# Video display eavesdropping – RF

Tai Yeow Kwang, Roland

5th November, 2009

## 1. Introduction

Computer security is not restricted to back door attacks where hackers could potentially intrude and steal confidential information from computer terminals. The best means to mitigate is by using cryptography-based mechanisms, but however the other form of attack that involved TEMPEST[1], where electronics equipment can emit unintentional electromagnetic signals which would allow eavesdroppers to detect and reconstruct sensitive information at stand-off distance. These unintentional leakage signals could leaves any electronics equipment in the form of radiated and conducted means.

## 2. History of TEMPEST

TEMPEST exploitation has started way back during World War I, where the German army managed to tap and eavesdropped the allied battlefield phone lines from the earth return loop current. The risk associated for this kind of attacks was available in the open domain from year 1966 onwards, but vanish in the late 1970s due to the highly sensitive emission security topics. It was not until 1985 , when van Eck demonstrated that the threats can be exploited with simple and cheap off the

1**TEMPEST** is a codename referring to investigations and studies of compromising emanations (CE). Compromising emanations are defined as unintentional intelligence-bearing signals which, if intercepted and analyzed, may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.
Quoted from http://en.wikipedia.org/wiki/TEMPEST

shelves equipment to detect and reconstruct video information from a CRT monitor. His moves has spurs researchers in the late 1990s to spin off investigations of several others electronics devices like the keyboard, smart card transactions and even LCD panel display. The signal that we are dealing with is very small where the civilian EMI test limits are usually not applicable. The TEMPEST limits are usually several factor down from a typical EMI standards aand these classified standards (for example the U.S. NACSIM 5100A that specify the test requirements and emission limits for Tempest protected equipment, and its NATO equivalent AMSG 720B) are still not openly available.

## 3. Phenomenon of TEMPEST

The phenomenon behind compromising emanation emissions lies within the circuits where transistors tends to operate at much faster transitions, which cause electromagnetic emissions to radiated from VHF up to the UHF range (300-3000 MHz). The intended signals often rides onto these emission frequencies where it is re-propagated via an efficient radiator. The PCB traces on board would effectively become a radiating antenna if the frequency wavelength as compared to the length of the traces are small. Some of the intended signals may also coupled onto power and signal line cables due to cross-talk.

## 4. Systems to detect Compromised Video signals

A TEMPEST test engineer will usually conduct equipment qualification test in a shielded enclosure to ensure what is being measured is coming from the particular equipment under test. Figure 1 shows a typical 10m semi-anechoic shielded chamber[2] to block out any external environmental noise for emission characterisation.

Figure 1: 10m semi-anechoic chamber for radiated emission measurement

2 extracted from http://www3.ntu.edu.sg/eee/emerl/images/semianechoicchamber.jpg

However, it is of great challenge to detect the unintentional radiated weak signals across the tight radio transmission in an open environment. The environmental noise over the main signal (S/N) has to be at least 10dB [3] (cited by Markus Kuhn on his thesis titled "Compromising Emanation:eavesdropping risk of computer display" page 97-98) for a fruitful reconstruction of the display screen. In some instances periodic averaging of the intended signal is needed to remove the external random noise.

Figure 2 shows the basic receiver system set-up for detecting video compromising emanation RF signals. To improve S/N , the RF front end will have a bandpass filter and LNA to extract the main signal and amplify it respectively. A lossless filter and a narrow band LNA (Low Noise Amplifier) with low noise figure of less than one is preferred. The intermediate frequency (IF) output from the receiver is fed to a reconstruction device where external supplied synchronisation pulses are combined with the video information to reconstructed video information.

