TDDC03 Project, Spring 2005

Literature study on emanations from displays

Daniel Larsson and Sarita Namuduri

Supervisor: Viiveke Fåk

IDA
University of Linköping

Linköping
2005-05-07

Abstract

It is a well-known fact that eavesdroppers can reconstruct the display content from the radio frequency emanations. We discuss the emanations from liquid crystal display (LCD) and cathode ray tube (CRT) display screens and some techniques for how eavesdropping is done on digital displays.

Contents

Introduction

Background

When modern electrical devices operate they generate electromagnetic fields. Digital computers, radio equipment, typewriters, and so on generate massive amounts of electromagnetic radiations, which if properly intercepted and processed will allow certain amounts of information to be reconstructed. Basically anything with a microchip, diode, or transistor, gives off these fields.

The US military has conducted research on these emanations since the1950s or 1960s [3, 4]. They are the ones responsible for the now widely known code word TEMPEST, which many people use when they talk about compromising-emanations. Most of their work on TEMPEST radiation remains classified including their test standards.

In 1985 the Dutchman Wim van Eck published his report "Electromagnetic Radiations from Video Display Units: An Eavsdropping Risk?" [1]. In the report van Eck shows that it is possible to intercept and interpret electromagnetic radiation from video display units (VDU), using only a slightly modified TV-set, an antenna and an amplifier. He also claims that the extension to the TV needed for this experiment can be designed and constructed by any electronic amateur within a few days.

Motivation

It is twenty years since van Eck published his report about compromising emanations from VDUs, and display technologies have undergone big changes in performance. CRTs have increased their pixel frequency and video bandwidth enormously, and they are currently being replaced by new types of flat panel displays.

In this report we will try to answer the questions: Is this kind of attack still possible? If so, how big are the risks for the average user? How big are the risks for a defense supplying company?

Scope

Besides the pure TEMPEST attack there are some other related attacks.

In his PhD thesis Markus G. Kuhn [2] introduces a new optical eavesdropping attack. In this kind of attack the eavesdropper picks up emanated light from the monitor. This can be feasible even if the attacker has no direct line of sight to the targeted monitor.

In a report from 1998 Markus G. Kuhn and Ross Anderson [3] discusses software-controlled emanations, this kind of intentional emanations is known as TEAPOT emanations. TEAPOT is like TEMPEST a US military code word. Simplified one can say that a TEAPOT attack is an active TEMPEST attack, active in the sense that the attacker creates malicious code that forces the targeted system to emanate in a certain way or more then usual. They also suggest that TEAPOT emanations can be used as copy- write protection.

In this report we focus on compromising-emanations from monitors and we have limited us to the radio frequencies.

Method

This is a literature study, which means that we have searched and read relevant reports and articles about compromising-emanations. We have not conducted experiments on our own so all conclusions are based on facts from these reports.

Cathode Ray Tube Displays (CRT)

CRT in theory

To draw something on a CRT display the electron canon at the back of the monitor bombards the phosphor in the front of the monitor with electrons. Depending on the intensity of the electrons the phosphor illuminates in different ways.

CRTs are like TVs raster-scan devices which means that the electron beam starts at the top left corner and proceeds with constant velocity, systematically row by row from the left to the right and down to the bottom right corner of the screen, figure 1.

To make the electron canon fire electrons the video signal feed by the computer has to be amplified by a factor of about 100, this makes it possible to distinguish these radiations from other radiated signals from the monitor. The produced radiation is quite similar to a television broadcast, which makes it easy to feed them into a TV-set.

But the signal lacks one very important part and that is the synchronization part of the video signal, the synchronization signal. The synchronization signal is the signal that controls the beam movements over the screen.

A TV or monitor needs a synchronization signal to draw its screen content correctly, without it the picture would be a mess. So in order to make a TV or monitor display the intercepted signal correctly the eavesdropper needs to produce a synchronization signal. According to van Eck one of the easiest and cheapest ways to solve that problem for a TV-set is to use two manually adjustable oscillators. [1, 2]

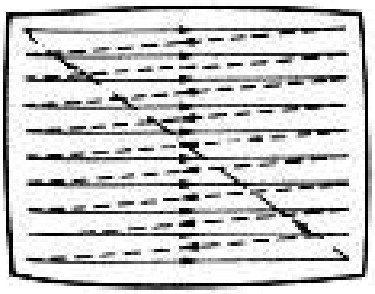


Figure 1. CRT screen build up.
Source: Wim van Eck [1].

CRT in practice

As mentioned above big changes in CRT performance has been made but the basic technology in CRTs remains the same, so in theory it should still be possible to mount a TEMPEST attack on modern CRT units.

In his PhD thesis [2] from 2003 Kuhn presents experimental results, which show the possibility to mount these kinds of attacks on modern CRTs. However the experiments also shows that this in not an easy task to perform. There are a number of things that needs to be considered in order to succeed with an attack.

