The rôle of hardware security

Protection of confidential information becomes easier:

→ availability of strong crypto primitives
→ CPU power (eliminates crypto performance penalty)
→ communication/storage cryptography now basic OS service
→ renaissance of mandatory access control

Professions depending on unauthorized information access such as

→ law enforcement / intelligence community
→ criminals
→ copyright license monitoring
→ market research

are increasingly interested in new/unorthodox access techniques.
Early use of compromising emanations

The German army started in 1914 to use valve amplifiers for listening into ground return signals of distant British, French and Russian field telephones across front lines.
Military History of Side-Channel Attacks

→ 1915: WW1 ground-return current tapping of field telephones.

→ 1960: MI5/GCHQ find high-frequency plaintext crosstalk on encrypted telex cable of French embassy in London.

→ Since 1960s: Secret US government “TEMPEST” programme investigates electromagnetic eavesdropping on computer and communications equipment and defines “Compromising Emmanations Laboratory Test Standards” (NACSIM 5100A, AMSG 720B, etc. still classified today).

→ Military and diplomatic computer and communication facilities in NATO countries are today protected by
  
  • “red/black separation”
  • shielding of devices, rooms, or entire buildings.

US market for “TEMPEST” certified equipment in 1990: over one billion dollars annually.
Open Literature on Compromising Emanations

→ 1985: Wim van Eck demonstrates eavesdropping on video displays with a modified TV set in BBC’s “Tomorrow’s World”.

→ 1990: Peter Smulders investigates electromagnetic eavesdropping on RS-232 cables.


→ 1998: We demonstrate steganographic forms of compromising video emanations.

→ 1999: Paul Kocher et al. demonstrate reconstruction of DES keys from power supply fluctuations in smartcard microcontrollers.
R1250 Wideband Tempest Receiver
Wideband Tempest Measurement Receivers

→ Can be tuned continuously from 100 Hz to 1 GHz.

→ Offers 21 bandwidths from 50 Hz to 200 MHz (1-2-5 steps).
  For comparison:
  
  ● AM radio: 2–10 kHz
  ● FM radio: 200 kHz
  ● TV set: 6 MHz

→ Especially robust antenna input (for listening on power lines).

→ Gain adjustable by a factor of $10^9$.

→ Automatic gain control circuit can be deactivated.

→ Demodulators: AM linear, AM logarithmic, FM, BFO.

→ Export controlled products, $\approx$ 30–100 k£.
Intermediate frequency bandwidth

R–1250 30–MHz IF filter characteristic

- 20 MHz
- 10 MHz
- 5 MHz
- 2 MHz
- 1 MHz

MHz

mV

0 1 2 3 4 5 6 7 8

10 15 20 25 30 35 40 45 50
Receiving impulse signals

IF impulse response

AM impulse responses

\[
\text{impulse width} = \frac{1}{\text{bandwidth}}
\]
Cross-correlation detection of weak binary signals in noise

\[ b(t) = (r \ast h)(t) + n(t) = \int_{0}^{\infty} r(t - t') h(t) \, dt + n(t) \]
Cross-correlation preconditioning alternatives for digital signals

(a)

(b)

(c)

(d)

(e)
Video Timing

The electron beam position on a raster-scan CRT is predictable:

Pixel frequency: $f_p$

Deflection frequencies:

$$f_h = \frac{f_p}{x_t}, \quad f_v = \frac{f_p}{x_t \cdot y_t}$$

Pixel refresh time:

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

The 43 VESA standard modes specify $f_p$ with a tolerance of $\pm 0.5\%$.