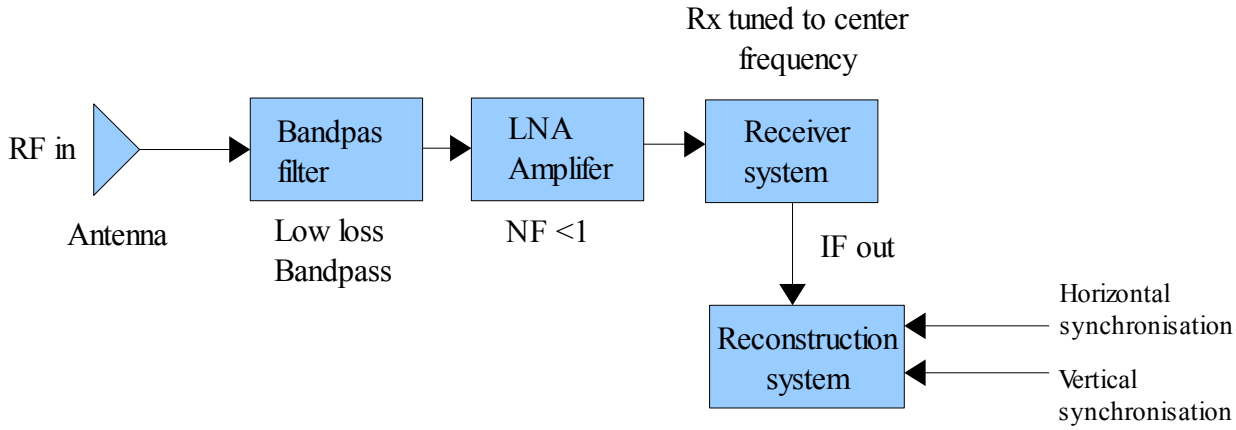



Figure 2: Typical Detection System

Van Eck and Markus Kuhn have demonstrated that it is feasible to reconstruct video display information on a CRT monitor with their respective receiver system [1,3] which is shown in Figure 2.1. Their systems comprises of an TV aerial antenna, a TV receiver and synchronisation oscillators. The basic concept in detecting the compromised video information is much the same, where Markus uses more complex, higher gain antenna and sensitive receiver to improve image quality and detection range. Low cost FPGA board are seen implemented to perform signal conversion from analogue to digital and complex image processing as well as to generate the required horizontal and vertical sync frequencies to stabilise the reconstructed video image.