First we have the equipment, Kuhn uses a special kind of receiver that fulfills the confidential NSA TEMPEST standards. The receiver differs from more commonly available radio receivers in a number of ways, see Kuhn's report for details.

Secondly in theory it is possible to connect an ordinary CRT monitor directly into the receiver and get the intercepted image on that monitor. But in order to succeed with this the eavesdropper has to supply his monitor with a very close approximation of the targeted monitors synchronization signal. To show how close approximation one would need Kuhn gives an example where the approximated synch signal differs with only one part per million (ppm) from the real signal. With the synch signals one ppm apart and with a screen refresh rate of 85Hz, the electron beams would be as much as 85 pixels of-synch in one second. This means that the picture would roll over the screen at a speed of 85 pixels per second.

This is not the end of it. The targeted frequency keeps fluctuating due to temperature changes in the circuitry, this is also true for the eavesdroppers equipment. As a result the frequencies can drift apart up to several ppm's within a few minutes. So an eavesdropper will constantly have to adjust his settings in order to get the picture right.

However the fact that the synch signal needs a very close approximation can be used by the eavesdropper to single-out one target in a group of many. Because it is highly unlikely that two targets have almost the same frequency on their sync signals (less then 1 ppm apart), even if it is the same equipment with the same settings.

When performing the experiments, Kuhn uses a different approach than plugging a monitor directly into the receiver. He records the signal with a digital storage oscilloscope that is capable

of averaging the data acquired. Then he converts the data into raster graphics files on a PC and after that the image can be viewed on a monitor.

This approach makes it possible to perform some data processing on the captured signal before it is feed to the monitor, but the eavesdropper still needs to produce a very close approximation of the synch signal.

When Kuhn conducted his experiment his oscilloscope was not able to do the averaging fast enough. Because of this he got a delay for about 10 minutes making it impossible to stay synchronized with the target. So he had to cheat and plug the real synch signal into his equipment, this would not be possible for a real eavesdropper. However he estimates that an eavesdropper with better equipment could cut the delay time down to about 3 seconds. And with a delay time of 3 seconds it is very likely that the attack would succeed.

Liquid crystal display (LCD)

LCD in theory

LCDs have no deflection coils like the CRT, which makes them – compared to CRTs – "low radiation" devices in the frequencies below 400 kHz, where field strengths are limited by a Swedish ergonomic standard [2]. LCDs can operate with low voltages and unlike CRTs do not amplify the video signal by a factor of about 100 to drive a control grid that modulates an electron beam. Experiments conducted by Markus G. Kuhn reveal that some types of flat-panel display do prove a realistic eavesdropping risk.

LCD in practice

Experiments have been conducted practically by Markus G.Kuhn to analyze the radio emanations from a laptop LCD and from a desktop LCD. In an experiment the Radio emanations from the LCD displays were connected to its graphical card with a Digital Visual Interface (DVI) cable. The video cable used to connect the display panel with the graphics controller turned was the main source of the leaking signal. A very deep understanding of the digital transmission is required for to sop the eavesdropping. When Kuhn deeply investigated he found that the digital video link was the main source of leakage .

The case study of a laptop display by Kuhn shows that a Toshiba satellite Pro 440CDX laptop with a Linux booting screen in an 800*600@75Hz video mode which emits an amplitude-demodulated and raster signal is shown in the figure2. The antenna was located at a 3m distance in the same room as the target device. A very fast scan through different frequencies in the 50-1000 MHz range showed that setting the AM receiver to a center frequency of 350 MHz and an intermediate-frequency band-width of 50MHz gave one of the clearest signals. The image shown is the average of 16 recorded frames, in order to reduce noise. The frames were recorded with a sampling frequency of 250 MHz. A coaxial cable was used instead of an antenna, to scan then there were no emissions came from the display module but the source of emission was the interconnected cable between the LCD module and the main board. A closer look at the laptop revealed that a digital video link was the origin of the emanations.

A number of observations distinguish the signal seen Fig. 3 from those typical
for CRTs:

– The low-frequency components of the video signal are not attenuated. Horizontal bright lines appear in the reconstructed signal as horizontal lines and not just as a pair of switching pulses at the end points, as would be the case with CRTs.

– Font glyphs appear to have lost half of their horizontal resolution, but are
still readable.

– In the 800×600@75Hz video mode used, the clearest signal can be obtained at a center frequency of about 350 MHz with 50 MHz bandwidth, but weaker signals are also present at higher and lower frequencies, in particular after every step of 25 MHz.[6]

- The mapping between displayed colours and the amplitude of the signal received for a pixel turned out to be highly non-monotonic. A simply gray-bar image resulted in a complex barcode like display, as if the generated signal amplitude were somehow related to the binary representation of the pixel value.

