Electromagnetic Eavesdropping Machines for Christmas?

Almost 3 years ago we published "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk by Wim van Eck of the Netherlands PTT. In Volume 4, Number 4 of *Computers & Security* in December 1985, van Eck stated in his abstract

"This paper describes the results of research into the possibility of *eavesdropping* on video display units, by picking up and decoding the electromagnetic interference produced by this type of equipment. During the research project, which started in January 1983, it became more and more clear that this type of information theft can be committed very easily using a normal TV receiver."

In June 1986 and again in September of that year we published supplementary reports about van Eck's "phenomenon, " as it was labeled by the popular press. We reported a conversation with an individual who purchased an RCA model AXR122 and within limits was able to replicate van Eck's work. That television set had a voltage-controlled oscillator (VCO) with no detents *(stops* between channels and no fine tuning). Information about this type of eavesdropping has been classified for about 20 years. The Tempest (**T**ransient **E**lectro**M**agnetic **P**ulse **E**manation **ST**andard) project has been a joint research and development effort of the U. S. National Security Agency (NSA) and the Department of Defense (DoD). Even the program's name had been classified for most of that period. Although reported widely by the press throughout Europe in 1985 and covered by the BBC in two broadcasts as well as CBC radio, the topic faded from the press. Aside from an article, "The Tempest over Leaking Computers," that I wrote and which was published in the Winter 1988 issue of *Abacus,* nothing more has appeared about this topic.

A Detailed Manual Available

Late this spring, I received a letter and a manual from John J. Williams of Consumertronics. Mr. Williams, a specialist in electronics and cryptography, has often communicated with me in the past about various topics. This time he sent me an extensive letter, a detailed manual and a letter received from Wim van Eck.

He had written to Wim van Eck after reading the article published in the journal to point out that some technical details were missing. Van Eck replied

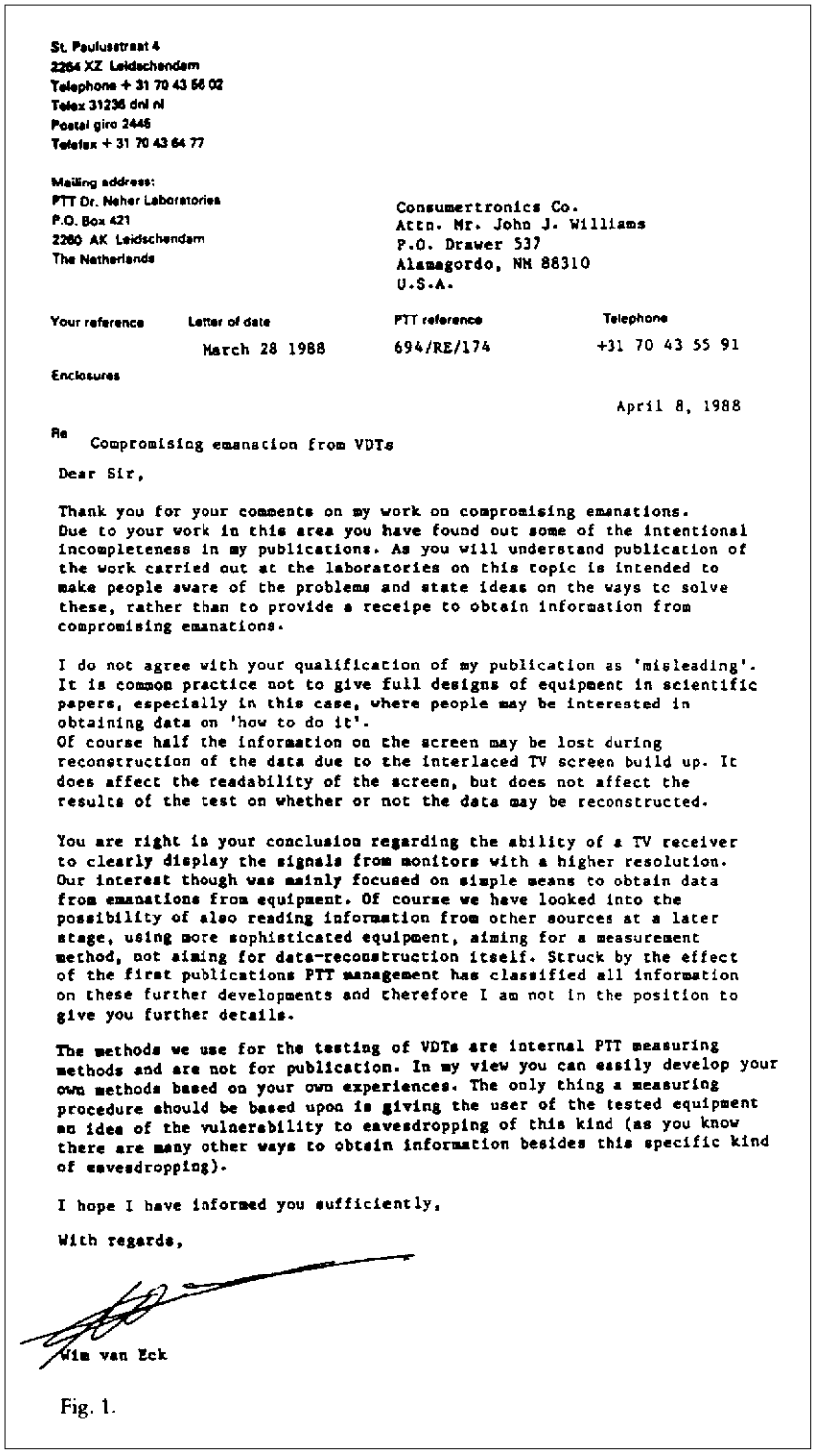
"the publication of the work carried out at the laboratories on this topic is intended to make people aware of the problem and state ideas on the ways to solve these, rather than to provide a recipe to obtain information from compromising emanations. "