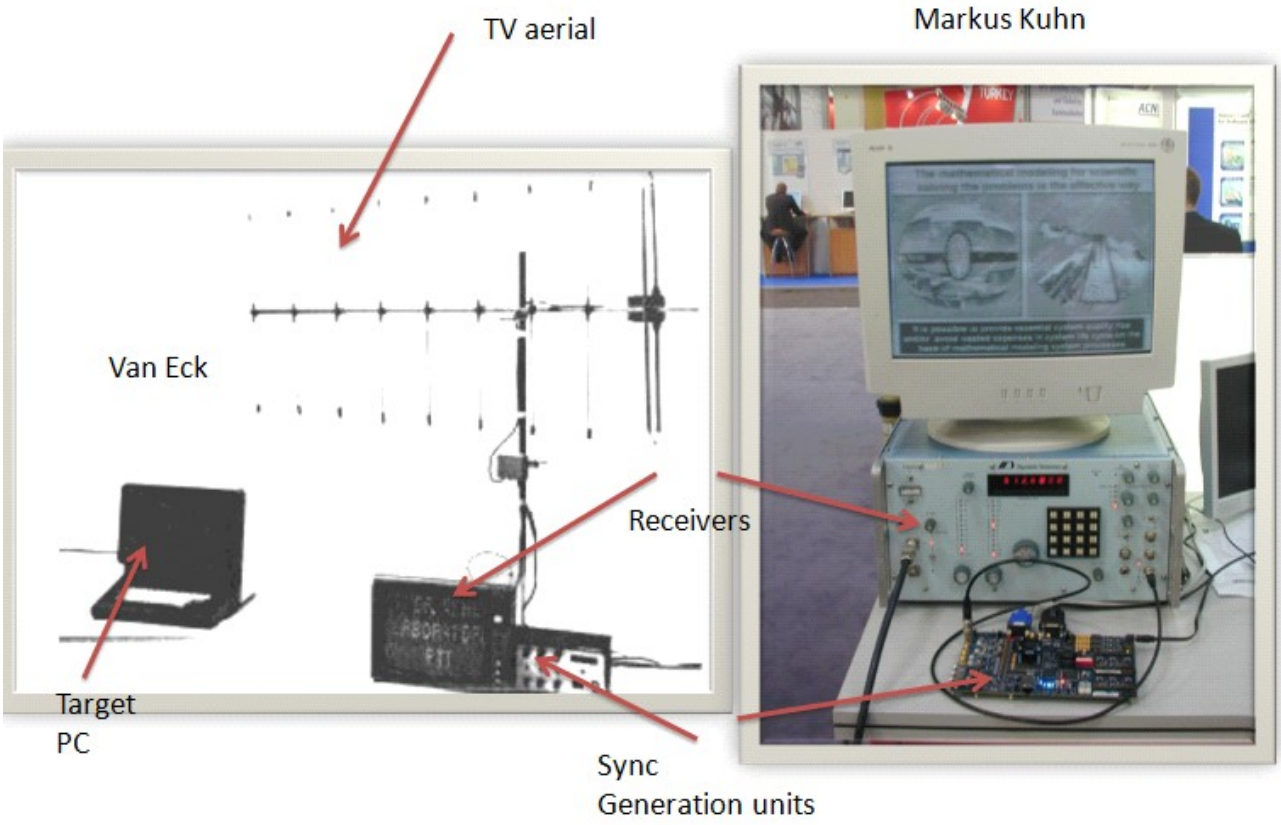



Figure 2.1 Detection system built by the Van Eck and Dr Markus Kuhn

## 5. The video timing information

In order to detect and reconstruct radiated RF video information, we need to understand the video timing signal. In a typical CRT monitor, the pixels are scanned across the screen from left to right (usually starts at the top left hand corner of the screen) all the way to the bottom of the screen at the lower bottom right of the screen to form a frame. It then repeat itself again (a periodic signal) from where it was started. The time where the pixel fly back to the original starting time is called the vertical synchronisation pulse (about 16msec or 60Hz). The time taken for the pixel to scan one line is called the horizontal synchronisation pulse (about 20usec or 