Security Limits for Compromising Emanations

Markus G. Kuhn

University of Cambridge, Computer Laboratory,
15 JJ Thomson Avenue, Cambridge CB3 0FD, United Kingdom
http://www.cl.cam.ac.uk/~mgk25/

Abstract. Nearly half a century ago, military organizations introduced "Tempest" emission-security test standards to control information leakage from unintentional electromagnetic emanations of digital electronics. The nature of these emissions has changed with evolving technology; electromechanic devices have vanished and signal frequencies increased several orders of magnitude. Recently published eavesdropping attacks on modern flat-panel displays and cryptographic coprocessors demonstrate that the risk remains acute for applications with high protection requirements. The ultra-wideband signal processing technology needed for practical attacks finds already its way into consumer electronics. Current civilian RFI limits are entirely unsuited for emission security purposes. Only an openly available set of test standards based on published criteria will help civilian vendors and users to estimate and manage emission-security risks appropriately. This paper outlines a proposal and rationale for civilian electromagnetic emission-security limits. While the presented discussion aims specifically at far-field video eavesdropping in the VHF and UHF bands, the most easy to demonstrate risk, much of the presented approach for setting test limits could be adapted equally to address other RF emanation risks.

Keywords: Eavesdropping, emission security, Tempest, protection standards, video displays, side channels.

1 Introduction

Electronic equipment can emit unintentional radio signals from which eavesdroppers may reconstruct processed data at some distance. The civilian computer-security community became aware of the risk through van Eck's demonstration of how to eavesdrop on video displays with modified TV sets [1]. More recent studies have shown that not only are contemporary CRT monitors still vulnerable [2], but so are flat-panel displays with digital interfaces [3]. Modular exponentiation parameters in an SSL accelerator module inside a closed server have been reconstructed from emanations picked up at 5 m distance [4].

Since about 1960, NATO governments have paid considerable attention to limiting compromising emanations of computers that handle classified information. They developed test standards and procured conforming protected products. The relevant standards and their rationales are still classified documents

J.R. Rao and B. Sunar (Eds.): CHES 2005, LNCS 3659, pp. 265–279, 2005.

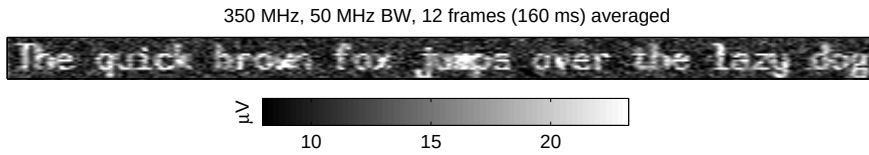

Fig. 1. Text signal received from a Toshiba 440CDX laptop at 10 m distance through two intermediate offices (3 plasterboard walls) using an omnidirectional antenna, a Dynamic Sciences R-1250 AM wideband receiver, a digital storage oscilloscope and postprocessing on a PC involving cross-correlation controlled periodic averaging. The calibration bar shows the rms voltage of a sine wave on the antenna input that would generate an equally strong signal. [3]

and conforming products remain export controlled. Although "Tempest"-certified equipment is, in principle, available to non-military customers, its use in civilian applications remains marginal.

Without open standards, emission security remains largely ignored in non-military applications, smartcard microcontrollers being a notable recent exception. There may be several reasons. Firstly, secret military specifications restrict the choice of suppliers to a small number of defense contractors with the necessary clearances and exclude the mass-market industry. In the absence of public literature, civilian product designers receive no training in emission security. Opportunities for simple low-cost countermeasures that require little more than awareness of the nature of such risks early in a design process are therefore missed. Secondly, with secret emission limits, users have no idea what level of protection is tested and how the unknown tradeoffs made in these specifications fit into their overall security concept and budget. And finally, academic researchers may simply find it less appealing to try advancing a field in which most existing work remains secret and much of the state of the art has to be reinvented first.

Recent Freedom-of-Information-Act requests to declassify the US "Tempest" standards resulted only in excerpts that describe some terminology and widely known EMC test and calibration methods [5,6,7,8,9]. The actual conformance limits and full test procedures remain unavailable, along with the literature that justifies the design of these standards.

Today, most information-processing facilities with high protection requirements use civilian off-the-shelf technology, procured according to open standards. This calls, in my opinion, for a new generation of emission-security test standards that is based entirely on published data and experimental techniques. Their development should follow the established procedures of international standardization. Any underlying data should be open to scrutiny by academic peer review, to prevent that any tradeoffs that have to be made could be influenced by conflicting concerns of the signal-intelligence community. A model for such an effort could be the work that led to international standards on electromagnetic compatibility [14].

Designing a comprehensive family of open emission-security standards will require a substantial interdisciplinary research effort. While similar principles can be applied to a wide range of information-leaking channels, the specific parameters, test procedures, and appropriate economic tradeoffs can vary by orders of magnitude across different applications, countermeasures and signal types.