ModeLine "1280x1024@85" 157.5 1280 1344 1504 1728 1024 1025 1028 1072

Image mostly stable if relative error of $f_h$ below $\approx 10^{-7}$. 
AM audio broadcast from CRT displays

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

300 and 1200 Hz tones at \( f_c = 1.0 \) MHz:

Play your MP3 music at home via CRT emanations in your AM radio:

http://www.erikyyyy.de/tempest/
Real-world VGA card pixel shapes

Video Graphics Adapter Pixel Shapes

- Matrox Millennium II (157.5 MHz)
- ATI 3D Rage Pro (157.5 MHz)
- Toshiba 440CDX (49.5 MHz)
Real-world VGA card frequency spectrum

Video Graphics Adapter Signal Spectra (100 kHz bandwidth)

- Matrox Millennium II (157.5 MHz)
- ATI 3D Rage Pro (157.5 MHz)
- Toshiba 440CDX (49.5 MHz)
Analog video signal spectra

Fourier transform

\[ \mathcal{F}[h](f) = \int_{-\infty}^{\infty} h(t) e^{2\pi jft} \, dt \]

\[ \mathcal{F}^{-1}[H](t) = \int_{-\infty}^{\infty} H(f) e^{-2\pi jft} \, df \]

Convolution theorem

\[ (g \ast h)(x) = \int_{-\infty}^{\infty} g(y) h(x - y) \, dy \]

\[ \mathcal{F}[g \cdot h] = \mathcal{F}(g) \ast \mathcal{F}(h) \]

\[ \mathcal{F}[g \ast h] = \mathcal{F}(g) \cdot \mathcal{F}(h) \]
**Sampling theorem**

Sequence of pixel values $v_0, v_1, v_2, \ldots$ produced with pixel frequency $f_p$ can be represented as continuous waveform

$$v(t) = \sum_i v_i \cdot \frac{\sin \pi(f_p t - i)}{\pi(f_p t - i)}$$

which contains no spectral energy in frequencies $|f| > f_p/2$.

**Impulse sequences**

The Fourier transform of a pulse sequence is again a pulse sequence, but with reciprocal spacing:

$$\mathcal{F} \left[ \sum_{i=-\infty}^{\infty} \delta(t - ik) \right] (f) = \frac{1}{k} \sum_{i=-\infty}^{\infty} \delta \left( f - \frac{i}{k} \right).$$

$\implies$ These concepts together describe every video-signal spectrum.
Amplitude spectrum of an idealised pixel

Rectangular impulse

\[ F \left[ A \cdot \Pi \left( \frac{t}{T} \right) \right] (f) = AT \cdot \frac{\sin \pi T f}{\pi T f} \]
Eavesdropping of CRT Displays

CRT Monitor amplifies with $\gg 100$ MHz bandwidth the video signal to $\approx 100$ V and applies it to the screen grid in front of the cathode to modulate the e-beam current. All this acts together with the video cable as a (bad) transmission antenna.

Test text used in the following experiments:

The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG! 6x13
!"#$%'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~

It is well known that electronic equipment produces electromagnetic fields which may cause interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may generate have been laid down by law in most countries. (from: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?)
292 MHz center frequency, 20 MHz bandwidth, 256 (16) frames averaged, 3 m distance

It is well known that electronic equipment generates electromagnetic fields which may cause interference to radio and television reception, the phenomena underlying this have been thoroughly studied over the past few decades, these studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These methods have been established because the various interference levels which equipment may generate have been found to vary for different countries. (From: Electromagnetic Radiation from Video Display Units: Are There Any Risks?)

292 MHz center frequency, 10 MHz bandwidth, 256 (16) frames averaged, 3 m distance

It is well known that electronic equipment generates electromagnetic fields which may cause interference to radio and television reception, the phenomena underlying this have been thoroughly studied over the past few decades, these studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These methods have been established because the various interference levels which equipment may generate have been found to vary for different countries. (From: Electromagnetic Radiation from Video Display Units: Are There Any Risks?)
It is well known that electronic equipment produces electromagnetic fields which may cause interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may generate have been laid down by law in most countries. (From: Electromagnetic Radiation from Video Display Units: An Exceedingly Risk?)

The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG!
740 MHz center frequency, 200 MHz bandwidth, 256 (16) frames averaged, 3 m distance

700 MHz center frequency, 100 MHz bandwidth, 256 (16) frames averaged, 3 m distance
Background noise and reception frequency

- Test text video signal
- Random dots video signal
- Antenna signal
- 10, ..., 200 MHz BW reception

MHz

mV

$10^{-2}$  
$10^{-1}$  
$10^{0}$  
$10^{1}$
Bandwidth and inter-character interference

200 MHz BW

50 MHz BW
Automatic Radio Character Recognition

Example Results (256 frames averaged):

The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG! 6x13
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz{|}~

It is well known that electronic equipment produces electromagnetic fields which may cause interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may generate have been laid down by law in most countries. (from: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?)