In the next experiment, the laptop with the same configurations and antenna are located about 10 m apart in different office rooms, separated by two other offices and three 105 mm thick plaster-board walls.

In this experiment 12 consecutive frames were acquired with a sampling rate of 50 MHz in one single recording of 160 ms (eight million samples)[7] .The exact frame rate which is necessary for correctly aligned averaging was determined with the necessary precision of at least seven digits from the exact distance of the first and last of the recorded frames. It was determined with an algorithm that calculated starting from a crude estimate of the frame rate the cross-correlation of these two frames, and then corrected the estimate based on the position of the largest peak found there (Fig. 2). (The process is not fully automatic, as due to other video signals in the vicinity, echo, and multiple peaks, it can sometimes be necessary to manually choose an alternative peak.)[7]

The signal which is received of amplitude about 12 µV corresponds with this antenna to field strength of 39 dBµV/m. There is a drop by 18 dB compared to the 57 dBµV/m in the previous 3 m line-of-sight measurement and can in part be attributed to the 10 dB free-space loss to be expected when tripling the distance between emitter and antenna.

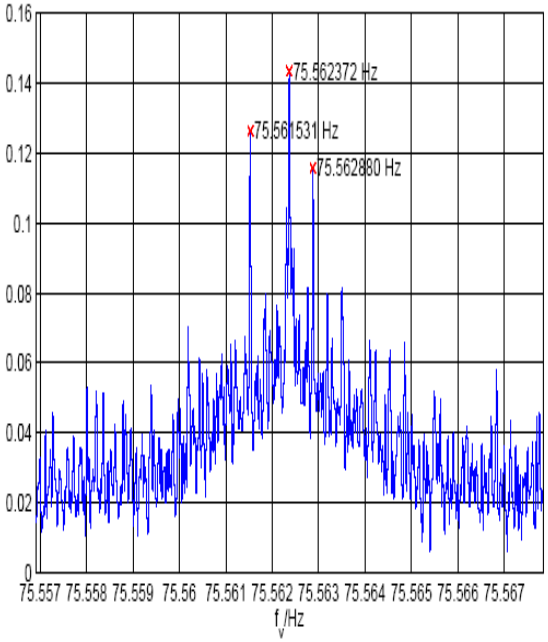
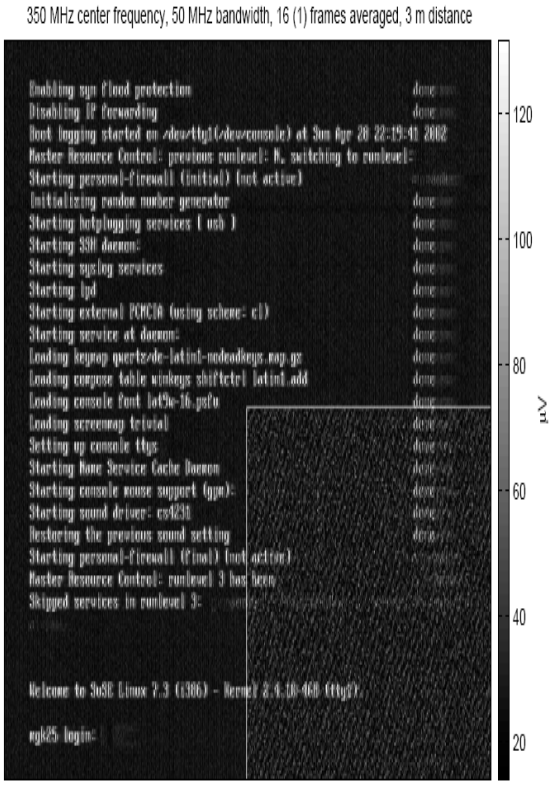


Figure 2: Determination of the frame rate fv for the multi-frame signal recorded



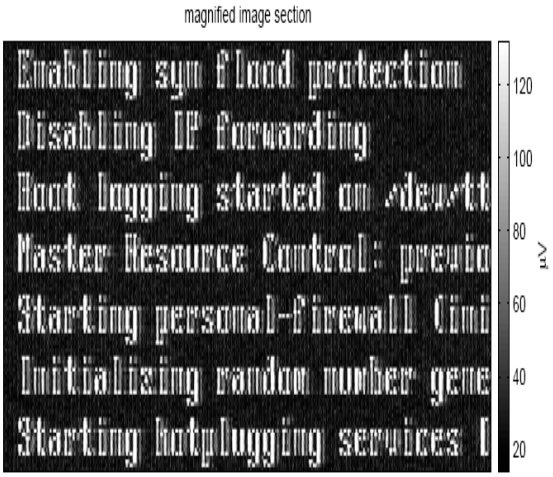


Figure 3: Eavesdrooped Linux boot screen visible on the LCD of a Toshiba 440CDX laptop

