REALISTIC EAVESDROPPING ATTACKS ON COMPUTER DISPLAYS WITH LOW-COST AND MOBILE RECEIVER SYSTEM

Fürkan Elibol[1,2], Uğur Sarac[1], Işın Erer[2]

(1) TÜBİTAK BİLGEM UEKAE 41470 Gebze-Kocaeli/Türkiye
(2) Department of Electronics and Communications Engineering, İstanbul Technical University, Maslak-İstanbul/Türkiye

ABSTRACT

It is known that the computer display images can be reconstructed from display's radio frequency emanations. This is a big information leakage threat for information security. Recently published eavesdropping systems are very expensive and not portable. Furthermore all the published eavesdropping attacks are demonstrated for distance up to 10 meters away from display. In this work, a low-cost and all-in-one mobile receiver is combined to capture emanations from long distance approximately 50 meters away from display and to reconstruct the display images. In our eavesdropping scenario, receiver system is in a building and the target display is in another building. These experiments show that 26 points and bigger fonts can be read easily from the reconstructed images which are captured from the target display approximately 50 meters away. With this new system, we can also capture emanations from 3 meters away of the target display in an office environment for comparison. In this latter experiment 9 points and bigger fonts can be read easily.

Keywords— TEMPEST, compromising emanations, information leakage, eavesdropping, video displays.

1. INTRODUCTION

All electronic equipments emit electromagnetic signals unintentionally. These electromagnetic radiations may contain information for Information Technology Equipments (ITE). An eavesdropper can reconstruct processed data from these radiated signals at a distance. This fact is a big threat for information security. There are some electromagnetic compatibility (EMC) studies which try to protect equipments and humans from these electromagnetic radiations. But these studies are not for information security protection for ITE. There are also some secret test procedures and emission limits to prevent electromagnetic information leakages. Some governments make huge investments for special TEMPEST hardware and try to apply some special security rules to protect their information from eavesdroppers.

One of the most important information sources are video display units. Because of the repeated structure of the video signals they are very risky for information security. The starting point of the studies about the eavesdropping risk of the displays was a research program carried out by the Dr. Neher Laboratories of Netherlands PTT [1] [2]. They picked up information displayed on a remote video screen placed in a building from a distance with a very high frequency (VHF) band antenna, a receiver system and a television screen. In [3] and [4], laptop displays and flat panel displays are used as target information sources and display images reconstructed. In [5], laptop displays and LCDs are used as target and electromagnetic emanations taken with near magnetic field probe and injection probe. In [6], there are some open electromagnetic emission limits to test video display units for electromagnetic radiation security. In [7], there are some tests for finding electromagnetic leakage quality. In [8], there are some countermeasures for eavesdropping such as filtering, shielding and jamming. And in [9], there is a software based countermeasure method which consists of some special filtered text fonts.

In this work, we have developed a portable and low-cost eavesdropping system. All the published systems are very expensive and very heavy so they are not suitable for a realistic eavesdropping scenario. They also use external waveform generators for producing synchronization signals. We also developed an algorithm to find synchronization frequency and to reconstruct display image. We tested our eavesdropping system and our algorithms with a realistic eavesdropping scenario. In our scenario, eavesdropper and target display are 46 meters away from each other and we can reconstruct display image with a high readability.

2. EAVESDROPPING TOOLS

For TEMPEST eavesdropping, an attacker needs at least an antenna, a receiver, a digitizer, a processor and a display. In most of the cases, eavesdropper also needs a waveform generator for horizontal and vertical synchronization signals. Figure 1 shows block diagram of a traditional eavesdropping system.

© EURASIP, 2012 - ISSN 2076-1465

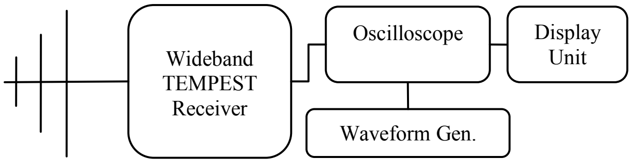


Fig. 1. Traditional eavesdropping system.

