

Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations

Markus G. Kuhn and Ross J. Anderson
Computer Laboratory



<http://www.cl.cam.ac.uk/~mgk25/ih98-tempest-slides.pdf>

The History of Compromising Emanations

- MI5 used in the late 1950s compromising emanations of French and Russian embassy equipment in London for counter-intelligence operations
- First civilian discussion in the early 1980s; public awareness of VDU emanation threats after van Eck paper in 1985
- Further studies in 1990 by Smulders on RS-232 cables and Möller on VDUs
- US "Tempest" programme started in the late 1950s to study the problem and to define anti-emanation test procedures and standards
- All Tempest standards such as NACSIM 5100A (US) and AMSG 720B (NATO) are still classified and conforming equipment is export controlled
- Civilian EMI and safety standards (ISO/IEC, MPR, TCO) are not applicable
- Over 50 vendors supply multi-billion US\$ market, practically exclusively military, diplomatic and government agency customers

Tempest design principles are containment (shielding), source suppression and red/black separation, occasionally also jamming. Shielding can be done at the device, room or building level. Tempest shielding can fail easily (dirty gaskets, etc.) and requires periodic testing.

Compromising Emanation Test and Attack Techniques

- Signals of interest to eavesdroppers can be orders of magnitude weaker than signals that are of concern in EMC and RFI tests.
- Good directional antennas, HF taps to power and communication lines, periodic averaging and long-time cross-correlation increase SNR by orders of magnitude
- Especially dangerous are periodic emanations like video signals and signals with a well-known structure like printer output with fixed character sets, which allow maximum-likelihood pattern-recognition techniques to be used
- Trojans/viruses could generate periodic emanations over CPU and device activity
- Test procedures should not only include spectral energy limits, but also long-time cross-correlation between internal signals and broadband antenna and line-tap receptions
- Cross-correlation allows to distinguish programme branches, for instance DES execution in smartcards is recognizable as 16 signal repetitions
- Related risks are cross-talk between cables and devices as well as microwave-resonance eavesdropping

Broadcasting Shortwave Audio Tones with Monitors

Video Timing:

Pixel rate: $f_p = 95 \text{ MHz}$

Line rate: $f_h = f_p / x_t = 64.5 \text{ kHz}$

Frame rate: $f_v = f_h / y_t = 68.7 \text{ Hz}$

Pixel Time:

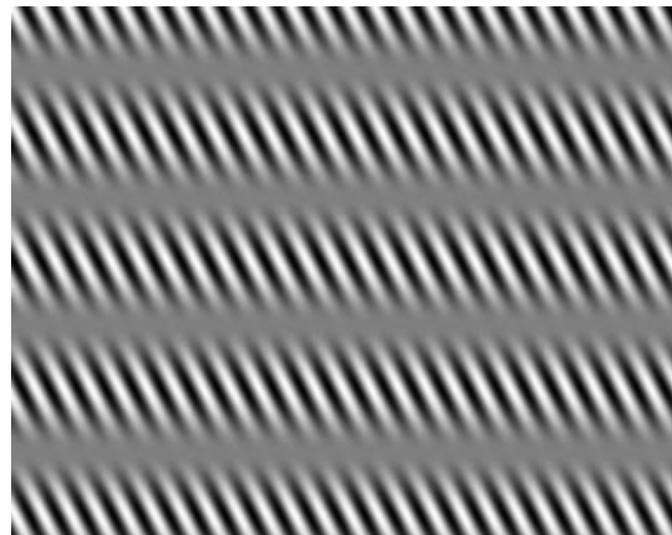
$$t = \frac{x}{f_p} + \frac{y}{f_h} + \frac{n}{f_v}$$

Amplitude Modulation:

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

with $A = \frac{255}{4}$ and $m = 1$.

Low-cost attack: Trojan screen saver, AM radio, cassette recorder, FSK demodulation using PC sound card.



