survival (ex: energy, weapons, explosives, etc.). Each catalog costs $2. Both cost $3. Both are FREE with any purchase. Both are available in printed and ASCII disk file formats.

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 tape recorders (active or dormant), hidden in a room is to sweep the room with microphones and observe the return of the first harmonics that result from non-linear junction action. In fact, it is this reason why the Soviets buried thousands of cheap radios in the walls of the new U.S. Embassy in Moscow. By swapping the Embassy, plus 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. content 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 EMI.

(4) The spectral density for typical digital waveforms decreases with freq. This is compensated for in the radiated field because high freqs. radiate more efficiently than 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
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 quiet section of a VHF band, set 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 TBS-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 radio section in the old VINTAGE DEVICES (V6) 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 its own characteristic signature that could be digitally recorded 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. It 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 of patterns consisting of herringbone, diagonal lines or bars, or a windshiled 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 garage. Although a mobile receiver can cover a much greater area than a stationary receiver, roaming around with a 30-foot directional antenna could prove embarrassing - especially with the increased awareness of Van Eck phreaking.

BEYOND 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 VCRs VHF antenna screws, which also served as the input from their VCR. Needless to say, much of their neighborhood shared their enjoyment. Only after receiving weird stares and obscene phone calls did they finally discover the embarrassing 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 1 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 VS/HS modulator and a detector BW of 2.5 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 (20-30 MHz wide) of the VDT's 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 557 ALAMOGORDO, NM 88310 (505) 434-0224

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 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 sharp 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 amplitude, the greater the image contrast, and the sharper the pulse skirt.

You can verify these things by playing around with your TV or computer monitor Brightness and Contrast controls. At this 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.
As you can see, in theory, the received signal has a flat PSD up to 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 (i.e. modulated) as it horizontally scans. The video signal is not a digital signal in which a logical zero turns OFF the beam (i.e. inhibits the spot), whereas a logical one turns ON the beam (i.e. creates a spot). Therefore, there is a direct and predictable relationship between the video signal modulation and the resultant image.

**SEE EXTERNAL SYNC. GENERATOR CIRCUIT**

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

1. Learn access codes, passwords, PINs and keys to later penetrate the system or defraud it or its subjects (i.e. clients, employees, patients, etc.) in some other manner.
2. Learn personal information about subjects for its intrinsic (i.e. gossip) value.
3. 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. Obtain government, trade or business secrets (e.g. client lists, price lists, supplier lists, product designs, publications, etc.). Such knowledge can be worth $ Millions! And such practices is most probably illegal.
5. Obtain knowledge on subjects of interest (e.g. medicine, law, government).
6. Obtain news and announcements before they are publicly known and before they are heavily censored.
7. Investigate a person, business or association.
The power spectral density of the video signal can best be described by the formula shown:

\[ S_x(f) = \frac{A}{\pi F_{TH}^2} \left( \frac{\sin \left( \frac{f}{F_{TH}} \right)}{\frac{f}{F_{TH}}} \right)^2 \frac{\sin \left( \frac{f + 1}{F_{TH}} \right)}{\frac{f + 1}{F_{TH}}} \]

Where \( F_{TH} \) is the duration of one bit in the (final video signal (Figure 2)}, \( T_f \) 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 \( 1/T_f \). The power spectral density of the signal is fairly constant up to the fundamental freq. of \( 1/T_f \). Beyond \( F_b \), the spectral density decreases by a rate of 20 DB per decade. Beyond \( F_b \), the low pass filter cut-off freq., decreases by a rate of 40 DB per decade.

In most practical cases, \( F_b \) is in the 20-50 MHz range, while \( F_t \) is in the 200-500 MHz range (depending upon the computer and monitor used). Thus, the radiated signal consists of the fundamental plus about 8 usable harmonics - spanning the entire VHF band (30-500 MHz), and the lower part of the UHF band (300-4000 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 monotoncoally increases with freq. at a rate of about 20 DB per decade. The actual rate is largely determined by the physical sizes of the VDTs' electronic components radiating the signal (i.e., 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, up to about \( F_b \), received signal lobes of uniform strength spaced uniformly apart along the spectrum well within the VHF receiving range of even the cheapest TVRs. 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, the Nyquist freq. \( 1/2 f_s \), 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

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 "phreaking" 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-300 ohm transformer (cable is 75 ohm, split-pair is 300 ohm). The VCR's VHF output is then hooked up to the TV.

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.

BEYOND VAN ECK PHREALKING

Many VTs are based on the same principle as European black-and-white TVs (not commonly available in the U.S.) - these VTs 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 VTs of this type can make remote eavesdropping on VTs a virtual breeze! Even if VTs 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 sync. 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:

\[ \text{FREQUENCY (Horizontal)} = N \times \text{FREQUENCY (Vertical)} \]

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 and 50 Hz VS signals (see Figure 5). TV circuits (VHF freq., such as from the HS freq. (15.75 KHz), derive it from the 50 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. (up to the HF 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 #15-1114. The output of this amp and the external sync. generator are combined using the 75-OHM, 5-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 sync. take effect, first one and then the other of these conditions are corrected. Combining adjustments between the external sync. 'tweakers' 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 sync. 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-
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 pulses are excluded. Some horizontal picture jitter will occur if the equalizing pulses at twice the HS freq.) are excluded with the blanking pulses.

