Hardware security – Part 1: Smartcards and other tamper-resistant modules

Markus Kuhn

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

http://www.cl.cam.ac.uk/~mgk25/

Applications of Tamper Resistant Modules

Security of cryptographic applications is based on secure storage of secret keys and unobservability of computation

Distributed and mobile applications allow attacker full physical access to hardware over extended period of time

- pay−TV access control
- electronic purses
- financial transaction terminals
- software copy protection
- prepayment meters
- anti−theft protection
- authentic telemetry
- protection of algorithms
- cellular phones
- ...

Tamper-resistant modules

1) Single chip systems

Consist of a microcontroller that contains the entire CPU, system bus, communication interface, firmware and non-volatile memory on a single chip. Examples: smartcards, SIMs, proximity cards, "dongles".

Advantages:

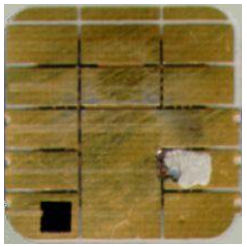
- → small
- → low cost
- → easy to handle with standard production technologies

Disadvantages:

- → limited capacity
- → no continuous power source for alarm mechanisms
- → access feasible with skillful use of semiconductor test equipment

Some Pay−TV Pirate Devices

"Battery−powered smartcard", Megasat Bochum



Conductive silver ink attack on BSkyB P10 card (top), with card CPU replaced by external DS5002FP (right)

BSkyB P9 deactivation blocker

ISO 7816 to RS−232 adapter (Season7)

Classes of Attacks on Security Modules

Microprobing

Open the package, access the chip surface with semiconductor test equipment, and observe and manipulate the internal data paths

Software Attacks

Use the normal communication interface and abuse security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation

Eavesdropping

Without opening the package, try to get access to protected information by analyzing compromising signals in emanated electromagnetic radiation, supply current fluctuations, leakage currents on signal lines, and protocol timings

Fault Generation

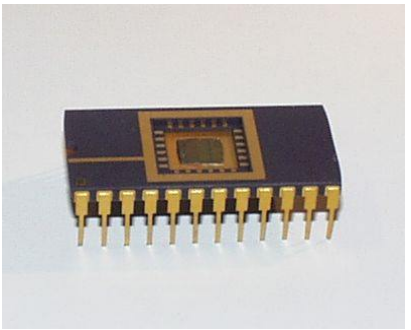
Provoke malfunctions by operating the device under environmental stress conditions such as high/low temperature, supply voltage variations and spikes, clock−phase jumps, ionising radiation, protocol violations, partial resets, etc.

Preparation I: Depackaging the Processor



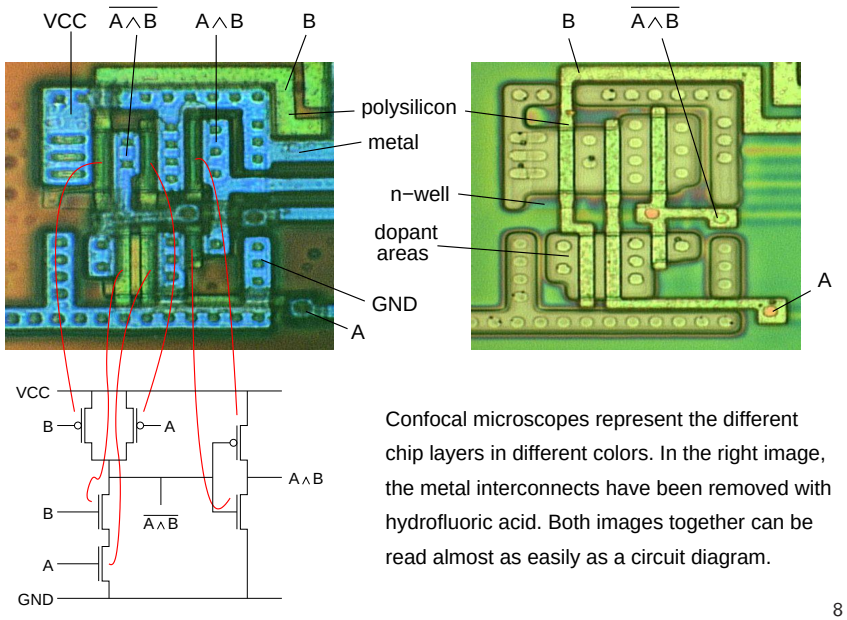

1) Heat up card plastic, bend it, and remove chip module
2) Dissolve package in 60 °C fuming nitric acid, then wash in acetone, deionized water, and finally isopropanol. The etching should be carried out under very dry conditions.

Preparation II: Bonding into a Test Package

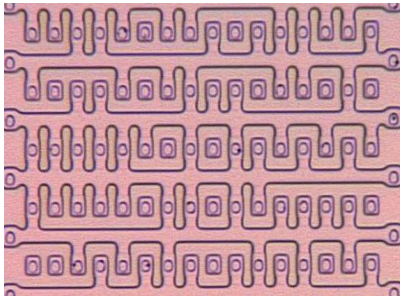
A manual bonding station establishes reliable contacts to the supply, communication, and test pads of the microprocessor using ultrasonic welding of a fine aluminium wire.

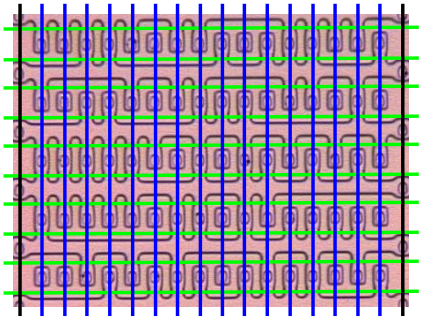
Optical Reverse−Engineering of VLSI Circuits



Confocal microscopes represent the different chip layers in different colors. In the right image, the metal interconnects have been removed with hydrofluoric acid. Both images together can be read almost as easily as a circuit diagram.

Optical Access to Diffusion Layer ROM Content

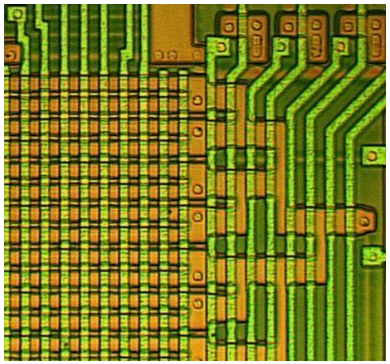




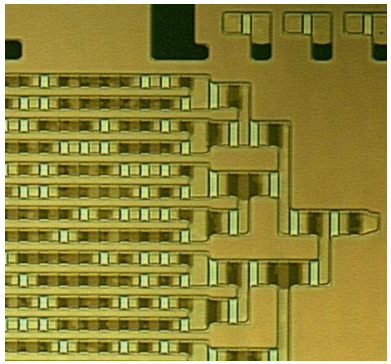
After all covering layers including the surrounding field oxide have been removed with hydrofluoric acid, the shape of the now visible diffusion areas will reveal the ROM content (here 16x10 bits).

polysilicon row access line
metal column access line
ground connection

Optical Reconstruction of Ion Implantation ROM Content



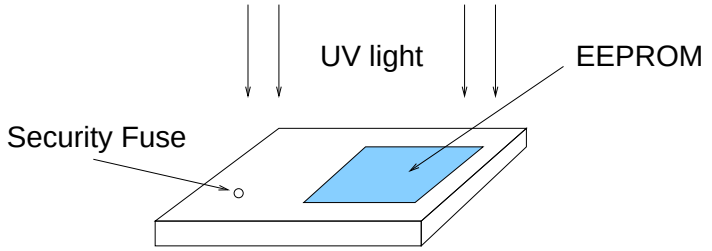
View of ROM with polysilicon intact



Diffusion layer after crystallographic etch

This type of ROM does not reveal the bit pattern in the shape of the diffusion areas, but a crystallographic staining technique (Dash etchand) that etches doped regions faster than undoped regions will still show the ROM bits.

UV Read−out of Standard Microcontrollers



Many microcontrollers have an EEPROM security fuse located outside the EEPROM program memory.