In the space of this paper, we will have to restrict the discussion, as an example, to one single class of signal, namely the radiated RF leakage of video signals. This remains a particularly easy to demonstrate risk, especially because of the redundancy offered by a repetetive signal, and because the eavesdropper needs to find only a small number of parameters to exploit the signal (namely, the rough pixel-clock frequency and the precise line and frame frequencies).

2 Existing Public Standards

No public emission-security standards exist today. Two types of electromagnetic-emission limits for information technology have been widely accepted by the market already, but – as this section will show – neither was designed to reduce the risk of information-carrying emanations, nor is any of them even remotely suited to do so.

2.1 Ergonomic Standards

Since about 1992, "low radiation" CRT computer monitors with improved electromagnetic shielding have been on the market. They confirm to standards aimed at reducing the exposure of humans to electromagnetic fields, to address fears about their potential biological effects [11,12]. The TCO'92 specification developed by the Swedish Confederation of Professional Employees (TCO) limits only low-frequency fields below 400 kHz, which are those generated by CRT deflection coils. Compromising emanations are typically significantly weaker and occur at much higher frequencies in the HF/VHF/UHF bands (3 MHz–3 GHz). Therefore, a TCO'92 conformance test will provide no information about emission-security properties of a video-display system.

2.2 Radio-Frequency Interference Standards

The second class of civilian electromagnetic emanation standards is aimed at minimizing interference with radio communication services. The international specification CISPR 22 [13] is today a legal requirement in most industrialised countries. This standard imposes the following radiated emission limits for "Class B" devices:

- Electric fields must not exceed 30 dBμV/m at 10 m distance in any 120 kHz passband in the frequency range 30–230 MHz.
- Electric fields must not exceed 37 dBμV/m at 10 m distance in any 120 kHz passband in the frequency range 230–1000 MHz.

The field strength is determined with a special AM measurement receiver with a *quasi-peak* detector specified in [14]; the output of such a detector rises with a time constant of only 1 ms and falls with a time constant of 550 ms. Less strict "Class A" limits are defined for devices that are only used in industrial environments. The standard also limits emissions below 30 MHz via power and communications cables.

A brief look at the motivation and design of the radio-interference test standards helps to understand why they are not suited for emission security purposes. Radio broadcasters aim at ensuring a minimum field strength of about 50–60 dBμV/m throughout their primary reception area [16]. The CISPR limits were selected about 20 dB below that level to ensure that, at 10 m distance, the interference from a device will not limit the received signal-to-noise ratio to less than 20 dB.

The quasi-peak detector is used as a psychophysical estimation tool. It provides a measure of the approximate annoyance level that impulses of various strengths and repetition frequencies cause for human users of analog audio and television receivers. Strong disturbance impulses are tolerated if they occur sufficiently rarely, and even weak disturbances can be annoying at high repetition rates.

3 Considerations for Emission Security Limits

Eavesdroppers can work with significantly lower signal levels than what might cause interference with radio and TV reception. They are concerned about how the emitted compromising signal compares in strength to the background noise, not to a broadcasting station. They can be expected to

- use high-gain antennas directed towards the emitting target device,
- look for the broadband impulses from digital signals in a quiet part of the spectrum, without interference from broadcasting stations,
- use notch filters to suppress strong narrow-band sources that interfere with the eavesdropped signal,
- use signal-processing techniques such as periodic averaging, cross-correlation, digital demodulation, and maximum-likelihood symbol detection, in order to separate the wanted information-carrying signal from unwanted background noise.

The emission limits, therefore, have to be based on an understanding of reasonable best-case assumptions of

- the minimal background noise that the eavesdropper faces even under good receiving conditions,
- the gain from antenna types that can be used covertly,
- the gain from the use of suitable detection and signal-processing methods for the signal of interest,
- the closest distance between antenna and target device for which protection is needed.

The goal of an emission-security test standard is to provide an upper bound for the signal-to-noise ratio S/N that a radio-frequency eavesdropper could achieve in practice. We then need a model that relates such a value to the outcome of practically repeatable measurements that can be performed as part of a security evaluation in a controlled test environment. If we combine the major factors that attenuate a compromising signal for an eavesdropper, compared to a laboratory measurement, with the major factors by which an eavesdropper can boost the signal, we obtain such a model in form of the formula

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

where

$\hat{E}_B$	is the maximum field strength that the test standard permits,
B	is the impulse bandwidth [14,17] of the receiver used in the test,
a_d	is the 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	is any additional attenuation in the radiation path (e.g. building walls),
G_a	is the gain of the best directional antenna that is feasible for use by the eavesdropper,
G_p	is the processing gain that can be achieved with signal processing,
$E_{\mathrm{n},B}$	is the field strength of natural and man-made radio noise at the location of the eavesdropping antenna within a quiet band of width B,
f_r	is the noise factor of the eavesdropper's receiver.