For eavesdropping, there must be a suitable antenna to catch electromagnetic emanations. This antenna must cover entire frequency range of interest and must be as compact as possible. Therefore log-periodic antennas are commonly used for eavesdropping. In [5], an Anritsu MP666A log-periodic antenna (20 to 2000MHz) is used. In [7] [10], A.H. Systems Inc. SAS-510-2 log-periodic antenna (290 to 2000MHz) is used. And in [3] [11], Dynamic Science R-1150-10A portable antenna kit (100 to 1000MHz) is used. In this work, we also used Dynamic Science R-1150-10A.

One of the most important parts of an eavesdropping system is the receiver part. Since computer video signals have very high transmission rates which vary from 20 to 150 million pixels per second [3], the receiver must be very sensitive and must have large bandwidth of at least 20MHz. Commercially available TEMPEST measurement receivers such as Rohde & Schwarz FSET and Dynamic Science are very expensive and very heavy. Therefore they are not suitable for a realistic eavesdropping scenario.

In this work, we used software controllable radio device (National Instruments PXI-e 5665) with a portable chassis that includes processor and display. NI PXIe-5665 is a three-stage superheterodyne analyzer. It covers all interested frequencies from 20Hz to 3.6GHz and it has very low noise floor of -165dBm/Hz which is good enough for eavesdropping from long distances. 256MB onboard memory is also available for capturing and processing long duration data. This system is very portable, lightweight and inexpensive in contrast to traditional eavesdropping systems. Figure 2 shows NI PXI based mobile eavesdropping system.

Fig. 2. Mobile eavesdropping system

In traditional methods, the eavesdropper receives video signal from electromagnetic emanations and gives vertical and horizontal synchronization signals from waveform generators to reconstruct the image [8]. We did not use any signal or waveform generator for vertical and horizontal synchronization. We made all the synchronization processes through software. In section 3 all reconstruction and synchronization are explained in detail.

3. IMAGE RECONSTRUCTION METHOD

The vast majority of modern computer video displays in the market are raster-scan devices. A raster-scan device scans the screen from left to right and from top to bottom in a regular pattern. So the image is a collection of these scan lines that have a constant length. There are visible and invisible pixels in a scan line. Invisible pixels are important to allocate extra time for synchronization pulses' transmission and movement of the electron beam [12]. These invisible pixels occur as black gaps in the reconstructed images. Figure 3 shows scan line, line gap, frame and frame gap on an image which is reconstructed from direct digitizing of the RGB cable data.

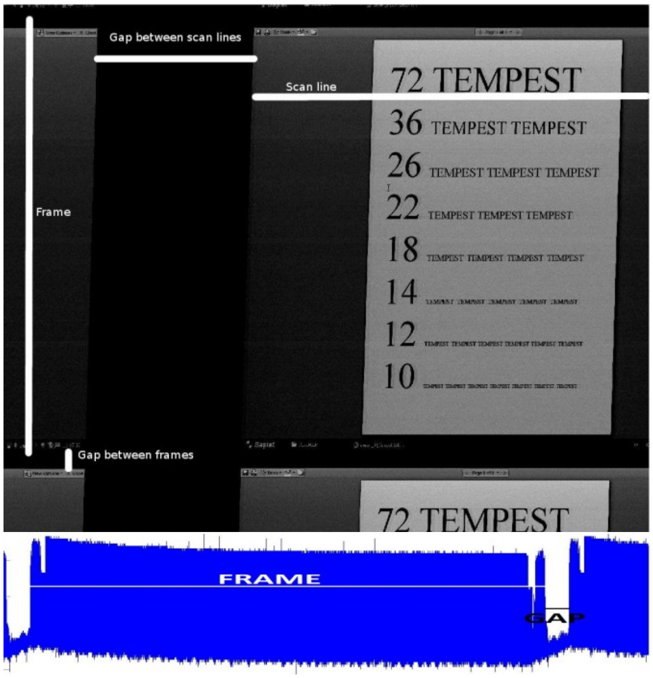


Fig. 3. RGB cable data.

All the lines and frames in a display unit have synchronization pulses. The line synchronization pulses' frequency is called horizontal synchronization frequency and the frame synchronization pulses' frequency is called vertical synchronization frequency. It is very important to find and adjust horizontal synchronization frequency as accurate as possible to make a meaningful image from electromagnetic emanations. But these synchronization pulses are not present in a usable form in the electromagnetic emanation signal. To solve this issue, waveform generators are used for regenerating the synchronization pulses independently [3] [5] [7] [11] [8]. Because of the temperature dependent frequency shifts of these waveform generators, it is still hard to obtain stable images. On the other hand, use of external waveform generators increases eavesdropping system price and decreases portability. Due to these reasons, we developed an algorithm to find horizontal synchronization frequency as accurate as possible. Then we used this frequency to raster scan lines. So there is no need to use external waveform generators for synchronization.