With only 16 frames averaged:

The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG! 6x13
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_'abcdefghijklmnopqrstuvwxyz{|}~

It is well known that electronic equipment produces electromagnetic fields which may cause interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may generate have been laid down by law in most countries. (from: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?)
Steganographic transmission of images

The user sees on her screen:
The radio frequency eavesdropper receives instead:

445 MHz center frequency, 10 MHz bandwidth, 1024 frames averaged, 3 m distance

Hidden analog transmission of text and images via the compromising emulations of a video display system can be achieved by amplitude modulation of a dither pattern in the displayed cover image.
Amplitude modulation of dither patterns

Hidden analog transmission of text and images via the compromising emanations of a video display system can be achieved by amplitude modulation of a dither pattern in the displayed cover image.

Cover image $C_{x,y,c}$, embedded image $E_{x,y}$, all normalized to $[0,1]$. Then screen display is

$$S_{x,y,c} = \left(C_{x,y,c}^{\tilde{\gamma}} + \min\{\alpha E_{x,y}, C_{x,y,c}^{\tilde{\gamma}}, 1 - C_{x,y,c}^{\tilde{\gamma}}, \cdot d_{x,y}\right)^{1/\tilde{\gamma}}$$

with dither function $d_{x,y} = 2[(x + y) \mod 2] - 1 \in \{-1, 1\}$ and $0 < \alpha \leq 0.5$. 

30
Filtered fonts as a protection measure

The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
Filtered fonts on the CRT screen

The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
The quick brown fox jumps over the lazy dog
Received radio signal

740 MHz center freq., 200 MHz bandwidth, 256 frames averaged, 3 m distance

Bi-level antialiased unhinted

20% 30% 40% 50%

Background

The quick brown fox jumps over the lazy dog.
Removing the top $30\%$ of the spectrum reduces peak emissions by $12$ dB, without significantly affecting user comfort. This means the eavesdropper has to come $3\times$ closer, into a $10\times$ smaller area.
Spectral effects of font filtering

![Graph showing spectral effects of font filtering](image-url)
Eavesdropping on flat panel displays

350 MHz center frequency, 50 MHz bandwidth, 16 (1) frames averaged, 3 m distance
100 $\mu$V signal amplitude at receiver input (rms equiv.)

57 dB$\mu$V/m (50 MHz BW) field strength at 3 m distance

equivalent isotropic radiated power around 150 nW
Eavesdropping across two office rooms

350 MHz, 50 MHz BW, 12 frames (160 ms) averaged

The quick brown fox jumps over the lazy dog.

It is well known that electronic equipment produces electromagnetic fields which may cause interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may generate have been laid down by law in most countries.

However, interference is not the only problem caused by electromagnetic radiation. It is possible in some cases to obtain information on the signals used inside the equipment when the radiation is picked up and the received signals are decoded. Especially in the case of digital equipment, this possibility constitutes a problem because remote reconstruction of signals inside the equipment may enable reconstruction of the data the equipment is processing.

This problem is not a new one; defence specialists have been aware of it for over twenty years. Information on the way in which this kind of “eavesdropping” can be prevented is not freely available. Equipment designed to protect military information will probably be three or four times more expensive than the equipment likely to be used for processing of non-military information.