48kHz depending on the resolution setting). Figure 3 show the the video timing waveforms[3] where it was scanned at three different line locations of the display. The video timing waveform will fluctuate and is dependent on the display screen. A high amplitude level represents a WHITE and a low amplitude level represents a BLACK. In the first timing waveform, an incremental staircase steps were observed because the image BLACK colour was gradually changed to WHITE. Every change in the step voltage will change the display tone. A BLACK image is represented by 0V and WHITE image at 0.7V. In between these voltages

3 extracted from http://www.sony.ca/ip/min_illumination/video/images/img_05.jpg

the image displayed shades of grey.

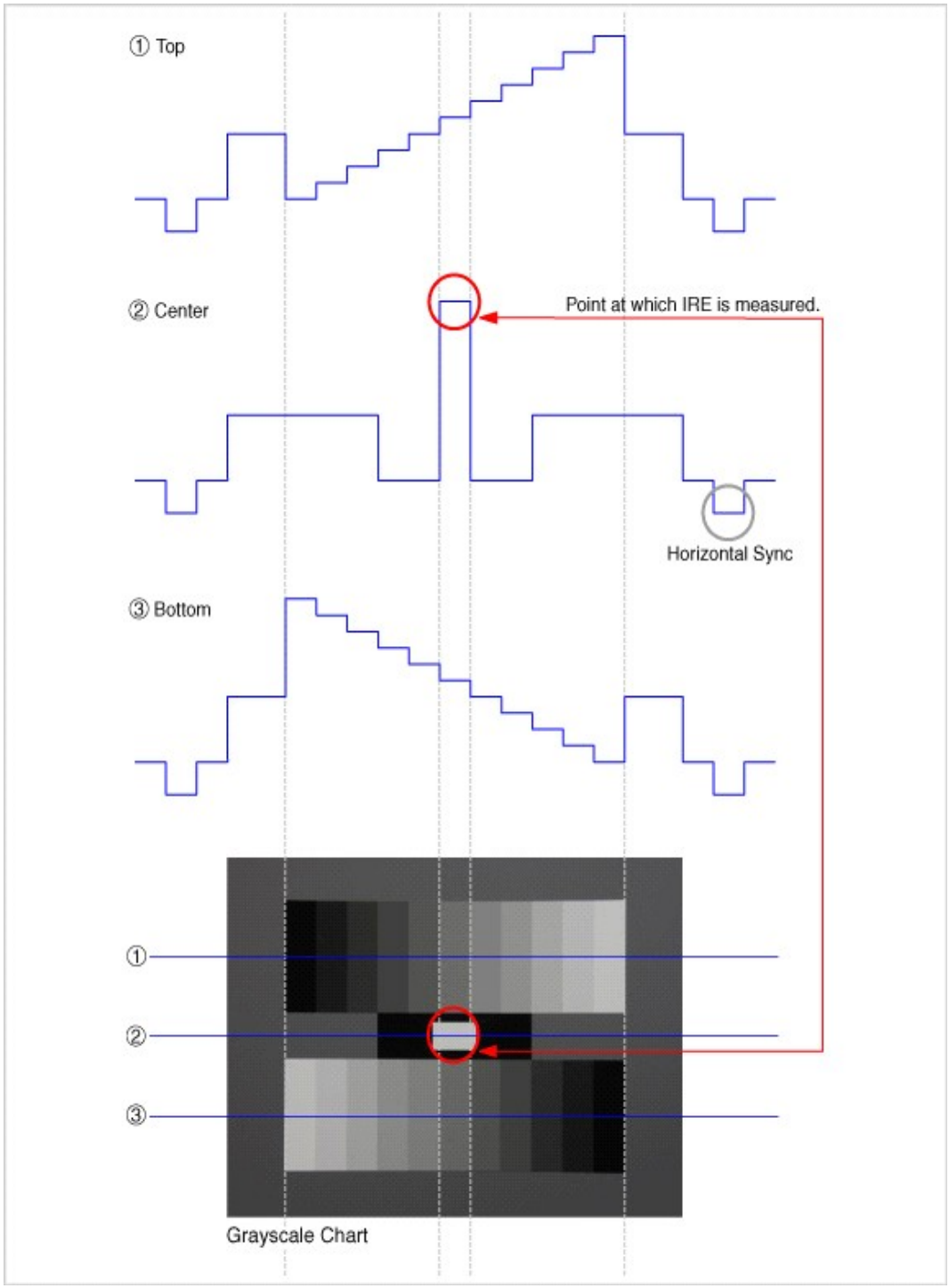
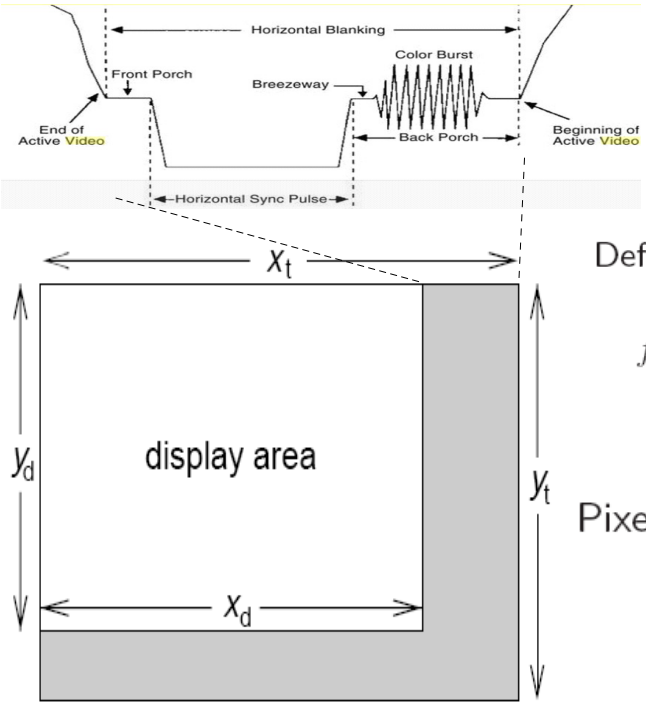