The expected noise levels and attenuation values in the above equation are random variables, which, in the absence of better data, have to be modeled as being normally distributed with some mean and variance determined from the statistical evaluation of a large number of measurements in various environments. For the other parameters, reasonable estimates based on practical demonstrations have to be made, so that an emission limit $\hat{E}_B$ can be selected that will keep the eavesdropper's signal-to-noise ratio below an acceptable level with sufficient probability. Different types of target signal are located in different frequency bands and permit different processing gains. Therefore, the above parameters will have to be estimated separately for each signal type of interest. General emission limits would have to consider for each frequency band the lowest acceptable source signal strength $\hat{E}_B$ for all types of compromising signals.

3.1 Radio Noise

A standard survey-data reference for the noise levels to be expected in various environments throughout the radio spectrum exists in the form of ITU-R Recommendation P.372 [18], which summarizes the results from numerous noise intensity measurements and categorizes their origin.

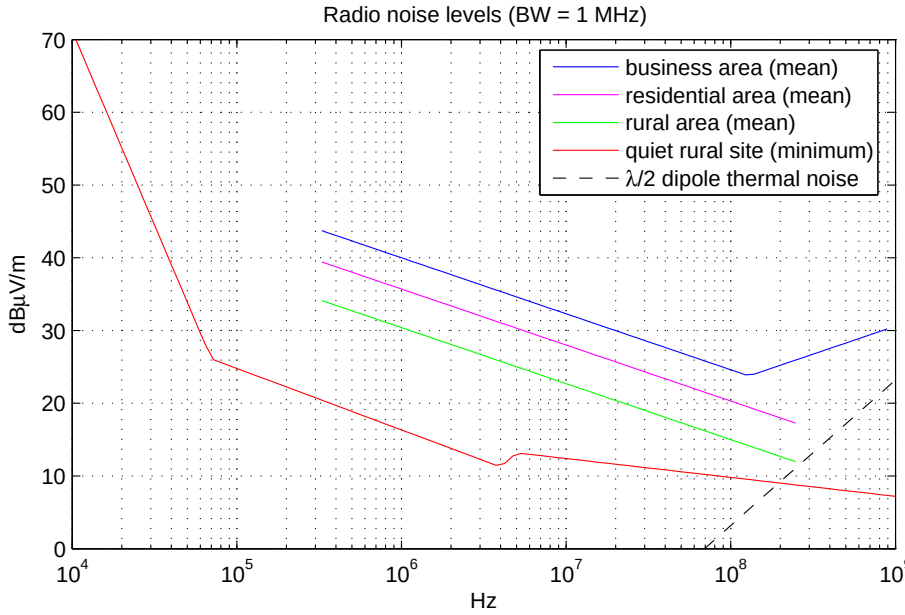

Fig. 2. Expected electric field noise levels $E_{\mathrm{n},1\ \mathrm{MHz}}$ excluding transmitter stations based on data from ITU-R P.372 [18]. The curves are for a receiver bandwidth of 1 MHz. Add 3/7/10/13/17/20 dB for bandwidths of 2/5/10/20/50/100 MHz, respectively. Subtract 37/20/9 dB for the 0.22/9/120 kHz bandwidth used in CISPR 16 measurements.

The mean noise levels are provided in ITU-R P.372 in form of an *external noise factor* $f_{\mathrm{a}} = P_{\mathrm{n},B}/kT_0B$ which compares the noise energy picked up over a bandwidth B by an antenna with the thermal noise energy from a resistor at room temperature T_0 (k is Boltzmann's constant).

Using the signal-power to field-strength relationship of an omnidirectional antenna (for details see [2, p. 91]), we can convert these noise figures into equivalent field strengths, which is the unit commonly used in electromagnetic emission standards.

Figure 2 uses these values, and others from [18], to estimate electric field levels at both quiet rural sites and business districts for 1 MHz bandwidth. In measurements, the receiver bandwidth will have to be smaller than the center frequency, therefore the shown curves are directly applicable only for frequencies of about 2 MHz and higher. For lower frequencies, lower bandwidths will have to be used. For noise, the received power increases proportional to the bandwidth of the receiver (10× larger bandwidth leads to 10 dB higher field strength).

It is worth noting that these are out-door levels and that this background noise might be attenuated if the eavesdropper and the target device are both located in the same building.

3.2 Radio Signal Attenuation

In free space (vacuum, dry air, etc.) the power flux density (power per area) of a radio signal drops with the square of the distance from a point source, because preservation of energy requires that the power flux density remains constant when it is integrated over the closed surface of a volume that contains the transmitter. The power flux density is proportional to the square of the electric field strength, therefore, the electric field strength will at distance d be reduced by a factor

$$a_{\mathrm{d}} = d/\hat{d} \tag{2}$$

compared to the value at a reference distance $\hat{d}$. In other words, increasing the distance to a transmitter in free space by a factor of 10 will reduce the signal strength by 20 dB.

