Experimental Estimation of a Potential Eavesdropping Distance for Electromagnetic Emanations of Video System

Alexander Bolshakov, Danil Tyulkin
MTUCI
Moscow, Russia
as.bolshakov57@mail.ru, tyulkin.danil.iv@gmail.com

***Abstract*—In this work an eavesdropping distance of a video system is estimated by measuring unintended electromagnetic signal from a distance of 1 meter and calculating a distance measured signal has to travel in order to be indistinguishable from the noise. Experimental setup is designed in order to measure unintended emissions with a discrete spectrum and maximal signal to noise ratio.**

I. Introduction

Worldwide steady increase of cybercrimes of all sorts has attracted a lot of attention from different industries to the issues occurring along with the computerization. However, it mostly attracted attention to software vulnerabilities and hardware probes while it has been known for many years that sensitive information can be reconstructed from incidental electromagnetic emanations. Some governments have been putting considerable effort in developing special TEMPEST hardware and applying security rules that regulate usage of electronic devices during second part of the 20th century.

Last decade there were many articles that either proved the fact that emanations are an actual big information leakage threat, provided a better solution to restoring data from these unintentional signals, or presented less cumbersome eavesdropping systems. While emission limits and test procedures used by governments are obviously kept secret, estimation of eavesdropping distance for public purposes is still possible with the use of a mathematical models proposed in unclassified papers.

In this paper we aim to provide an example of such estimation in order to improve non-classified estimation methods and to demonstrate results that already existing mathematical model and estimation method can produce.

II. Sources of compromising emissions

More than 30 years ago, in 1985, Wim van Eck published the first unclassified technical analysis of the security risks of emanations from computer monitors [1]. Van Eck successfully eavesdropped on a real system, at a range of hundreds of meters, using just $15 worth of equipment plus a television set.

Even if development of Information Technology Equipment made many designs like CRT monitors largely obsolete new designs are still vulnerable to electromagnetic eavesdropping. Markus G. Kuhn in [2] proved the possibility of eavesdropping on modern flat-panel displays with an equipment constructed in a university lab for less than US$2000.

While video displays are considered a major security threat among Information Technology Equipment it should be noted that almost any unprotected device or information system component emanates signals that can be used to reconstruct information processed by eavesdropped device or component.

In [3] Zhang et al. collected leaked electromagnetic signals of USB cable using the near field coupling coil and meanwhile used oscilloscope to save the signals. After that they used the ESN (echo state network) to extract the characteristics of the collected electromagnetic signals and then use the SVM (support vector machine) method to pattern identify the characteristics of signals.

In [4] Vuagnoux and Pasini implemented sidechannel attacks and their best practical attack fully recovered 95% of the keystrokes of a PS/2 keyboard at a distance up to 20 meters, even through walls. They also tested 12 different keyboard models bought between 2001 and 2008 (PS/2, USB, wireless and laptop). All of them proved to be vulnerable to electromagnetic eavesdropping attacks. Moreover, according to [5] even the shielded keyboards compromise the keystroke information, which indicates the keyboards with shielding measures do not give enough protection against information leakage via electromagnetic emanations.

Data communication equipment sometimes emit modulated optical signals that carry enough information for an eavesdropper to reproduce the entire data stream being processed by a device. According to [6] modulated optical radiation from LED status indicators appear to be significantly correlated with information being processed by the device. Experiments show that it is possible to intercept data under realistic conditions at a considerable distance of 20-30 meters. Authors have successfully recovered error-free data at speeds up to 56 kbits/s but they claim that the physical principles involved ought to continue to work up to about 10 Mbits/s. In [7] one of the authors revisited this problem 16 years later and while apparently this problem is not present in standard

office computers it can still be present in new designs of ITE if monitoring or diagnostic LED indicators are incautiously situated. In recent years there have been numerous articles like [8] that researched use of optical signals as a covert channel instead. These problems lie outside of the scope of our paper since our target is estimating side channel emanations.

