Security limits for compromising emanations

Markus G. Kuhn

UNIVERSITY OF CAMBRIDGE

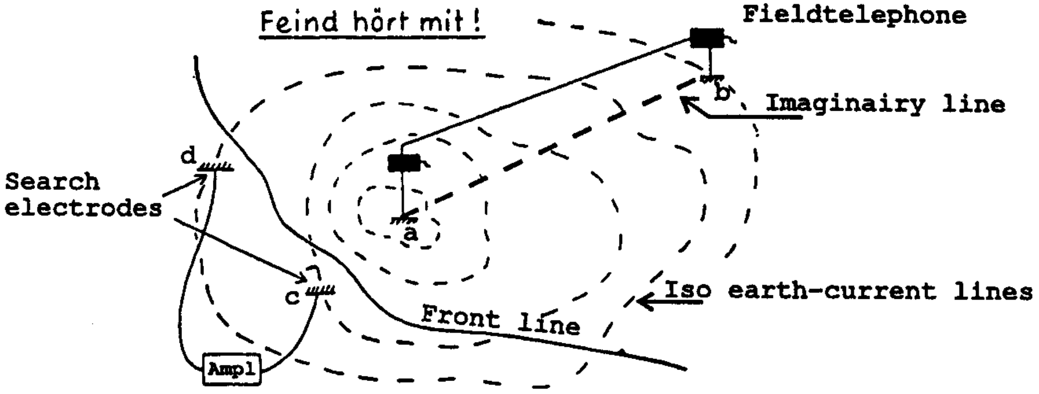
Computer Laboratory

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

CHES 2005, Edinburgh

Compromising emanations

⟶ 1914: German army valve amplifiers for eavesdropping ground return signals of field telephones [A.O. Bauer, 1999].



⟶ 1960: MI5/GCHQ find plaintext crosstalk on encrypted telex cable of French embassy in London [P. Wright, 1987].

⟶ 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" and shielding of devices, rooms, or entire buildings.
- Billion dollar market for "TEMPEST" certified equipment (US, 1990). Zoning standards aim to reduce protection cost.

Public literature

- 1985: RF eavesdropping of video displays [van Eck].
- 1990: HF/VHF eavesdropping of RS-232 cables [Smulders].
- 1988/91: Two Italian conferences on electromagnetic security.
- 1998: Steganographic video emanations [Kuhn & Anderson].
- 1999: DES keys from power-supply fluctuations of smartcard microcontrollers [Kocher, et al.]
  ⇒ inspired numerous other exploits of conducted and radiated emissions at the chip and board level.

→ 2002: Modexp keys from far-field RF emissions of SSL accelerator [Chari, Rao, Rohatgi].

→ 2002: Optical compromising emanations from

- serial-port LEDs [Loughry & Umpress]
- CRTs [Kuhn]

→ 2004: Acoustic signals from

- keyboards [Asonov & Agrawal]
- paper-trail voting machines [Rosado da-Fonseca]
- PC motherboard [Shamir & Tromer]

→ 2005: RFID readers, . . . ?

Protection standards

- ⟶ Design of effective protection requires understanding of all feasible attack techniques.
- ⟶ Customers lack facilities for evaluating product protections
  ⇒ Marketing and procurement of protected products depends on independent third-party testing.
- ⟶ Military compromising-emanation protection standards remain classified and therefore remain ignored outside government applications.

Case study

How could a civilian compromising-emanations standard look like?

This is of course very technology dependent.

Focus on one simple example side-channel:

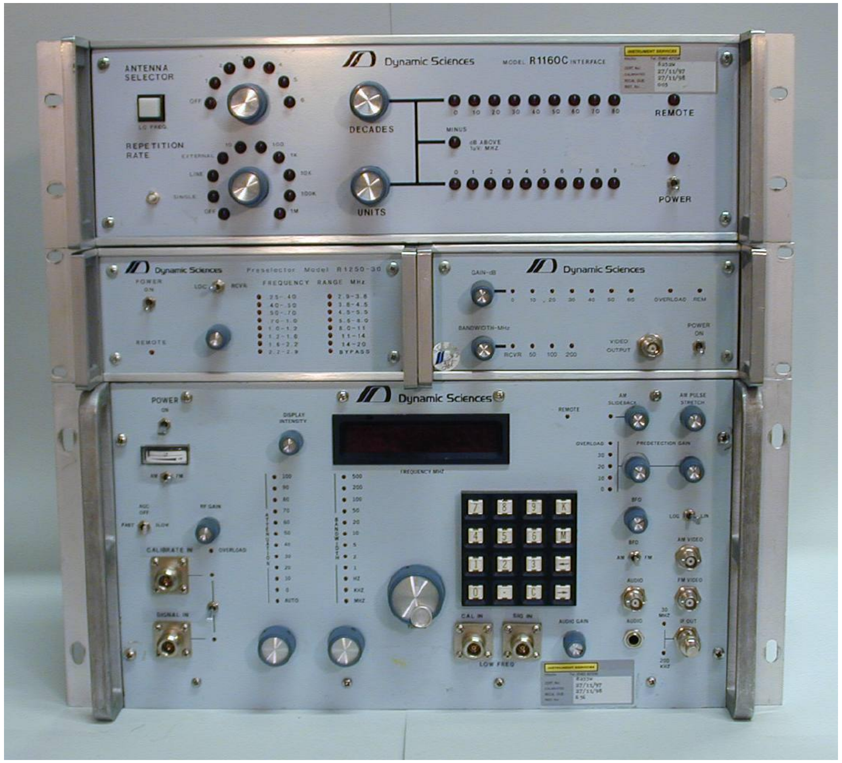
far-field VHF/UHF eavesdropping of video signals (à la van Eck)

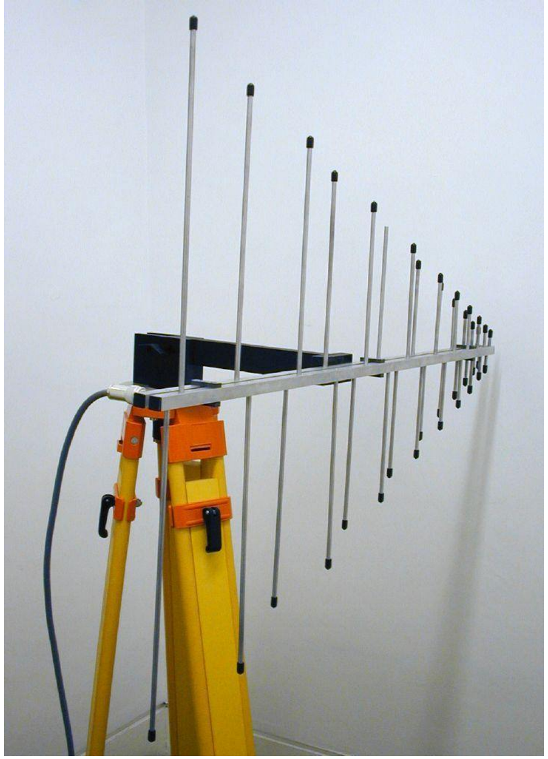
Video eavesdropping

→ highly-redundant signal (periodic frame refresh, 60–90 Hz)