Target in room GE16 and antenna in room GE10 of the William Gates building, with two offices and three plasterboard walls (−2.7 dB each) in between.
Remote video timing estimation via cross-correlation
FPD-Link — a digital video interface

LCD module and video controller are connected in Toshiba 440CDX laptop by eight twisted pairs (each 30 cm), which feed the 18-bit RGB parallel signal through the hinges via low-voltage differential signaling (LVDS, EIA-644).

```
g2 r7 r6 r5 r4 r3 r2 g2 r7  
g3 b3 b2 g7 g6 g5 g4 g3 b3 b2  
b4 cx cy cz b7 b6 b5 b4 cx cy  
```

25 MHz cycle
## Minimal/maximal reception contrast

<table>
<thead>
<tr>
<th>line</th>
<th>description</th>
<th>foreground</th>
<th>background</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>RGB</td>
<td>signal</td>
<td>RGB</td>
</tr>
<tr>
<td>1</td>
<td>black on white</td>
<td>00 00 00</td>
<td>000000x 0x00000 xxx0000</td>
</tr>
<tr>
<td>2</td>
<td>maximum contrast</td>
<td>a8 50 a0</td>
<td>010101x 0x01010 xxx1010</td>
</tr>
<tr>
<td>3</td>
<td>maximum contrast (gray)</td>
<td>a8 a8 a8</td>
<td>010101x 1x10101 xxx1010</td>
</tr>
<tr>
<td>4</td>
<td>minimum contrast</td>
<td>78 00 00</td>
<td>001111x 0x00000 xxx0000</td>
</tr>
<tr>
<td>5</td>
<td>minimum contrast</td>
<td>78 60 00</td>
<td>001111x 0x01100 xxx0000</td>
</tr>
<tr>
<td>6</td>
<td>minimum contrast (phase shift)</td>
<td>70 70 00</td>
<td>001110x 0x01110 xxx0000</td>
</tr>
<tr>
<td>line</td>
<td>description</td>
<td>foreground</td>
<td>background</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------------</td>
<td>------------</td>
<td>------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RGB signal</td>
<td>RGB signal</td>
</tr>
<tr>
<td>7</td>
<td>text in most significant bit, rest random</td>
<td>r1rrrrrx</td>
<td>r0rrrrrx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rx1rrrrr</td>
<td>rx0rrrrr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>xxx1rrrr</td>
<td>xxx0rrrr</td>
</tr>
<tr>
<td>8</td>
<td>text in green two msb, rest random</td>
<td>rrrrrrrx</td>
<td>rrrrrrrx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rx11rrrr</td>
<td>rx00rrrr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>xxxrrrr</td>
<td>xxxrrrr</td>
</tr>
<tr>
<td>9</td>
<td>text in green msb, rest random</td>
<td>rrrrrrrx</td>
<td>rrrrrrrx</td>
</tr>
<tr>
<td></td>
<td></td>
<td>rx1rrrrr</td>
<td>rx0rrrrr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>xxxrrrr</td>
<td>xxxrrrr</td>
</tr>
</tbody>
</table>

The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
The quick brown fox jumps over THE LAZY DOG
Minimal/maximal reception contrast

350 MHz center frequency, 50 MHz bandwidth, 16 frames averaged, 3 m distance
Only random bit jamming effective

285 MHz center frequency, 50 MHz bandwidth, 16 frames averaged, 3 m distance
Data transmission demonstration

The text “Tempest in a Teapot” encoded in ASCII (padded with start- and end-of-text control characters) DSSS-modulated.
Result of convolving the received signal received with the random-bit sequence. Negative peaks mark the start of each byte and positive peaks are the 1 bits (MSB first).

Decoding result: Tempest in a Teapot
Transition Minimised Differential Signaling (TMDS)

New industry standard (DVI) for connecting desktop flat-panel displays.

- Differential Gbit/s signaling on three twisted pair channels.
- Coverts byte stream into sequence of 10-bit words.
- Attempts to reduce number of bit transitions.
- Balances the total number of 0 and 1 bits transmitted.
- Embeds sync signals using special words.

The DC balancing step adds encoding state and only 52 byte values lead to balanced words that are immune against the balancing algorithm.

High-contrast pair:

- 00001000, 00001000, ... → 0000111110, 0000111110, ...
- 10101010, 10101010, ... → 1100110010, 1100110010, ...
Maximum/minimum contrast for DVI

324 MHz center frequency, 50 MHz bandwidth, 5 frames averaged, 3 m distance
\[ \text{difference} = |F\{\text{tmds}(0x10)\}| - |F\{\text{tmds}(0x55)\}| - |F\{\text{tmds}(0x55) - \text{tmds}(0x10)\}| \]
RF emission limits

What test standards provide adequate protection?