Despite impressive experimental and theoretical results described in above-mentioned papers successful eavesdropping attacks on displays are conducted at distances even greater than in case with other devices. For example, in [9] the display images are reconstructed from emanations captured from long distance of approximately 50 meters away from display using a low-cost and all-in-one mobile receiver. While only 26 points and bigger fonts could be read easily from such reconstructed images it still serves as a solid proof of an electromagnetic eavesdropping on distances that can easily exceed controlled zones surrounding target systems.

Before conducting experiment SNR values of compromising emanations from video system, USB flash drive and PS/2 keyboard were measured. SNR of video system's emanations in the experimental environment of our choice proved to be the higher than in case with USB while wired keyboard's emanations were indistinguishable from the noise. Considering this, the way video systems cable makes an unintended antenna and the fact that [9] had the longest eavesdropping distance of all abovementioned examples video system was chosen as a source of electromagnetic emanations for this experiment.

III. Estimation method

This paper uses both a mathematical model and an estimation method proposed in [10]. This method requires electromagnetic emanations to be measured from a distance of 1 meter while a video system is working in a test mode. Test mode means that monitor is displaying black and wide 1 pixel-wide vertical lines ("black pixel – white pixel" sequences) as can be seen on Fig. 1. This setup provides discrete spectrum and highest radiation of emanations in order to estimate the maximal potential eavesdropping distance. Since measured emanations are radiated by video cable strength of electric component is of main interest.

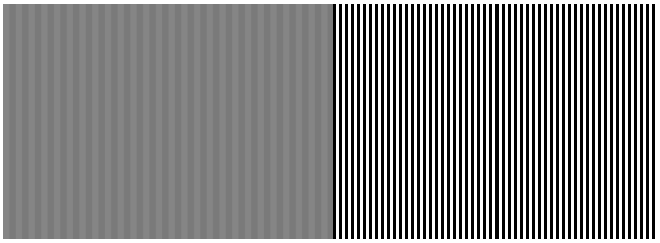

Fig. 1. Screenshot of a test mode (magnified image section to the right)

By measuring strength of electric component of compromising electromagnetic emanations field $E_{c,i}$ and assuming that passband of an input filter is $\Delta F = 1/\tau$ one can estimate SNR at the input of an eavesdropping device for every frequency range containing compromising emissions as follows:

$$q_j \approx \frac{2 \cdot n_j}{\Delta F_j} \sum_{\Delta F_j} \left(\frac{E_{c,i}}{E_{a.n,i} \cdot V_{r,i}} \right)^2 \quad (1)$$

where q_j - SNR at the input of an eavesdropping device for j-th frequency range, $E_{c,i}$ − strength of the electric component of the magnetic field's i-th spectral component of the j-th frequency range, mkV/m; $V_{r,i}$ – fading coefficient of the emanations at the i-th frequency; $E_{a.n,i}$ – spectral sensitivity of the antenna at the i-th frequency, measured at $SNR = 1$ and $\Delta F = 1$ Hz, mkV/(m·√Hz); ΔF_j − j-th frequency range, Hz; n_j – number of spectral components measured in the j-th frequency range.

Frequency ranges ΔF_j are calculated as follows:

$$\Delta F_j = f_{\max,j} - f_{\min,j} = \Delta F \quad (2)$$

$$f_{\min,j} = \frac{10^{-6} \cdot (j-1)}{\tau} \quad (3)$$

$$f_{\min,j} = \frac{10^{-6} \cdot j}{\tau} \quad (4)$$

where τ is the duration of impulses during the test mode, s.

When measuring strength of unintended emanations measuring antenna can be located either in a near-field region, a transition region or a far-field region depending on the wavelength of a signal in question. Near regional boundaries are defined by this equation:

$$r \le \lambda / 2\pi \quad (5)$$

while the far-field is the region for which

$$r > (3...10)\lambda \quad (6)$$

In this method far-field regional boundaries are defined as $r = 6\lambda$.

In the near-field region electric component of an electromagnetic field E_c fades inversely with the cube of distance and in the far-field region it fades inversely to the distance. It is assumed that in the transition region electric component E_c fades inversely with the square of the distance.