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

\[ N = 8 \times 1000 \times N_1 + 100 \times N_2 + 10 \times N_3 + N_4 \]

Where:
- \( N_1 \) = Value of J13-J16,
- \( N_2 \) = Value of J9-J12
- \( N_3 \) = Value of J5-J8,
- \( N_4 \) = Value of J1-J4

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

\[ N = 10 \times 1000 \times N_1 + 100 \times N_2 + 10 \times N_3 + N_4 \]

Where:
- \( N_1 \) = Value of J13-J16,
- \( N_2 \) = Value of J9-J12
- \( N_3 \) = Value of J5-J8,
- \( N_4 \) = 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 915-1141C 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, SL. This freq. is divided down by U1, a programmable divide-by-N counter. The N is determined by SW1b and U9/10 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 VDTs (else tear occurs), for best results, sync. pulse widths should conform to the TV.
BEYOND VAN ECK PHREAKING

Q8 (bottom) generates the identical blanking and VS freqs. B8 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 the different TVs. The compromise 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 U8 (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 U9's output is low (before and after the 18 count), the HS signal is gated to the output. Actually, U8 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 U8 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, U8's output goes high and it stays high until the count of 13, when U7's output goes high. U8 is switched low when U7's output is gated to U8's master reset thru U10.

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. One of the TV reception mode 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 exist before. Note that the "stabilizer" is not a VDT signal, all "video stabilizers" provide for a missing syncs., 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 available 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 nulls 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 video signal using a tunable narrow bandpass filter. The resultant signal is a 15-35 KHz sine wave, 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 sine wave 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 1: (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, U8 and U10. It may drift a little, but it's much simpler to build. The five SK ceramic caps (20-turn preferred) are individually tuned for "fine" and the Composite Sync, output in the 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 6: BR 15-1141C 75-OHM, 3-WAY, COAXIAL COUPLER/COMBiner can be used as shown in (B) to combine an external sync. 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 sync. 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. IC2a allows for the selection of normal or inverse video. IC2b 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 use, IC3e 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 (220) Manual.

(A) 15-18 DB GAIN RF AMP: Amidon T50-6 (yellow) toroid cores are best for optimum Q for T1 and T2 (T3 duplicates T1 but with no tap). The core is wrapped with a maximum number of turns (evenly spaced single layer) using 28-30 gauge 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 T3 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) 13-15 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 Q connection to ground). The primary 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).

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.

The TV's reconstruction of the VDT image may not start on line #1 or end on line #352 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 sync. upon the vertical ramp waveform. See Figure 12. The ramp voltage waveform can be adjusted by using the vertical height adjustment on the TV.

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 char./line, reading 80 char./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 (see ENA).
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 LP 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 step — is controlled by the Contrast Control. The brightness of the reproduced image of the VDT on the TV is like a negative photo. For TVs, the height of the pulse defines the black level while the white level is defined by the pulse's baseline.
(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 kH (for VHF) to several hundred MHz (for UHF). The cage should be made of a thick metal, such as steel or copper, and should be grounded. The cage should be connected to the ground terminal of the VDT, and the ground terminal should be connected to the outlet ground. This will provide a path for the EMI to flow to the ground, rather than through the television set. The cage should also be designed to prevent interference with the VDT's operation. The cage should be securely fastened to the desk or other surface, and should be large enough to accommodate all equipment, including cables and other accessories. The cage should be as large as possible, and should be made of a conductive material such as metal. The cage should be properly grounded, and should be connected to the building's ground system. The cage should be designed to minimize any leakage of EMI, and should be secured to prevent tampering. The cage should be designed to be easily accessible for maintenance and repair. The cage should be designed to be as strong as possible, and should be able to withstand the weight of the equipment. The cage should be designed to be as energy-efficient as possible, and should be able to operate for long periods of time without overheating. The cage should be designed to be as flexible as possible, and should be able to accommodate changes in equipment and layout. The cage should be designed to be as easy to install as possible, and should be able to be assembled quickly and easily. The cage should be designed to be as durable as possible, and should be able to withstand harsh environments. The cage should be designed to be as cost-effective as possible, and should be able to be purchased at a reasonable price. The cage should be designed to be as secure as possible, and should be able to prevent unauthorized access to the equipment. The cage should be designed to be as ergonomic as possible, and should be able to accommodate the user's needs. The cage should be designed to be as versatile as possible, and should be able to accommodate a variety of equipment. The cage should be designed to be as scalable as possible, and should be able to accommodate growth in the future.