→ MPR II / TCO’92: Measure only below 400 kHz (deflection coils) and are therefore irrelevant for video signals.

→ CISPR 22 Class B (CE, FCC, etc.): 37 dBμV/m at 10 m distance in any 120 kHz passband.

→ MIL-STD-461E (R102): 24 dBμV/m at 1 m distance in any 100 kHz passband.

→ My proposal: 24 dBμV/m at 1 m distance in any 5 MHz passband (option: only for periodic averaging results).

The civilian RFI limits do not prevent receivability at quiet site over hundreds of meters with compact directional antenna array and periodic averaging. Impulse level raises linearly with bandwidth, noise level increases normally with square root of bandwidth.
Optical eavesdropping

→ RF emissions are just an unwanted side effect.

→ Displays were designed to emit *light*.

→ Projective observation (telescopes, mirrors, etc.).

→ Observation of light intensity variation.
Display spying with telescopes

Diffraction limit for angular resolution:

\[ \theta = \frac{1.22 \cdot \lambda}{D}, \]

Aperture required for pixel size \( r \) at distance \( d \) and viewing angle \( \alpha \):

\[ D = \frac{1.22 \cdot \lambda \cdot d}{r \cdot \cos \alpha} \]

Example:

Typical pixel size: \( r = 0.25 \) mm
\( (320 \times 240 \text{ mm} = 1280 \times 1024 \text{ pixels}) \)

Aperture: \( D = 300 \) mm
(amateure astronomy reflector)

Range: \( d \approx 60 \) m
Time-domain observation of CRT light

Overall light emitted by CRT is proportional to (gamma corrected) video signal $v_\gamma(t)$ convolved with phosphor impulse response $P(t)$:

$$I(t) = \int_{0}^{\infty} v_\gamma(t - t') P(t') \, dt'$$

→ What does the impulse response curve of commonly used CRT phosphors look like?

→ Does it have very fast decay components that preserve the high-frequency areas of the video signal spectrum?

→ Are practically usable light sensors available to detect these?

→ What limits are there and is this a practical risk?

→ What countermeasures are there?
CRT phosphor types

Monitor manual says “P22”, but this is just the generic designation for all RGB phosphor triplets designed for NTSC color TV.

Worldwide Type Designation System (WTDS): XXA, XXB, XBA, . . .

Substances:

→ **Red**: yttrium oxysulfide doped with europium ($Y_2O_2S:Eu$), zinc phosphate with manganese ($Zn_3(PO_4)_2:Mn$).

→ **Green**: zinc sulfide doped with copper ($ZnS:Cu$) and sometimes also with aluminium and/or gold, or zinc silicate doped with manganese and silver ($Zn_2SiO_4:Mn,Ag$).

→ **Blue**: The blue phosphor is usually zinc sulfide doped with silver ($ZnS:Ag$) and in some cases also aluminium or gallium.
Light sensors

Requirements:

→ very sensitive (to reduce preamp noise)

→ very fast (bandwidth comparable to $f_p/2$, ideally $>100$ MHz or $<5$ ns rise and fall time)

Options:

→ PIN photodiode (typical sensitivity $0.2–0.6$ A/W, $\mu$s–ns)

→ Avalanche photodiode (internal gain, typical sensitivity $10^2$ A/W, $<1$ ns raise/fall time)

→ Photomultiplier tube (significant internal gain, typical sensitivity $10^1–10^5$ A/W, $<1$ ns raise/fall time)
The photomultiplier tube (PMT)

Choice: Hamamatsu H6780-01 Photomultiplier tube module with integrated high-voltage circuit allows easy operation from 12 V lab power supply.
Control voltage $0.25 < U_c < 0.9$ V adjusts radiant sensitivity to

$$1.5 \times 10^5 \text{ A/W} \cdot \left(\frac{U_c}{1 \text{ V}}\right)^{7.2}$$

Thanks to high internal gain no need for video pre-amplifier, allowing direct connection to 50 $\Omega$ DC input of digital storage oscilloscope.
Measured P22 intensity decay curves