We used correlogram based frequency spectrum estimation method to find horizontal frequency from electromagnetic emanation signals.

First we applied local averaging to one dimensional emanation signal to find highest energy part in the signal. We need the highest energy part to be sure that we did not use frame gap or full black lines to calculate correlogram, since frame gaps or full black lines are not suitable for horizontal frequency calculations. Let x be the emanation signal and M is the filter length. The averaged signal x_w can be obtained as,

$$x_w(n) = \frac{1}{M}\sum_{k=1}^{M} x(n-k) \qquad (1)$$

We calculated correlogram of only the highest energy part and we found that the maximum peak in the correlogram is horizontal synchronization frequency. Since frame signals consist of periodic lines, we can see this periodicity in the correlogram. We also know that horizontal synchronization frequency is varying around 30 and 115 kHz [12]. So we can find local maximum of the correlogram for this range. The correlogram x_c is given as,

$$x_c(k) = \sum_{j=1}^{N} x_w(j) w_N^{(j-1)(k-1)} \qquad (2)$$

where

$$w_N = e^{(-2\pi i)/N}$$

Figure 4 shows correlogram of an electromagnetic emanation signal which is taken from 3m away from an LCD. Because of the noise, there is not a strong DC component in the correlogram. If correlogram were calculated from RGB cable data, there would be a strong DC component.

After finding horizontal synchronization frequency, we need to find how many samples create one line. Dividing duration of one line by duration of one sample gives number of samples in one line.

$$n_{line} = \frac{durat\ ion\ of\ one\ line}{duration\ \ of\ one\ sample} = \frac{{}^{1}/_{f_H}}{{}^{1}/_{f_s}} = \frac{f_s}{f_H} \qquad (3)$$

In equation (3), n_{line} is the number of samples in one line, f_H is the horizontal synchronization frequency and f_s is the sampling frequency of digitizer. We do not get integer value for number of samples in one line since horizontal frequency is not a sub multiple of the sampling frequency. If we round it up or down, we get right or left tilted images as shown in Figure 3. To overcome this challenge we have to calculate exact number of samples of all the lines.

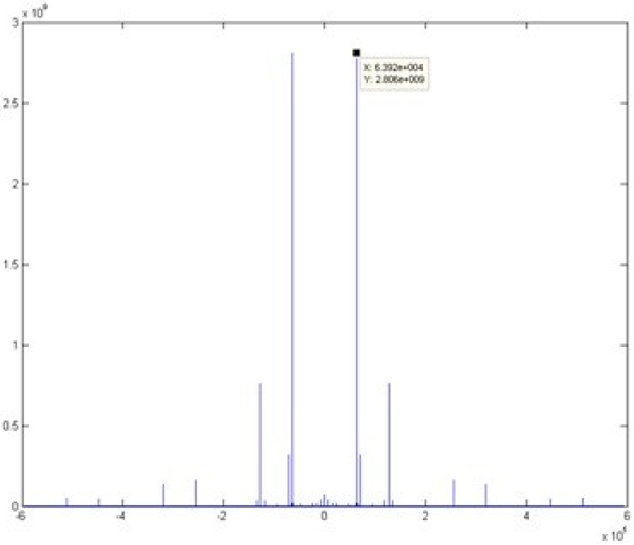


Fig. 4. Correlogram of the eavesdropped signal.

In one frame, there are scan lines and gaps between these lines. So if we calculate convolution of one frame with itself, we get periodic triangle wave as shown in Figure 5.

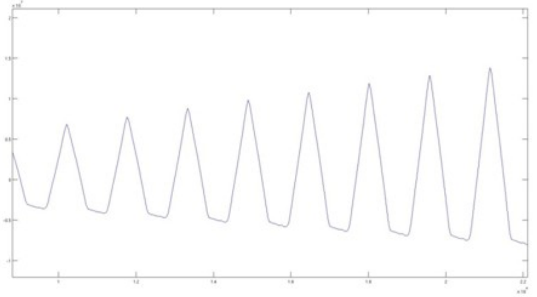


Fig. 5. Convolution of eavesdropped signal.

