Considerations for Emission Security Risks From the Perspective of Signal Processing Techniques

Răzvan Bărtuşică, Mircea Popescu, Alexandru Boitan
The Special Telecommunications Service
Bucharest, Romania
razvan.bartusica@sts.ro, mircea.popescu@sts.ro,
alexandru.boitan@sts.ro

Simona Halunga
University Politehnica of Bucharest, Electronics
Electronics, Telecommunications and Information
Technology Faculty
Bucharest, Romania
simona.halunga@upb.ro

***Abstract*—The main scope of this paper is to improve the security risk analysis of critical communication and information systems. One of the major security objectives is to ensure the security emissions generated by electronic equipment, which may contain confidential data. A rigorous risk analysis helps to establish optimal protection solutions to prevent information leakage through compromising emissions. This work analyzes some security threat, reflected in the technical capabilities of the interceptor in the processing of compromising signals, which supports substantially risk analyzes for the protected system. The estimation of the signal to noise ratio of compromising emissions, at the boundary of protected area, had been tested and validated by measurements.**

Keywords— compromising emissions; emission security; EMSEC.

I. INTRODUCTION

Ensuring the confidentiality of data processed by information systems against leakage of information through the secondary electromagnetic emissions generated by IT equipment has become a priority in the context of IT & C technology evolving at an impressively fast.

The risk analysis of Emissions Security (EMSEC) for a communications and information system is generally studied in a correlated manner, combining the vulnerabilities and the threats, in order to protect the electronic system against possible hacking attempts. A rigorous EMSEC risk analysis helps to establish the TEMPEST protection measures against electronic systems information leakage through compromising emissions.

A large number of studies in the domain of information leakage due to accidentally electromagnetic emissions, underlining the importance of the EMSEC domain. In [1-4] the authors concentrated on evaluating and reducing compromising emissions, while in [5-7] a number of test methods to evaluate radiated and conducted emission had been presented. Several approaches to information leakage mitigation and TEMPEST countermeasures are shown in [8-13]. In some of their previous work [9-10], the authors presented results regarding the efficiency of shielding and filtering for IT&C equipment under TEMPEST evaluation.

In this work we study the influence of the processing techniques of the compromising signals that are generated by a commercial computer, when increasing the signal to noise ratio received at the boundary of protected area, and implicitly growing the risk of interception of these electromagnetic emissions by a hostile receiver. Based on the developed test bed, the estimated value of signal to noise ratio is then verified in lab.

The paper is organized as follows - Section II establishes the theoretical basis for estimating the signal–to–noise ratio depending on the processing gain of compromising emissions, obtained in a scenario in which a commercial computer should be protected; Section III tests the theoretical approaches presented in section II, by laboratory tests; Section IV is dedicated for conclusions.

II. ESTIMATE OF EMISSION SECURITY RISKS FROM THE PERSPECTIVE OF SIGNAL PROCESSING TECHNIQUES

In order to analyze the risk of intercepting compromising emissions generated by devices, one should study (1) the vulnerabilities of the security environment, such as electromagnetic attenuation of the buildings and free space between the equipment and the perimeter of the protected area, the ambient radio noise in site; (2) the vulnerabilities of the information system, such as the level of secondary RF emissions generated by equipment, the signal-to-noise ratio at the protected area boundary and (3) make an estimation of the possible threats, like the noise factor of the eavesdropper's receiver, the gain of the directional antenna and the processing gain achieved with signal processing used by the eavesdropper[17-18].

In order to study the influence of signal interception processing techniques on the risk of emissions security, one should determine the signal to noise ratio for the compromising emissions generated by the computer systems, from EMSEC point of view [1].

$$SNR = \frac{\hat{E}_B \cdot G_a \cdot G_p}{a_d \cdot a_w \cdot E_n \cdot F_r} \quad (1)$$

where $\hat{E}_B$ is the maximum limit allowed for compromising emissions generated by information systems, G_a is the gain of the best directional antenna used by the eavesdropper, G_p is the processing gain achieved with signal processing, a_d is the free-space path loss at distance d between the eavesdropper's antenna and the target device, E_n is the radio noise field strength at the installation site receiving antenna, F_r is the noise factor of the eavesdropper's receiver, SNR is the signal–to–noise ratio and a_w is the additional attenuation conferred by the architectural shielded of facility in which the target device is located. This can also be evaluated in logarithmic values:

$$[SNR]=\left[\hat{E}_b\right]+[G_a]+\left[G_p\right]-[a_d]-[a_w]-[E_n]-[F_r] \quad (2)$$

where $[x]=20\lg(x)$ is the value of a general parameter x in dB.