Figure 3: Video timing information

## 5.1 Pixel clock and deflection frequencies

There is a total of $x_t$ and $y_t$ amount of horizontal and vertical pixels as shown in Figure 4. To display an image on the screen, the required number of pixels needed is lesser, as it has to take into account on the time to bring the pixel back to the starting point. The pixel clock frequency $f_p$ is the time taken for each pixel to scan from one point to to another. The deflection frequency and the pixel refresh time can be calculated based on equation (1) and (2) respectively[4].




Deflection frequencies:

$$f_h = \frac{f_p}{x_t}, \quad f_v = \frac{f_p}{x_t \cdot y_t} \quad ...(1)$$

Pixel refresh time:

$$t = \frac{x}{f_p} + \frac{y}{f_h} + \frac{n}{f_v} \quad ...(2)$$

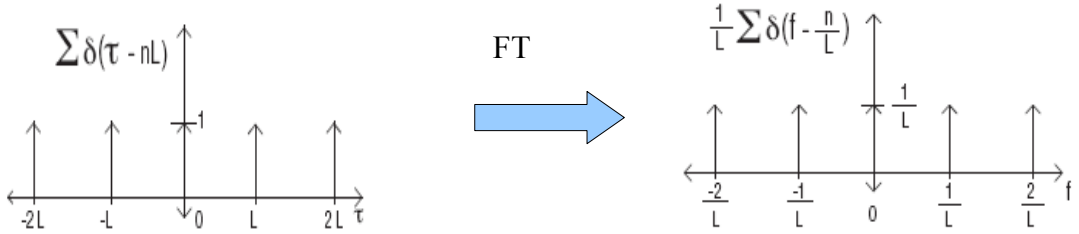
Figure 4: Pixel clock and deflection frequencies

Where: $x_t$: Horizontal pixels.
$y_t$: Vertical pixels.
$f_h$: horizontal synchronisation frequencies.
$f_v$: vertical synchronisation frequencies.
$n$: number of frames.