(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 50 ns chips on a 4 usec 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 (i.e. antennas) and as reflector for horizontal ones inside the computer, keyboard and VDT, thus increasing 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 1-2-1-2 cycle. By selecting the scan 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 char across (typical of most spreadsheets) is much preferred over 80 char. 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 "809 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 mistake the distance (and perhaps direction) of an abnormal video signal, thus misidentifying 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 TV stations 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 identical VDTs, the produced EMI 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.

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

SOLD FOR EDUCATIONAL PURPOSES ONLY
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 four possible directions of VDT EMI, it is not enough to measure the strength and free, distribution of the combined EMI. 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 screening screens. Both signals 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 separator to the TV thru an optical link as their distances may exceed 1000 yards (although under 100 yards is more common for unshielded VDTs and 40 yards for shielded VDTs), and optical cable 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 motionless and the same 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 of at least 1 MHz minimum. At 1 MHz, the presence of a page of text is discernable but the test itself is not readable. For readable readability from CA TV, the detection BW must be at least 4.75 MHz. Optimum results for TVs are obtained at 5 MHz, particularly for EGA, VGA and multisection monitors. The IF frequency 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 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.

BEYOND VAN ECK PHREAKING

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. Although 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 512 Ke, using SUPERPAINT on an IMAGEWRITER I printer. Also we generally prefer 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 hackers legends (I just can't remember who), I have been able to obtain what has been represented to me, a schematic 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 messed-up and messed-up pile of loose-leaf notes in my hot, sweaty hands were really THE TOP SECRET WIM VAN ECK SYN 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, dynamite 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 VDTs 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. You usually end up often manually adjusting these pots. PLL time-constant is about 0.29 seconds. The PLL's VCO operates at 2 x the VFO frequency. The PLL can be adjusted to increase/decrease its locking range thru its V7K pot. The LED indicates when the PLL is in lock.
The output signal of the PLL (after division by two) is used as the horizontal sync signal. The PLL YCO's signal is fed into the FREQUENCY DIVIDER. Its divider 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 divider 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 PCC and Multisync). If the displayed signal is greater than 21.85 KHz, you are probably locked onto the VDT's second harmonic. If so, adjust the PLL's lock pot so that it locks onto the VDT's fundamental frequency.

Both sync signals are logically ANOed, and are then buffered and fed into the OR (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 OR 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 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 23-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 OR 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 OR or turn OFF the SYNREST, its signal is lost and K1 drops out and reconnects up the Video Amp.

SOLD FOR EDUCATIONAL PURPOSES ONLY
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 $99.50 (+$2.50 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 output) to study its capability to scramble nearby TV reception, add $15.

Because a TV receiver cannot produce as sharp 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 success in all that you do.
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 MAgAZINE. P.O. Box 751, 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 for corporate. Back issues are available for $25 per year, from 1984 thru 1987.

Although this article does not directly relate to Van Dick phreaking, the topic is a sister subject since phone traffic (which can be monitored with TVRO) and another state-of-the-art method used to remotely eavesdrop on computers.

CONSUMER TRONICS
311 Crescent Dr., P.O. Drawer 137
Albuquerque, NM 87109

The public service article, written by a couple of years ago and appeared in a number of technical and computer magazines, demonstrates that TVRO is a powerful and easily available means of electronic warfare and phone jacks. It is an excellent way to avoid violation of the law and an enjoyable and educational activity:

Understand that the example transmission, and even the most powerful TVRO system, is not a substitute for a legal system. The fact that a TVRO system can be used to listen to FAX data, phone conversations, and the like does not mean that it is legal for you to do so. In fact, TVRO systems, like all other electronic surveillance devices, are illegal to use without the permission of the person being monitored. TVRO systems are legal to use because they are used to monitor the phone lines of others, not the phone lines of your own.

Further, unlike a simple phone system, TVRO systems are not used to monitor the phone lines of others in the same way that a simple phone system is used to monitor the phone lines of others. TVRO systems are used to monitor the phone lines of others that are not accessible to the general public. In addition, TVRO systems are used to monitor the phone lines of others that are not accessible to the general public. TVRO systems are used to monitor the phone lines of others that are not accessible to the general public.

TVRO systems are not used to monitor the phone lines of others in the same way that a simple phone system is used to monitor the phone lines of others. TVRO systems are used to monitor the phone lines of others that are not accessible to the general public. In addition, TVRO systems are used to monitor the phone lines of others that are not accessible to the general public. TVRO systems are used to monitor the phone lines of others that are not accessible to the general public.

TVRO systems are not used to monitor the phone lines of others in the same way that a simple phone system is used to monitor the phone lines of others. TVRO systems are used to monitor the phone lines of others that are not accessible to the general public. In addition, TVRO systems are used to monitor the phone lines of others that are not accessible to the general public. TVRO systems are used to monitor the phone lines of others that are not accessible to the general public.