Using this relationship we evaluated the [SNR] dependency on the processing gain [G_P], under the assumptions of maximum allowable limits for the compromising emissions, as results from [1]. We presumed that the maximum allowable radiated VHF field strength levels, [$\hat{E}_B$], does not exceed 41 dBµV/m measured in the laboratory tests, at a distance of 1 m from the IT equipment, with a resolution bandwidth of 50 MHz; the gain of the directional antenna used by eavesdropper is [G_a]=16dBi; the eavesdropper's receiver does not get closer than d = 10 m, so [a_d]=20lg(10m/1m)=20 dB; the attenuation value of the building materials is [a_w]=5 dB; the noise figure of eavesdropper's receiver (type Rohde&Schwarz FSET22) is [F_r]=7 dB; the background noise level in one typical to a rural environment, measured with a resolution bandwidth of 50 MHz in VHF range, is [E_n] = 27 dBµV/m. With those settings, the dependency of the [SNR] dependency on the processing gain [G_P] is shown in Fig. 1, allowing us to establish the upper limits for the measured [SNR].

One can observe that, for a processing gain [G_p]=2 dB, it results a [SNR]=0 dB at a distance of 10 m from the IT system target, which means that the risk of detection and interception of the compromising signal is very low. But for [G_p] = 8 dB, we obtain a [SNR]=6 dB, which is the threshold value of detection of useful signals sought in the spectrum in radio monitoring, so, as the processing gain increase, same does the risk that the compromising emission might be intercepted

In the EMSEC risk analysis, the value [SNR]=6 dB, equivalent to free space attenuation into 2 m, is a critical one, since it changes the TEMPEST site protection class, if the analysis is made at the boundary between two TEMPEST zones, or determine the selection of an electronic equipment with increased electromagnetic attenuation of compromising emissions.

To prevent information eavesdropping due to compromising emissions, possible countermeasures are the reduction of leaked radiated and conducted electromagnetic emission from informatics systems or the increase of difficulty to reconstruct the original signal, if leaked compromising emissions are intercepted. These goals can be achieved through compromising signal reduction and radio noise generation for masking signals; both methods are taken into account in order to decrease signal-to-noise ratio of the leaked signal at eavesdropper's receiver.

III. Validation Method of Calculation

In order to validate the theoretical approach, described in Section II, several tests had been performed in the lab. The setup for measurement is presented in Fig. 2, where EUT is the equipment under test, Rx is the receiver, type Rohde&Schwarz FSET22, DSO is digital storage oscilloscope, type MSO 5204B, and SPS is the signal processing system endowed with software for processing.

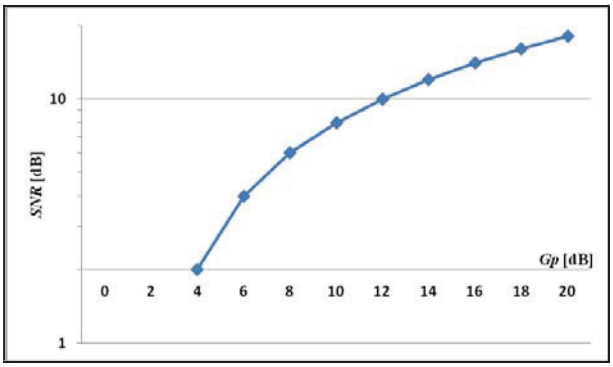

Fig. 1. Variation [SNR] depending on processing gain, [Gp], for compromising emissions received at 10 m from the comercial equipment, with a resolution bandwidth of 50 MHz.

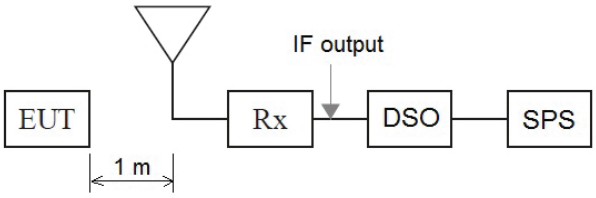

Fig. 2. Test setup for validation of claculation processing gain, at a distance of 1 m from the IT equipment, with a resolution bandwidth of 50 MHz.