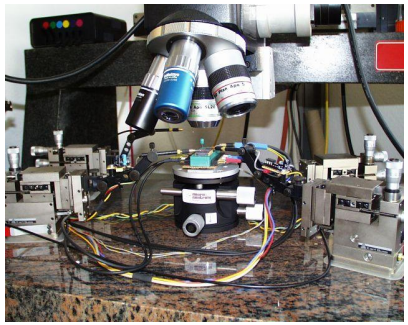
→ Open chip package

→ Cover program memory with opaque material

→ Reset security fuse in UV EPROM eraser

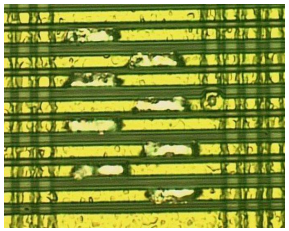
→ Access memory with program/verify commands

Access to CPU Bus via Laser Depassivation and Microprobing

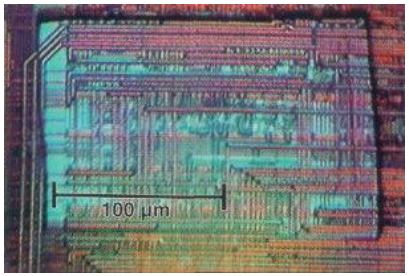


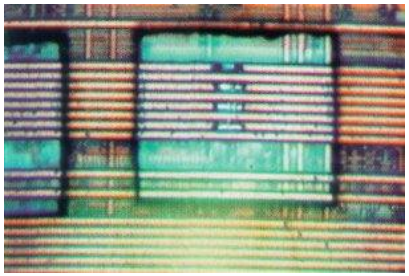
Top: A complete microprobing station consisting of a micro−scope (Mitutoyo FS−60), laser cutter (New Wave QuikLaze), four micropositioners (Karl Suss), CCD camera, PC with DSP card for card protocol interface handling and data acquisition, oscilloscope, pattern generator, power supply, logic analyzer, etc. Right: Eight depassivated data bus lines.

Photos: ADSR

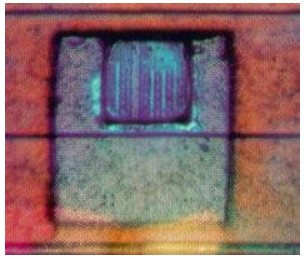


Laser cutter as a powerful reverse engineering tool



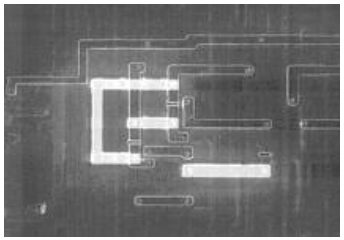


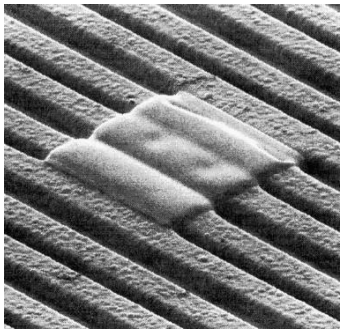
- Local removal of passivation layer with <1 µm precision (355 nm UV light)
- Removal of oxide (532 nm green light)
- Exposure of lower metal layers for probing
- Cuts in metal and polysilicon lines (532 nm)
- Order of magnitude less expensive than FIB



Photos: New Wave Research

Focused Ion Beam Workstations for IC Modification





Focused ion−beam machines make high−resolution images of chip structures and allow us to both remove and deposit materials (metal and insulators) with 0.01 µm resolution. Gallium ions are accelerated with 30 kV and process gases like iodine or an organo−metallic compound are injected near the target location.

Left Photo: Dept. of Material Sciences, University of Cambridge

Microprobing Access to All Memory Locations

Passively monitoring and recording all memory−bus accesses might not be sufficient to attack all applications. Carefully designed smartcard software makes it difficult to trigger memory accesses to all secrets in a laboratory.

- Card software that calculates a full memory checksum after each reset simplifies attacks considerably!

Solution for Attacker:

Abuse existing processor hardware as an address generator that accesses all memory locations predictably. A single probing needle can now capture all memory values, probing one bus line at a time.

Options:

- Disable instruction decoder, such that no JMP/CALL/RET/HALT instructions are executed (preferably only NOP−like instructions should be allowed).
- Disable program−counter load gate

In many smartcard processors, this can be accomplished with just a single probe!

Restricted Program Counter

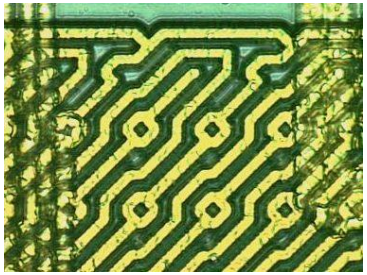
A standard program−counter mechanism is too easily abused as an address−sequence generator. Tamper−resistant design of the instruction decoder is difficult. Watchdog circuitry requires many transistors and simple forms are also easily disabled.

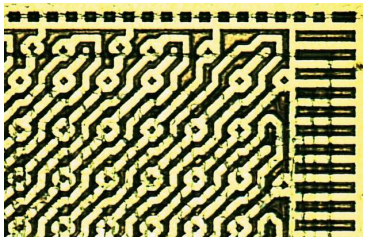
Solution:

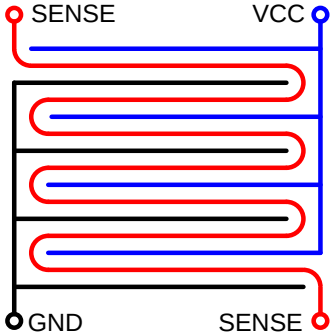
- Replace the normal program counter (e.g., 16 bit) by a combination of a full−size segment register S and a short (e.g., 7 bit) offset register O.
- Instructions are fetched from address S+O.
- Only O is automatically incremented after every instruction. An overflow of O will halt the processor.
- A jump to address X is performed by loading X into S and setting O to zero.
- Unconditional jump commands must be less than 128 bytes apart, which an assembler preprocessor used by the developer can ensure automatically.

Now, no simple FIB edit can cause the program counter to cover all addresses.

Example of a Top−Layer Sensor Mesh



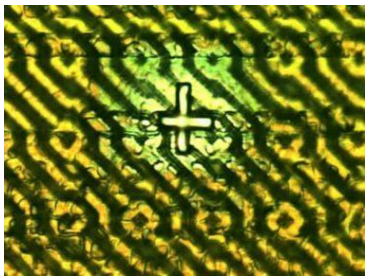




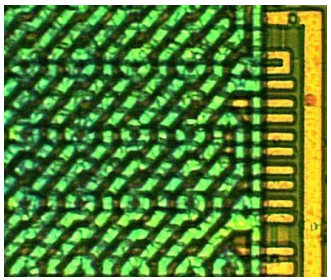
The sensor line is checked during operation for interruptions or short−circuits, which trigger alarms (e.g., processor halt or flash erase). The power lines are at some places used to supply the circuits below.

ST16SF48A

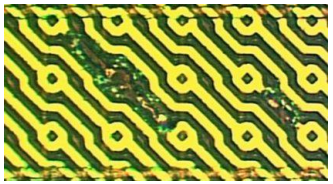
Sensor Meshes: Vulnerabilities and Attacks



a)



b)



c)

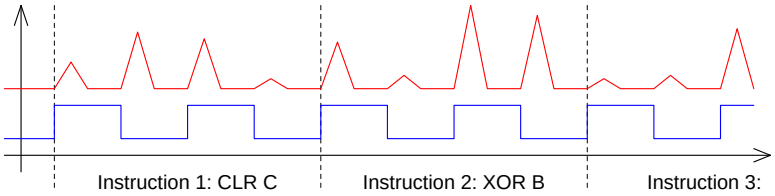
a) FIB workstation can be used to place a new via between mesh lines with an access cross on top for easy microprobing.

b) Design flaw: redundant bus lines extend beyond the sensor mesh, allowing easy microprobing access ("Freedom for imprisoned crypto bits!").

c) Not all power supply lines are used, so they can be removed with a laser cutter to allow access to signals below the mesh.

Power Supply Current Forms a Significant Covert Channel

Record current in VCC/GND connection with 12−bit, 30−MHz ADC, in order to reconstruct executed instruction sequence and observe cryptographic computations.



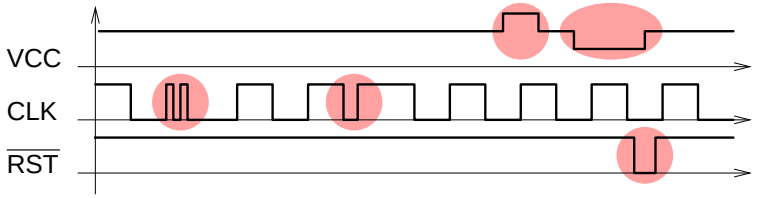
→ Characteristic current spikes can identify executed instruction

→ Data values appear in power profiles either as differential Hamming weights (~0.5−1 mA/bit) or as individual bits, e.g. with multiplication or shift instructions

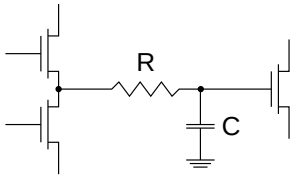
→ Current signature depends on accessed memory type (SRAM−write short circuit, EEPROM read−out amplifier, etc.)

