Notes on Tempest

Nolan Chandler

Soft Tempest[1]

Introduction

Some history:

- Britain joining EEC, recovered plaintext from France's cipher machine
- Red/black separation: red sensitive must be shielded from outward facing black
- van Eck: first to reconstruct image using low-cost home built equipment

Unwanted leakage comes from many sources, most unintentional, but attackers can also cause some as well (resonant freq of keyboard cable to sniff keypresses)

Not a lot has been written recently; RF equipment is big $, little published data on modern hardware's emissions

Shortwave audio xmissions

Carrier freq f_c, tone freq f_t

$$s(t) = A * \cos(2\pi f_c t) * [1 + m * \cos(2\pi f_t t)]$$

$$= A*\{\cos 2\pi f_c t + \frac{m}{2} * \cos[2\pi(f_c - f_t)t] + \frac{m}{2} * \cos[2\pi(f_c + f_t)t]\}$$

- f_p = *Pixel clock freq*, reciprocal of time electron beam travels from center of pixel to center of next
- $f_h = f_p/x_t$, *Horiz. deflection freq*
- $f_v = f_p/y_t$, *Vert. deflection freq*
- x_t, y_t = width/height of pixel field if no delay to move to new line
- x_d, y_d = actual width/height of displayed image

Beam is in the center of pixel (x, y) at time

$$t = \frac{x}{f_p} + \frac{y}{f_h} + \frac{n}{f_v}$$

Set (x, y) to $(\frac{255}{2} + s(t) + R)$ with $A = \frac{255}{4}$ and $m = 1$, $0 \leq R < 1$, uniform random

References

[1] M. G. Kuhn and R. J. Anderson, "Soft tempest: hidden data transmission using electromagnetic emanations."