The compromising signal was received on the frequency of 133 MHz, with Resolution Bandwidth RBW = 50 MHz, and, at the IF output of the receiver. Received signal is represented in Fig. 3. It has been introduced into the oscilloscope for processing and, using the oscilloscope tools, a Fast Fourier Transform (FFT) has been applied to detect the waveform spectral components. The spectral representation of the received signal is shown in Fig. 4.

The received IF signal has been attenuated with 20 dB, equivalent to 10 m emission attenuation in free space propagation, and, in order to increase the frequency resolution, the number of BINs, N_{BIN}, has been increased to detect more accurately the spectral components.

The advantage of using the FFT for the IF signal at the output of the receiver is that it allows us to select a higher sensitivity and resolution in the frequency than the one offered by conventional analogue receivers, for the same frequency span BW_{BIN}. In our measurements, in order to obtain the

desired processing gain, we increased the number of FFT points, N_{BIN},, keeping constant the sampling frequency at 100MS/s.

Thus, the noise level displayed in the spectral representation is controlled by the additional processing cost: $N_{BIN} = FFT_{size}/2$, $RBW = Fs/(2*N_{BIN}) = F_{max}/N$. The displayed Noise Level is $[DNL] = -174$dBm + $[NF]$ + $10xlog(RBW/Hz)$, with $RBW = BW_{BIN}$. The resulting processing gain obtained by increasing the N_{BIN} parameter is $[G_P] = 10log(N_{BINmax}/ N_{BINmin})$.

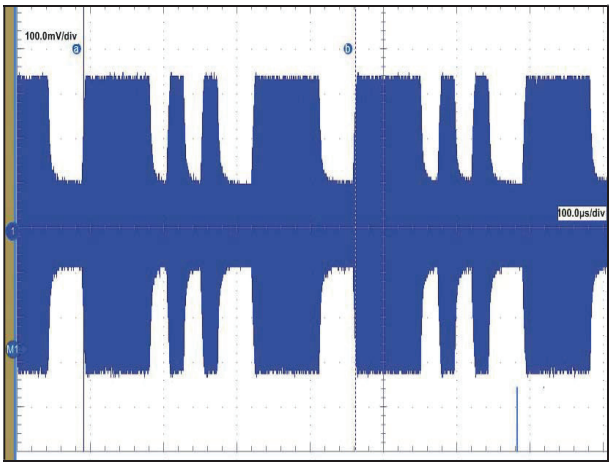

Fig. 3. The waveform of the compromising signal received on the 133 MHz frequency, with a resolution bandwidth of 50 MHz.

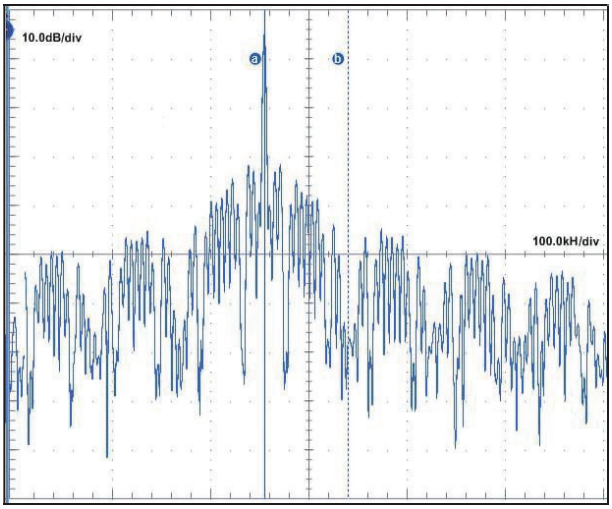

Fig. 4. Representation of FFT applied to the unattended waveform compromising signal.

Using an 10^5 FFT points, the resulting spectrum is shown in Fig. 5. Based on this, we evaluated the $[SNR_{process}]$ at 18.12dB.