→ Activation of EEPROM programming−voltage charge pump observable, which allows to abort before state changes (e.g., with bad retry counters)

Change single instructions by signal glitches



Fault model:



→ Links between transistors form RC delay elements
→ R and C vary between links and individual chips
→ Maximum RC of any link determines maximum CLK frequency
→ $\overline{\text{RST}}$ signal sometimes not latched, which allows partial resets
→ Transistors compare VCC and V_C , which allows VCC glitches

Glitch attack on an output loop

Typical data output routine in security software:

```
1   b = answer_address
2   a = answer_length
3   if (a == 0) goto 8
4   transmit(*b)
5   b = b + 1
6   a = a − 1
7   goto 3
8   ...
```

Cause CLK or VCC glitch when instruction 3 or 6 is being fetched, in order to extend loop length to send additional memory content to port.

Destruction of Test Circuitry

Attackers and test engineers share similar interests. Both need easy access to the on−chip bus lines with as few probes as possible.

Commonly used test circuitry:

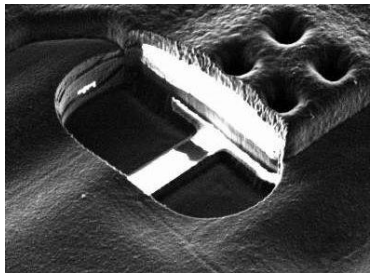
- → Parallel/serial converters for full bus
- → Full bus available on large probing pads

Pads usually disabled by blowing a poly fuse, but can easily be reconnected via FIB.

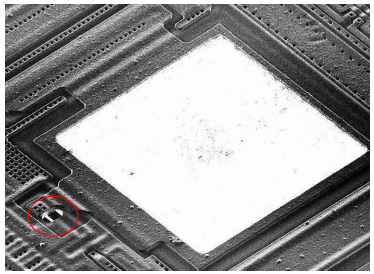
Solution:

Test circuitry must not only be disabled by blowing fuses. It must be structurally destroyed.

Test circuitry can be located on the 80−200 µm wide area between the dies that is removed during wafer cutting.



Blown polysilicon fuse near test pad (Motorola)



Tamper-resistant modules

2) Secure packages

A security shield encloses an entire printed circuit board. The only non-volatile memory is battery-backed static RAM (SRAM). The alarm mechanism, when triggered, shortcuts the SRAM power supply, thereby erasing the confidential data.

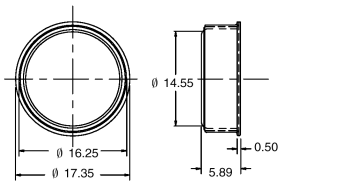
Advantages:

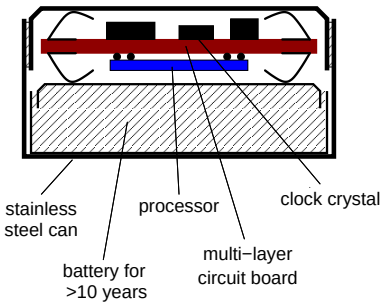
- → fairly high security

Disadvantages:

- → more complex to manufacture
- → no ventilation ⇒ power limits
- → only macroscopic mechanic security

iButtons − An Alternative Tamper−Resistant Module Form





- → battery−buffered on−chip SRAM
- → sealed steel can provides mechanical stability and EMI shielding, which allows very sensitive alarm mechanisms
- → multiple layers of sensor wires on chip and in circuit board
- → chip layout facing circuit board
- → difficult to open can without interrupting battery voltage
- → pressurized with nitrogen

Tamper-resistant modules

3) Bus encryption

The CPU chip incorporates a unit that encrypts both the data and address bus. The secret key used is stored on the CPU chip in a battery-backed SRAM register. External memory contains only encrypted data that is decrypted when fetched into the CPU cache.

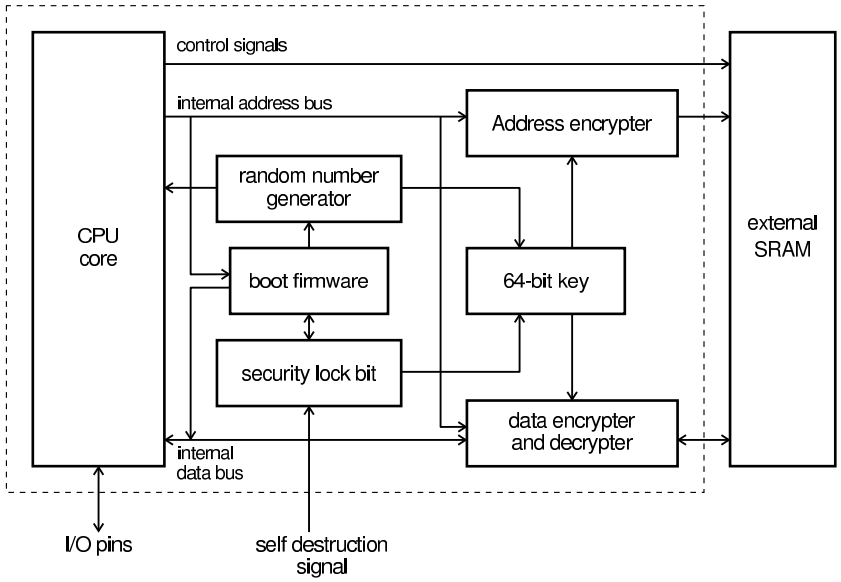
Advantages:

- ⟶ no capacity limit
- ⟶ SRAM registers are difficult to access for attackers
- ⟶ simple to manufacture (no off-chip alarm envelope)
- ⟶ can easily be combined with a secure package

Disadvantages:

- ⟶ design tradeoff between good cryptography and low bus latency
- ⟶ traces of external memory accesses lead to information leaks

Bus Encryption in the DS5002FP:

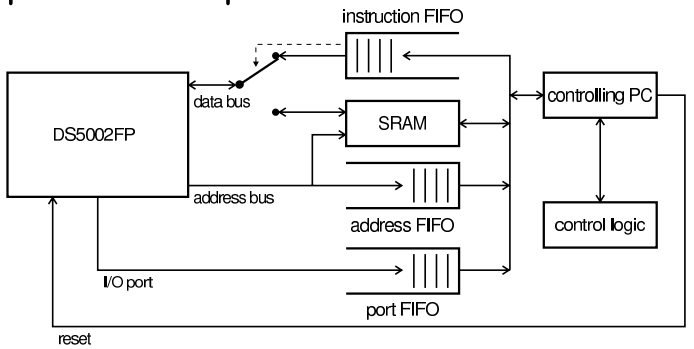


Attack Concept:

Search systematically cipher bytes for the following instructions:

```
00        NOP             ; no operation
75 90 xx  MOV 90h, #xxh   ; output value xxh on port 1
```

Experimental Setup:



Details: M.G. Kuhn: *Cipher instruction search attack on the bus-encryption security microcontroller DS5002FP*. IEEE Trans. on Computers **47**(10), October 1998, pp. 1153–1157.

Classification of Attackers

Class I: **Clever Outsiders.** Often very intelligent, have insufficient knowledge of the system, have access to moderately sophisticated equipment, use existing weaknesses in the system.

Class II: **Knowledgeable Insiders.** Substantial specialized technical education and experience, varying degrees of understanding of the system but potential access to most relevant information, often highly sophisticated tools.

Class III: **Funded Organizations.** Teams of specialists with complementary skills, great funding resources, capable of in−depth analysis and design of sophisticated attacks, most advanced tools, access to knowledgeable insiders.

[according to Abraham, Dolan, Double, Stevens: Transaction Security System, IBM Systems Journal, Vol. 30, No. 2, 1991.]

Tamper Resistance versus Tamper Evidence

Invasive attacks

- → Microprobing
- → FIB editing
- → Layout reconstruction

violate tamper resistance requirement (FIPS 140−1 Level 4)

Require between hours and weeks in a specialized laboratory, therefore the owner of the card is likely to notice the attack and can revoke certificates for keys that might be lost.

Non−invasive attacks

- → Glitch attacks
- → Power analysis
- → Software vulnerabilities

violate in addition tamper−evidence requirement (FIPS 140−1 Level 2)

Can be performed within a few seconds inside a Trojan terminal in a Mafia−owned shop, therefore card owner will not notice that card secrets have been stolen and will not revoke keys.