300 Hz tone at 2.0 MHz AM



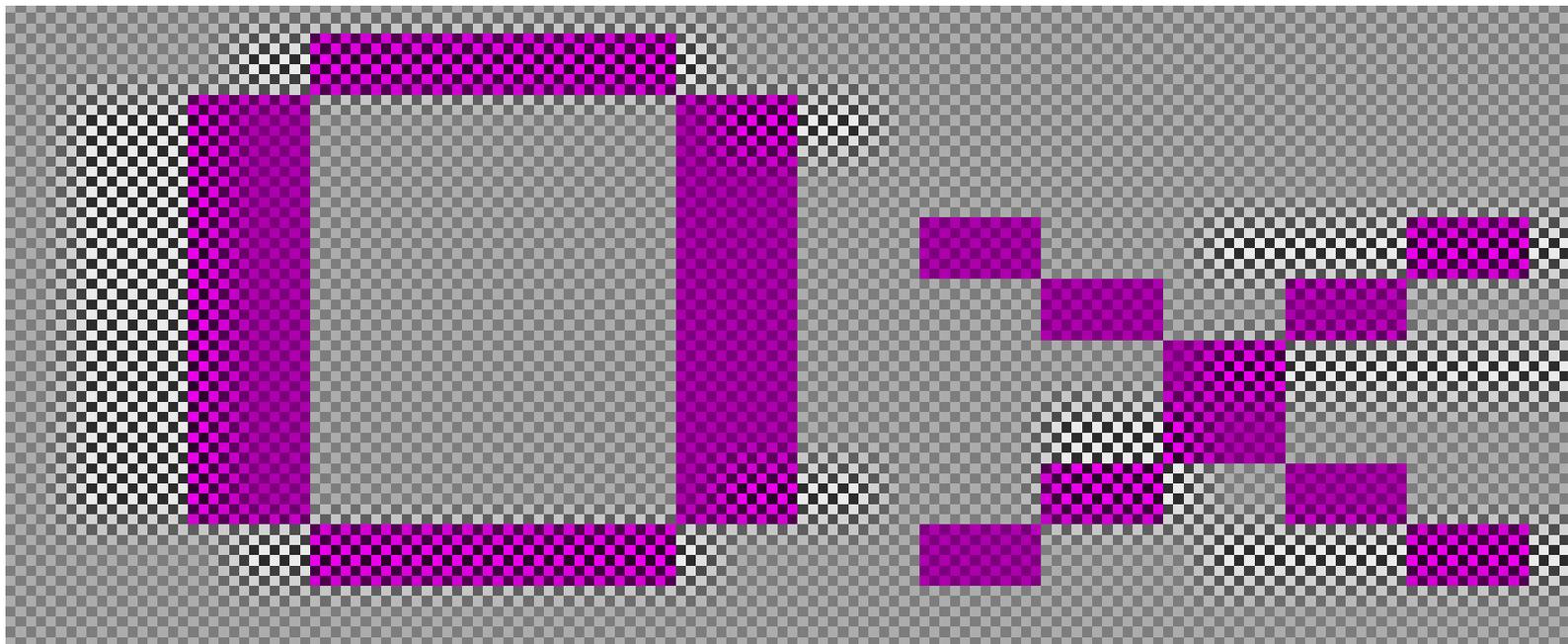
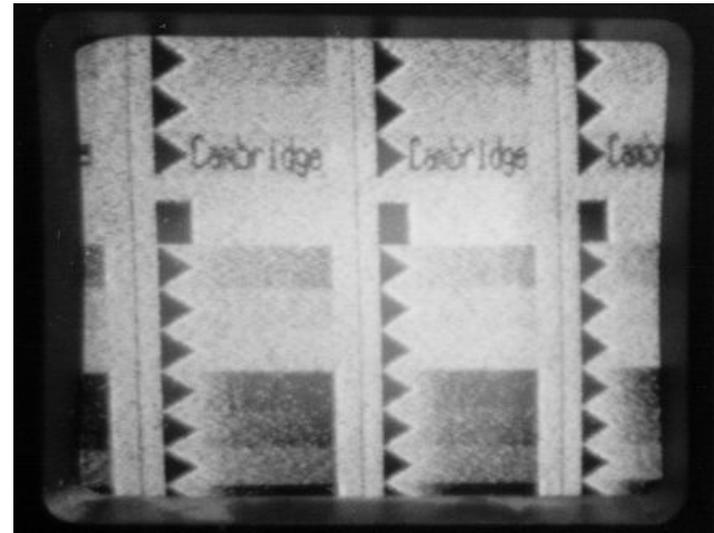
1200 Hz tone at 2.0 MHz AM