If the number of FFT points is increased to 10^7, the IF spectrum obtained is represented in Fig. 6 and the resulting $[SNR_{process}]$ is 35.83dB. So, due to the difference in FFT points from 10^5 to 10^7, we have obtained a processing gain of $[Gp]$ = 17.71dB. This gain, used in relation (2), determines a $[SNR]$ at the boundary of the EMSEC protected area, of $[SNR]$=15.71dB, which represents a high EMSEC risk of intercepting the compromising signal. To neutralize this risk, mitigation measures should be implemented at equipment or site level, or the boundary of the protected area should be extended by more than 6 m.

These goals can be achieved through compromising emissions reduction and radio noise generation in order to mask emissions and decrease interception risk.

In future work we will evaluate the effect of shielding the equipment, filtering its power lines, generating radio noise and other technical measurements in order to improve the level of protection against compromising emissions.

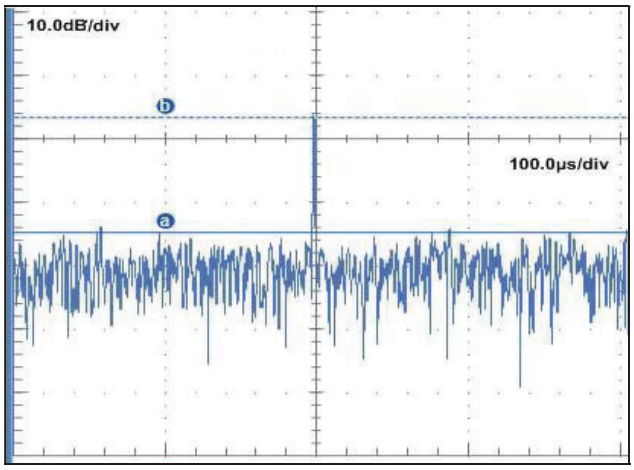

Fig. 5. The spectrum for 10^5 FFT points, applied to the waveform compromising signal

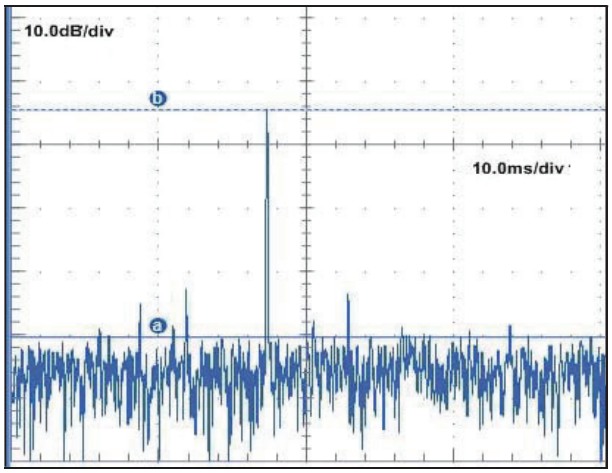

Fig. 6. The spectrum for 10^7 FFT points, applied to the waveform compromising signal.

IV. Conclusions

The method using an FFT with high number of points at the receiver has the effect of increasing frequency sensitivity and resolution, obtaining superior results compared to

conventional analogue spectrum analyzers (for the same frequency span).

The processing gain obtained by increasing the number of FFT points and RBW reduction, confirms the theoretical values and allows accurate detection of spectral components with low SNR.

By increasing the number of FFT points from 10^5, leading to a measured [*SNR*] = 18.12 dB to 10^7, leading to a measured [*SNR*] of 35.83 dB, relative to the carrier, a processing gain of 17.71 dB was obtained.

Those results show that, in order to protect an electronic device from potential eavesdropper's intrusion, as the processing capabilities of such intruders increase with the technological development, one has to take caution measures like shielding, filtering or other protection methods to avoid such type of intrusion.

ACKNOWLEDGEMENT

This work was supported by a grant of the Ministry of Innovation and Research, UEFISCDI, project number 5 Sol/2017 within PNCDI III, Integrated Software Platform for Mobile Malware Analysis (ToR-SIM), and partially funded under Contract no. 213PED/2017, OFDM System based on FFT with non-integer argument (FractOFDM).

REFERENCES

[1] M. G. Kuhn, "Compromising emanations: eavesdropping risks of computer displays", University of Cambridge Computer Laboratory, Cambridge, Technical Report UCAM-CL-TR-577, 2003. [Online] Available: http://www.cl.cam.ac.uk/TechReports.