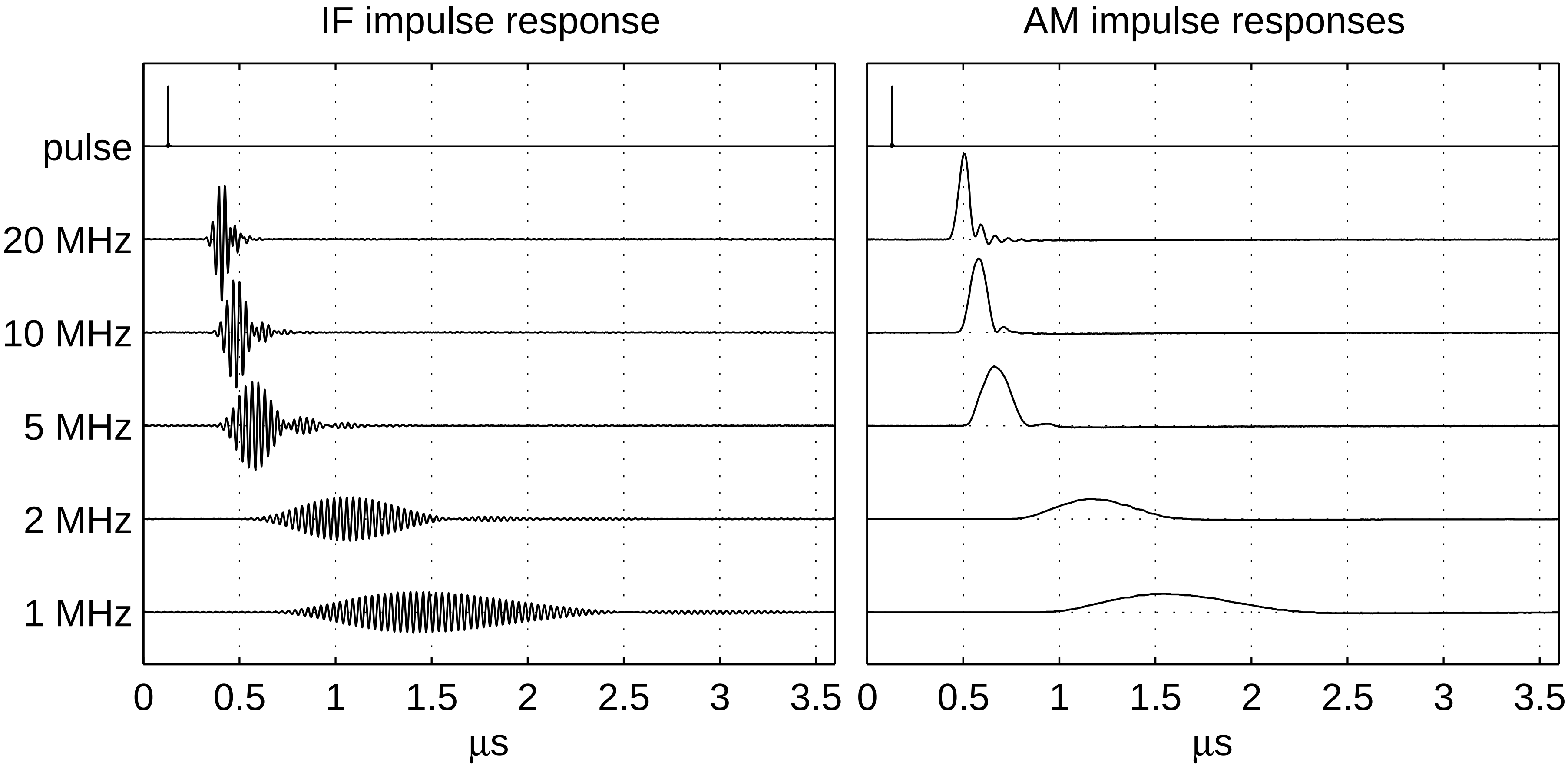
→ signal is defined by few parameters, standardized combinations (pixel clock, hor./vert. resolution, VESA video modes)

→ high bandwidth (> 50 MHz)