Compared with the available references on out-door radio noise, somewhat less clear data is available in the literature on the in-door radio signal attenuation by building materials. Two survey publications [19,20] provide data for the frequency range of 900 MHz to 100 GHz. However, this data shows only a few trends and mostly documents a significant variability between different buildings.

A model in [19] suggests for 900 MHz a path loss of $a_{\mathrm{d}} \cdot a_{\mathrm{w}} = (d/\hat{d})^{1.65}$ for typical wall spacings and materials for an office environment on the same floor. An additional loss factor of 0/9/19/24 dB has to be added if the two antennas are 0/1/2/3 floors apart in a building. In large open rooms, attenuation is dominated by free-space loss ($a_{\mathrm{d}} \cdot a_{\mathrm{w}} = (d/\hat{d})^{1}$). In corridors it is slightly lower ($a_{\mathrm{d}} \cdot a_{\mathrm{w}} = (d/\hat{d})^{0.9}$), because walls can reflect the signal or act like a wave guide. The literature survey in [20] lists a number of alternative, but similar, models that have been used to describe attenuation in buildings, e.g. where the exponent applied to $d/\hat{d}$ increases from 1 to 6 as the distance increases from 1 m to 40 m. It also features measurements of individual building components, e.g. 3.8 dB for a double plasterboard wall or 7 dB for a 200 mm concrete block wall. Less data is available for VHF frequencies (30–300 MHz), for example [21], which suggests that building attenuation a_{w} is mostly in the range 5–45 dB. This reference also notes that VHF field strength can vary inside buildings by as much as 20 dB within a meter, which agrees with my own experience from eavesdropping demonstrations with handheld antennas inside office buildings.

Given the wide variability of radio-signal attenuation encountered in buildings, it seems not prudent to base a protection standard on any higher value for a_{w} than what is encountered in the lower decile of the available statistics, namely in the region of $a_{\mathrm{w}} = 5$ dB, a typical attenuation provided by 1–2 walls.

3.3 Antenna Gain

The compact broadband antennas that are commonly used for radio-interference compliance measurements, such as biconical, log-periodic, log-spiral, or double-ridged-horn designs, have only little directional gain G_{a}, typically about 2–6 dBi ("dBi" refers to a decibel gain compared to an isotropic antenna).

One of the most practical families of high-gain antennas for the UHF and higher VHF frequency range is the Yagi-Uda type, some forms of which are well known through their widespread use for domestic terrestrial UHF TV reception. Such an antenna is half as wide as the wavelength λ and can be designed such that its gain is

$$G_\mathrm{a} = 7.8\ \mathrm{dB} \cdot \log_{10} \frac{l}{\lambda} + 11.3\ \mathrm{dBi}, \tag{3}$$

where l is the length of the antenna [23, p. 458]. Increased gain and length of an antenna comes with reduced bandwidth. For the frequencies (200–400 MHz) and bandwidths (50 MHz) that are often best suited for video-signal eavesdropping, Yagi antennas with four elements seem to be an acceptable compromise, with a gain of 8.6 dBi and a length $l \approx \lambda/2$. Further gain can be achieved by connecting a group of Yagi antennas together, and each doubling of their number will in practice increase the directional gain by 2.5–2.8 dB.

As a practical example, a 2×3 group of six Yagi antennas with four elements, each tuned for the 350 MHz center frequency from Fig. 1, would be $0.43 \times 1.3 \times 1.1$ m large [2, p. 95] and could be hidden and handled quite easily behind a window or inside a suitable vehicle. It would provide a gain of about $G_\mathrm{a} = 16$ dBi. Doubling the reception frequency roughly quadruples the number of dipoles that can fit into the same space, leading to 5–6 dB more gain.

3.4 Processing Gain

Averaging is a practical and highly effective technique for increasing the signal-to-noise ratio of a periodic signal, such as that generated by the image-refresh circuitry in a video display system.

If X_i are independent random variables, then the variance of their sum will be the sum of their variances: $\mathrm{Var}(\sum_i X_i) = \sum_i \mathrm{Var}(X_i)$. The variance of a radio-signal voltage corresponds to its average power. If we add two sine waves with a random phase relationship together, the expected power of the result is the sum of the powers of each input signal. However, if we add two identical sine waves together, their voltage will add up and thus their power quadruple.

Similarly, adding two recorded segments of independent noise together will double the power of the noise and increase its root-mean-square voltage by a factor of $\sqrt{2} = 3$ dB. On the other hand, adding two phase-aligned repetitions of the same waveform together will increase its voltage by a factor of $2 = 6$ dB (and will therefore quadruple its power). When two recorded signals contain both independent noise and a wanted phase-aligned signal, then adding the two together will increase the signal-to-noise ratio by 3 dB. (Dividing by the number of added signals, to complete the average calculation, will not affect the SNR.)