Therefore, fading of the emanations V_r is calculated as follows [11]:

1) For the emanations with a frequency f>1800 MHz.

$$V_r \approx r \quad (7)$$

2) For the emanations with a frequency 47,75 MHz < f ≤1800 MHz.

$$V_r = \begin{cases} r^2 & if \quad r \le \dfrac{1800}{f} \\ \dfrac{1800 \cdot r}{f} & if \quad r > \dfrac{1800}{f} \end{cases} \tag{8}$$

3) For the emanations with a frequency f ≤ 47,75 MHz.

$$V_r = \begin{cases} r^3 & if \quad r \le \dfrac{47.75}{f} \\ \dfrac{47.75 \cdot r^2}{f} & if \quad \dfrac{47.75}{f} \le r \le \dfrac{1800}{f} \\ \dfrac{8.59 \cdot 10^4 \cdot r}{f^2} & if \quad r > \dfrac{1800}{f} \end{cases} \tag{9}$$

Here f is a frequency of the measured emanation, MHz; r is a distance between device in question and eavesdropping device, m.

Estimation is made in regards to a probability of the compromising emanations being recognizable in noise. The case where a probability of a mistake is commensurate to a probability of correct recognition of the emanations P_{det} is the case of the most uncertainty when it comes to deciding whether compromising emanation is present. According to [10] such probability P_{det} is approximately 0.3.

Since emanations in question are bursts of identical incoherent non-fluctuating impulses probability of false negative recognition $P_{f.n.}$ can be estimated from a following equation [12]:

$$P_{\text{det}} \approx \Phi\left(q \cdot \sqrt{N} - \Phi^{-1}\left(1 - P_{f.n.}\right)\right) \tag{10}$$

μ and N are in in turn defined as follows:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp\left(-\frac{t^2}{2}\right) dt \tag{11}$$

$$N = F_k \cdot T_d \tag{12}$$

where q – SNR at the input of the eavesdropping device; N – number of averaged impulses; F_k – horizontal scan rate of the eavesdropped display, Hz; T_d – amount of time a displayed image is idle, s.

SNR limit value for eavesdropping device input can be estimated as follows:

$$\delta \approx \frac{\Phi^{-1}\left(P_{\text{det}}\right) + \Phi^{-1}\left(1 - P_{f.n.}\right)}{\sqrt{N}} \tag{13}$$

Therefore, for probabilities $P_{\text{det}} = 0.3$ and $P_{f.n.} = 0.001$ we get SNR limit value

$$\delta = 2.68 \Big/ \sqrt{N} = 2.68 \Big/ \sqrt{F_k \cdot T_d} \tag{14}$$

Estimation of a maximal potential eavesdropping distance r follows these steps:

1) Distance r is assumed to be 1 meter.

2) For every frequency range that contains compromising emanations SNR q_j should be estimated using equation (1).

3) These q_j are to be compared to δ value, in our case it should be value from (14).

4) As long at least one q_j from all frequency ranges exceeds δ value it means current r is less than maximal potential eavesdropping distance and therefore r should be incremented by 1 meter.

5) Steps 2-4 should be repeated until all q_j from all frequency ranges are less than δ value, or to put it in other words:

$$R = \min\{r\} \big| q_j \le \delta \tag{15}$$

IV. Experimental estimation

A. Experimental setup

Target video system of this experiment was RoverScan Optima 171 monitor connected to Radeon 9200 PRO Family graphical card by an unshielded VGA cable. Measurements were taken with a biconic measurement antenna «НБА-02» (As far we know manufacturer don't have any information regarding their products in English so antenna name is provided in Russian. Also we deemed necessary to include all relevant information since antenna characteristics are crucial for experimental estimation method.) and a spectrum analyzer Rohde & Schwarz R&S FPC1000. Antenna characteristics are listed in Table I. Its spectral sensitivity histograms are also provided as Fig. 2.1 – 2.3.