Summary and conclusions

- ⟶ With sufficient effort, invasive techniques may extract all data from microcontrollers and smartcard CPUs.
- ⟶ Obfuscated chip design remains standard security technique for single-chip systems without active alarms.
- ⟶ Non-invasive attacks (glitching, power analysis) are the main concern in tamper-evidence applications (access control, banking, signatures), where compromised keys affect only individual users or accounts and can be revoked easily.
- ⟶ The smartcard form factor may be unsuitable for applications with strong tamper-resistance requirements (e.g., pay-TV conditional access, digital restrictions management) ⇒ battery-backed SRAM with active alarms
- ⟶ Extremely careful engineering needed to design tamper-evident single-chip systems without active alarms.

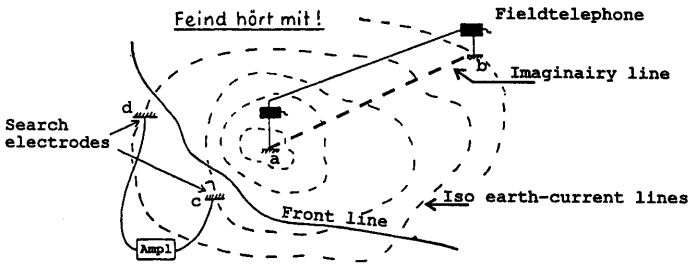
Hardware security – Part 2: Electromagnetic eavesdropping on computers

Markus Kuhn

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

http://www.cl.cam.ac.uk/~mgk25/

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 [Bauer, 1999].

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.

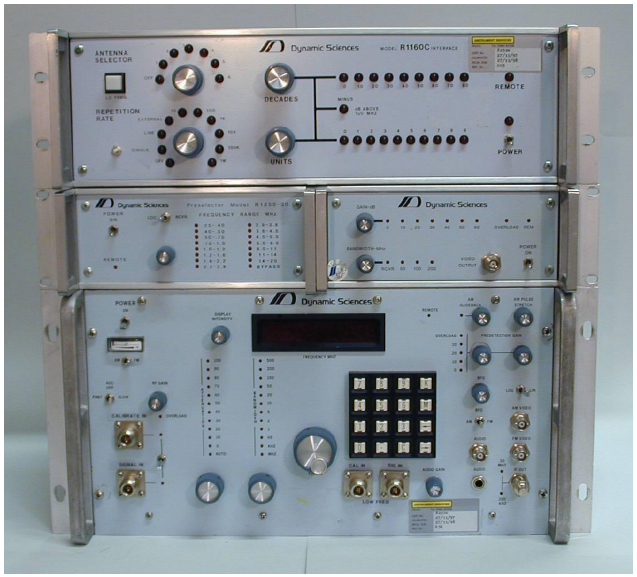
→ Since 1960s: Secret US government "TEMPEST" programme investigates electromagnetic eavesdropping on computer and communications equipment and defines "Compromising Emanations Laboratory Test Standards" (NACSIM 5100A, AMSG 720B, etc. still classified today).

→ 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.

R1250 Wideband Tempest Receiver

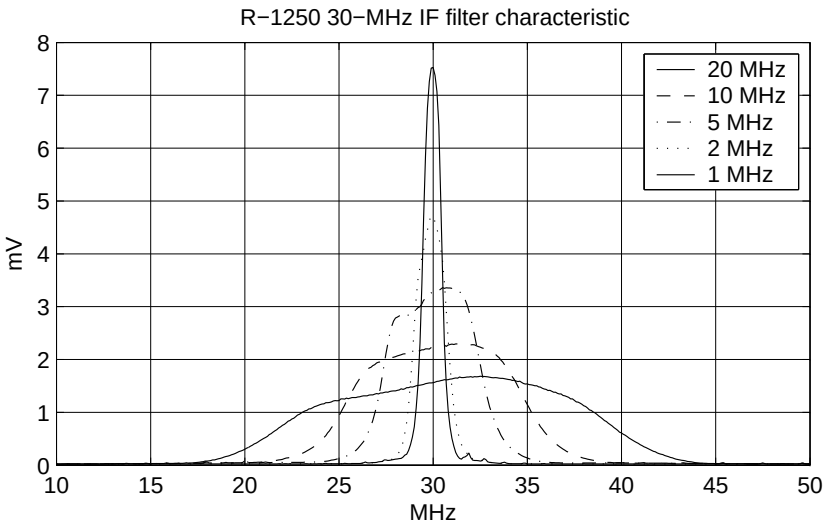


Wideband Tempest Measurement Receivers

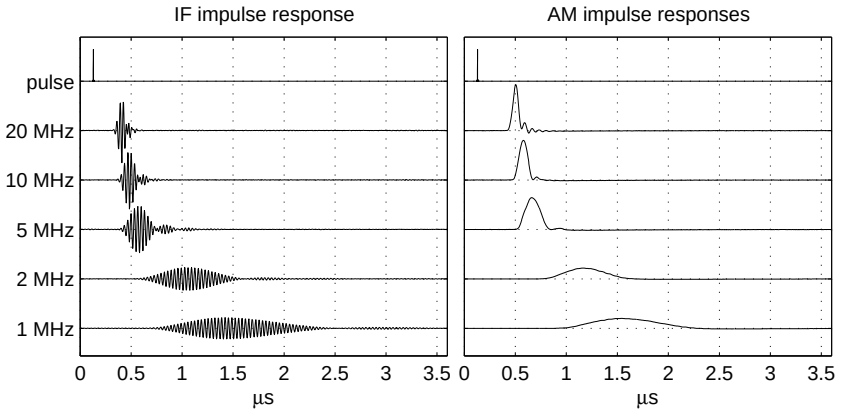
- ⟶ Can be tuned continuously from 100 Hz to 1 GHz.
- ⟶ Offers 21 bandwidths from 50 Hz to 200 MHz (1-2-5 steps).

  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, ≈ 30–100 k£.
  Second hand offers on Internet for < 1 k£

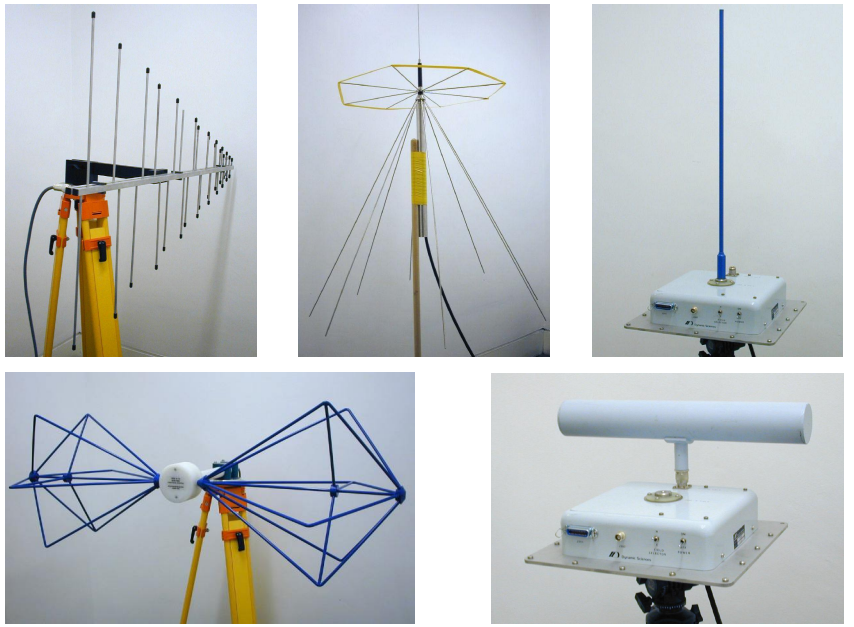
Intermediate frequency bandwidth



Receiving impulse signals



$$\text{impulse width} = \frac{1}{\text{bandwidth}}$$



Video Timing

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

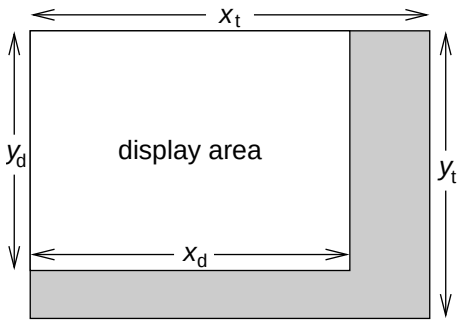
Pixel frequency: f_p

Deflection frequencies:

$$f_\mathrm{h} = \frac{f_\mathrm{p}}{x_\mathrm{t}}, \quad f_\mathrm{v} = \frac{f_\mathrm{p}}{x_\mathrm{t} \cdot y_\mathrm{t}}$$

Pixel refresh time:

$$t = \frac{x}{f_\mathrm{p}} + \frac{y}{f_\mathrm{h}} + \frac{n}{f_\mathrm{v}}$$



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

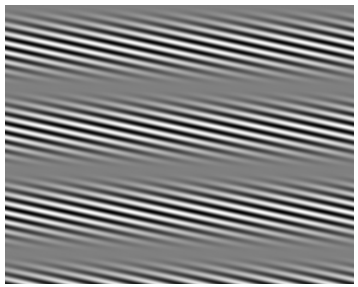
```
ModeLine "1280x1024@85"  157.5  1280 1344 1504 1728  1024 1025 1028 1072
```

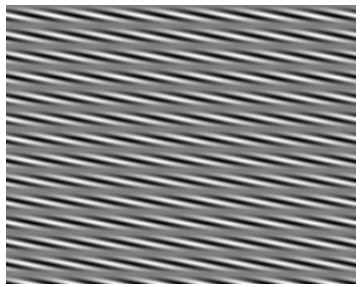
Image mostly stable if relative error of f_h below $\approx 10^{-7}$.