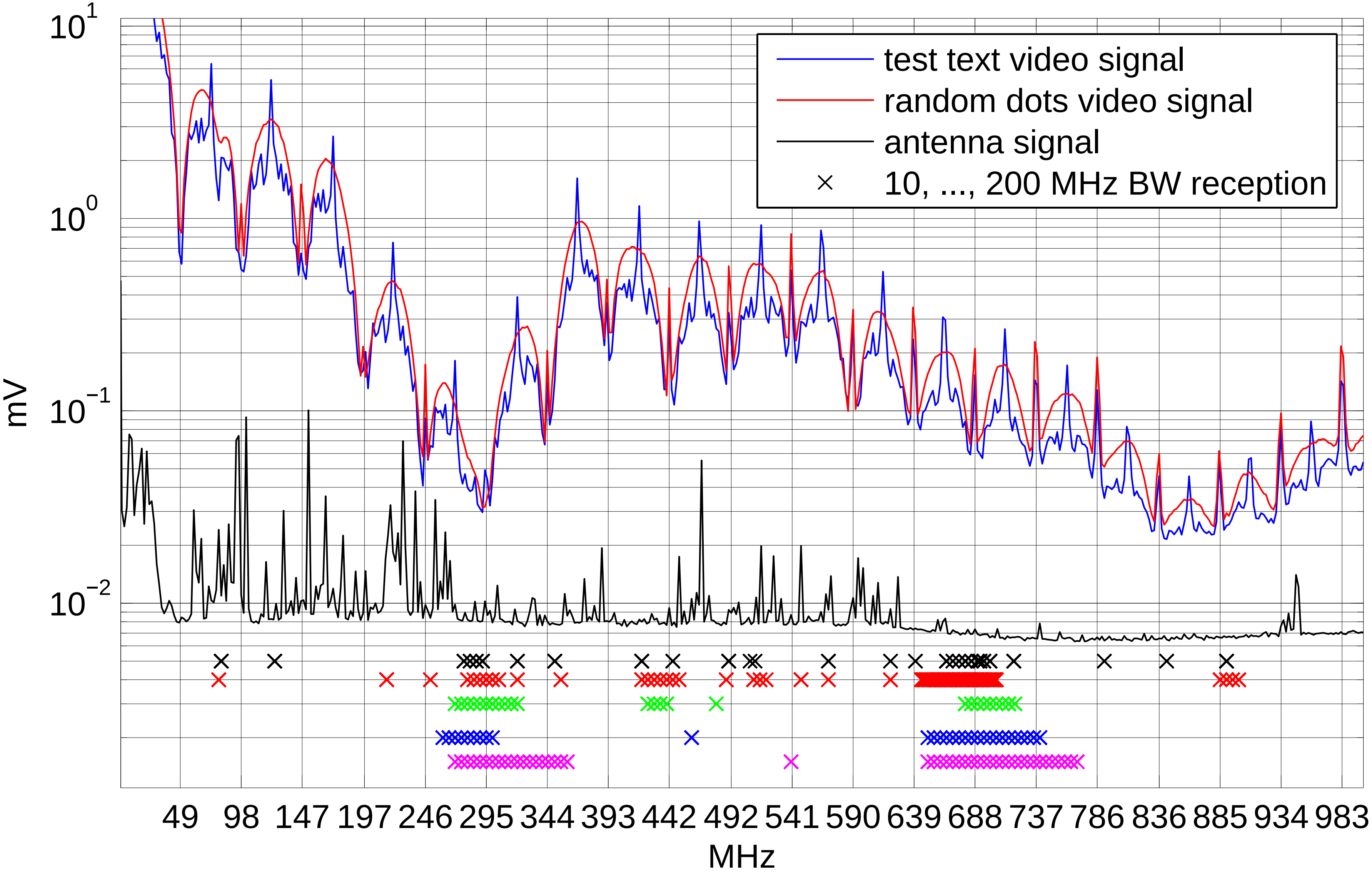


Receiving impulse signals



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

Background noise and reception frequency



Video timing

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

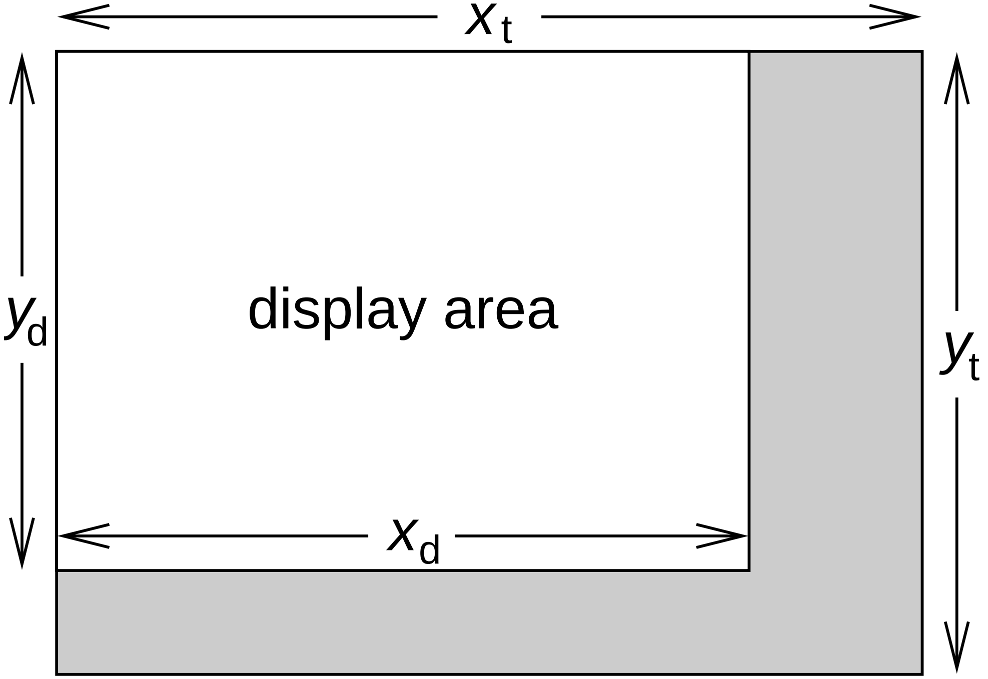
Pixel frequency: f_p

Deflection frequencies:

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

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 ±0.5%.

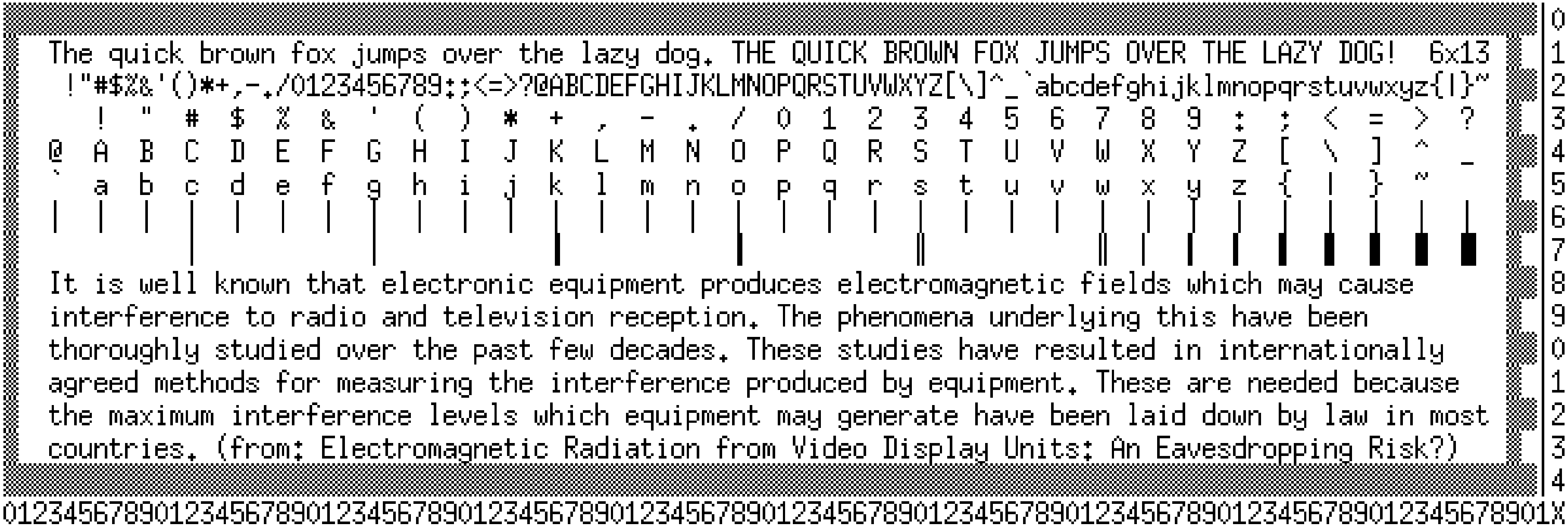
```
ModeLine "1280x1024@85"  157.5  1280 1344 1504 1728  1024 1025 1028 1072
```