The DataSafe/ESL Model 400 Tempest Emission Monitor

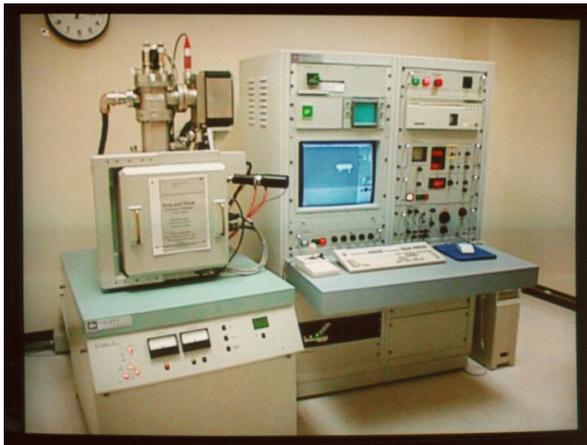


- basically a modified b/w TV receiver with manually adjustable sync pulse generators
- frame rates 40.0-99.9 Hz
- line rates 10-20 kHz -> ~1985 VDUs
- tunable from 20 MHz (60 μ V) to 860 MHz (5 μ V)
- 4 m folded dipole antenna
- better results with 0.2-2.0 GHz spiral log conical antenna
- 8 MHz bandwidth
- tests on iiyama Vision Master Pro17

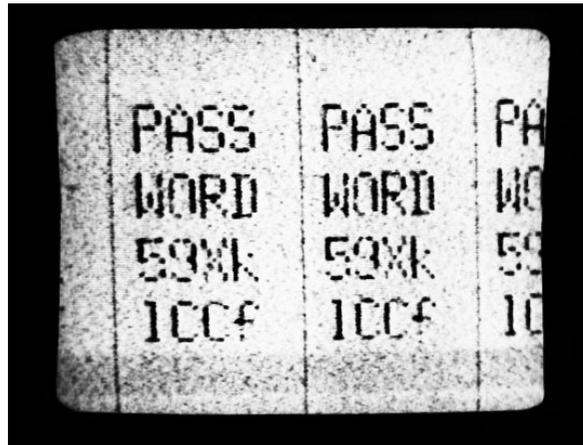
Broadcast Messages Hidden in Dither Patterns



Embedding Arbitrary Greyscale Images in Screen Content



Cover display seen by user



Emitted secret message



Emitted image

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

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

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

CRT luminosity $L = \text{const} \cdot V^\gamma$ for video voltage V . Equivalent luminosity of dither pattern with $\bar{V} = (\frac{1}{2}V_1^\gamma + \frac{1}{2}V_2^\gamma)^{1/\gamma}$. Inconspicuous dither embedding must preserve average luminosity. Exponent γ has to be replaced by lower $\tilde{\gamma}$ for chequered dither patterns (e.g., $\gamma = 2.0$ and $\tilde{\gamma} = 1.28$ for our monitor).

Broadband Transmission Techniques

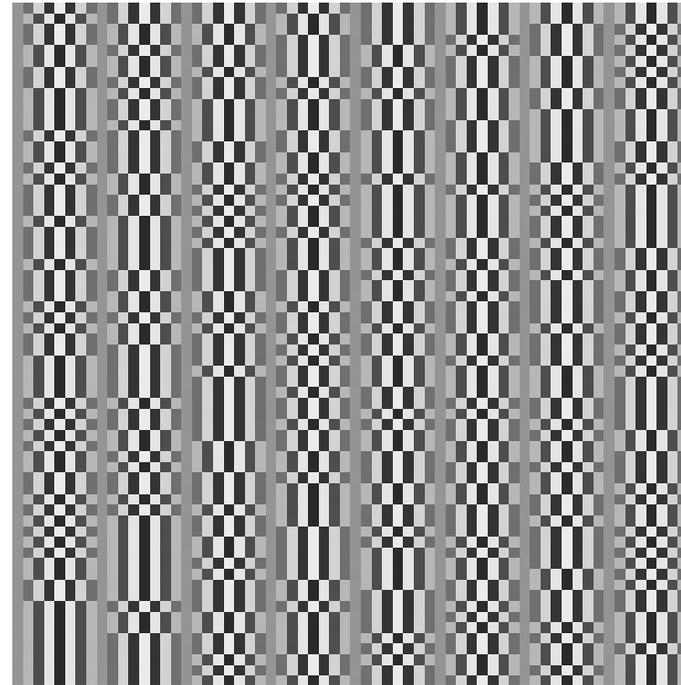
Embedding of visible text and images only for demonstration purposes and for low-cost attacks with modified TV sets.

