Considerations on Estimating the Minimal Level of Attenuation in TEMPEST Filtering for IT Equipments

Mircea Popescu[1](✉), Răzvan Bărtuşică[1], Alexandru Boitan[1],
Ioana Marcu[2], and Simona Halunga[2]

[1] The Special Telecommunications Service, Bucharest, Romania
mpopescu@sts.ro
[2] University Politehnica of Bucharest, Bucharest, Romania
imarcu@radio.pub.ro

Abstract. The main purpose of this research is to improve the security of critical computer systems with minimal costs. One of the main problems in such cases is the secondary emissions generated by electronic equipment that, sometimes, might contain confidential information stored inside a secured computer network. The implementation of a set of measures necessary to prevent information leakage through compromising emissions is generally expensive. This paper analyzes some minimal requirements that have to be fulfilled by the filtering devices in order to protect the existing commercial IT equipment against compromising emissions.

Keywords: Compromising emissions · TEMPEST · Electrical filter

1 Introduction

Protection against electromagnetic disturbances is becoming an increasingly important issue for all researchers that have to deal with critical information, such as banks, commerce and security, given that our daily activity becomes more dependent on computers and telecommunications. As they become more and more sophisticated, they tend to become less resistant to electromagnetic interferences.

Both filtering and shielding are designed to reduce the electromagnetic radiation, so these two operations can be seen as a synergy, each complementing the other. Thus it is important to understand that inappropriate filtering can easily increase the risk of radiated coupling and inappropriate shielding can lead to conductive coupling.

A proper design of the filters may prevent interferences from electrical wires inside or outside the protected area through metallic interfaces, reducing the conductive coupling, as well as the radial coupling to and from the cables. In TEMPEST protection [1] filters are used to prevent these interferences generated in computer equipment to propagate outward as compromising emissions transmitted through the power supply network.

A large number of research and studies in the area of compromising emissions in the interconnection lines of electrical equipment are under development, underlining

O. Fratu et al. (Eds.): FABULOUS 2017, LNICST 241, pp. 9–15, 2018.
https://doi.org/10.1007/978-3-319-92213-3_2

the importance of the domain. In [1–3] the authors concentrated on evaluating and reducing the compromising radiations of LCD/TV sets, while in [4] a number of TEMPEST security testing models and countermeasures are illustrated. In [5] the authors presented the results obtained in reconstruction of laser printer information based on the leakages in the media of electromagnetic radiation, power and signal lines. A model and testing procedures for critical systems to severe electro-magnetic threats are given in [6] while in [7] the authors show a number of results related to efficiency of shielding for communication equipment under TEMPEST evaluation.

In this paper we estimate a minimum level of attenuation of an electrical filter installed on the supply line of commercial computer equipment, so that at the exit of the controllable zone the compromising signals generated by the equipment cannot be detected and intercepted by a hostile receiver. Based on the developed testbed the estimated value is then verified under worst case scenario.

The paper is organized as follows: Sect. 2 sets the theoretical basis for estimating the minimum attenuation value of an electric filter for TEMPEST protection of commercial computer; Sect. 3 illustrates by relevant laboratory tests the theoretical considerations presented in Sects. 2 and 4 contains the main conclusions drawn from tests in Sect. 3.

2 Estimation of the Minimum Attenuation Level for an Electrical Filter in TEMPEST Protection

To establish the minimum level of attenuation of the filter installed on the power line to ensure TEMPEST protection of an IT system, we assume the following: the target computer equipment is commercial type (COTS) and meets the electromagnetic disturbance requirements specified in European Standard EN 55022 [8]; the signal-to-noise ratio (*SNR*) received on the power line in the controllable space is limited to 1 (or 0 dB) to reduce the probability of detecting compromising emissions generated by computer equipment; the attacker has the ability to connect sensitive receivers directly to the building's power supply, communication cables or other metal structures near the target device as well as to receive and process compromising signals with low levels comparable to electrical noise; the electrical noise received by the interceptor on the power line is specific to the residential environment; the interceptor searches for broadband pulses in a quiet zone of the spectrum, with as little external interference as possible; it uses "notch" filters to suppress strong emissions from narrowband radio stations as well as strong signal processing techniques to extract the information carrier from the unwanted background noise.