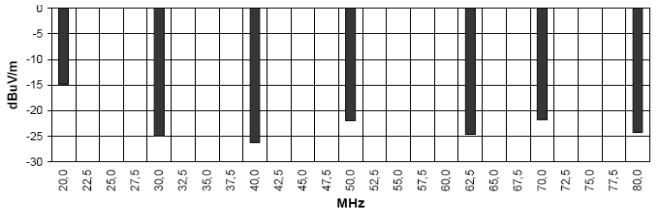

Fig. 2.1. Antenna spectral sensitivity histogram for frequencies from 20 MHz to 80 MHz

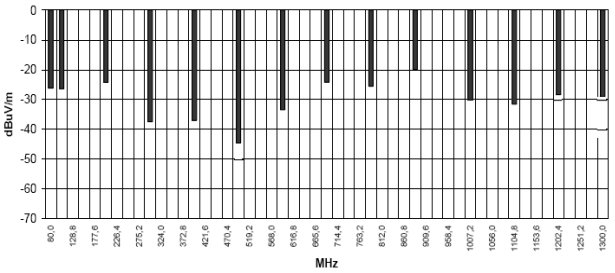

Fig. 2.2. Antenna spectral sensitivity histogram for frequencies from 80 MHz to 1.3 GHz

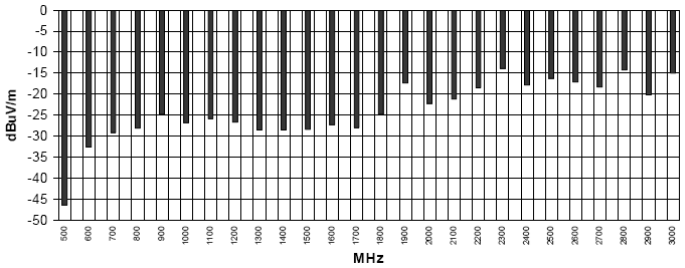

Fig. 2.3. Antenna spectral sensitivity histogram for frequencies from 0.5 GHz to 3 GHz

TABLE I. MEASUREMENT ANTENNA CHARACTERISTICS

Characteristics	Antenna name
	«НБА-02»
Antenna type	Electric biconical measuring antenna
Operating frequency range	0,009 - 2500 MHz
Calibration coefficient's measuring range	14 - 56 dB
Limits of permissible absolute error of calibration coefficient	±2,0 dB
Standing Wave Ratio (SWR)	± 2,0
Highest measurable electric field strength	140 dB (dBμV/m)
DC power supply	6 V
Uninterrupted operation time with a fully charged battery	≥ 10 hours
Type of RF output connector	N-Type

Experiment took place in a city environment in a building with numerous working computers resulting in a considerable noise level. Room where experiment took place had no shielding and was separated by wall from a room with 10 running computers providing us with a setup similar to a realistic office environment. Target video system was part of a running computer. Video mode was set to 1280x1024@60Hz. Target system was working in a test mode "black pixel – white pixel" mentioned earlier. Antenna was placed at distance of 1 meter away from target. Duration of impulses of signal sent during test mode from video card to display via VGA cable was measured beforehand using oscilloscope connected to a VGA cable wire (Fig. 3).

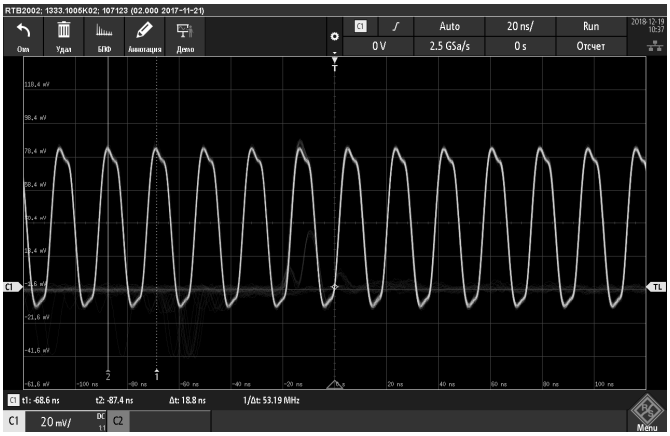

Fig. 3. Pixel scan measured on a "RED" channel wire

With a duration of impulses during test mode τ being equal to 9.2 ns emanations are expected to occur on frequencies that are multiplies of 54 MHz.