[2] Y. Suzuki, R. Kobayashi, M. Masugi, K. Tajima, H. Yamane, "Development of Countermeasure Device to Prevent Leakage of Information Caused by Unintentional PC Display Emanations," Proceedings of European Electromagnetics 2008 - EuroEM2008, Lausanne, Switzerland, pp. 44-52, 2008.

[3] H. Tanaka, "Information leakage via electromagnetic emanations and evaluation of TEMPEST countermeasures", Information Systems Security Springer Berlin Heidelberg, pp. 167-179, 2007.

[4] M. Kinugawa, Y. Hayashi, T. Mizuki, H. Sone, "Information Leakage from the Unintentional Emissions of An Integrated RC Oscillator", Electromagnetic Compatibility of Integrated Circuits (EMC Compo), 8th Workshop, pp. 164-168, 2011.

[5] Recommendation ITU-T K.84, „Test methods and guide against information leaks through unintentional electromagnetic emissions", Telecommunication Standardization Sector of ITU, 2011.

[6] Sekiguchi, H., Seto, S., „Measurement of Radiated Computer RGB Signals", Progress In Electromagnetics Research C, Vol. 7, pp. 1-12, 2009.

[7] Sekiguchi, H., Seto, S., „Measurement of Computer RGB Signals in Conducted Emission on Power Leads", Progress In Electromagnetics Research C, Vol. 7, pp. 51-64, 2009.

[8] Y. Suzuki, M. Masugi, H. Yamane, K. Tajima, "Countermeasure Technique for Preventing Information Leakage Caused by Unintentional PC Display Emanations", Proceedings of International Symposion on EMC 2009, pp. 9-12, 2009.

[9] M. Popescu, R. Bărtusica, A. Boitan, S. Halunga, " Considerations on estimating the minimal level of attenuation in TEMPEST filtering for IT equipments ", Springer Berlin Heidelberg, Proceedings of 3rd EAI International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures - FABULOUS 2017, Bucharest, 2017.

[10] M. Popescu, V. Bîndar, R. Crăciunescu, O. Fratu, "Estimate of Minimum Attenuation Level for a TEMPEST Shielded Enclosure", Proceedings of 11th International Conference on Communications – COMM 2016, Bucharest, pp 521-526, 2016.

[11] V. Bîndar, M. Popescu, R. Crăciunescu, "Aspects of Electromagnetic Compatibility as a Support for Communication Security Based on TEMPEST Evaluation", Proceedings of 10th International Conference on Communications - COMM 2014, Bucharest, pp. 529-532, 2014.

[12] V. Bîndar, M. Popescu, A. Vulpe, „Considerations Regarding Shielding Effectiveness and Testing of Electromagnetic Protected", Proceedings of 10th International Conference on Communications - COMM 2014, Bucharest, pp. 481-486, 2014.

[13] L. Jinming, J. Mao, J. Zhang, L. Yongmei, "The Designing of TEMPEST Security Testing Model." TELKOMNIKA Indonesian Journal of Electrical Engineering 12, no. 2, pp. 866-871, 2014.

[14] Z. Zhang, Y. Yu, "Quality Evaluation Model of Information Reconstruction via Electromagnetic Emanation", TELKOMNIKA Indonesian Journal of Electrical Engineering, vol. 12, no. 3, pp. 1960-1964, 2014.

[15] L. Zhu, Y. Shi, L. Deng, H Shi, "Electromagnetic Vector Sensor array parameter estimation method", TELKOMNIKA Indonesian journal of electrical engineering, vol.12, no. 3, 2013.

[16] K. Taishi, H. Yu-ichi, M. Takaaki, H. Naofumi, A. Takafumi, S. Hideaki, "Suppression of information leakage from electronic devices based on SNR", Proceedings of IEEE International Symposium Electromagnetic Compatibility (EMC), pp.112-116, 2011.

[17] Recommendation ITU-T K.87, „Guide for the application of electromagnetic security requirements", Telecommunication Standardization Sector of ITU, 2011.

[18] ITU-T Handbook, "Security in Telecommunications and Information Technology – An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications", 2003.