AM audio broadcast from CRT displays

$$s(t) = A \cdot \cos(2\pi f_\mathrm{c} t) \cdot [1 + m \cdot \cos(2\pi f_\mathrm{t} t)]$$

300 and 1200 Hz tones at $f_\mathrm{c} = 1.0$ MHz:

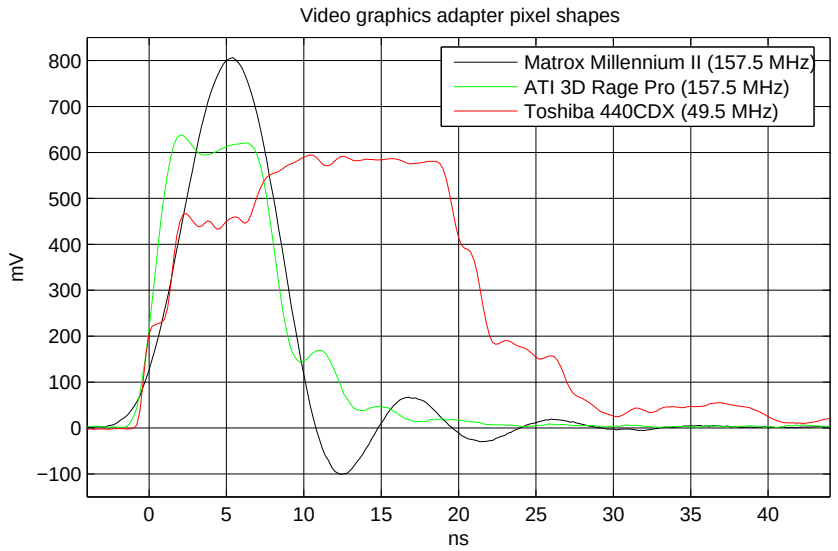




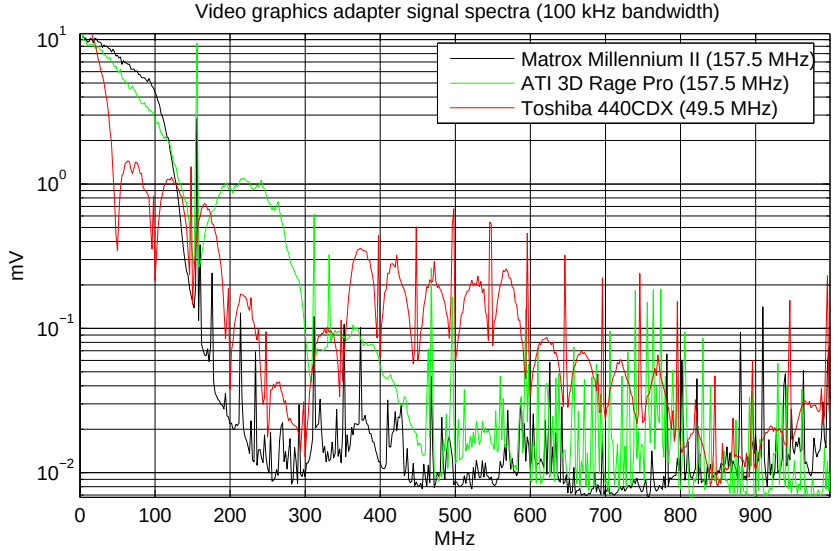
Play your MP3 music at home via CRT emanations in your AM radio:

`http://www.erikyyy.de/tempest/`

Real-world VGA card pixel shapes



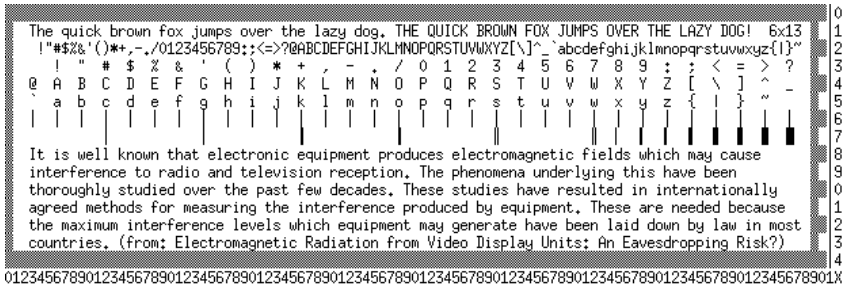
Real-world VGA card frequency spectrum



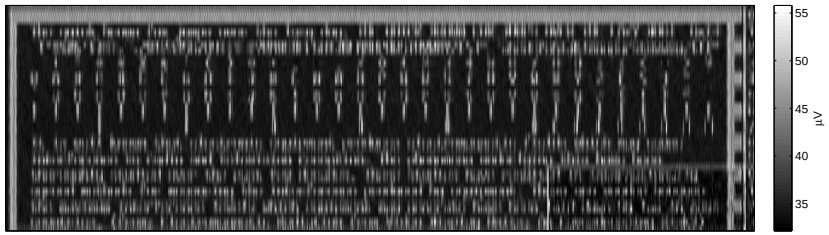
Eavesdropping of CRT Displays

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.

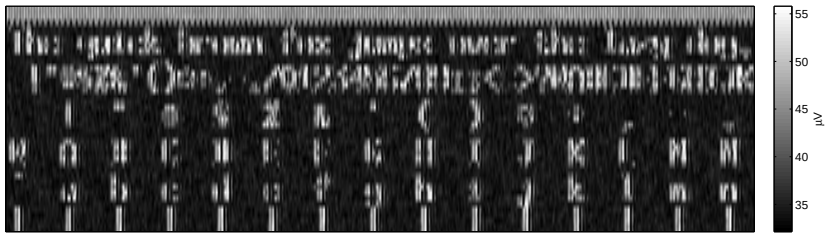
Test text used in the following experiments:



480 MHz center frequency, 50 MHz bandwidth, 256 (16) frames averaged, 3 m distance



480 MHz center frequency, 50 MHz bandwidth, magnified image section



AM receiver bandwidth equal to eavesdropped pixel rate distinguishes individual pixels.