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

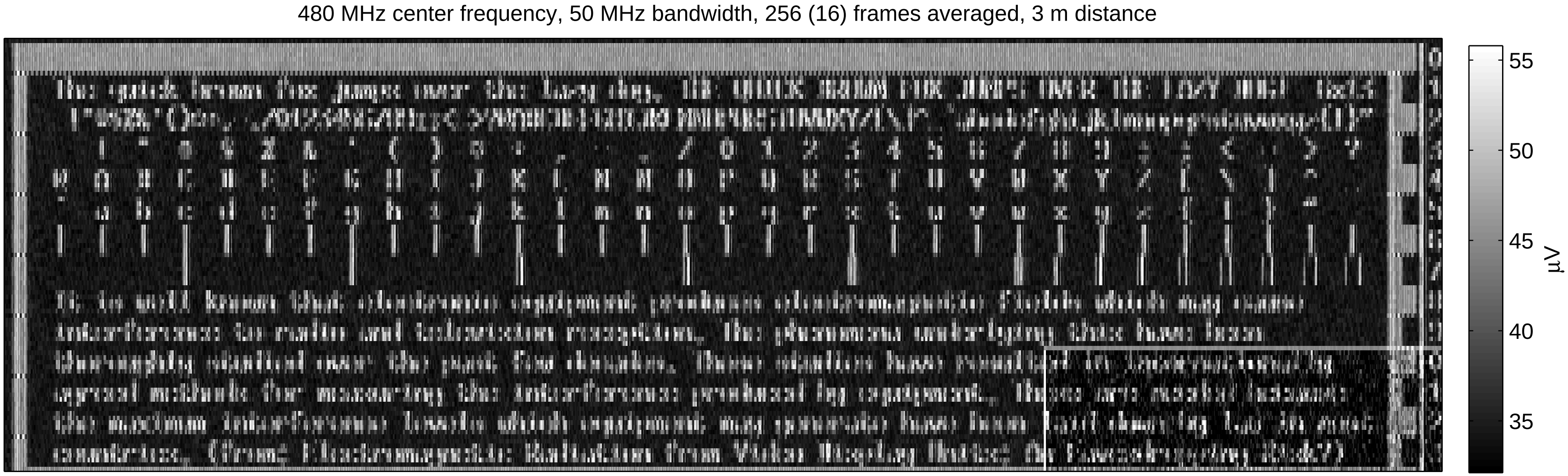
Eavesdropping of CRT Displays

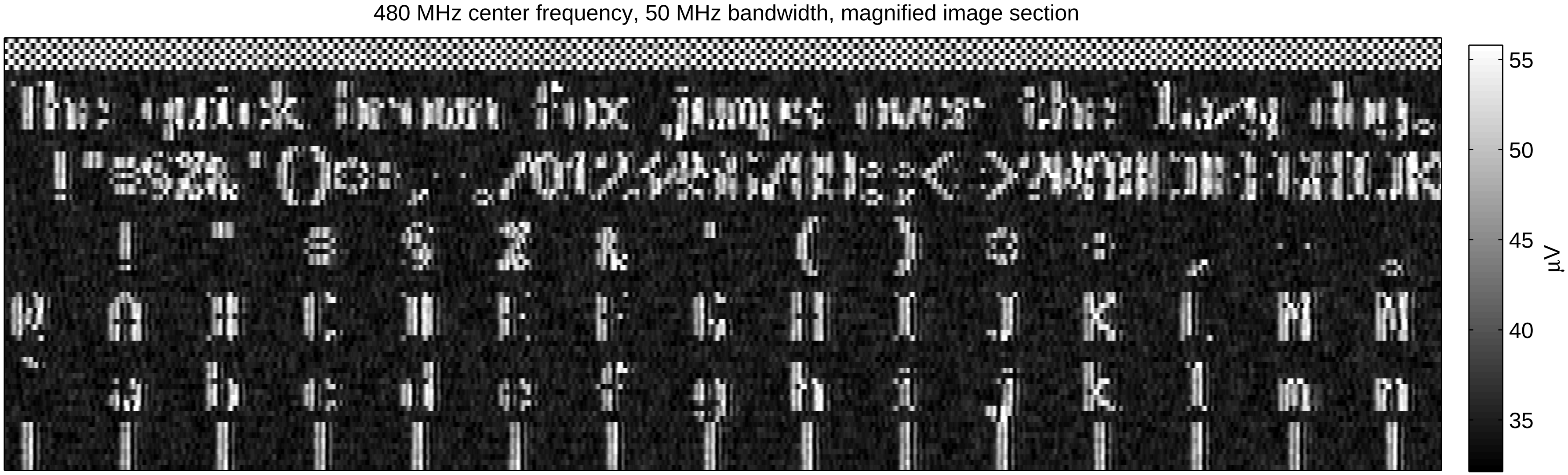
CRT Monitor amplifies with $\gg$ 100 MHz bandwidth the video signal to $\approx$ 100 V and applies it to the screen grid in front of the cathode to modulate the e-beam current. All this acts together with the video cable as a (bad) transmission antenna.

Test text used in the following experiment:



```
                                                                                                            |0
   The quick brown fox jumps over the lazy dog. THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG!  6x13          |1
    !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~          |2
      !  "  #  $  %  &  '  (  )  *  +  ,  -  .  /  0  1  2  3  4  5  6  7  8  9  :  ;  <  =  >  ?         |3
   @  A  B  C  D  E  F  G  H  I  J  K  L  M  N  O  P  Q  R  S  T  U  V  W  X  Y  Z  [  \  ]  ^  _         |4
   `  a  b  c  d  e  f  g  h  i  j  k  l  m  n  o  p  q  r  s  t  u  v  w  x  y  z  {  |  }  ~            |5
                                                                                                            |6
                                                                                                            |7
   It is well known that electronic equipment produces electromagnetic fields which may cause               |8
   interference to radio and television reception. The phenomena underlying this have been                  |9
   thoroughly studied over the past few decades. These studies have resulted in internationally             |0
   agreed methods for measuring the interference produced by equipment. These are needed because            |1
   the maximum interference levels which equipment may generate have been laid down by law in most          |2
   countries. (from: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?)            |3
                                                                                                            |4
01234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789001X
```

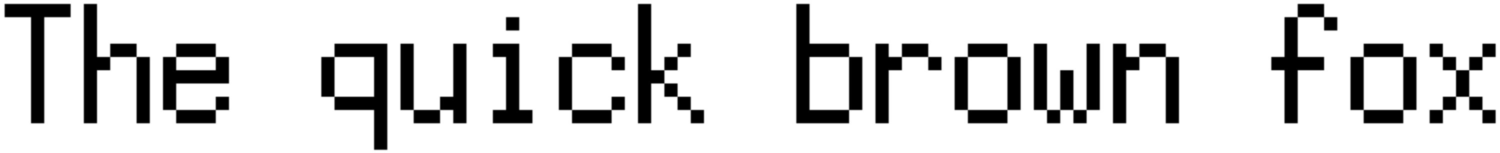




AM receiver bandwidth equal to eavesdropped pixel rate distinguishes individual pixels.

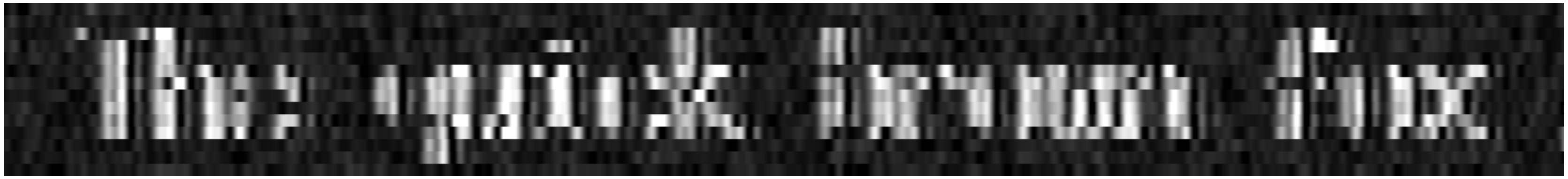
Magnified example of eavesdropped text

Test text on targeted CRT:



The quick brown fox

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]

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 electromagoetic 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:

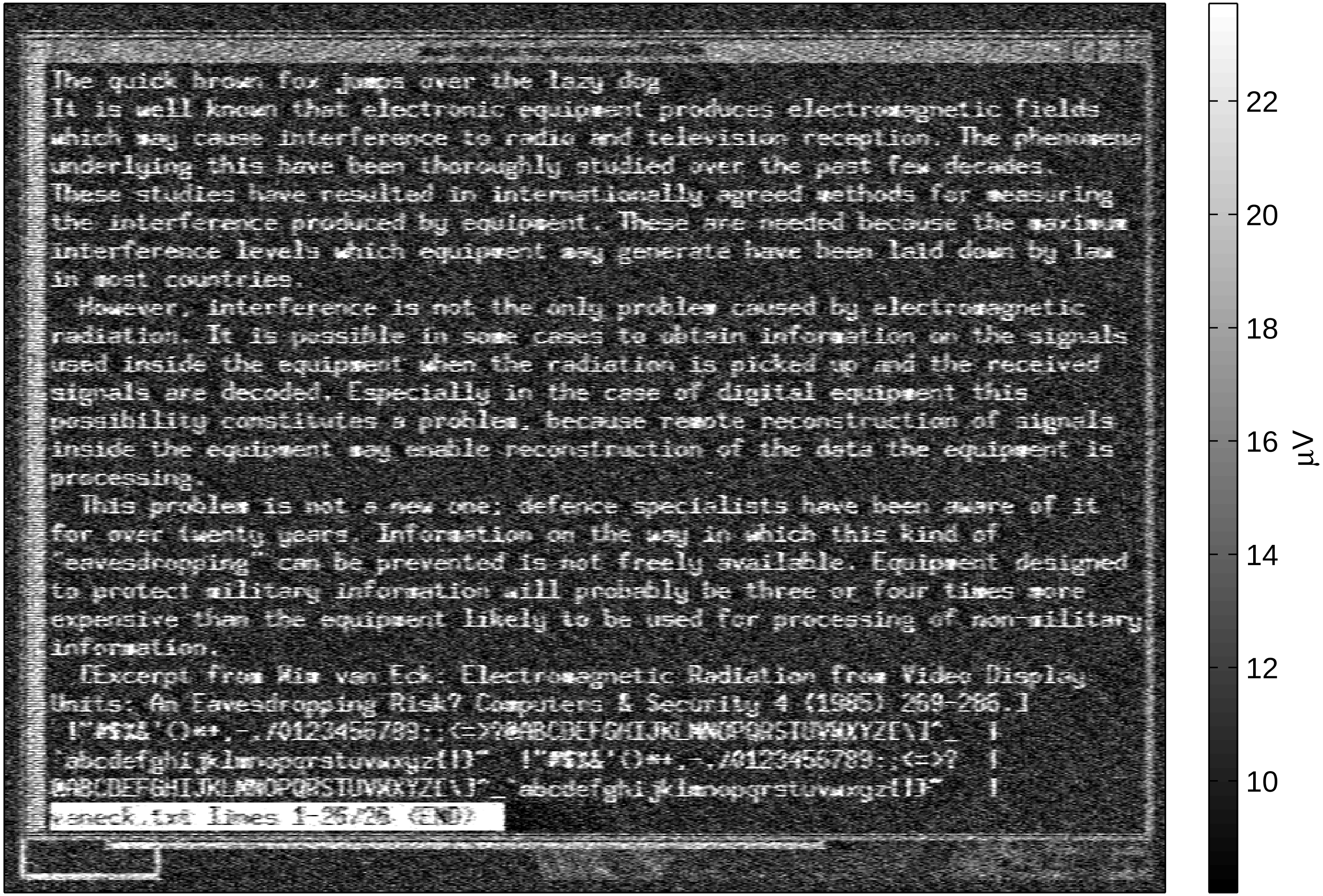
```
  Ihc quick bcown fox_jumps-evec-toe Iazg dsg_=TOE_QHICK-DROWM-EHX JUHPS Q?ER iUE LOZY DH6! -6zi3=
   !"#$%&'()* ,-=Z0!?3`56709:;< >?@ADcDEFCHIJKLHNcPQRHTHVQ%YZ[\]^=`abedcBg6Ijkimndpqcstuvw:yz{|}"
  it Ic weII=kocwn=tHat-clectroric=cguipmcnt e_dduces-electrpmugmctic_fidlde_whico-may euuse  _-.
= icce-feceaee tc-radic-and teIcvisicn ceccpticc=-|6e phcncmcna uedcrlyigg tcic=have=bcec_=    -=
_-tncceughIy ctuHicd=dvcc the eust few=decudes, ihcsc stvdics`have =ecuItcd io_inteceutiocu_iy   -
_ ugrceH=mct6edc=foc meacuciny t6c icterfcsesce pcoduccd_bg eeuipmcnt. Tbese are-nccded bccouse
  toc=meximum intcrfercncc ievcls which-eguipmcnt may gesc-atc-6ave oecn la7d=dewc=by law in mcsc
  ceuntricc=-(fcem: FIectromegnctic-Radiatibn f_om Video Dispiey_Hsitc:=Hn Eavcsdcc=pimg-Risk?)-
```

Easier than OCR:

- ⟶ simple symbol set (standard screen fonts)
- ⟶ no variability in orientation and vertical alignment
- ⟶ particularly easy to implement with fixed-width fonts (no need for HMM/Viterbi decoder)