Broadcasting software for professional receiver embeds direct-sequence spread-spectrum modulation style signal in image, which can be detected by a DSP receiver much easier in a noisy environment.

Advantages:

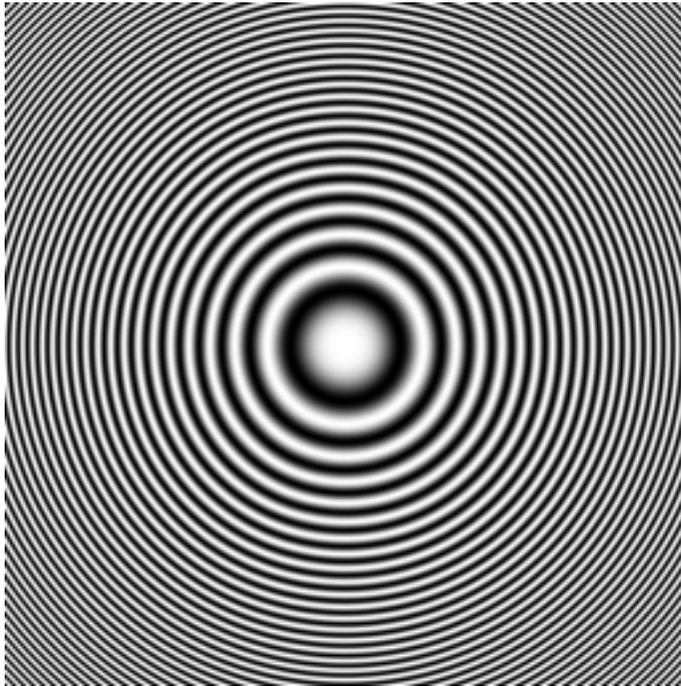
- Better range, higher data rates
- Less screen area needed (e.g., toolbar)
- Automatic acquisition easier

Potential commercial application: Software broadcasts license number over VDU to allow the operation of software-piracy detector vans.



Phase modulated 512-bit PRBS
hidden as a 16x16 mm uniform field

Frequency Response of Monitor Eavesdropping



Zoneplate frequency test signal on computer monitor $[\cos(x^2+y^2)]$ has local frequencies proportional to coordinates



Eavesdropping receiver response is restricted mostly to the upper 30% of the horizontal spectrum

Filtered Fonts as an Eavesdropping Protection



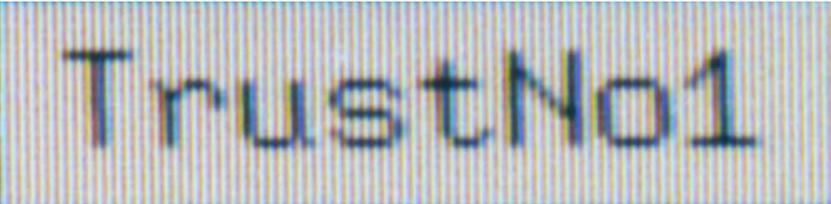
TrustNo1

Normal display font



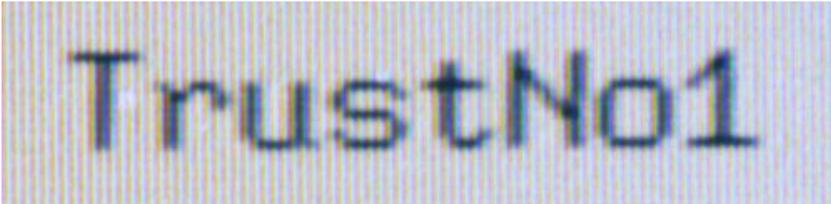
TrustNo1

Font with top 30% of horizontal spectrum attenuated to reduce emanations



TrustNo1

Screen appearance of normal font
(21×5 mm)