(a) Emission decay of a single pixel ($f_p = 36$ MHz)

The sensor output voltage is shown here as the equivalent radiant intensity (power per solid angle) of the light source.
Measured P22 intensity decay curves

(b) Emission decay of a 320–pixel line

- red
- green
- blue
- white
- video signal
- model
Modeling phosphor impulse responses

- Exponential decay curve of a typical phosphorescent substance:

\[ I_e(t) = I_0 \cdot e^{-\frac{t}{\tau}} \]

Note that this is for

\[ \tau = \frac{1}{2\pi f} = RC \]

the impulse response of a first-order Butterworth low-pass filter.

- Power-law decay curve of zinc-sulfide based phosphors:

\[ I_p(t) = \frac{I_0}{(t + \alpha)^\beta}. \]

(Results in asymptotically straight line on loglog scale.)
Closed form impulse response model

Real impulse response curves have to be approximated by a linear combination of exponential and power-law curves:

\[
P_{P22R}(t) / \frac{W}{V \cdot s \cdot sr} = 4 \times e^{-2\pi t \times 360 \ \text{Hz}} + 1.75 \times e^{-2\pi t \times 1.6 \ \text{kHz}} + \\
2 \times e^{-2\pi t \times 8 \ \text{kHz}} + 2.25 \times e^{-2\pi t \times 25 \ \text{kHz}} + \\
15 \times e^{-2\pi t \times 700 \ \text{kHz}} + 29 \times e^{-2\pi t \times 7 \ \text{MHz}}
\]

\[
P_{P22G}(t) / \frac{W}{V \cdot s \cdot sr} = 210 \times 10^{-6} \times \left( \frac{t + 5.5 \ \mu s}{1 \ \text{s}} \right)^{-1.1} + 37 \times e^{-2\pi t \times 150 \ \text{kHz}} + \\
100 \times e^{-2\pi t \times 700 \ \text{kHz}} + 90 \times e^{-2\pi t \times 5 \ \text{MHz}}
\]

\[
P_{P22B}(t) / \frac{W}{V \cdot s \cdot sr} = 190 \times 10^{-6} \times \left( \frac{t + 5 \ \mu s}{1 \ \text{s}} \right)^{-1.11} + 75 \times e^{-2\pi t \times 100 \ \text{kHz}} + \\
1000 \times e^{-2\pi t \times 1.1 \ \text{MHz}} + 1100 \times e^{-2\pi t \times 4 \ \text{MHz}}
\]

\[
P_{P22} = P_{P22R} + P_{P22G} + P_{P22B}
\]
Double-log plot of reconstructed P22 impulse response

\begin{figure}
\centering
\includegraphics[width=\textwidth]{figure.png}
\caption{Double-log plot of reconstructed P22 impulse response.}
\end{figure}
Integrated impulse response curves
Estimated P22 frequency characteristic
Test image shown on target monitor

This image was captured with the help of a light sensor from the high-frequency fluctuations in the light emitted by a cathode-ray tube computer monitor which I picked up as a diffuse reflection from a nearby wall.

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001
Rasterized raw signal from PMT

VESA mode 640×480@85 Hz, 8-bit sampled at 250 MHz, 256 frames (3.0 s, 753 MB) averaged, scaled to 0.1% saturation
High-pass filtering result

First-order Butterworth high-pass filter applied, 3 dB cutoff at 4 MHz.
Deconvolution result

CAN YOU READ THIS?

This image was captured with the help of a light sensor from the high-frequency fluctuations in the light emitted by a cathode-ray tube computer monitor, which I picked up as a diffuse reflection from a nearby wall.