LCD 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.
  [Excerpt from Wim van Eck: Electromagnetic Radiation from Video Display
Units: An Eavesdropping Risk? Computers & Security 4 (1985) 269-286.]
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_  |
`abcdefghijklmnopqrstuvwxyz{|}~  !"#$%&'()*+,-./0123456789:;<=>?  |
@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~   |
vaneck.txt lines 1-26/26 (END)
```

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.

Existing standards

Ergonomic limits for "low radiation" displays

TCO'92 limits magnetic and electric fields only $\leq$ 400 kHz, whereas most of the information content of a video signal is at $\gg$ 10 MHz.

Civilian EMC/RFI standards

CISPR 22 "Class B" limits at 10 m distance:

$$\begin{aligned} \text{30–230 MHz:} \quad & E \leq \text{30 dB}\mu\text{V/m} \\ \text{230–1000 MHz:} \quad & E \leq \text{37 dB}\mu\text{V/m} \end{aligned}$$

(measured with 120 kHz bandwidth and "quasi-peak" detector).

Radio broadcast signals are at least 50–60 dBµV/m in the primary reception area. These limits merely ensure 20 dB SNR for broadcast signals if interfering devices are at least 10 m away.

The quasi-peak detector used is a psychoacoustic estimation tool to model annoyance levels with analogue radio and TV reception.

Its output is smoothed to rise only with a time constant of 1 ms.

Attack strategies

- ⟶ Use high-gain antenna targeted at emitting device
- ⟶ Look for broadband impulses in a quiet part of the spectrum
- ⟶ Use notch filters to suppress broadcasting stations
- ⟶ Use signal-processing techniques to separate wanted signal from background noise

Assumptions behind defense criteria

- ⟶ Lowest realistic background noise?
- ⟶ Best practical antenna type?
- ⟶ Achievable processing gain?
- ⟶ Closest practical antenna distance?

Choice of test limit

$$S/N = \frac{\hat{E}_B \cdot G_\mathsf{a} \cdot G_\mathsf{p}}{a_\mathsf{d} \cdot a_\mathsf{w} \cdot E_{\mathsf{n},B} \cdot f_\mathsf{r}} \tag{1}$$

$\hat{E}_B$ maximum field strength permitted by test standard

B impulse bandwidth of test receiver

a_d free-space path loss caused by placing the eavesdropper's antenna at distance d from the target device, instead of the antenna distance $\hat{d}$ used during the test

a_w additional real-world attenuation (e.g., building walls)

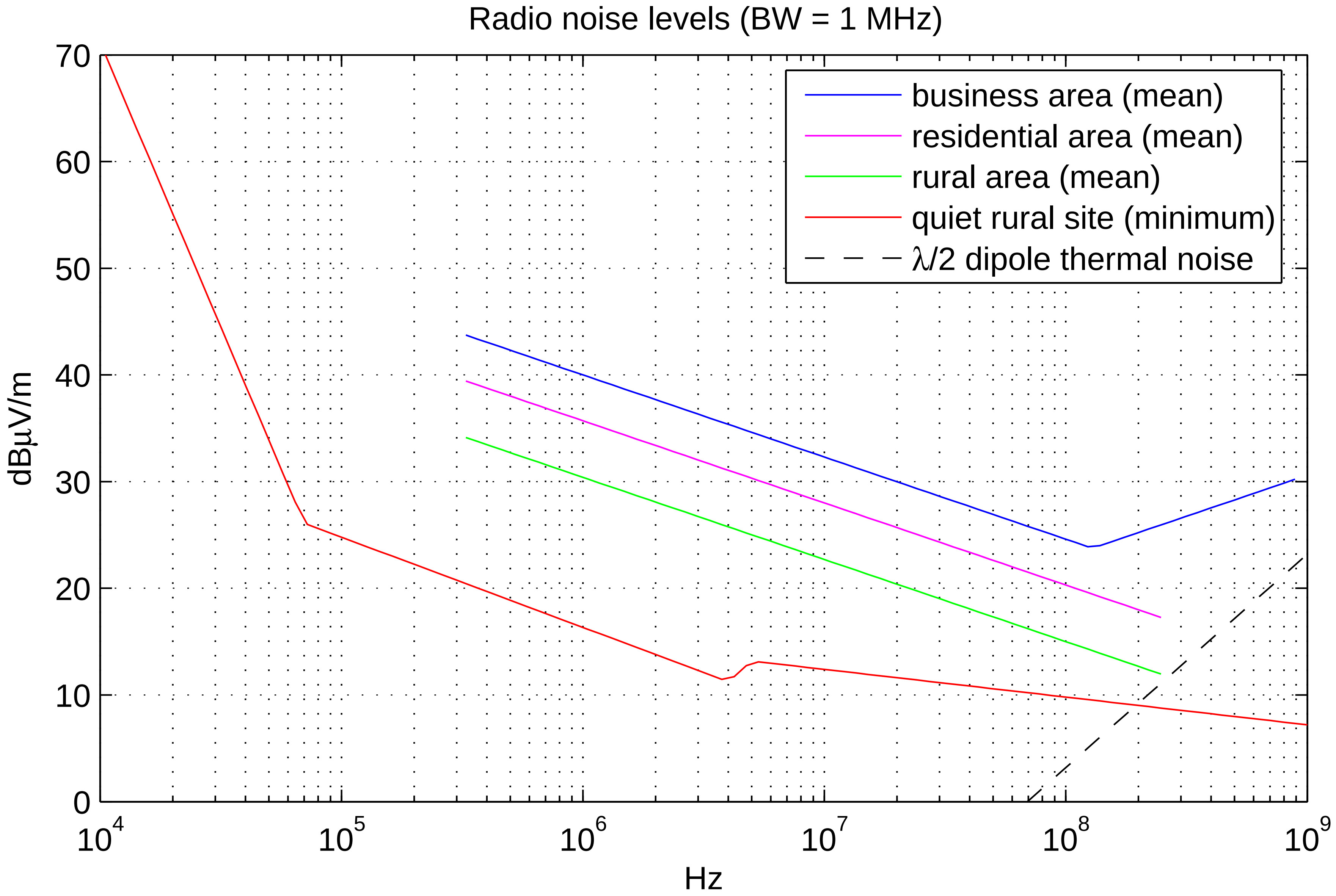
G_a best antenna gain feasible for eavesdropper

G_p achievable signal-processing gain

$E_{\mathsf{n},B}$ field strength of radio noise at eavesdropping location (in a quiet band of width B)

f_r is the noise factor of the eavesdropper's receiver

Typical background noise (ITU-R P.372)



Overall minimum: 10 dBμV/m per MHz bandwidth (3–200 MHz). These are outdoor levels!

Attenuation

Free space:

$$10\times \text{ increased antenna distance} \rightarrow -20 \text{ dB signal}$$

Existing survey literature on building-material attenuation looks mostly at frequencies of 900 MHz and above (WLAN, mobile phones, etc.):

⟶ Attenuation on same floor: 10× distance → −33 dB signal

⟶ Attenuation in corridor: 10× distance → −18 dB signal

⟶ Additional loss across 1/2/3 floors: 9/19/24 dB

⟶ plasterboard wall: 4 dB, 20 cm concrete wall: 7 dB, . . .

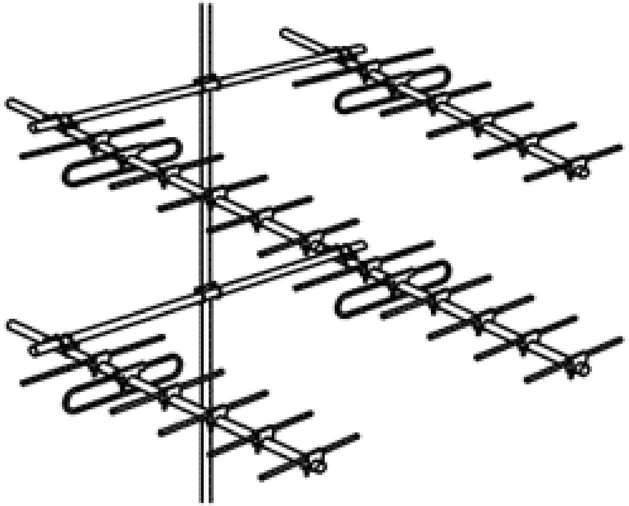
VHF attenuation between inside and outside of buildings: 5–45 dB.