The minimum filter attenuation level installed on the power line to reduce the probability of detecting and intercepting compromising emissions by a hostile receiver at the limit of controllable space can be determined by [1]

$$A_F \frac{U_B \cdot G_p}{U_{n,B} \cdot A_c \cdot f_r \cdot SNR}. \qquad (1)$$

where *UB* is the maximum voltage of the conducted disturbances allowed by EN 55022 [8] received with equipment with the IF bandwidth *B*; *Gp* is the processing gain obtained by specific techniques (e.g. periodic mediation, correlations) for recovering the information from the compromising signal; *Un,B* is the root mean square of the background noise noticed by the IF receiver with the bandwidth *B*; *AF* is the attenuation of the electrical filter installed on the power line between the target equipment and the hostile receiver; *Ac* is the attenuation of the signal through the conductor network between the target equipment and the hostile receiver; *fr* is the noise figure of the interceptor receiver.

Rewriting (1) on a logarithmic scale

$$[A_F] = [U_B] + [G_p] - [U_{n,B}] - [A_c] - [f_r] - [SNR], \tag{2}$$

where $[x]$ = *20lg (x)* is the value of parameter x expressed in dB.

The noise and cable attenuation values in the above equations are random variables, which, in the absence of standardized data, might be modeled as a normal distribution with mean and variance evaluated statistically based on a large number of measurements in different environments. For other parameters, reasonable estimates must be made, based on the values used in most practical applications, such that the [*SNR*] should be below an acceptable level with a sufficient detection probability.

Different types of target signals are received on different frequency ranges and allow different processing gains. Thus all parameters must be estimated separately for the different types of signal of interest. In this paper we assume that the signals have the data rate equal to 5 MHz (e.g. the signal generated by the video card).

The EN 55022 EMC standard imposes that the maximum allowed voltage disturbances measured across a 50 Ω impedance in parallel with 50 μH should not exceed 46 dBμV in the frequency range 0.5 ÷ 5 MHz, respectively 50 dBμV in the frequency range 5 ÷ 30 MHz measured with a average detector having a resolution bandwidth of 9 kHz [8]. The compromising emissions of modern digital signals contains wideband impulses so the receiver passband has to be extended from 9 kHz (specified in EN 55022 standard) to 2 or 5 MHz. Hence, the received signal strength increases by 20lg (2 MHz/9 kHz) = 47 dB for signal with the bandwidth of 2 MHz, and 20lg (5 MHz/9 kHz) = 55 dB for signal with the bandwidth 5 MHz.

To determine the value of the electrical filter attenuation, [*AF*], the worst case scenario has been taken into consideration corresponding to the case in which the electronic equipment generates secondary emissions on the power line to the maximum allowed level. Applying this correction (i.e. for 5 MHz resolution bandwidth) we obtain the limits for the conducted emissions: [*UB*] = (46 + 55) = 101 dBμV, for RBW@5 MHz, in the frequency range 0.5 ÷ 5 MHz and [*UB*] = (50 + 55) = 105 dBμV for RBW@5 MHz in the frequency range 5 ÷ 30 MHz.

The eavesdropping receiver used for tests is a Rohde& Schwarz FSET 7 with IF bandwidths of 2 or 5 MHz and noise figure [*fr*] = 7 dB [7]. Using time domain averaging to increase the signal-to-noise ratio of a periodic signal [1] with *N* repetitions of a properly in phase aligned signal the processing gain can be calculated by

$$G_p = \sqrt{N} \text{ or } [G_p] = 10 \cdot \lg N \ (\text{dB}). \tag{3}$$

Assuming that the attacker applies signal processing techniques by mediating the received signal on $N = 10$ frames, the resulting processing gain is approximately 10 dB. The noise on the power supply is expected to be at least 30 dB above the thermal noise level [1, 9] which is 0 dBμV at $B = 5$ MHz. Therefore $[Un,5] = 30$ dBμV might be a plausible value of the electrical noise received on the power line at $B = 5$ MHz. From experimental measurements the attenuation between two outlets in a building for the frequency range 1 ÷ 60 MHz can be, on average, around 10 dB if the sockets are in the same circuit, and 40 dB if they are located in different circuits [1, 9]. From (3) there can be determined the minimum attenuation value, $[AF]$, for a low- pass filter in the HF/VHF frequency range installed on the power supply line of the computer system, so, at the building boundary, the compromising signals accidentally emissions transmitted on the power circuit from a COTS computer system cannot be detected by an attacker, is given by

$$[A_F] = 105 + 10 - 30 - 10 - 7 - 0 = 68 \text{ dB} \tag{4}$$

Thus we can conclude that a low-pass electrical filter with attenuation equal to 70 dB, evaluated for HF/VHF frequency range, provides adequate TEMPEST protections if all the COTS informatics equipment operated indoor comply with EN55022 limits.