The distances between sequential peaks in this convolution give actual number of samples of that line. We found that the numbers of samples for sequential lines are not equal. The lengths of the lines are varying between n_{line}-1 and n_{line}+1. When we realign the electromagnetic eavesdropped one dimensional signal by considering this actual number of samples, we can reconstruct stable images as in Figure 7 and Figure 8.

The reconstruction steps can be summarized as,

1. Apply local averaging to the emanation signal.
2. Calculate the correlogram of the averaged signal.

3. Find maximum peak of the correlogram as horizontal synchronization frequency.
4. Using equation (3) and horizontal synchronization frequency, find the average number of samples in one line.
5. Using the distance between sequential peaks in the convolution, find the exact number of samples in one line.
6. Realign the 1D emanation signal to obtain the 2D image.
7. Repeat steps 1-6 to obtain several images.
8. To increase the SNR, average all the images and obtain the final image.

4. EXPERIMENTAL RESULTS

It is very important to show that the TEMPEST is a big threat for information security. In this work, we did experiments with two different setups. In the first setup we want to show a realistic eavesdropping scenario with our portable and low-cost hardware. The target LCD is 17” Philips 170C monitor which is connected to a laptop. The LCD shows Microsoft Office Word with black color text in a white background. The text fonts decrease from 72 points to 12 points at each line. In this experimental setup, eavesdropper and the target LCD are placed in different buildings which are 46 meter away from each other as shown in Figure 6.

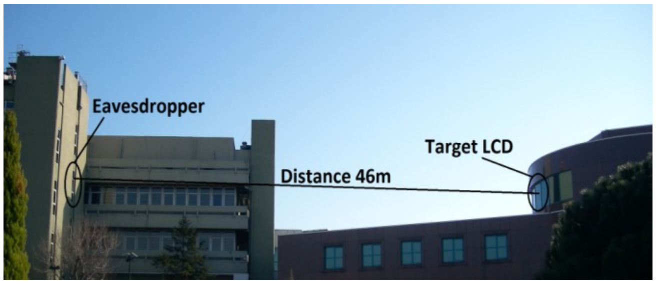


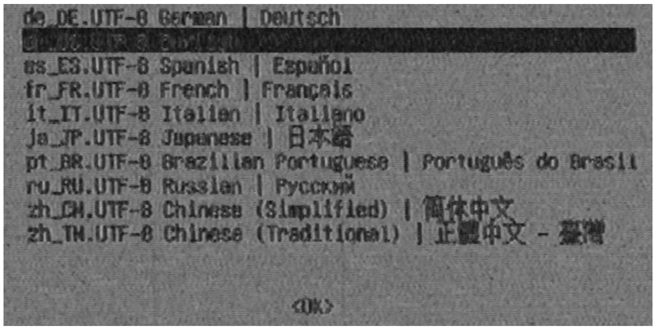
Fig. 6. Eavesdropping setup.

In the second setup we want to show that how the reconstructed image quality changes when eavesdropper is 3 meter away from the target in an office environment. The second target is an Acer laptop. The text size is 9 points in this setup. Table 1 summarizes these two setups.

	Target Type	Distance	Content
Setup 1	LCD	46 m	Text in MS WORD
Setup 2	Laptop	3 m	Text in Xterm

Table 1. Experimental setups.

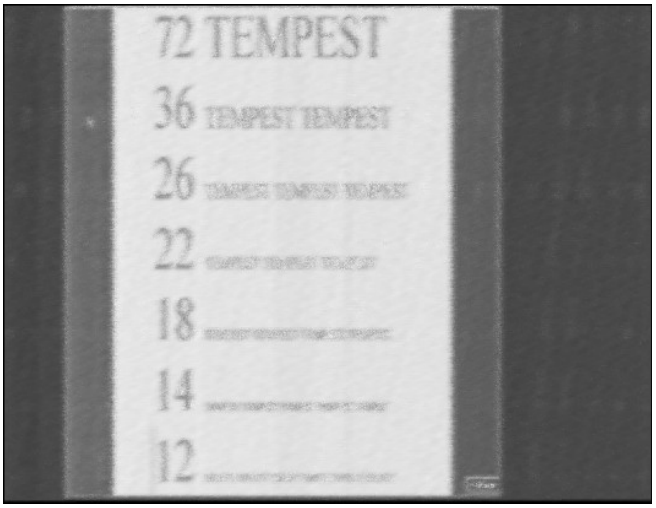
Even though we did not use any waveform generator for syncronization, we achieved to get stable image from 46 and 3 meters away as shown in the Figure 8 and Figure 7 respectively.



```
de_DE.UTF-8 German | Deutsch
[illegible]
es_ES.UTF-8 Spanish | Español
fr_FR.UTF-8 French | Français
it_IT.UTF-8 Italian | Italiano
ja_JP.UTF-8 Japanese | 日本語
pt_BR.UTF-8 Brazilian Portuguese | Português do Brasil
ru_RU.UTF-8 Russian | Русский
zh_CN.UTF-8 Chinese (Simplified) | 简体中文
zh_TW.UTF-8 Chinese (Traditional) | 正體中文 - 臺灣

<OK>
```