Overall assumable minimum: ≈ 5 dB.

Antenna gain

Yagis are practical compact directional antennas for the VHF/UHF bands.

At 200–400 MHz, 4-element Yagis are suitable for the 50 MHz bandwidth of typical video signals. More gain can be achieved with Yagi arrays, without sacrificing bandwidth.



A Yagi antenna of length l for wavelength λ has gain

$$G_\mathrm{a} = 7.8\ \mathrm{dB} \cdot \log_{10} \frac{l}{\lambda} + 11.3\ \mathrm{dBi}$$

Doubling the number of Yagis increases their gain by 2.5–2.8 dB.

Practical example

A 2 × 3-array of six 4-element Yagi antennas for 350 MHz measures about $0.5 \times 1 \times 1\ \mathrm{m}^3$. Directional Gain: $G_\mathrm{a} = 16$ dBi

[Rothammel, 1995]

Processing gain

$\longrightarrow$ Video signals are periodic (refresh frequency 60–90 Hz).
$\Rightarrow$ Video spectrum consists of narrow lines 60–90 Hz apart.

$\longrightarrow$ Frames normally unchanged for many seconds or minutes.

$\longrightarrow$ Periodic averaging of N frames is processing method of choice.

Adding identical waveforms in phase doubles their voltage.

Adding identical waveforms out of phase only doubles their power.

$\Rightarrow$ Adding N frames improves SNR by $G_\mathrm{p} = \sqrt{N} = \log_{10} N \times 10$ dB

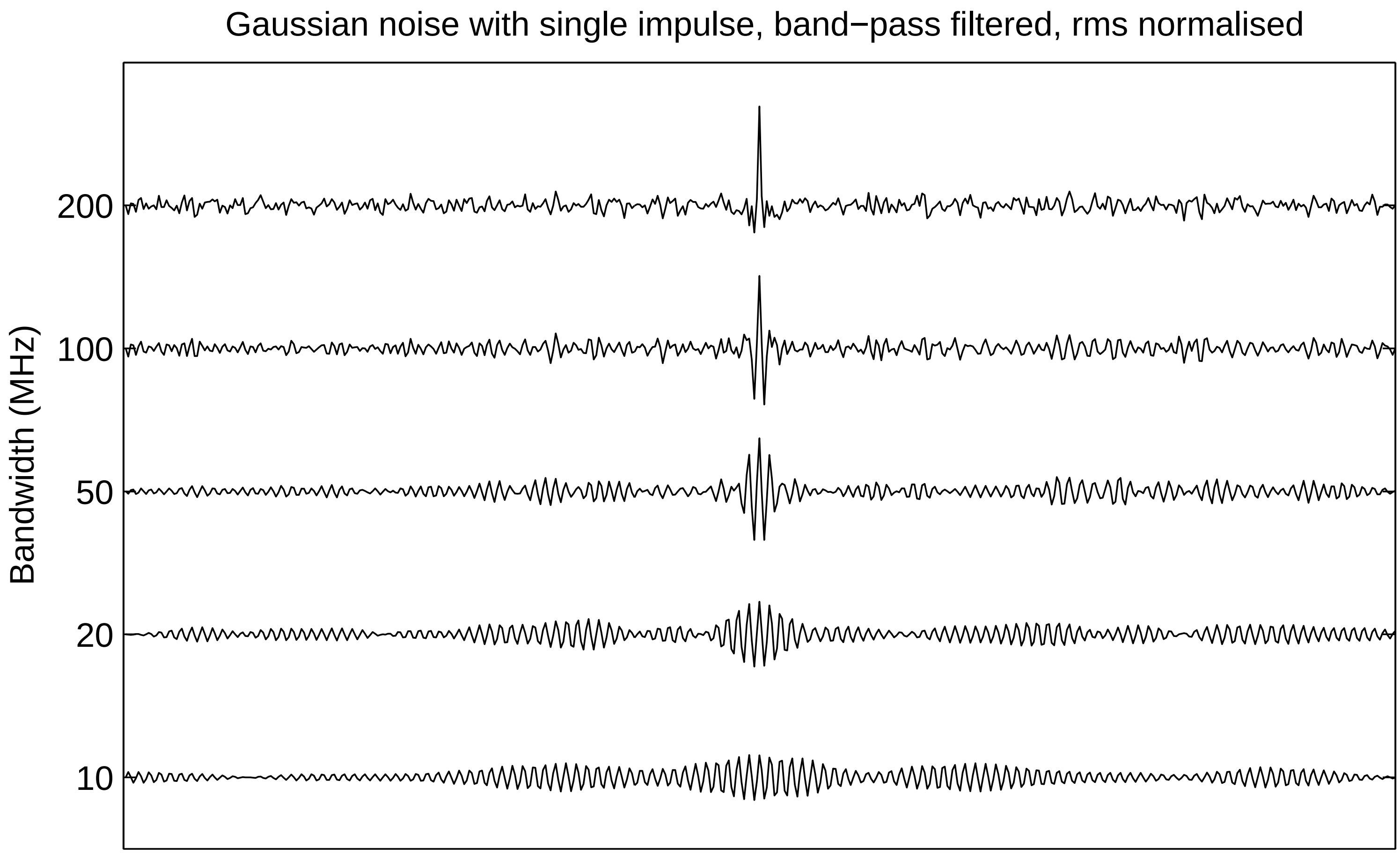
Prerequisite: refresh frequency f_v must be known with a relative error of less than $[2x_\mathrm{t}y_\mathrm{t}(N-1)]^{-1} \approx 10^{-7} \ldots 10^{-8}$.

Bandwidth

Doubling the bandwidth of a receiver will

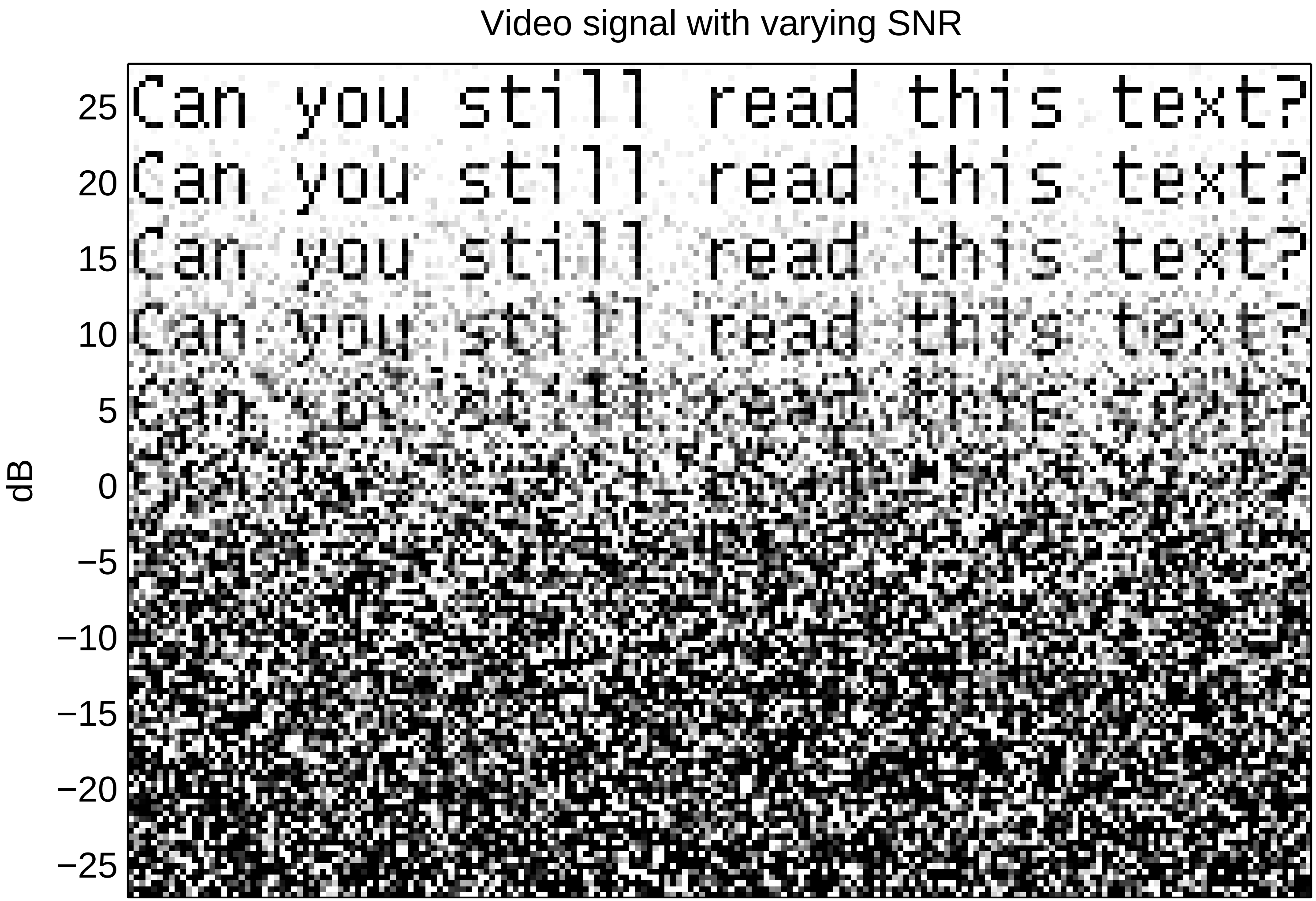
– double power (+3 dB) from narrowband and thermal noise sources;

– double voltage or quadruple power (+6 dB) from wideband impulses.



10× BW: +10 dB thermal noise, +20 dB impulse energy ⇒ +10 dB SNR on impulse signals.

Expolitable signal/noise ratio



Text generally well readable if SRN $>$ 10 dB, but neither recognizable manually nor automatically if SRN $<$ 0 dB (after periodic averaging).

Suggested limits for far-field video signals

Example design choices for test limits

→ Antenna distance during test: $\hat{d} = 1$ m

→ Eavesdropper: $1 \times 1 \times 0.5$ m^3 Yagi array with gain $G_\mathsf{a} = 16$ dBi

→ Eavesdropping distance 30 m in a quiet rural area: $a_\mathsf{d} = 30$ dB (equivalently 10 m in a 10 dB noisier business environment)

→ Building attenuation: 5 dB (lowest decile in available statistics)

→ Receiver bandwidth $B = 50$ MHz and noise figure $f_\mathsf{r} = 10$ dB

→ Periodic averaging of $N = 32$ frames $\Rightarrow G_\mathsf{p} = 15$ dB

→ Minimum background noise at quiet rural site at 3–300 MHz: 10 dBµV/m per MHz (thermal noise dominates above 200 MHz). Equivalent at 50 MHz: 27 dBµV/m.

All these added up according to (1):

$$\hat{E}_{50\ \mathsf{MHz}} \leq 41\ \mathsf{dB\mu V/m}$$

Equivalently at lower measurement bandwidths:

$$\begin{aligned}\hat{E}_{5\ \mathsf{MHz}} &\leq 21\ \mathsf{dB\mu V/m}\\ \hat{E}_{1\ \mathsf{MHz}} &\leq 7\ \mathsf{dB\mu V/m}\end{aligned}$$

Verifying this limit at 5 MHz is just about feasible with the noise floor of good spectrum analyzers and passive antennas.

This limit should be applied in the range 10–100 MHz.

With passive dipole antennas thermal noise lifts the noise level from 100 MHz to 1 GHz by about 10 dB. The attacker suffers the same problem, therefore the limit can raise proportional to the frequency above 100 MHz to $E_{5\ \mathsf{MHz}} \leq 31$ dBμV/m at 1 GHz.