4 The above Figures and equations were obtained from (1) presentation slides on : Electromagnetic eavesdropping on computers, Markus Kuhn and (2) Textbook:How Video Works, Marcus Weise and Diana Weynand

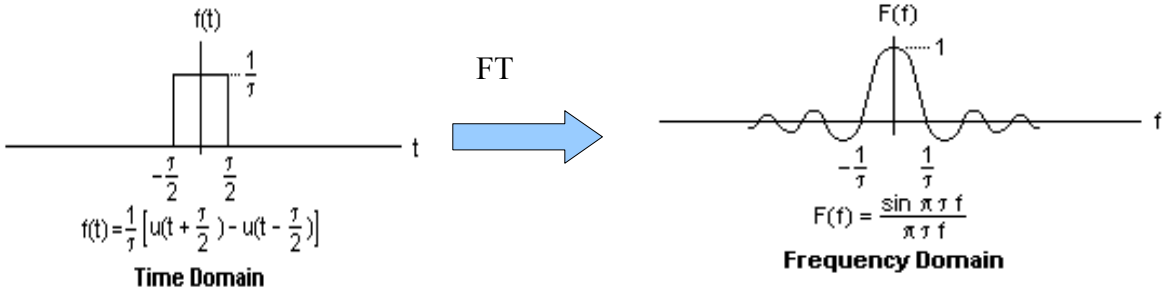
## 6. Analogue video spectra

The analysis of the video timing information can be further elaborated in the frequency domain spectra. The discrete time sampling of the video information can be represented by a series of equidistant Dirac function as shown in Figure 5. The Fourier transform of the Dirac function is another Dirac with reciprocal of the pixel time. The pixel information can be approximately represented as a rectangular pulse where the Fourier transform of it will give sinc function of amplitude 1 as shown in Figure 6. A multiplication of both the Dirac impulse series and the rectangular pulse video information is equivalent to convolution of these signals in the frequency domain. Figure 7 showed that the result of such convolution will have the video information appearing across the spectrum at every interval multiples of the pixel clock frequency.




Where L = $t_p$

Figure 5: Fourier transform of equidistant Dirac function




where $\tau = t_p$

Figure 6: Fourier transform of a rectangular pulse

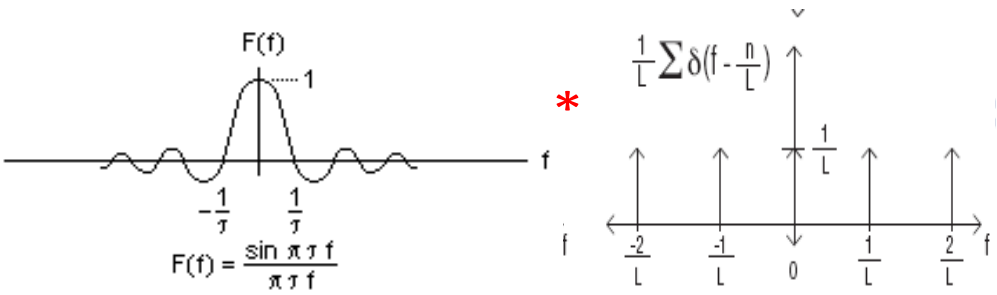



Figure 7: Sinc function of a rectangular pixel convolved with the series impulse signal

## 7. Recovering the video information

The recovering of video information would mean that the receiver has to tune to one of these multiple pixel clock frequencies that carries the video content. Thus the pixel clock is crucial for detection of the video image. The important information to note that for CRT monitor the pixel clock information will change according to the display resolution settings. The detailed information for different display resolution can be found from the VESA display standard. However for a LCD monitor, the pixel clock frequency is usually fixed based on native resolution (total number of pixels) of the display.

When attempting to reconstruct the video image, the RF signal received by the receiver does not contain both the horizontal and vertical synchronisation frequencies. These information is usually supplied separately with an external source generator to stabilise the video image. The video RF signal detected is AM demodulated to give the baseband video.

## 8. Passive attack via Conducted and Radiated RF

The amount of leakage compromising emanation signals depends largely on the design and layout of the electronics within the PCB. Electronics designer are forced to design their electronic systems to comply with strict EMC limits (FCC or CISPIR standards) to ensure that the emission levels are controlled to prevent interference to another systems.

Despite this strict restriction, there is some degree of unintended weak compromising video information that will leak through conducted and radiated means. Every PCB traces carry current which produces electromagnetic field properties that radiates the signal at its resonant frequeny based on the length. This mean that if the intended compromised signal that has wavelength much

longer (which is low frequency) than the signal trace path/s, the RF signal could not effectively radiates out. However, as the frequency gets higher with the wavelength (about a quater) approaches the length of the trace/s, it will effectively radiate the signal.