Fig. 7. Reconstructed image from 3 meters away.



72 TEMPEST

36 TEMPEST TEMPEST

26 TEMPEST TEMPEST TEMPEST

22 [illegible]

18 [illegible]

14 [illegible]

12 [illegible]

Fig. 8. Reconstructed image from 46 meters away.

5. CONCLUSIONS

This work shows that TEMPEST is a big threat for information security. An eavesdropper can easily reconstruct a target display with portable and low-cost hardware like our proposed configuration. With these experiments, we also show that even 46 meters away from target, an eavesdropper can steal display images and easily read text which is bigger than 26 points font. If eavesdropper can be close enough to the target, the eavesdropper can read bigger fonts than 9 points.

In addition, we showed an algorithm to find horizontal synchronization frequency and reconstruction of stable display image without using any external waveform generator.

In the future, we will try to enhance reconstructed image quality. Therefore it is very important to obtain a stable initial image for image processing algorithms. The proposed synchronization and reconstruction algorithms achieve stable reconstructed image from electromagnetic emanations of display units.

6. REFERENCES

[1] W. Van Eck, “Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?”, *Computers & Security, No.4,* August 1985.

[2] W. Van Eck, J. Neessen, P. Rijsdijk, “On the Characteristics of the Electromagnetic Field Generated by the Video Display Units”, *Proceedings of IEEE International Symposium on Electromagnetic Compatibility,* 1991.

[3] Markus G. Kuhn, “Eavesdropping attacks on computer displays”, *Information Security Summit*, Prague, 24-25 May 2006.

[4] Markus G. Kuhn, “Electromagnetic Eavesdropping Risk of Flat Panel Displays”, *4th Workshop on Privacy Enhancing Technologies,* Toronto, Canada, 26-28 May, 2004.

[5] Tanaka Hidema, Takizawa Osamu, Yamamura Akihiro, “A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave”, *Journal of the National Institute of Information and Communications Technology Vol.52*, 2005.

[6] Markus G. Kuhn, “Security Limits for Compromising Emanations”, *Workshop on Cryptographic Hardware and Embedded Systems,* 29 August–1 September 2005.

[7] Hidenori Sekiguchi, S.Seto, “Proposal of an Information Signal Measurement Method in Display Image Contained in Electromagnetic Noise Emanated from a Personal Computer”, *IMTC 2007 IEEE Instrumentation and Measurement Technology Conference*, Vancouver Island, British Columbia, Canada, 12-15 May 2008.

[8] Hidema Tanaka, “Information Leakage Via Electromagnetic Emanations and Evaluation of Tempest Countermeasures”, *Information Systems Security Lectures Notes in Computer Science*, 2007, pp. 167-179.

[9] Markus G. Kuhn, Ross J. Anderson, “Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations”, *Information Hiding, Second International Workshop*, Portland, Oregon, USA, April 15-17, 1998.

[10] Hidenori Sekiguchi, “Information leakage of input operation on touch screen monitors caused by electromagnetic noise”, *IEEE International Symposium on Electromagnetic Compatibility*, Fort Lauderdale, Florida, USA, 25-30 July 2010.

[11] Markus G. Kuhn, “Compromising emanations: eavesdropping risks of computer displays”, *Technical Report, University of Cambridge, Computer Laboratory*, December 2003.

[12] VESA Monitor Timing Specifications, Version 1.0, Video Electronics Standards Association, September 1998.