A complete copy of van Eck's reply appears in Fig. 1. In one portion of his letter to me, Mr. Williams wrote

"On van Eck's methods, I had a pretty good idea of what he did and how to duplicate his experiments from a four column-inch newspaper article. I did kick myself for not conceiving this technique before van Eck did. All one needs is moderate expertise in both computers (particularly VDTs) and TVs. That combination is not that all unique If you've seen articles over the last decade published in Radio Electronics for example, those on descrambling and laser surveillance, it is clear that many controversial topics are already discussed and described fully in the traditional news media

One then must question how effective it is to conceal that information, particularly in a technical publication that largely reaches responsible people."

I agree completely with Mr. Williams about concealing information, particularly from a responsible, technical audience. None the less, the U. S. government appears to have gone to embarrassing lengths to prevent open discussion and demonstration of electronic eavesdropping equipment. The U.S. government is not alone; such action has also taken place in the United Kingdom at a major security product conference in London.



St. Paulusstraat 4
2264 XZ Leidschendam
Telephone + 31 70 43 56 02
Telex 31236 dnl 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

Consumertronics Co.
Attn. Mr. John J. Williams
P.O. Drawer 537
Alamagordo, 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

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 tc 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

Fig. 1.

In the States, for example, an exhibitor planning to demonstrate such equipment and protective measures developed by that company, withdrew from an exhibition of the Computer Security Institute in November 1986. At another professional conference, a demonstration and paper by Wang Research Laboratories (Wang is the largest producer of Tempest equipment) was canceled because NSA stepped in and classified the speech just before it was to be given. At Interface '87, a company canceled its seminar, "How Computer Security Can Be Compromised," demonstrating passive eavesdropping techniques, noting that it was done at the request of NSA.

Two Details NOT Included by van Eck

In preparing the original copy of the van Eck paper, one element had not been included since he did not wish to reveal the electronic circuitry. Another omission was made when we did the final editing since we too felt that full data should not be disclosed.

Mr. Williams pinpoints these two details in his manual,*"Beyond van Eck Phreaking"*. The two major obstacles to good van Eck TV reception he noted are: (a) TV receiver tuning and (b) replacement of the synchronization signal.

His manual notes that "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, but the best way is to use a VCR, a home video recorder."

He also notes that "many VDTs are based upon the same principle as European black-and-white TVs (not commonly available in the United States). These TVs can sometimes be tuned to generate nearly the same frequency with their internal free-running synchronization oscillators as the VDT being monitored. . . Using TVs of this type can make remote eavesdropping on VDTs virtually a breeze."