This can be generalized to a processing gain of

$$G_\mathrm{p} = \sqrt{N} = 3\ \mathrm{dB} \cdot \log_2 N = 10\ \mathrm{dB} \cdot \log_{10} N \tag{4}$$

when N repetitions of a signal can be observed and added up with correct phase alignment.

How many frames of a video signal can be averaged in practice depends on a number of factors:

- When the screen content is stable for a time period T, then obviously up to $f_\mathrm{v}T$ frames can be received, where f_v is the frame rate or vertical deflection frequency of the screen. T can range in practice, depending on user behavior, from a few seconds to many minutes or longer, limiting N to about 10^2–10^6.
- Periodic averaging of a video signal can only be successful if the refresh frequency f_v can be determined with a relative error of less than $[2x_\mathrm{t}y_\mathrm{t}(N-1)]^{-1}$, where $x_\mathrm{t}y_\mathrm{t}$ is the total number of pixels including those representing the blanking intervals, if we demand that pixel intervals in the first and last averaged frame overlap by at least half a pixel time [2]. The frequency of crystal oscillators used in graphics cards wanders out of such a tight frequency tolerance within a small number of seconds, limiting N to less than 10^3 for averaging based on a manually adjusted vertical sync signal generated in an independent oscillator.
- An alternative to reconstructing the sync signal and averaging in real-time is to record the receiver output and then search for peaks in the auto-correlation of this signal. This way, the precise repetition frequency can be determined in a more compute-intensive post-processing step (as was done in Fig. 1). The number of frames will here be limited by the available acquisition memory. Storage oscilloscopes offer today 16–64 MB, which limits N to 10^1–10^2 frames. The available memory and processing power can be expected to grow further with Moore's law. They are limited in purpose-built hardware only by the eavesdropper's budget. With enough signal processing power available, this auto-correlation – which will only be evaluated for peaks near the expected frame time f_v^{-1} – could even be performed in real-time, leading not only to unlimited integration time but also to real-time monitoring of the result.

3.5 Bandwidth

A further consideration is the receiver bandwidth. We can expect an eavesdropper to work with a bandwidth B somewhere near the pixel frequency f_p of the video mode, as this is necessary to separate the impulses received from individual pixels and reconstruct the full video bandwidth. For larger fonts, text might remain intelligible with somewhat lower bandwidths.

In general, independent of the bit rate or pixel frequency of an eavesdropped digital signal, a higher bandwidth will lead to an improved signal-to-noise ratio. This is, because the compromising emanations of digital waveforms are in the form of switching impulses, which are inherently ultra-wideband signals. The frequency components of an impulse are correlated and therefore received impulse voltages will grow linearly with B (20 dB for every ten-fold increase in bandwidth), whereas thermal noise and narrow-band background signals are usually not correlated and their voltage will therefore only grow proportional to $\sqrt{B}$. As a result, in the best case, the signal-to-noise ratio can grow proportional to $\sqrt{B}$.

In practice, the ratio will grow somewhat less, because some of the unwanted background noise (for example emissions from other nearby computers) also has the form of broadband impulses. A reason for keeping the bandwidth small in an eavesdropping receiver is that this will make it more likely to find a quiet window in the radio spectrum that is not used continuously by powerful narrow-band transmitters such as radio and TV broadcast stations. Overall, a bandwidth in the order of $B = 50$ MHz would be a typical practical compromise for a readable video signal.

3.6 Signal-to-Noise Ratio

For the reconstruction of human readable text, a signal-to-noise ratio of at least 10 dB is necessary [2]. This requirement could perhaps – especially with much larger fonts – be reduced by a few dB when a symbol detector is used to automatically recognize characters, but the additional gain achievable here depends a lot on the font and will be significantly below the square-root of the number of pixels per character, as many characters such as `i,l,I,1` or `o,c,e` differ only in a few pixels. Therefore, a SNR of not more than 0 dB seems to be a reasonable security requirement.

4 Suggested Emission Limits

Based on all these considerations, we can now bring together possible values for equation (1). A calculation like the following example illustrates how a rationale for the emission limits in a compromising emanations test standard for video signals could look like:

- We measure field strength in the laboratory tests at a distance of $\hat{d} = 1$ m, which is already common practice in military EMC standards, e.g. [15].
- We assume our eavesdropper uses a directional Yagi antenna array like the one described in section 3.3 with $G_\mathrm{a} = 16$ dBi.
- We assume that an attacker will not get closer than $d = 30$ m with this type of antenna, therefore $a_\mathrm{d} = 30$ dB. In a quiet rural site, securing the area 30 m around a device should be feasible, whereas in an urban environment, space is typically more confined, but noise levels are also 10 dB higher, providing the same protection against attackers at 10 m distance. If the threat model includes attackers in nearby rooms in the same building ($d = 3$ m), the resulting test limits will have to be lowered 10 dB further.
- We want to ensure protection even for rooms whose attenuation by building materials is located in the lowest decile of the available statistics and therefore use $a_\mathrm{w} = 5$ dB.
- We assume the attacker uses a receiver with a noise figure of $f_\mathrm{r} = 10$ dB (the value given for the Dynamic Sciences R-1250 wideband Tempest receiver)
- We assume a receiver (impulse) bandwidth of $B = 50$ MHz.
- We assume that an attacker will in practice have difficulties with aligning the antenna, tuning to a suitable center frequency, and synchronizing to the