Magnified example of eavesdropped text

Test text on targeted CRT:

Rasterized output of AM demodulator at 480 MHz center frequency:

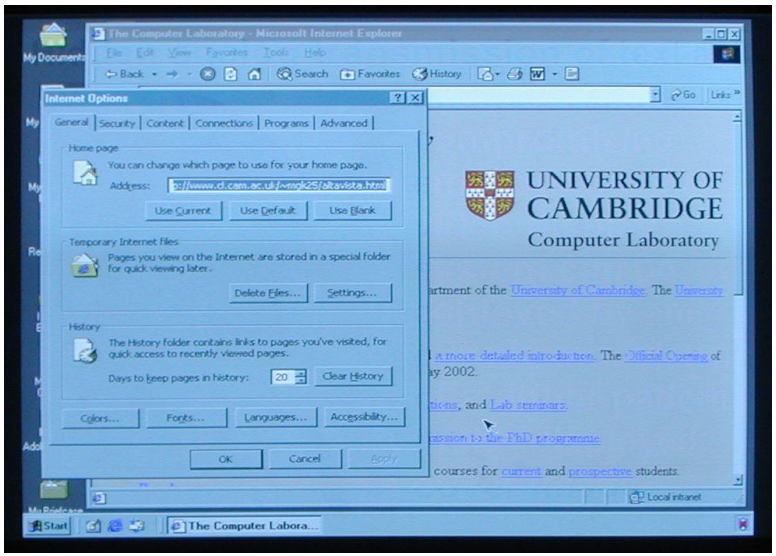
Characteristics:

- ⟶ Vertical lines doubled
- ⟶ Horizontal lines disappear (reduced to end points)
- ⟶ Glyph shapes modified, but still easily readable unaided

Pixel frequency: 50 MHz, IF bandwidth: 50 MHz, AM baseband sampling frequency: 500 MHz, measured peak e-field at 3 m: 46 dBµV/m, corresponds to 12 nW EIRP. [Kuhn, 2003]

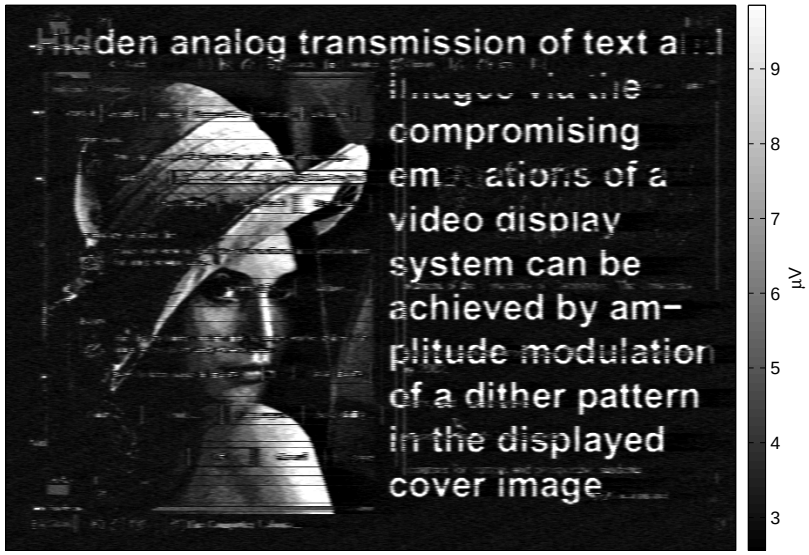
Steganographic transmission of images

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



Amplitude modulation of dither patterns

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

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

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

Filtered fonts as a protection measure

(1) The quick brown fox jumps over the lazy dog
(2) The quick brown fox jumps over the lazy dog
(3) The quick brown fox jumps over the lazy dog
(4) The quick brown fox jumps over the lazy dog
(5) The quick brown fox jumps over the lazy dog
(6) The quick brown fox jumps over the lazy dog
(7) The quick brown fox jumps over the lazy dog
(8)

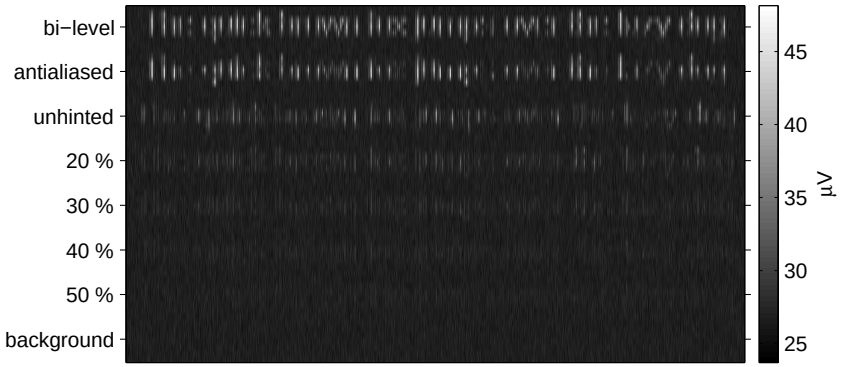
The above lines show (1) bi-level text, (2) anti-aliased text, (3) anti-aliased text without "hinting", (4–7) anti-aliased text lowpass filtered to remove to 20, 30, 40, and 50 % of the spectrum $[0, f_{\mathrm{p}}/2]$, respectively. Font: Microsoft's Arial (TTF), rendered at 12 pixels-per-em. [Kuhn, 2003]

Filtered fonts on the CRT screen

(1) The quick brown fox jumps over the lazy dog
(2) The quick brown fox jumps over the lazy dog
(3) The quick brown fox jumps over the lazy dog
(4) The quick brown fox jumps over the lazy dog
(5) The quick brown fox jumps over the lazy dog
(6) The quick brown fox jumps over the lazy dog
(7) The quick brown fox jumps over the lazy dog
(8)

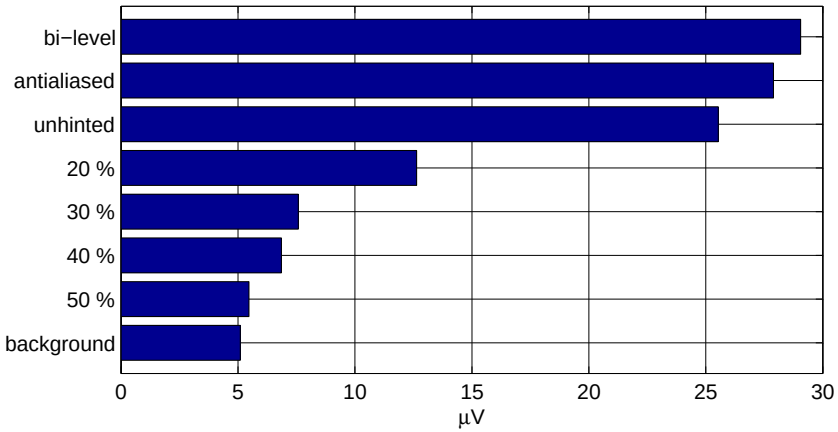
Received radio signal

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



Filtered fonts peak-amplitude comparison

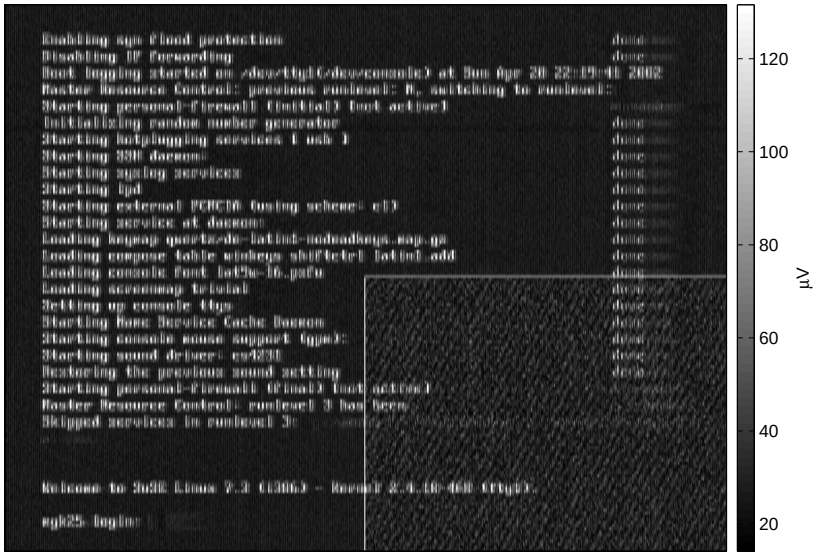
Peak voltages (antenna rms voltage equiv. at DC−free AM output)



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.