Conducted leakage is mainly cause by cross-coupling due to the tight design contraint within the PCB. Signals cross coupled between traces will occur if the design layout within the PCB is not done properly. If the intended signal of interest gets cross coupled onto the external cables that are connected to the equipment, it will carry the signal across the lines. Thus it is important that the signal cable that exit a particular equipment be properly treated, and ensuring that they are grounded to prevent them from acting as stray antenna.

The detection frequencies of these compromising emanation signals could range from VHF band all the way to the UHF region. The attack is non-intrusive and the operator has no mean to know that someone is spying information out of his/her computer terminal. Figure 8 and 9 show the typical attack senarios where a user is processing classifed information in a room.

If we assume that F1 being one of the compromising frequencies emitted out from his/her laptop, this frequency will be intercepted by an adverary residing in another room by means of raidated and conducted leakage emissions. For conducted leakage, the detection principle relies on the cable infrastruce where common lines like signal and power are shared on a common connection point. A current magnetic loop sensor[5] is used to extract out the information from the line.

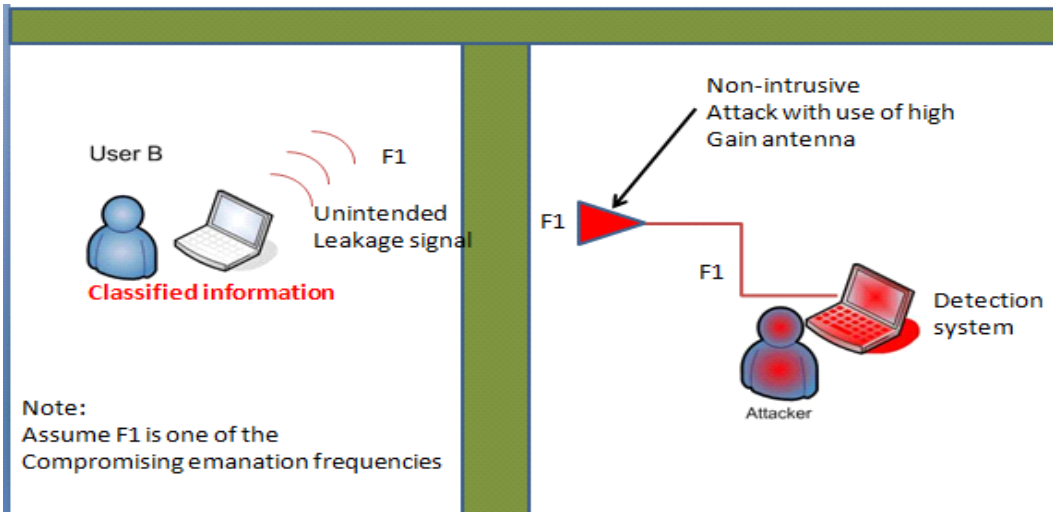



Figure 8: Radiated TEMPEST scenario

5 http://www.ahsystems.com/catalog/data/info/ocBCP-510.gif

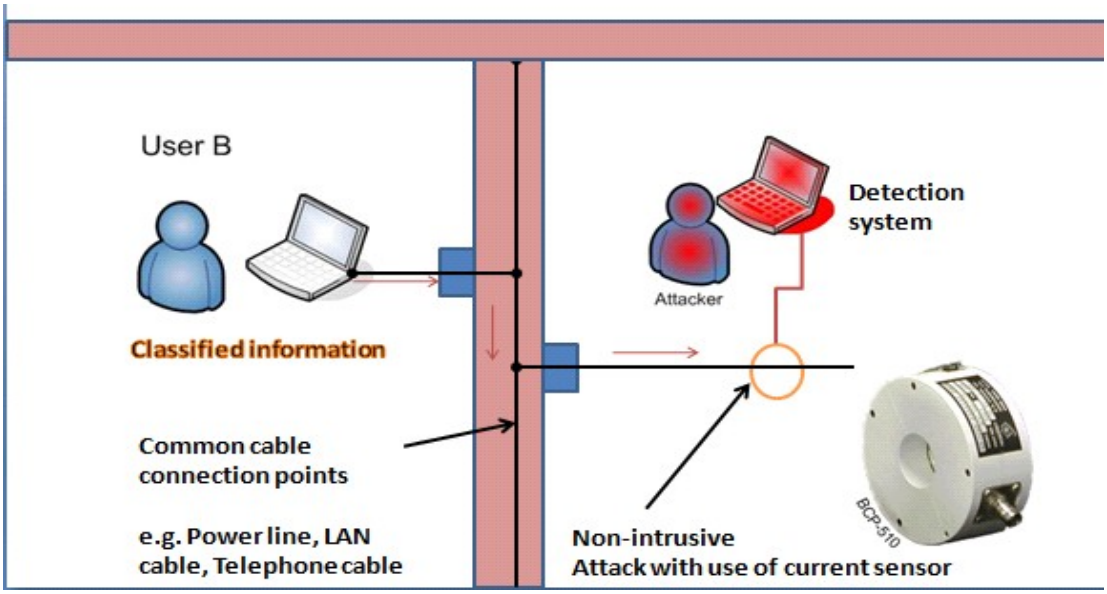
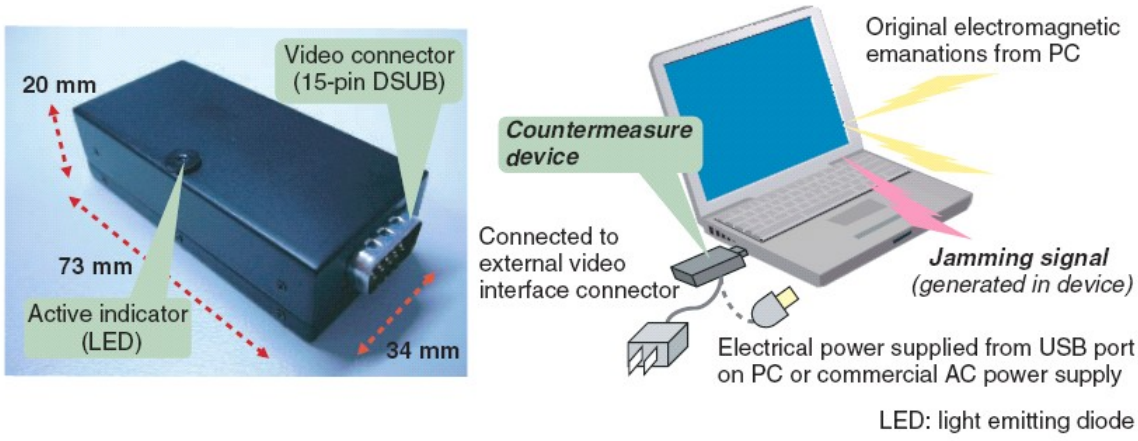


Figure 9: Conducted TEMPEST scenario

## 9. TEMPEST countermeasures

There are several countermeasures which ranged from both hardware and software to safeguard the classified information that is being processed. Figure 10 show the various protection aspects against TEMPST attack which I have found from the internet. The hardware protection aspects could be building a Faraday cage with 6 sided metallic walls to prevent RF emissions from leaving the define area. This could be constructed on the entire building or just a standalone room by implementing architectural shielding. The other form is shielding the individual PC if the amount needed to process classified information is low. The last aspect in protecting RF leakage information is through signal masking, This is done by generating a wide spectrum of RF emissions of sufficient amplitude level that could masked out the unintended compromising signals.

(a) (b) (c )




(d)

Figure 10: (a)Architectural shielding with six sided wall coated with metallic film[6]. (b) conductive fabric tent[7]. (c ) shielded PC and (d) Signal masking device generate emission levels higher than unintended compromising emanation signals[8].

The other form of protection is through the used of software. They comprises of soft-fonts and message hiding through dithering. There are two types of soft-font protection discussed in [3,4]. Soft-fonts work on the principle of low pass filtering to remove the high frequency components since the RF eavesdropper will only get to receive the upper portion of the baseband information spectrum. Figure 11 shows an example of using soft-font techniques which I have extracted out from [4] for illustration.

6 http://www.euro-emc.co.uk/images/architectural_medical%20_shielding_4_small.jpg
7 http://www.ramayes.com/_images/SFI/Shielded_Tent_PVC_1.jpg
8 "Countermeasures to prevent Eavesdropping on Unintentional Emanations from Personal Computers", Yasunao Suzuki,Masao Masugi, Kimihiro Taijma and Hiroshi Yamane.