exact frame rate if there is no visibly usable signal after averaging $N = 32$ frames and therefore we assume a possible processing gain of $G_\mathrm{p} = 15$ dB.
- From Fig. 2 we can see that for the HF and VHF frequency range of 3 MHz to 300 MHz the background noise level $E_{\mathrm{n},1\ \mathrm{MHz}}$ remains above about 10 dBμV/m, even at a quiet receiver site. Above 200 MHz thermal noise from the antenna itself becomes the limiting factor, increasing with 20 dB per decade. After adjusting the bandwidth, we get $E_{\mathrm{n},50\ \mathrm{MHz}} = 27$ dBμV/m.

When we require $S/N \leq 0$ dB and use all of the just listed parameters in (1), we end up with

$$\begin{aligned}\hat{E}_{50\ \mathrm{MHz}} &\leq \frac{S/N \cdot a_\mathrm{d} \cdot a_\mathrm{w} \cdot E_{\mathrm{n},50\ \mathrm{MHz}} \cdot f_\mathrm{r}}{G_\mathrm{a} \cdot G_\mathrm{p}} \\ &= 0\ \mathrm{dB} + 30\ \mathrm{dB} + 5\ \mathrm{dB} + 27\ \mathrm{dB\mu V/m} + 10\ \mathrm{dB} - 16\ \mathrm{dBi} - 15\ \mathrm{dB} \\ &= 41\ \mathrm{dB\mu V/m}.\end{aligned}$$

4.1 Feasibility of Verification

It would be desirable if the suggested limits were verifiable with off-the-shelf EMC measurement equipment, such as a normal spectrum analyzer. Unlike a sophisticated eavesdropper, a spectrum analyzer will not be able to utilize the processing gain offered by periodic averaging. Therefore, eavesdroppers can still use signals that are not visible on a spectrum analyzer. To compensate for this, we have to bring during spectrum analyzer tests the antenna as close as possible to the equipment under test, that is $\hat{d} = 1$ m, even if that means that we might encounter some near-field effects.

Like the eavesdropper, the test procedure should work at as high a bandwidth as possible to make use of the fact that impulse voltage will grow proportional to B, whereas noise voltage grows proportional with $\sqrt{B}$. A wide-band receiver suitable for video eavesdropping uses extra-high intermediate frequencies in order to provide large bandwidths of 50 MHz and more. Measurements at such bandwidths are not possible with commonly used spectrum analyzers, whose intermediate frequencies only allow a maximum impulse bandwidth of 5 or 1 MHz. The corresponding limits would be 20 or 34 dB lower, respectively:

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

The limits have to be above the receiver noise floor of a spectrum analyzer to be verifiable. For example, the Agilent E4402B spectrum analyzer with preamplifier has, according to manufacturer claims [24, p. 235], at a resolution bandwidth of 1 kHz a noise level of −133 dBm. This corresponds to 4 dBμV at 1 MHz and 11 dBμV at 5 MHz. The antenna factor (ratio between field strength in V/m and voltage) for a typical passive measurement antenna at frequencies up to 100 MHz is not more than 10 dB. Therefore, the noise floor of the above spectrum analyzer corresponds to field strengths of 14 dBμV/m at 1 MHz and 21 dBμV at

5 MHz bandwidth. This makes spectrum analyzer verification of the electric field strength limits problematic at a bandwidth of 1 MHz, and just about feasible at 5 MHz, at least with passive antennas. Active antennas designed for use in anechoic chambers[1] might therefore have to be used instead, which offer a 20 dB lower antenna factor and a sensitivity of 6 dBμV/m at 1 MHz.

Growing antenna factors make the limit of $\hat{E}_{5\ \mathrm{MHz}} = 21$ dBμV/m also problematic to verify for frequencies above 100 MHz, but the eavesdropper would experience thermal noise as well here at the assumed quiet receiver site. Therefore it seems acceptable to increase the limit proportional to the frequency, starting at 100 MHz, up to at least 1 GHz. For higher frequencies, the eavesdropper can use parabolic antennas with higher gain to overcome the thermal noise.

4.2 Comparison with Limits in Other Standards

In order to compare these proposed limits with those defined in CISPR 22 Class B, we have to take into account the different bandwidths and antenna distances. To increase the impulse bandwidth from 120 kHz to 5 MHz, we have to raise the permitted field strength by 32 dB, in order to keep the equivalent spectral density constant. The limits have to be raised further by 20 dB to convert the measurement distance from 10 m to 1 m.