Eavesdropping on flat panel displays

350 MHz center frequency, 50 MHz bandwidth, 16 (1) frames averaged, 3 m distance



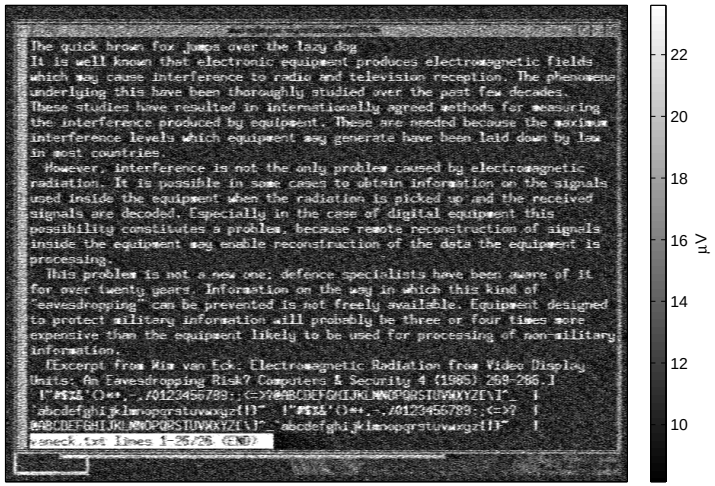
magnified image section

- ⟶ Horizontal lines intact (⟶ no analog video signal)
- ⟶ Horizontal resolution reduced
- ⟶ 100 µV signal amplitude at receiver input (rms equiv.)
- ⟶ 57 dBµV/m (50 MHz BW) field strength at 3 m distance
- ⟶ equivalent isotropic radiated power around 150 nW

Target display: Toshiba 440CDX laptop, 800×600@75Hz, $f_\mathrm{p} = 50$ MHz

Eavesdropping across two office rooms

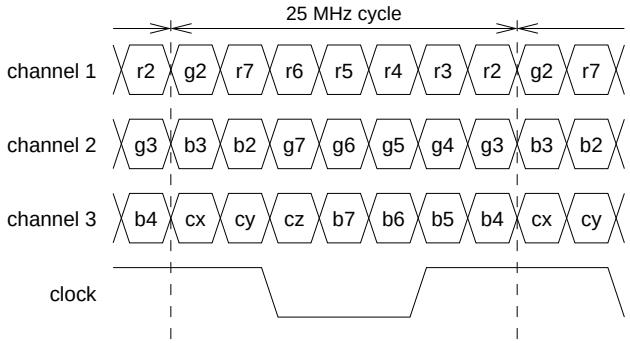
350 MHz, 50 MHz BW, 12 frames (160 ms) averaged



Target and antenna in a modern office building 10 m apart, with two other offices and three plasterboard walls (−2.7 dB each) in between. Single-shot recording of 8 megasamples with storage oscilloscope at 50 Msamples/s, then offline correlation and averaging of 12 frames.

FPD-Link – a digital video interface

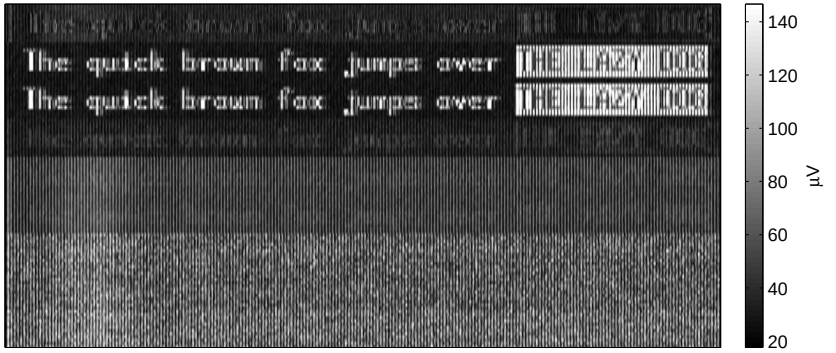
LCD module and video controller are connected in Toshiba 440CDX laptop by eight twisted pairs (each 30 cm long), which feed the 18-bit RGB parallel signal through the hinges via low-voltage differential signaling (LVDS, EIA-644).



FPD-Link chipset: NEC DS90CF581

Minimal/maximal reception contrast

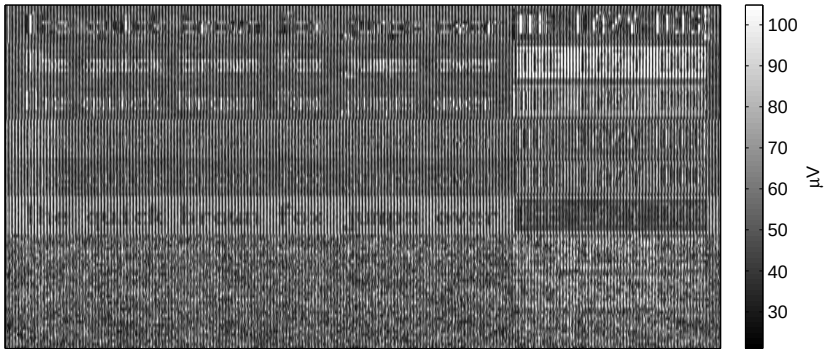
350 MHz center frequency, 50 MHz bandwidth, 16 frames averaged, 3 m distance



1: black on white text, 2: maximum-contrast bit patterns fg=010101 and bg=000000 in all channels, 3: same but out of phase across channels, 4–6: different attempts to find minimum-contrast colour combination by shifting edges between channels, 7–9: make the least significant bits random in each channel.

Only random bit jamming effective

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



Random LSB jamming

Random bits can be added to a text image to generate a phase-locked jamming signal that cannot be averaged away by an attacker. Considerations:

- ⟶ Foreground/background colors with equal number of bit transitions.
- ⟶ Randomize less significant bits of each color channel.
- ⟶ These random bits must *only* be changed when the text changes:
  - Changing the random bits continuously (like TV noise) would help the attacker to average away the jamming signal.
  - Not changing the random bits when the text changes would help the attacker to average away the text and obtain this way a copy of the random signal that can then be subtracted from the received signal.
- ⟶ Independent noise bits must be used for *each* occurrence of a character. Beware of glyph caches from which the same bitmap might be used several times.

Open research question: How to jam without leaking update rate of displayed text?

Structure of compromising video signals

Mathematical tools:

- ⟶ Fourier transform: time domain ↔ frequency domain
- ⟶ Convolution theorem: multiplication in time domain is convolution in frequency domain, and vice versa.
- ⟶ Sampling theorem: Sampled time-domain signal is periodic in the frequency domain, and vice versa.

Result:

- ⟶ Symmetric spectrum of digital 2-color video signal repeats itself at frequency intervals f_p
- ⟶ Amplitudes of the individual repetitions of the spectrum are predicted by the difference between the DFTs of the two color code words used.

⇒ Eavesdropping colors can be optimized to place signal energy into quiet part of UHF radio spectrum.

Details: M. Kuhn, Technical Report UCAM-CL-TR-577, 2003.

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 $P(t)$:

$$I(t) = \int_0^\infty v_\gamma(t - t')\, P(t')\, \mathrm{d}t'$$

- ⟶ 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?

Light sensors

Requirements:

- ⟶ very sensitive (to reduce preamp noise)
- ⟶ very fast (bandwidth comparable to $f_\mathrm{p}/2$, ideally >100 MHz or <5 ns rise and fall time)

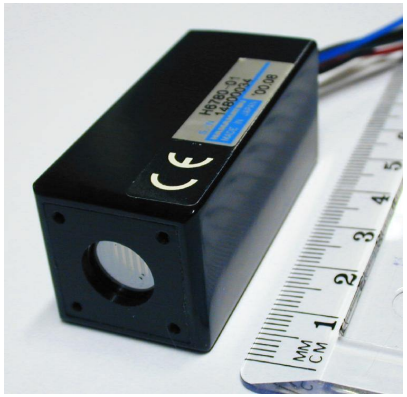
Options:

- ⟶ PIN photodiode (typical sensitivity 0.2–0.6 A/W, µs–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 $0.25 < U_\mathrm{c} < 0.9$ V adjusts radiant sensitivity to

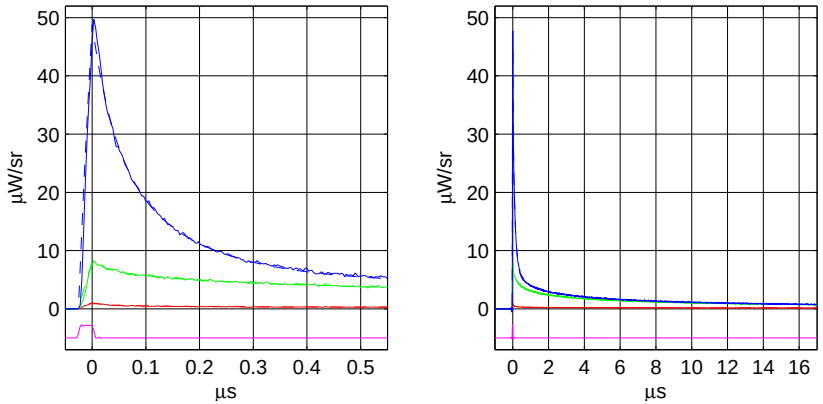
$$1.5 \times 10^5 \text{ A/W} \cdot \left(\frac{U_\mathrm{c}}{1 \text{ V}}\right)^{7.2}$$



Thanks to high internal gain no need for video pre-amplifier, allowing direct connection to 50 Ω DC input of digital storage oscilloscope.

Measured phosphor 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.