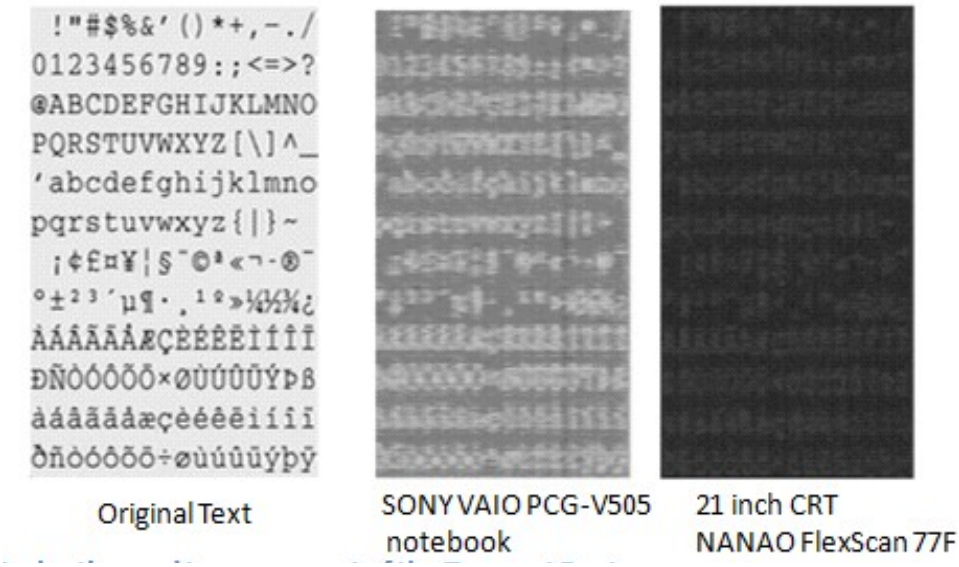
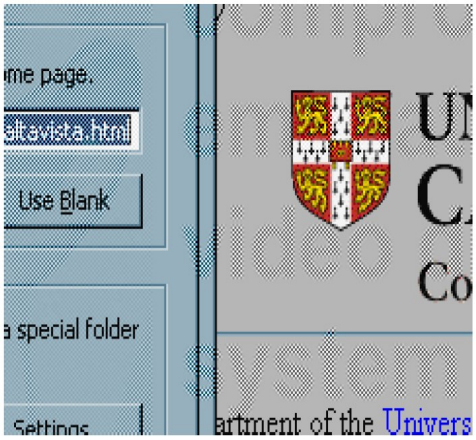
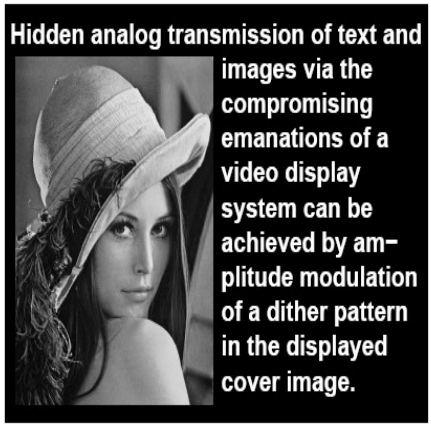



Figure 11: Soft-fonts using low pass Gaussian filter to cut off the high frequency component

Figure 12 show another type of software protection extracted from [3] page 57 onwards) called message hiding, where it covertly embed an image inside the display screen content. What the users see is only the display screen content and not the embedded image. It make use on the principle that the human eye is less sensitive for contrast as spatial frequency increases and the video compromised RF emission is usually carried in the higher frequency band. The difference in spectral sensitivity between the users and the eavesdropper would mean that one can intentionally transmit an image that contains high frequency component (e.g. a black and white image) and display a constant colour as the display screen content. The eavesdropper will only see the black and white image when detecting the video RF compromised signals.




(a)




(b)

Figure 12: Message hiding by transmitting the picture information that contain the highest frequency components which the eavesdropper will detect more easily. (a) A zoom in view to show that an image is embedded inside the display screen content. (b) The embedded image that is covertly transmitted.

## 10. Summary

In this essay, I have briefly summarise the phenomenon of RF video eavesdropping based on the reference papers stated in section 11. I have also mentioned the critical components that are needed for successful interception and reconstruction of compromised video emanations signal. With the awareness of such threats, the various countermeasures protection are mentioned which involved both hardware and software. There are many other interest TEMPEST areas to look into not limited to video detection but also on keyboard detection, hard-disk data reading and even deciphering encrypted information in clear format due to the two nature of information leakage via through conduction and radiated means.

## 11. References

[1] van Eck:Electromagnetic radiation from video display units: an eavesdropping risk? Computers & Security 4(269–286) .

[2] Kuhn, Anderson: Soft Tempest: hidden data transmission using electromagnetic emanations. IHW 1998,LNCS 1525 .

[3] Kuhn: Compromising emanations: eavesdropping risks of computer displays, Chapter 3: Analog video displays.UCAM-CL-TR-577.

[4] Hidema Tanaka, Osamu Takizawa, and Akihiro Yamamura: Evaluation and Improvement of the Tempest Fonts. NIICT.