This way, we can compare the emission security test limits proposed here with the established EMC emission limits. Radiated VHF field strength has to be 61 dB lower than allowed in CISPR 22. This corresponds to a reduction of the maximum tolerated eavesdropping distance by a factor of 10^3. In other words, the CISPR 22 EMC limits do not prevent devices from emitting pulses that could, under ideal conditions, be received kilometers away.

We can conclude from this that a shielded room with an attenuation of 60 dB across the HF/VHF/UHF frequency range for radiated emissions should provide adequate protection, if everything operated inside it complies with the CISPR 22 Class B limits, as can be expected from all currently available office equipment. It is worth stressing that this entire analysis concentrates on VHF video emanations. It should be applicable to similar high-speed digital signals such as those from system busses, but it does not take into account any low-frequency magnetic or acoustic emanations from electromechanic equipment, as they might have been a concern, for example, with some historic printers.

If the protection provided by the shielded room must be effective immediately outside the room at a very quiet site ($d = 0.3$ m), and not only in 30 m distance, then another 40 dB attenuation is required, leading to the 100 dB attenuation defined in the NSA specification for shielded enclosures [10].

The US military EMC standard MIL-STD-461E [15] provides in its requirement R102 for mobile Army and Navy equipment radiated electric limits field limits similar to those suggested here, namely measured at 1 m distance not more than 24 dBμV/m from 2 to 100 MHz, and then increasing with 20 dB per decade up to 18 GHz. However, the measurement bandwidth is with 10 kHz

[1] e.g., Rohde & Schwarz AM524 low-noise active antenna system

up to 30 MHz, 100 kHz in the 30–1000 MHz range and 1 MHz for frequencies above 1 GHz comparable to what CISPR 22 uses, and therefore still 37 dB less sensitive for broadband impulse signals than the limits proposed here.

The different emission-control standards can also be compared via the spectral density of the strongest radiated impulse that they permit (measured at 100 MHz and 1 m distance). It has 68 dBμV/(m · MHz) under CISPR 22 Class B, 44 dBμV/(m · MHz) with MIL-STD-461E/R102, and 7 dBμV/(m · MHz) for the emission-security limit proposed here.

Dropping the logarithmic scales and the dependence on a measurement distance, we can also compare the radiated impulse emission limits in terms of the peak effective isotropic radiated power (EIRP) permitted within a given bandwidth. For a 50 MHz wide band, this would be about 0.5 mW under CISPR 22 Class B, 2 μW under MIL-STD-461E/R102, and 0.3 nW under the limit proposed here. For comparison, the peak EIRPs observed during clearly readable eavesdropping demonstrations in [2] were in the range 10–240 nW. The 10 dB stricter limit to protect even against an eavesdropper in a neighbor room in an urban environment would be 30 pW.

4.3 Other Considerations

The general measurement procedure and setup (use of a wood table over a ground plane, arrangement of cables and impedance stabilization networks, etc.) in an emission security standard could be adopted largely from existing EMC specifications such as CISPR 22 or MIL-STD-461E. Some changes that would have to be made include:

- CISPR 16-1 suggests that the ambient noise levels at a test site should be 6 dB below the measurement limits, for perfect results even 20 dB below. While CISPR 22 describes the use of an open area test site, this will hardly be feasible with the emission security limits proposed here. A well-shielded anechoic chamber will be required instead as a measurement site, to remain at least 6 dB below the measurement limits.
- While the CISPR 22 limits are for a quasi-peak detector, emission security tests should be performed with peak detectors, because rather than perceived annoyance, the separability from noise is the concern. The video bandwidth should not be limited in spectrum analyzer measurements.

The HF/VHF/UHF emission limits suggested here are justified based on video signal eavesdropping, but they are also likely to provide adequate protection against other forms of radiated compromising emanations above about 5 MHz. It seems unlikely that other emanations will offer substantially higher processing gain than video signals, except perhaps carefully encoded intentional broadcasts by malicious software. In addition, the suggested limits are already very close to what seems technically feasible in the form of generic limits on spectral energy as it can be measured with EMC broadband antennas and spectrum analyzers in anechoic chambers.

Different measurement techniques can be used in order to apply the same limits to specific signals that are suspected of being emitted. In the case of a periodic signal, such as the output of a video refresh circuit, it is possible to use a wide-band receiver, just as an eavesdropper would, together with a suitable storage oscilloscope that is triggered from the vertical sync signal. Averaging $N = 1024$ frames (about 12 s of video signal) will lead to a processing gain of 30 dB. If all 1024 lines of the test image are identical and averaged as well, this will lead to another 30 dB gain, making the measurement in principle better than one that took place inside a shielded room with 60 dB attenuation.

The limits discussed here are aimed at products in which emission security is achieved by signal suppression and shielding. Other eavesdropping countermeasures, such as jamming, would require rather different protection standards.