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001.
Deconvolution

We can model highly accurately the sensor signal blurred by the phosphor afterglow as the convolution of the beam current $v_\gamma$ and the impulse-response function $P_{P22}$

$$I(t) = \int_0^\infty v_\gamma(t - t') P_{P22}(t') \, dt'$$

which a Fourier transform turns into a multiplication of frequency-domain signals:

$$\mathcal{F}\{I\} = \mathcal{F}\{\tilde{v}_\gamma\} \cdot \mathcal{F}\{P_{P22}\}.$$

Deconvolution can be accomplished simply by division in the frequency domain, followed by an inverse FFT, leading to the shown estimate of the original beam current:

$$\tilde{v}_\gamma = \mathcal{F}^{-1} \left\{ \frac{\mathcal{F}\{I\}}{\mathcal{F}\{P_{P22}\}} \right\}$$
Threat analysis

Number of signal photons received per pixel:

\[ N_p = \frac{Q_p \lambda}{hc} \]

where \( Q_p \) is the amount of energy received from a single pixel.

Number of photons received from background light:

\[ N_b = \frac{nt_p A A_r L_b \lambda}{hc d^2} \]

where

\[ A = \text{observed area [m}^2\text{]} \]
\[ A_r = \text{receiver aperture [m}^2\text{]} \]
\[ d = \text{observer distance [m]} \]
\[ L_b = \text{wall radiance [W/(sr \cdot m}^2\text{)]} \]
\[ t_p = f_p^{-1} = \text{pixel duration [s]} \]
\[ n = \text{number of frames averaged} \]
Arrival of photons at a sensor is a Poisson process

- we expect $N_b$ photons per pixel
- the standard deviation of photon count will be $\sqrt{N_b}$
- “shot noise”

Risk zone
Eavesdropped signal must dominate background-light shot noise:

$$N_p > \sqrt{N_b}$$
Number of photons reflected of a wall

\[ N_p = \frac{\varrho n t^2_A A_r V P(0) \lambda}{2\pi h c d^2 d'^2} \]

where

\[
\begin{align*}
\varrho & = \text{reflectivity of wall (white } \approx 0.8) \\
P(t) & = \text{phosphor impulse response function } [W/(V \cdot s \cdot sr)] \\
V & = \text{video voltage (gamma corrected) } [V] \\
d' & = \text{distance wall/CRT } [m] \\
d & = \text{distance wall/receiver } [m]
\end{align*}
\]

The detection process is approximated here by integrating \( P_{P22}(t) \approx P_{P22}(0) \) over pixel time \( t_p \) to estimate pixel brightness after high-pass filtering.

More accurate estimate with numerical simulation of detection and deconvolution.
CRT risk zone calculation

Upper limit for receiver distance to wall:

\[
d < \frac{VP(0)}{d'^2} \sqrt{\frac{\varrho n \lambda t^3 AA_r}{4\pi E_b h c}}
\]

Applied to some example values:

\rightarrow \text{Illuminance 2 lux ("late twilight") corresponds to irradiance } E_b = 1 \text{ mW/m}^2 \text{ onto the wall (} A = 2 \text{ m}^2 \text{ and } \varrho = 0.5)\]

\rightarrow \text{CRT at } d' = 2 \text{ m from the wall has an initial impulse response of } P(0) = 10^3 \text{ W/(V \cdot s \cdot sr)} \text{ and } V = 1 \text{ V for a white pixel.}\]

\rightarrow \text{Eavesdropper has } A_r = 0.3 \text{ m}^2 \text{ telescope and averages } n = 100 \text{ frames.}\]

Then

\[
d < 50 \text{ m}
\]
Diffuse reflection of status indicator light

Of 39 tested communication devices, 14 emitted serial port data in light from transmit/receive line status LEDs. [Loughry/Umphress, 2002]

Model number $N$ of photons received by eavesdropper as normal distribution with

$$\mu = \begin{cases} N_b + N_p & \text{when LED on} \\ N_b & \text{when LED off} \end{cases}$$

$$\sigma = \sqrt{N_b}$$

Detector compares $N$ with threshold $N_b + \frac{1}{2}N_p$, resulting in bit-error rate

$$p_{BER} = Q \left( \frac{N_p}{2\sqrt{N_b}} \right) \quad \text{with} \quad Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{y^2}{2}} \, dy$$
LED bit-error rate calculation

\[ N_p = \frac{t_p A_r I_p \lambda}{h c d^2}, \quad N_b = \frac{t_p A A_r \varrho E_b \lambda}{\pi h c d^2} \]

Applied to some example values:

→ Green (\( \lambda = 565 \text{ nm} \)) LED with 7 mcd (corresponds to radiant intensity \( I_p = 10^{-5} \text{ W/sr} \)) located \( d' = 2 \text{ m} \) from wall shows 10 kbit/s signal (\( t_p = 10^{-4} \text{ s} \)).