Above 1 GHz, parabolic reflectors become feasible, therefore the limit should remain constant above there. An appropriate upper frequency limit would be in the region of 50× the maximum signal clock frequency (e.g., 5–10 GHz); with a lower limit near 0.1× the clock frequency.

Comparison with other standards

Since the received voltage from impulse signals is proportional to B and $1/d$, we can compare test limits with those of other standards only after normalizing these measurement parameters:

At 100 MHz centre frequency, 1 MHz bandwidth, 1 m distance:

CISPR 22 “Class B”	68 dBµV/m
MIL-STD-461E/R102 (mobile US Army/Navy equipment)	44 dBµV/m
this proposal	7 dBµV/m

Or in terms of peak equivalent radiated power at 50 MHz bandwidth:

CISPR 22 “Class B”	≈ 0.5 mW
MIL-STD-461E/R102	≈ 2 µW
this proposal	≈ 0.3 nW

For comparison, the eavesdropped signals demonstrated in [Kuhn, 2003] had, at 50 MHz bandwidth, power levels in the range 10–240 nW.

Other considerations

- $\longrightarrow$ To protect even against reception in directly adjacent neighbour rooms ($d = 3$ m), decrease limits by another 10 dB.
- $\longrightarrow$ Measurement procedure could be adopted from existing CISPR and MIL-STD-461 methods. No quasi-peak detector.
- $\longrightarrow$ Use shielded measurement chamber (environment 6 dB below limit) and spectrum analyzer, or wide-band receiver and periodic averaging (like attacker).
- $\longrightarrow$ **Warning:** Modern flat-panel displays perform scan-rate conversion and emit the video signal with **two** refresh frequencies! $\Rightarrow$ Periodic-averaging measurements only after full review of circuit diagrams.
- $\longrightarrow$ This proposal is aimed at source suppression and shielding.
- $\longrightarrow$ Approach could be adapted for jamming standard. Needs to distinguish between thermal noise, impulse noise and periodic-noise jammers.

Summary and conclusions

⟶ No public emission-security test standards exist; other standards inappropriate for detecting UWB impulse signals.

⟶ Case study: far-field VHF/UHF video-signal eavesdropping.
⇒ Permitted leaking signal power must be in the order of a million times below what current civilian RFI standards permit.

⟶ No single standard test will be adequate for all applications.

⟶ Framework for a modular protection standard should consist of suitable reference data and practical numeric models for

- antenna/transducer/receiver performance
- expected background noise and attenuation levels
- achievable signal-processing gains
- exploitable symbol error rates

and application-specific profiles that combine these to actual test requirements.

Future work and open questions

- ⟶ Existing noise surveys (ITU-R P.372) do not yet distinguish between narrowband/thermal and impulse noise ⇒ man-made-noise figures may be unrealistic for ultra-wideband or indoor reception.
- ⟶ Practical evaluation
- ⟶ Development of similar security criteria for other types of compromising emanations:
  - Conducted video emanations, near-field
  - Acoustics, optics [Kuhn, 2002]
  - Network hardware, printers
  - RFID readers
  - CPU boards and individual chips running crypto algorithms (modexp, AES, etc.)
  - intentional broadcast