5 Conclusions

We outlined design considerations for a security standard on radiated compromising emanations from video systems. Due to the redundancy of a periodic signal and due to the ultra-wideband nature of compromising emanations from digital baseband signals, meaningful emission limits end up near the performance limits of modern spectrum analyzers. If the protection is to be achieved by shielding and attenuation, the permitted signal power must be several million times lower than what civilian radio-interference standards permit.

References

1. Wim van Eck: Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? Computers & Security, Vol. 4, pp. 269–286, 1985.
2. Markus G. Kuhn: Compromising emanations: eavesdropping risks of computer displays. Technical Report UCAM-CL-TR-577, University of Cambridge, Computer Laboratory, December 2003. `http://www.cl.cam.ac.uk/TechReports/`
3. Markus G. Kuhn: Electromagnetic Eavesdropping Risks of Flat-Panel Displays. 4th Workshop on Privacy Enhancing Technologies, 23–25 May 2004, Toronto, LNCS 3424, Springer.
4. Suresh Chari, Josyula R. Rao, Pankaj Rohatgi: Template Attacks. 4th International Workshop on Cryptographic Hardware and Embedded Systems, LNCS 2523, Springer, 2002, pp. 13–28.
5. National Security Telecommunications and Information Systems Security Advisory Memorandum NSTISSAM TEMPEST/1-92: Compromising Emanations Laboratory Test Requirements, Electromagnetics. National Security Agency, Fort George G. Meade, Maryland, 15 December 1992. Partially declassified transcript: `http://cryptome.org/nsa-tempest.htm`
6. NACSIM 5000: Tempest Fundamentals. National Security Agency, Fort George G. Meade, Maryland, February 1982.
   Partially declassified transcript: `http://cryptome.org/nacsim-5000.htm`
7. National Security Telecommunications and Information Systems Security Advisory Memorandum NSTISSAM TEMPEST/2-95: RED/BLACK Installation Guidance. National Security Agency, Fort George G. Meade, Maryland, 12 December 1995. Transcript: `http://cryptome.org/tempest-2-95.htm`

8. National COMSEC/EMSEC Information Memorandum NACSEM-5112: NONSTOP Evaluation Techniques. National Security Agency, Fort George G. Meade, Maryland, April 1975.
Partially declassified transcript: http://cryptome.org/nacsem-5112.htm
9. National Security Telecommunications and Information Systems Security Instruction NSTISSI No. 7000: TEMPEST Countermeasures for Facilities. National Security Agency, Fort George G. Meade, Maryland, 29 November 1993. Partially declassified transcript: http://cryptome.org/nstissi-7000.htm
10. Specification NSA No. 94-106: Specification for Shielded Enclosures. National Security Agency, Fort George G. Meade, Maryland, 24 October 1994. Transcript: http://cryptome.org/nsa-94-106.htm
11. TCO'99 – Mandatory and recommended requirements for CRT-type Visual Display Units (VDUs). Swedish Confederation of Professional Employees (TCO), 1999. http://www.tcodevelopment.com/
12. Procedure for Measurement of Emissions of Electric and Magnetic Fields from VDUs from 5 Hz to 400 kHz. European Computer Manufacturers Association, Standard ECMA-172, June 1992. (also IEEE Std 1140-1994)
13. Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement. CISPR 22, International Electrotechnical Commission (IEC), Geneva, 1997. (also EN 55022)
14. Specification for radio disturbance and immunity measuring apparatus and methods. CISPR 16, International Electrotechnical Commission (IEC), Geneva, 2000.
15. Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment. MIL-STD-461E, US Department of Defense, Interface Standard, 20 August 1999.
16. Reinaldo Perez (ed.): Handbook of Electromagnetic Compatibility. Academic Press, 1995.
17. IEEE Standard for the Measurement of Impulse Strength and Impulse Bandwidth, ANSI/IEEE Std 376-1975.
18. Radio noise. Recommendation ITU-R P.372-7, International Telecommunication Union, Geneva, 2001.
19. Propagation data and prediction methods for the planning of indoor radiocommunication systems and radio local area networks in the frequency range 900 MHz to 100 GHz. Recommendation ITU-R P.1238-2, International Telecommunication Union, Geneva, 2001.
20. Homayoun Hashemi: The Indoor Radio Propagation Channel. Proceedings of the IEEE, Vol. 81, No. 7, July 1993, pp. 943–968.
21. L. P. Rice: Radio Transmission into Buildings at 35 and 150 mc [MHz]. Bell System Technical Journal, Vol. 38, No. 1, January 1959, pp. 197–210.
22. M. Zimmermann, K. Dostert: A Multipath Model for the Powerline Channel. IEEE Transactions on Communications, Vol. 50, No. 4, April 2002, pp. 553–559.
23. Karl Rothammel, Alois Krischke: Rothammels Antennenbuch. Franckh-Kosmos, Stuttgart, 1995.
24. Test & Measurement Catalog 2001, Agilent Technologies, USA.