Optical remote eavesdropping risks of CRT displays

Markus G. Kuhn

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group / TAMPER Lab

A new eavesdropping technique can be used to read cathode-ray tube (CRT) displays remotely. The light generated by a monitor flickers invisibly with high frequency as the electron beam targets pixel after pixel. These light fluctuations are proportional to the video signal blurred by the phosphor afterglow. From that, the displayed image can be reconstructed with digital signal processing techniques. The eavesdropper only needs to see monitor light reflected from a nearby wall or face, not the monitor itself.

CRT monitors are raster-scan devices. As in television receivers, an electron beam traverses the screen surface line by line, addressing one pixel at a time with a current proportional to the pixel brightness. In 1985, van Eck described how unwanted radio-frequency emissions generated by monitor electronics broadcast the video signal outside rooms. To avoid this information security risk, critical military applications use carefully shielded "Tempest" equipment. However, radio-frequency shielding alone does not eliminate all compromising emanations from CRTs.

The electron beam deposits energy into the screen phosphor, some of which is released within a millisecond as photons. Careful measurements of the pixel-afterglow decay for a typical PC monitor (Dell D1025HE) using a very fast and sensitive light sensor (photomultiplier) resulted in the phosphor impulse-response curves shown below. Convolving these with the video signal provides a good model for the high-frequency fluctuations of the light emitted by the CRT.

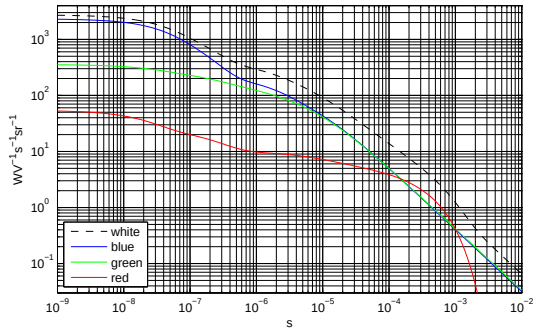
The afterglow drops significantly within a fraction of a microsecond after the electron beam has passed, especially for the blue phosphor. As a result, a flash of light illuminates the surroundings for each bright pixel. After reflection from nearby surfaces, such as the user's face or a wall, an eavesdropper could capture and record this signal through a window.

Shown below is a test image displayed in a demonstration experiment on a monitor in a dark room. After reflection from a nearby wall, this light reaches a photomultiplier. The resulting photo current was digitized (8 bits, 250 MHz) and averaged over 256 scans (3 s). Converted into a raster image, the signal is very blurred due to the afterglow. Using a closed-form model of the impulse response, an FFT-based deconvolution deblurrs this image well enough to recover a readable signal.

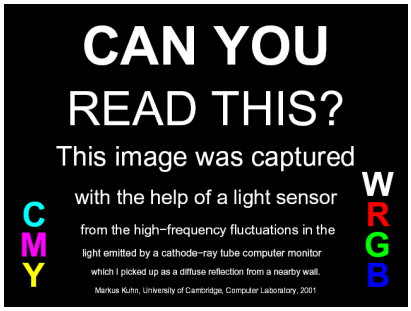
This new eavesdropping technique poses a risk in relatively dark environments (e.g., late twilight conditions) for reception distances in the 10–50 m range. Broadband shot noise from background light is a limiting factor. A determined eavesdropper would use a telescope to increase sensor sensitivity and select a wall area with good signal-to-noise ratio. Wavelength filtering can be used to differentiate colors and attenuate background light. Possible protection measures are good illumination or RF-shielded flat-panel displays, because these update a row of pixels at a time.

M.G. Kuhn: *Optical time-domain eavesdropping risks of CRT displays.* Proceedings 2002 IEEE Symposium on Security and Privacy, Berkeley, California, 12–15 May 2002, pp. 3–18.
`http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf`

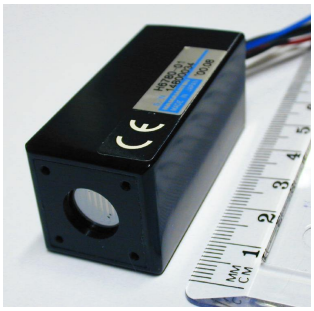
typical phosphor impulse response

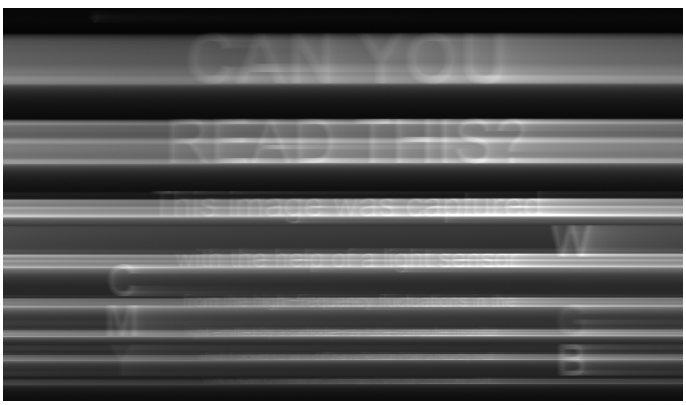


test image on targeted monitor

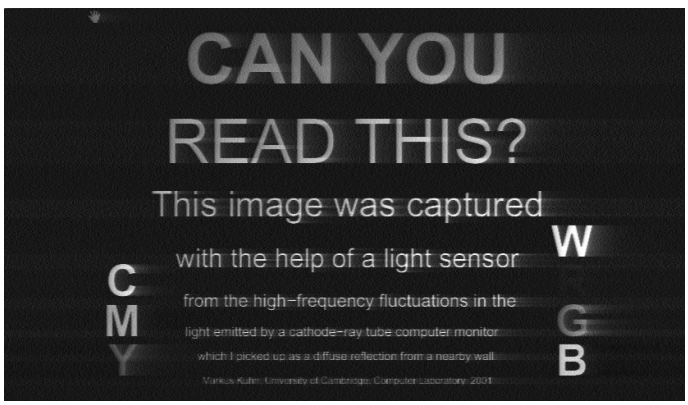


photomultiplier





rasterized raw photomultiplier current



eavesdropping result after deconvolution

2002-08-23