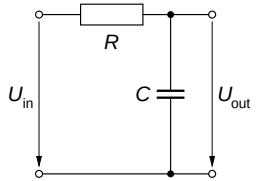
Modeling phosphor impulse responses

→ Exponential decay curve of a typical phosphorescent substance:

$$I_\mathrm{e}(t) = I_0 \cdot \mathrm{e}^{-\frac{t}{\tau}}$$

Note that this is for

$$\tau = \frac{1}{2\pi f} = RC$$



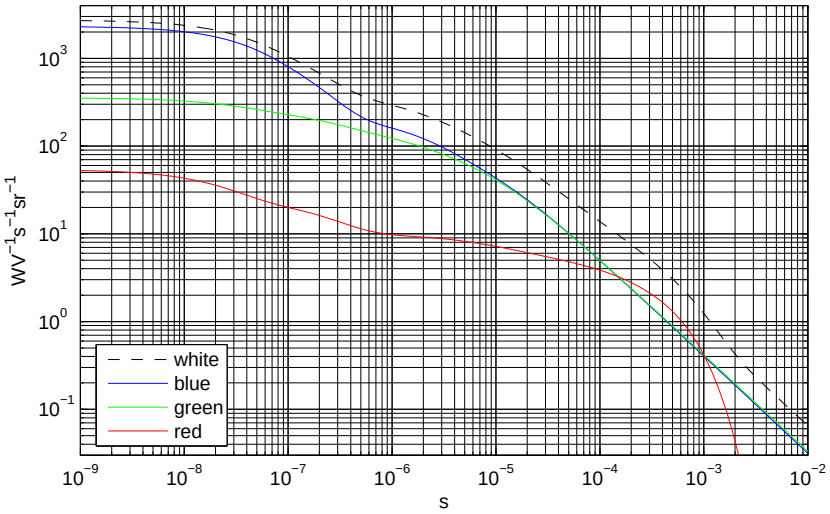
the impulse response of a first-order Butterworth low-pass filter.

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

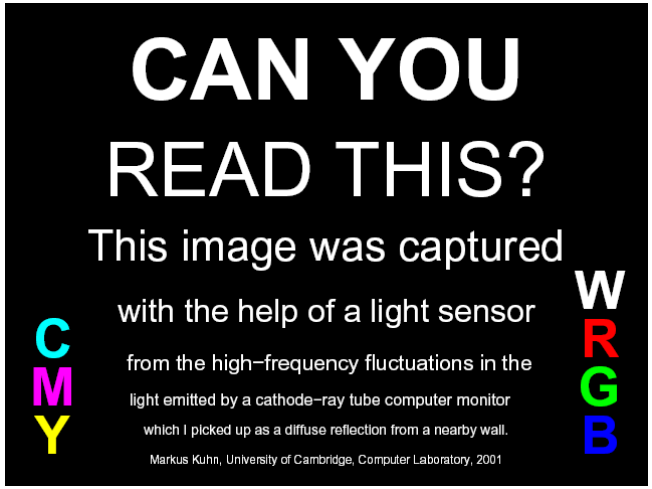
$$I_\mathrm{p}(t) = \frac{I_0}{(t+\alpha)^\beta}.$$

(Results in asymptotically straight line on loglog scale.)

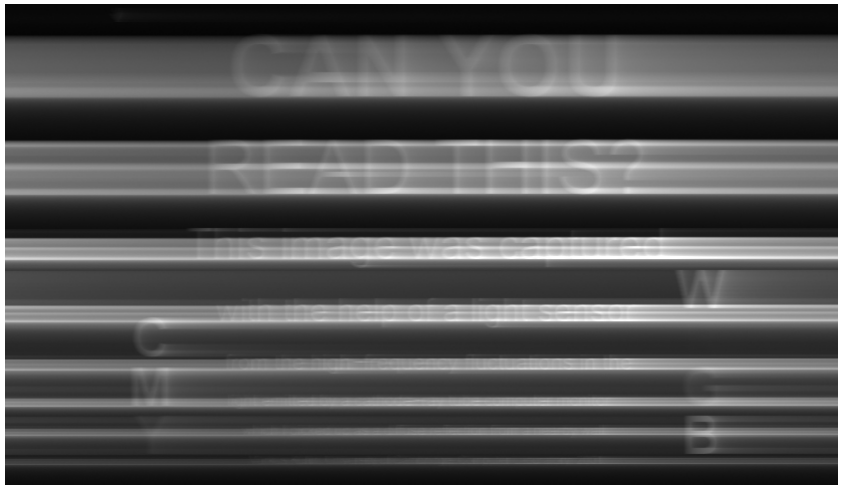
Double-log plot of reconstructed P22 impulse response



Test image shown on target monitor

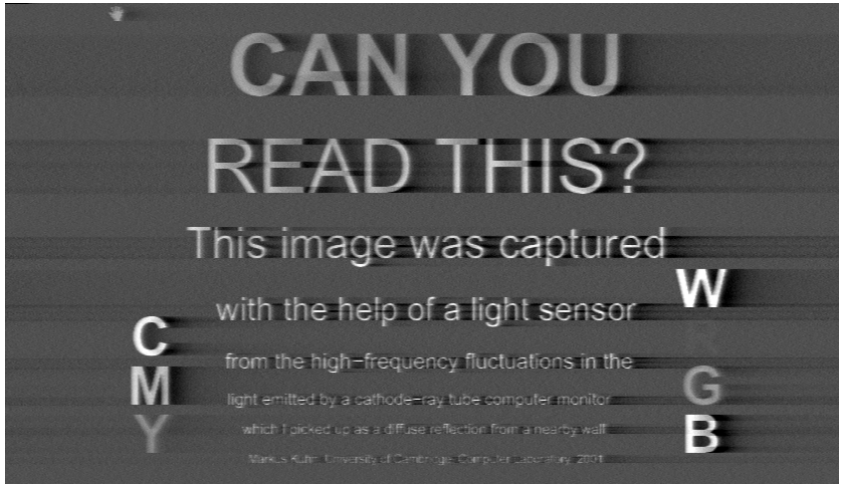


Rasterized raw signal from PMT



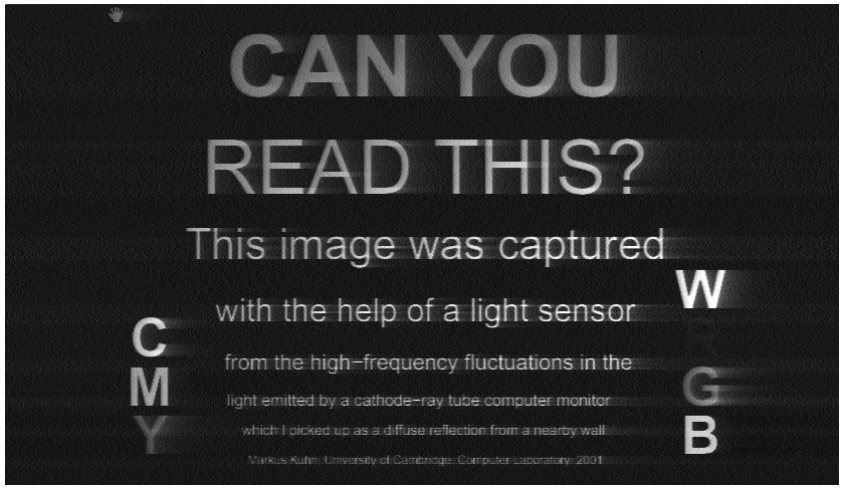
VESA mode 640×480@85 Hz, 8-bit sampled at 250 MHz, 256 frames (3.0 s, 753 MB) averaged, scaled to 0.1% saturation

High-pass filtering result



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

Deconvolution result



Deconvolution

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

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

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

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

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:

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

Other compromising emanations

New forms of compromising emanations are still being discovered:

Acoustic eavesdropping on keyboards

Like a drum changes its sound, depending on where it is hit, the main board of a keyboard is excitied into different modes of vibration, depending on the location of the key being hit. Asonov and Agrawal have demonstrated that it is practical to train a neural network to distinguish keystrokes based on this effect.

D. Asonov, R. Agrawal: Keyboard acoustic emanations. Proceedings 2004 IEEE Symposium on Security and Privacy, IEEE Computer Society, pp. 3–11.

Ultrasonic CPU emanations from PC motherboards

Shamir and Tromer have presented preliminary results that show that the run-time of certain cryptographic loops appears in the spectrum of microphone signals recorded near a PC motherboard. It appears as if the CPU current fluctuations are emitted by blocking capacitors or other power-supply componenets as acoustic and ultrasonic waves.

A. Shamir, E. Tromer: Acoustic cryptanalysis – On nosy people and noisy machines.
`http://www.wisdom.weizmann.ac.il/~tromer/acoustic/`

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