3 Experimental Validations of the Results

In order to validate the theoretical aspects presented in Sect. 2, a series of tests and measurements were carried out in Special Telecommunications Service (STS) TEMPEST lab.

The first test aimed to detect compromising emissions generated by a commercial computer on the power line and recover the information contained in the received emissions. To achieve this, a test receiver Rohde& Schwarz FSET 7 with IF bandwidths of 5 MHz was used and a line impedance stabilization network (LISN) was installed on the supply line of the test equipment. The results, presented in Fig. 1a, show the level of the secondary emissions through the power line from a computer with an image displayed on the monitor (red trace) and without an image displayed on the monitor (green trace). From the spectral analysis a compromise emission around 25 MHz has been determined, which in this case contains the video signal from the video card. Using a dedicated software package for TEMPEST evaluation, the signals received at the 25.37 MHz frequency were filtered, correlated and the image displayed by the test computer monitor was restored, as shown in Fig. 1b.

The second test has been developed to validate the estimated value for the attenuation of the electrical filter obtained in Sect. 2. For this, the test configuration in Fig. 2a has been used, where PG is the pulse generator, RFG is the radiofrequency signal generator Rohde & Schwarz SMP04, ATT is the variable attenuator, REC is the TEMPEST test receiver, Rohde & Schwarz FSET7 and AQ&PC are the data

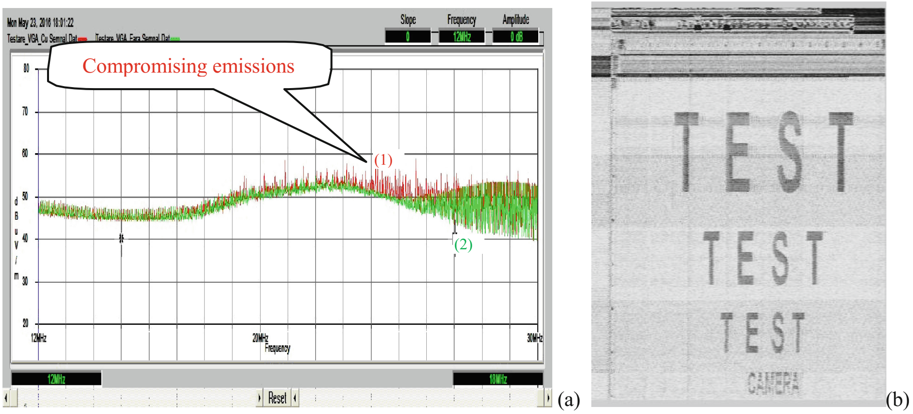

Fig. 1. (a) The comparative spectral analysis of the secondary emissions in power line by a computer using an image displayed on the monitor (trace 1) and no image displayed on the monitor (trace 2), and (b) recovered image processed from secondary emissions by a computer, from power line. (Color figure online)

acquisition board and processing computer. To simulate the compromising signal generated by an electronic device, we use a periodic radio pulse as reference signal, with the carrier frequency of 25 MHz, the modulating frequency of 5 MHz and the modulation index of 50%. The RF generator has been set for a signal level of 105 dBμV, which is the level corresponding to the EMC limit of the EN 55022 converted for the 5 MHz band. This reference emission obtained with the RF generator was injected into the power line of a computer using an absorbing clamp Rohde & Schwarz MDS21. The computer power cable with the length of 10 m was inserted into the LISN. The RF output from LISN was connected to a variable attenuator, used to simulate the attenuation introduced by an electrical filter interposed between the computer equipment and the hostile receiver. In the reception chain a test receiver (Rohde & Schwarz FSET 7) set on 5 MHz IF bandwidth was connected. The receiver video output was connected to the acquisition board and a computer for spectral analysis and data processing. The reference electrical signal injected onto the computer power line is shown in Fig. 2b.

Next, the variable attenuator was incrementally increased until the reference signal was covered by the power line radio frequency, so [*SNR*] = 0 dB was obtained. Thus, it has been concluded that for 65 dB attenuation, the electrical signal from the power line cannot be restored. From the comparative analysis between theoretical and practical results, it has been concluded that a 70 dB attenuation of the electrical filter installed on a computer's power line ensures the TEMPEST protection of the information system against leakage through secondary emissions.