→ Eavesdropper observes \( A = 2 \text{ m}^2 \) wall at \( d = 50 \text{ m} \) distance with \( A_r = 0.3 \text{ m}^2 \) telescope.

→ Wall reflects \( \varrho = 0.5 \) of ambient illuminance \( E_b = 1 \text{ mW/m}^2 \) ("late twilight").

Resulting bit-error rate due to shot-noise limit:

\[ p_{BER} > 10^{-4} \]
Clock recovery and detection of serial data

(a)

(b)

(c)

(d)

(e)

(f)

(g)
Receiver design considerations

- Use zoom telescope and mechanism to mask area of interest with best signal-to-noise ratio.

- Use large-aperture optics (imaging quality less relevant).

- Characterize phosphor impulse response in different wavelength subbands.

- Use filter set or spectrometer to select wavelength range with best signal-to-noise ratio.

- Where older fluorescent lamps driven with 50/60 Hz currents are used, collect signal during dark periods (gated PMT).

- Use analog preprocessing of photomultiplier output to reduce quantization and amplifier noise.
Spectral coverage of CRT phosphors and fluorescent lamps
Possible countermeasures

→ Avoid line-of-sight access to displays, keyboards, documents.
→ Ensure good background illumination that covers the entire spectrum of wavelength emitted by the CRT phosphors.
→ Avoid fluorescent lamps driven with low-frequency currents.
→ Using only the red channel to display particularly critical information has two advantages: (1) video signal is filtered better, (2) incandescent light jams red better than blue.
→ CRT and phosphor manufacturers should document phosphor impulse response curves in data sheets (double-logarithmic diagram with $10^{-9}$–$10^{-2}$ s timescale). Monitor manufacturers should document exact CRT types used.
→ CRT type security certification.
→ Common types of flat panel displays (LCD) seem to pose no threat because of parallel addressing of pixel rows and slower response times.
Conclusions (optical)

→ It is feasible to reconstruct the image displayed on a raster screen CRT from the emitted light, even after diffuse reflection.

→ A sufficiently dark environment (i.e., after sunset) is needed to avoid shot noise dominating the signal.

→ Etched/frosted/milky window glass does not necessarily prevent readability of CRT displays at a distance.

→ Off-the-shelf equipment sufficient for a lab demonstration.

→ Real-world attacks will require specially designed receivers and patience.

→ The threat level seems roughly comparable to that of compromising radio-frequency emanations.
Conclusions (RF)

- Digital video interfaces used with flat panel displays can emit significantly stronger and better signal than CRTs.

- CRT emissions dependent significantly on graphics card.

- Human-readable text and radio character recognition is possible with contemporary video modes and equipment in nearby rooms even without directional antennas.

- Various low-cost software countermeasures possible (filtered fonts, random bit jamming).

- First civilian RF emission security test standard could be based on MIL RFI standard with increased bandwidth.

- Emission security remains a valid concern in applications with high confidentiality requirements, predictable device usage and easy longterm access to neighbour rooms.
Open questions and future research

→ Software radio instead of AM/FM demodulator (to preserve polarity of pulses), phase lock center and pixel frequency, etc.

→ Larger product vulnerability surveys

→ Intentional broadcasts via non-periodic sources (bus lines, etc.)

→ Test and documentation of rumoured historic exploits (acoustic and power-line emanations of IBM golfball printer)

→ Refinement of test standard proposal (power lines, distinction between signal types, unshielded rooms, etc.)

→ Licence enforcement applications

→ Search for further new vulnerabilities and emanation channels

→ Stimulate FOI release of past military research