Mr. Williams also provides the reader of his manual with a comprehensive schematic diagram, including the microchips and their names, to build the external synchronization unit. This had purposely been left out of van Eck's paper. The manual also includes the necessary formulae to adjust horizontal and vertical frequencies.

Also missing from the van Eck paper was information about interfacing the external synch unit and the TV receiver. These are provided in the manual as shown in Fig. 2.

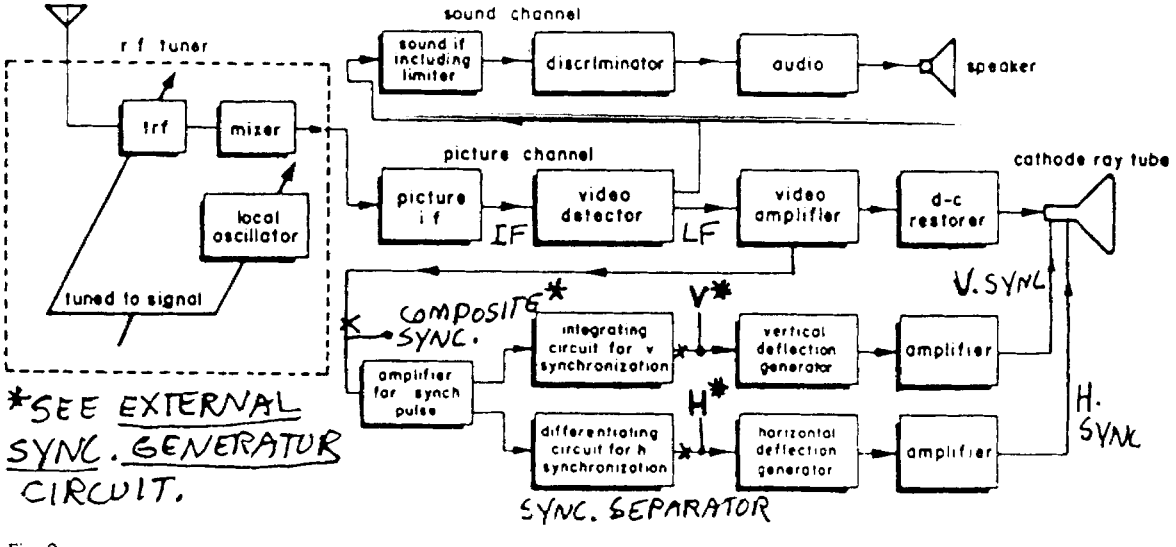


Fig. 2.

Evaluation of the Threat

Electromagnetic eavesdropping is currently *not* a major threat in computer security. It is a time consuming and costly procedure, particularly if one wishes to obtain clean screen reproductions.

Contrary to general belief, this operation does not require having a person sit for hours and/or days peering at the interceptor's monitor. Once the unit has been "sighted" on its target, it can be left

unattended. A time-lapse VCR to shoot the screens can do the job. All the snooper has to do is come to the equipment van periodically and replace the video tape. We have advanced technologically so that we can "transfer" the video tape data to a computer disk. All that remains is the use of a good search program for keywords or critical numbers to scan the data.

When a company spends hundreds of thousands of dollars to analyze possible oil deposits before it bids millions for a lease from the government, how much is it worth to obtain that data? If one could obtain advanced information about a company acquisition attempt or a pending stock merger and has large sums to invest, would a quarter of a million investment in eavesdropping be costly?

What Happens Next?

When the van Eck paper first appeared, I received numerous phone calls and letters from technical personnel for assistance in their building of the equipment. I did not provide the missing data. However, some of those who called and/or wrote communicated with me at a later date to explain how they overcame the missing details.

Because more and more individuals were able to fill in the missing data, I noted at Elsevier's COMPSEC 87 workshop that it was now only a matter of a few years before one of the popular hobby publications in the States prints the schematic diagrams, a parts list and step-by-step instructions.

During a conversation with the director of computer security of a multinational petroleum company recently, I told him about the

William's manual . As we were saying good-bye, he asked me if I thought that Radio Shack (Tandy) would be selling kits or completed electromagnetic eavesdropping units by Christmas. I do not know whether it will be a kit or a finished unit. If they do not market the product, someone else will undoubtedly do so.