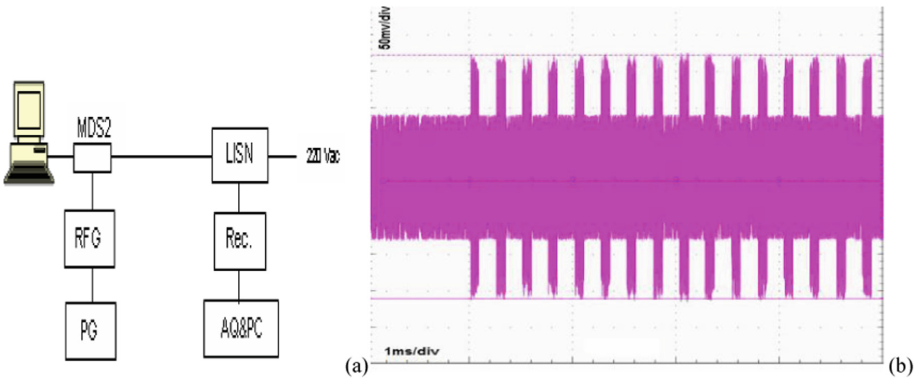

Fig. 2. (a) Test setup for validation of evaluation the minimum level of filter attenuation (b) the waveform of reference electrical signal

4 Conclusions

Based on the evaluations and tests performed we can conclude that, for commercial computer system installed in a residential environment, an electrical filter with an attenuation of 70 dB in the HF/VHF frequency range for conducted emissions, provide adequate TEMPEST protection against leakage of compromising emissions if the electrical equipment it complies to the EN 55022 limits. This value was achieved in the worst case scenario in which the IT equipment is of a commercial type, without TEMPEST protection measures (shielding, interconnection filtering, etc.), the distance between the source of the compromising emission and the hostile receiver was only 10 m, the electrical noise on the power line was only generated by the computer equipment because the entire test system was isolated by LISN from the power supply and the tests were carried out in the shielded room.

Whereas the technical measures to prevent information leakage through compromising emissions are generally expensive, this study is applicable in practice by the fact that recommends minimum technical requirements for security of emissions that can be implemented at low cost and with commercial resources.

Open issues that can be addressed in the future are oriented towards the study of the minimum attenuation for the electrical filters installed on the interconnection circuits of the information systems (data network, voice communications, etc.), as well as analyzing the compromising emissions conducted in the grounding circuit of a computer.

Acknowledgments. This work was supported by a grant of the Ministry of Innovation and Research, UEFISCDI, project number 5 Sol/2017 within PNCDI III.

References

1. Kuhn, M.G.: Compromising emanations: eavesdropping risks of computer displays. University of Cambridge Computer Laboratory, Technical report (2003)
2. Sekiguchi, H., Seto, S.: Measurement of computer RGB signals in conducted emission on power leads. Prog. Electromagnet. Res. C **7**, 51–64 (2009)
3. Kuhn, M.G.: Compromising emanations of LCD TV sets. In: Proceedings of the IEEE International Symposium on Electromagnetic Compatibility, pp. 931–936 (2011)
4. Jinming, L., Mao, J., Zhang, J.: The designing of TEMPEST security testing model. TELKOMNIKA Indonesian J. Electr. Eng. **2**, 866–871 (2014)
5. Ulaş, C., Aşık, U., Karadeniz, C.: Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines. Comput. Secur. **58**, 250–267 (2016)
6. Christopoulos, C.: Electromagnetic Compatibility (EMC) in Challenging environments. In: Daras, N.J., Rassias, T.M. (eds.) Operations Research, Engineering, and Cyber Security. SOIA, vol. 113, pp. 95–115. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-51500-7_5
7. Popescu, M., Bîndar, V., Crăciunescu, R., Fratu, O.: Estimate of minimum attenuation level for a TEMPEST shielded enclosure. In: Proceedings of COMM 2016, Bucharest (2016)
8. EN 55022 Standard: Information technology equipment - Radio disturbance characteristics-Limits and methods of measurement. European Committee for Standardization (1998)
9. Recommendation ITU-T K.84: Test methods and guide against information leaks through unintentional electromagnetic emissions. International Telecommunication Union (2011)