Soft Tempest: Hidden Data Transmission Using Electro-magnetic Emanations

Markus G. Kuhn and Ross J. Anderson

November 24, 1999

1 Background

It has been known to people that computer generate electro-magnetic radiation which not only interferes with radio reception but also leaks information about the data processed. The paper is talking about a technique about Tempest: Technique of Electro-Mechanical Protection against Emission and Spurious Transmission for both the attackers and protectors.

In 1960, Dr. Wright successfully detect a plain-text from a faint secondary signal from the French cipher equipment.

Now, sensitive government systems employ expensive metallic shielding of individual devices, rooms and sometimes entire buildings. Even inside the shielded environment, the “red” and “black” separation principle is followed. “red” is for equipment carrying confidential data and “black” equipment handles or transmit unclassified data. Equipment with both “red” and “black” such as cipher machine requires particularly thorough testing. U.S. standard NACSIM 5100A specifies the test requirements for the Tempest protected equipment. But not available to the public.

Using correlation averaging over millions of samples, even weak trace of the processed information can be indentified, this method especially useful for the attackers when they can capture the periodic signal and the signal structure is known or when they are snooping the CPU is running a known algorithm.

The author found that even shielded RS-232 cable can leak very weak information. And due to the fund reason or commercial reason, Tempest is not a hot research field so far. He wants to propose a cheap way to in protect the computer information from Tempest threat.

2 Short Audio Transmissions

Suppose we have written a computer virus which has been successfully sent into a system from which we want to steal information, say a bank system. We
don’t want to get a hardcopy of the information and we don’t want to break the firewall to get information from the Internet. While we want to let the monitor to broadcast some audio signal which is encoded from the information and record these signals and decode them.

- represent an audio signal \( s(t) = A \cdot \cos(2\pi f_c t) \cdot [1 + m \cdot \cos(2\pi f_l t)] \). Here \( f_c \) is the carrier frequency and \( f_l \) is the audio signal frequency.

- The timing of a digital video display system is characterized by the pixel clock frequency \( f_p \). Horizontal and vertical deflection frequencies is:

\[
\begin{align*}
  f_h &= \frac{f_p}{x} \\
  f_v &= \frac{f_p}{y}
\end{align*}
\]

Here \( x \) and \( y \) are the total width and height of the pixel field that we would get if the electron beam needed no time to jump back to the start of the line of frame. However the displayed image on the screen is only \( x_d \) pixels wide and \( y_d \) pixels high as the time allocated to the remaining \( x_1 y_1 - x_d y_d \) virtual pixel is used to bring the electron beam back to the other side of the screen.

At any time \( t \), the electron beam will be in the center of the pixel \((x,y)\) at time \( t = \frac{x}{f_p} + \frac{y}{f_h} + \frac{y}{f_v}\).

We set the pixel \((x,y)\) to an 8-bit grey-scale value of

\[
\left[ \frac{255}{2} + s(t) + R \right]
\]

With different \( s(t) \) we can have different pattern on the screen and get different signal.

Different frequency of signal can be used to represent 0 and 1, when we record these signals we can use any synchronizations and decoding methods described in any digital communications textbook.

In order to get better quality, the carrier frequency \( f_c \) shall avoid the nearby broadcast stations. And because the broadcast pattern is visible, the attack shall be done in the night. Actually, when the computer monitor is off but the PC is not off, a noticeable signal still can be sent by the VDU cable.

3 The Video Display Eavesdropping Receiver

The author is using ESL model 400 Tempest monitor receiver which is a test and demonstration tool to work with the video display technology. The horizontal deflection can be select from 10 - 20kHz with millihertz resolution and vertical deflection frequency can be selected in the range 40.0 - 99.9 Hz with 0.1 Hz resolution.

It can be freely tuned in four bands in the range 20 - 860 MHz and has a sensitivity ranging from 60 \( \mu \)V at 20 MHz to 5 \( \mu \)V at 860 MHz.
4 Hiding Information in Dither Patterns

The author observed that the above mentioned Tempest receiver can display the high frequency part of the video signal. The strongest useful spectral components are at frequency close to the pixel frequency and its harmonics.

The modern video display technology let the eavesdropper can receive roughly the derivative of the video signal. On modern high-resolution monitors, users cannot easily distinguish between a medium grey and a checked half-toning pattern of black and white pixels. For the eavesdropper, the high-frequency black/white dither pattern creates the strongest possible signal while a constant color results in the weakest.

The author used difference in the spectral sensitivity of the user and the eavesdropper to present different information to them.

The Tempest amplitudes for three primary colors red, green, and blue are different. it might be possible for an eavesdropper to reconstruct some colors. By increasing the amplitude of the dithering, the attacker can embed some information in the original pattern and because the eavesdropper is only sentive to some amplitude, the information can be sent.

The color value is liner to the voltage supplied to the monitor. But the luminosity L is not linear to that. Approximated as $L = const V^\gamma$ which is known as gamma correction. The overall luminosity of a two-color dither pattern depends on the arithmetic mean of the luminosity L rather than the voltage V. To remain inconspicuous for the viewer, amplitude variations in the dither pattern must be performed such that the average luminosity is preserved.

5 A New Protective Measure: Tempest Fonts

Since only the high frequency components of the video signal can be picked up by the eavesdropper and the author found that this frequency peak reaches $\frac{f_p}{2}$. Also he found that only the horizontal frequency of the signal determines what is received. If we look at the Fourier transform of the horizontal sequence of pixels, only information present as frequency $f$ in the range $0.7f_p/2 \leq f \leq f_p/2$ can be received. Then we remove the top 30 percent of the Fourier transform of the signal can stop the attacking.

A short random wait routine inside the key-matrix scan loop can stop the correlation averaging on what we have typed and also can be applied for the disk driver reading.

6 Conclusions

Compromising emanations continue to be a fascinating field of research, although they are mostly unexplored in the research literature.
Tempest is not only about RF engineering, but it can mount new attack on software, new defense are going to be invented.

Here the author propose a simple and cheap way to stop the attacking, but proof need to be proposed too.