B. Results

Compromising emanations occurred with a frequency of 54 MHz as can be seen on Fig. 4. At frequencies higher than 1134 MHz harmonics became completely undetectable. All significant detected emanations are listed in Table II.

TABLE II. DETECTED COMPROMISING EMANATIONS

J	*f*. MHz	U_{s+n}, dB(dBμV/m)	U_n, dB(dBμV/m)
1	53.552	40.1	4.8
1	53.616	40.4	4.8
1	53.681	36.7	4.8
1	53.744	33.4	4.8
1	53.808	43.4	4.8
1	53.873	53.6	4.8
1	53.937	53.4	4.8
1	54	63.7	4.8
1	54.065	53.8	4.8
1	54.129	54.7	4.8
1	54.193	45.6	4.8
1	54.256	36.4	4.8
1	54.321	40.8	4.8
1	54.385	43.6	4.8
1	54.449	47.6	4.8
1	108	35.3	3.8
2	162	58.1	1.6
2	216	56.7	23.5
3	270	52.1	-2
3	324	46.3	15.1
4	378	38.8	-0.4
4	423	36.8	19.3
5	486	47.8	-0.4
5	540	32.6	4.9
6	593.82	24.6	0.5
6	593.884	31.1	0.5
6	593.948	30.2	0.5
6	594.013	42.7	0.5
6	594.077	31.6	0.5
6	594.14	32.4	0.5
6	594.205	24.8	0.5
6	648.014	19	17.4
7	702.015	28.4	-2.8
7	756.016	30.7	17.6
8	864.018	24.9	19.3
9	917.892	8.9	-4
9	917.955	7.6	-4
9	918.02	16.8	-4
9	918.085	8.7	-4
9	918.149	10.4	-4
9	972.021	8.9	-1.5
11	1134.02	6.7	-8

Fig. 4. Spectrogram of the compromising emanations

In order to calculate strength of the detected electromagnetic signals antenna calibration factor was added to measured values.

$$E_{s+n} = U_{s+n} + K_a(dB\mu V/m) \quad (16)$$

$$E_n = U_n + K_a(dB\mu V/m) \quad (17)$$

Detected emanations were grouped into ranges using (2)(3)(4) resulting in 11 ranges of ΔF = 108.696 MHz, with no emanations detected in the 10th range.

After converting these values to mV/m strength of the signal was deducted from strength of a signal mixed with noise.

$$E_n = \sqrt{E_{s+n}{}^2 - E_n{}^2}\,(mV/m) \quad (18)$$

Assuming that displayed image would be idle for 120 seconds SNR limit δ for this setup (14) is 0.03158.

Harmonic at 486 MHz proved to be the most compromising component of emanations in question due to its high SNR. Its estimated SNR exceeding limit only at approximate distance of 58 meters. Estimated SNR values for all frequency ranges during two last steps of incrementing the distance are shown in Table III.

TABLE III. ESTIMATED SNR

Frequency range j	**SNR q_j**	***Frequency range j***	**SNR q_j**
r =57 m.		***r =58 m.***	
1	0,00115	1	0,00111
2	0,00107	2	0,00104
3	0,00903	3	0,00872
4	0,00085	4	0,00082
5	0,03186	5	0,03077
6	0,00611	6	0,00591
7	0,00003	7	0,00003
8	0,0000007	8	0,0000007
9	0,000003	9	0,000003
11	0,0000004	11	0,0000004

V. CONCLUSION

Due to large number of unpredictable factors, it is not possible to calculate the power of unintended electromagnetic emanations. Therefore, an assessment of the possibility for intercepting these emanations for each system is to be carried out using an instrumental and computational method that involves measuring strength of the electromagnetic field's electric component at a distance of 1 meter and measuring or calculating the fading of the signal in question.