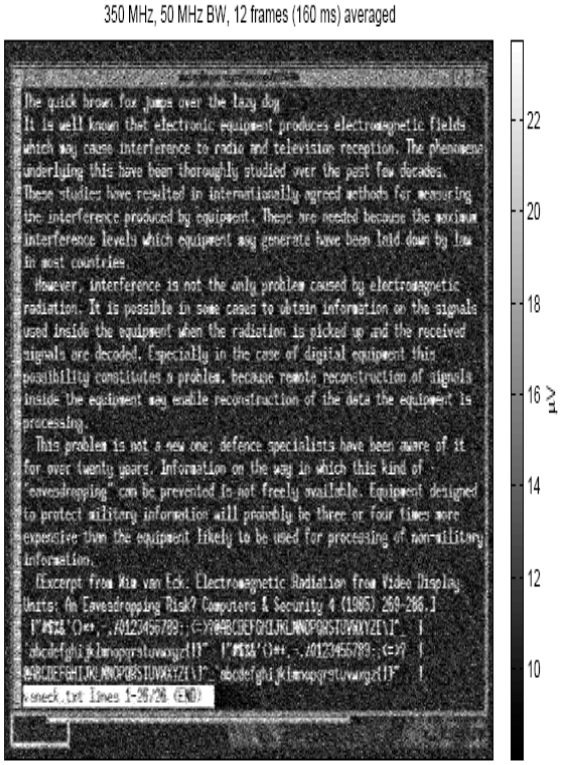


Figure4: Text message received from a 440CDX laptop at 10m distance through two intermediate walls

Discussion

Although twenty years have passed since van Eck conducted his experiments on VDUs and despite all the technological changes that has been made to modern display units, Kuhn has shown that it is still possible to use the emanations from both CRTs and LCDs to reconstruct the screen content of such device.

However the difficulty to perform this kind of attack seems to have grown quite a bit. In van Eck's report it is said that the equipment for making the sync signal can be designed and constructed by any electronic amateur within a few days. When Kuhn performs his somewhat equivalent experiment on modern CRTs he seems to have a lot more trouble making the synch signal. Further he has to cheat because of equipment limitations, even though he got some special equipment.

When searching for reports and articles concerning this topic one realizes that it is very hard to find good, reliable and up to date sources. Kuhn's report is actually the only almost up to date report containing experimental data that we have found. However the military seems to conduct a lot of research on this topic, unfortunately most of their work remains classified. To make things worse the open research seems to always come in behind due to lack of recourses and equipment [2]. This fact makes it hard to do a correct risk analysis, but it also makes us believe that this kind of attack works outside the laboratory.

The eavesdropping risk in less in LCD displays than the CRT displays when connected through a digital interface to the video controller. Since a very deep understanding of the encoding algorithms is required for encoding data from the emitted signal.

Our conclusion is that it is possible to mount a TEMPEST attack but that it is difficult and very time consuming. An attacker would need a lot of technical knowledge, a lot of time and some special equipment that is probably expensive. This limits the field of potential attackers to those with very strong motivation and a lot of resources.

Because of this the TEMPEST threat to an average user is neglectable, especially since most average users are easy targets for more conventional attacks. For a defense supplying company the threat level looks different, they have something of value that a potential attacker with a lot of recourses might want and they are hopefully protected against most conventional attacks. Defense supplying companies along with military installations, diplomatic buildings and other high security facilities should consider TEMPEST radiations in their security policies and maybe install some TEMPEST shielding.

References

[1] van Eck, Wim. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Computers & Security, Vol. 4 (1985).
[2] G. Kuhn, Markus. Compromising emanations: eavesdropping risks of computer displays (2003).
[3] Kuhn, Markus G. & Anderson, Ross. Soft TEMPEST: Hidden Data Transmission Using Electromagnetic Emanations (1998).
[4] Joel McNamara: The Complete, Unofficial TEMPEST Information Page. Internet Web page, URL < http://www.eskimo.com/%7Ejoelm/TEMPEST.html>
[5] G.Kuhn, Markus: Electromagnetic Eavesdropping Risks of Flat-Panel Displays

Other sources and suggested literature

Anderson, Ross. Security Engineering. John Wiley & Sons (2001)
Electromagnetic Eavesdropping Machines for Christmas? Computers & Security, Vol. 7 (1988). A follow-up article to the van Eck paper available at < http://jya.com/bits.htm>
Ward, Grady. TEMPEST in a teapot (1993). An article about TEMPEST protection, available at <http://www.eff.org/Privacy/Security/TEMPEST_monitoring.article>

The picture on the front page is taken from Joel McNamara's page "The Complete, Unofficial TEMPEST Information Page" and is the logo for the US Army Blacktail Canyon TEMPEST Test Facility.