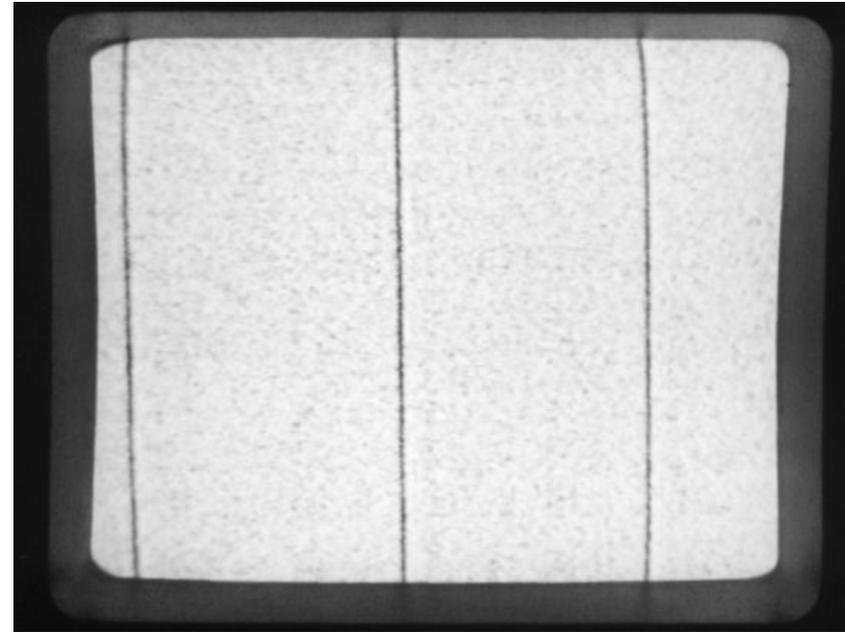
TrustNo1

Screen appearance of filtered font

Filtered Fonts on the Eavesdropping Monitor



Normal display font



Screen content with top 30% of horizontal spectrum attenuated

While practically no difference between the fonts can be perceived by the user on a computer monitor, the filtered text disappears from our eavesdropping monitor even with the antenna very close to the monitor, while the normal text can be received clearly.

Other Possible Tempest Software Countermeasures

Keyboard

Keyboard-microcontroller scan loop is periodic and dependent on pressed key.
Introduce random delay and random scan order.

Harddisks

Idle Harddisks continuously read and amplify the same track.
Move head to track with unclassified data when request queue is empty.

Variable Fonts

A fixed known font simplifies automatic character recognition by eavesdropper.
Use font with small random variations of glyph shapes.

How Expensive are Compromising Radiation Attacks?

Cost in 1980:

In a government signals agency, three HF engineers work six months to design and set up an eavesdropping post in a building next to an embassy to observe several data terminals and matrix printers. Custom built antennas, wideband receivers and analog processing units have to be designed specifically for the observed devices.

Cost in 2010:

Graduate student with background in digital signal processing buys for 1000 US\$ a HAM software radio, in which a 3-GIPS DSP-array processes directly a 20 MHz bandwidth IF signal. She makes some sample recordings, experiments with MATLAB to find suitable filters and detectors, uploads those into the high-speed DSPs in the software radio and can show an eavesdropping demonstration after two weeks of experimentation. Sophisticated Tempest DSP libraries become freely available for various software radios and targets.

Conclusions

- Interesting field of study, mostly unexplored in the open literature
- Problem will not go away quickly and might get worse due to
 - High cost and difficulty of physical shielding
 - Increasing clock frequencies
 - Arrival of low-cost universal software receivers
- Software can make a difference, this is not just an RF engineering problem
- Attacks with broadcasting malware possible
- Some protection with Soft Tempest fonts and other software measures possible
- Software license enforcement is one interesting commercial application