Resulting estimation of 58 meters is within expected distances considering that VGA cable of eavesdropped system acts as an antenna transmitting compromising emanations. While experimental setup was made with the idea of realistic public environment in mind it should be noted that estimation was made with numerous assumptions. Most notable assumption is the amount of time displayed image remains idle. This assumption was made as an evaluation of a period of time a fixed image containing sensitive information would be displayed by video system without significant changes in displayed image. This value is essential for the final result of the estimation since it defines the SNR limit value. Statistical evaluation of this parameter should improve method used in this paper.

Most of other assumptions were made considering how unlikely it would be for video system of unregulated (in terms of TEMPEST) workplace to have settings that specifically lower SNR of compromising emanations.

Overall, chosen mathematical model is based on possibility of detecting, recognizing and acquiring enough samples for restoring information from captured signal and is considered to be sufficiently accurate. We believe that this paper properly demonstrated how relatively easy it is to calculate estimated eavesdropping distance with a estimation method of our choice.

ACKNOWLEDGEMENT

We would like to thank Anatoliy Horev for developing estimation method used in this paper and Denis Smirnov from National Research University of Electronic Technology (MIET) who helped us with the installing and adjusting the equipment used in this experiment.

REFERENCES

[1] Wim van Eck, "Electromagnetic radiation from video display units: An eavesdropping risk?" *Computers & Security*, Vol. 4, Iss. 4, Dec.1985, pp. 269-286.

[2] M.G. Kuhn, "Electromagnetic eavesdropping risks of flat-panel displays", *In Proceedings of 4th International Conference on Privacy Enhancing Technologies*, May 2004, pp.88-107.

[3] C. Zhang, H. Zhang, J. Luo and Yu. Du, "TEMPEST in USB", *2017 IEEE 5th International Symposium on Electromagnetic Compatibility (EMC-Beijing)*, Oct. 2017, pp. 129-132.

[4] M. Vuagnoux and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards", *In Proceedings of the 18th conference on USENIX security symposium*, Aug. 2009, pp. 1-16.

[5] L. Wang and B. Yu, "Analysis and measurement on the electromagnetic compromising emanations of computer keyboards", *Proceedings - 2011 7th International Conference on Computational Intelligence and Security, CIS,* Dec. 2011, pp. 640-643.

[6] D.A. Umphress and J. Loughry, "Information leakage from optical emanations", *ACM Transactions on Information and System security,* No. 5*,* Iss. 3, Aug. 2002, pp. 262-289.

[7] J. Loughry, "Optical TEMPEST", *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE),* Aug. 2018, pp. 172-177.

[8] M. Guri, B. Zadov, A. Daidakulov and Y. Elovici, "xLED: Covert data exfiltration from air-gapped networks via router LEDs", *arXiv preprint arXiv:1706.01140*, Jun. 2017.

[9] U. Sarac, I. Erer and F. Elibol, "Realistic eavesdropping attacks on computer displays with low-cost and mobile receiver system", *Proceedings of the 20th European Signal Processing Conference (EUSIPCO 2012)*, Aug. 2012, pp. 1767-1771.

[10] A.A. Horev, "Evaluation of the possibility of detection side compromising electromagnetic emanations video PC", *Proceedings of TUSUR University,* №2 (32), Mar. 2014, pp.207-213. (In Russian)

[11] A.P. Zaicev, A.A. Shelupanov, P.V. Mesheryakov, S.V. Skryl and I.V. Golubyatnikov, *Tehnicheskie sredstva i metody zashity informacii [Technical devices and methods of protecting information]*. Moscow: Izdat. Machinostroenie, 2008, p. 322. (In Russian)

[12] A.A. Korostilev, N.P. Kluev and Y.A. Melnik, *Teoreticheskye osnovy radiolocatcii: Uchebnoe posobie. dlya VUZov, 2-e izdanie [Theory of radiolocation: Textbook for higher education institutions, 2nd Edition]*. Moscow: Sov. Radio, 1978, p 608 p. (In Russian)