PROCESSING GAIN CONSIDERATIONS ON COMPROMISING EMISSIONS

RĂZVAN BĂRTUŞICĂ, BOITAN ALEXANDRU, M**ĂDĂLIN MIHAI**
THE SPECIAL TELECOMMUNICATIONS SERVICE BUCHAREST, ROMANIA

OCTAVIAN FRATU
UNIVERSITY POLITEHNICA OF BUCHAREST, TELECOMMUNICATIONS DEPARTMENT, ROMANIA

AGENDA

- **Introduction**
- **Processing gain evaluation**
- **Measurement results**
- **Conclusions: security risk and further studies**

INTRODUCTION

Emission Security (EMSEC)

Role:

- **Evaluate compromising emissions**
- **Testing procedures**
- **Prevent information recovery**

Objective:

- **Confidentiality**
- **Optimal protective measures**
- **Trusted solution**

Compromising Emissions

- **Source: electronic equipment**
- **Vulnerability: electromagnetic emissions**
- **Target: classified information**
- **Processing techniques: information recovery**
- **Method: passive attack, undetected**

Possible sources of compromising emanations:

Any equipment, peripheral, power supply, CPU, IC, data line, etc. that processes classified information.

PROCESSING GAIN EVALUATION

Signal-to-noise ratio (SNR)

at the boundary of the protected area

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

Attacker's PROS

$\hat{E}_B$ - maximum limit allowed for compromising emission

G_a - antenna gain

G_P - processing gain

Attacker's CONS

a_d - free space loss

a_w - architectural attenuation

E_n - boundary ambiental noise level

F_r - attacker's receiver noise factor

SNR dependency on the processing gain G_P

- Eq. 1 written in logarithmic form:

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

- Processing gain [G_p] can be evaluated as follows:

$$G_p = \begin{cases} G_{avg} \cdot G_{FFT} \cdot G_{filt}, & \text{for periodic like signals} \\ G_{FFT} \cdot G_{filt}, & \text{other} \end{cases} \quad (3)$$

Parameter	Formulae	Description
$[G_{avg}]$	$10 \cdot \log(N)$	N averages, periodic-like signals
$[G_{FFT}]$	$10 \cdot \log\left(\frac{N_{BIN\max}}{N_{BIN\min}}\right)$	N_{BIN} - *number of FFT points*
$[G_{filt}]$	$10 \cdot \log\left(\frac{BW}{BW_{filt}}\right)$	BW_{filt} - bandpass of selective digital filters

- **Digital band selection is used for retaining the spectral components of compromising emission (BW_{filt}) from the acquisition bandwidth (BW)**

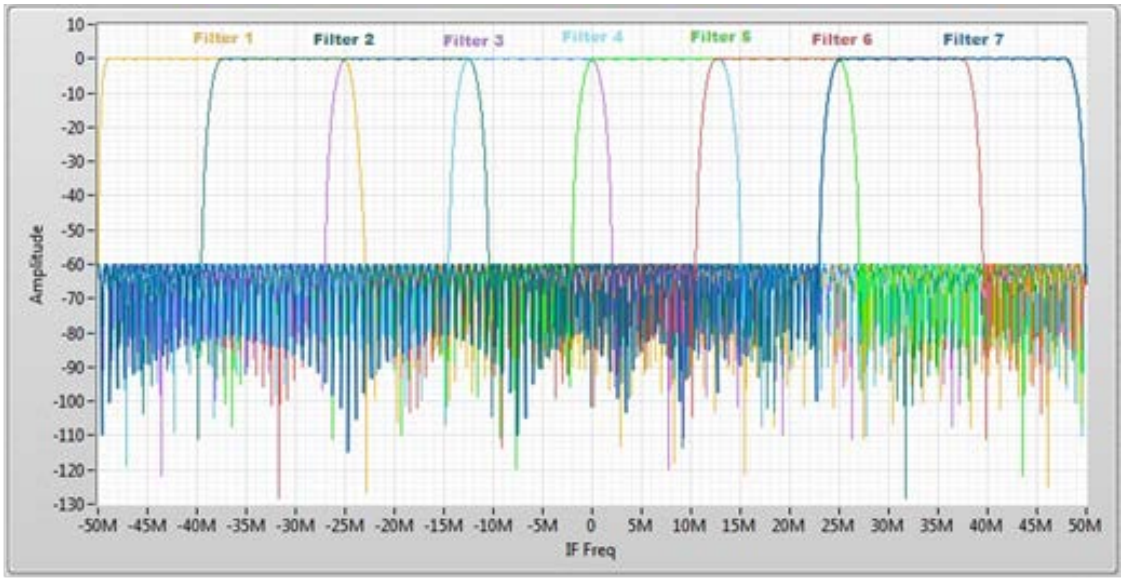

Fig.1 - Magnitude response of digital band selection filter bank, with 50% overlap

- **Increased detection resolution (PROS)**
- **Supplementary processing stages (CONS)**

MEASUREMENT RESULTS

- **Measurements performed in real operating environment**

Testing conditions	
EUT	VGA display unit
Distance	5m
Acquisition BW	100MHz
Filter BW	25MHz
Overlap	50%
Reconstruction	Raster
Estimated [G_P]	6dB, G_{filt}

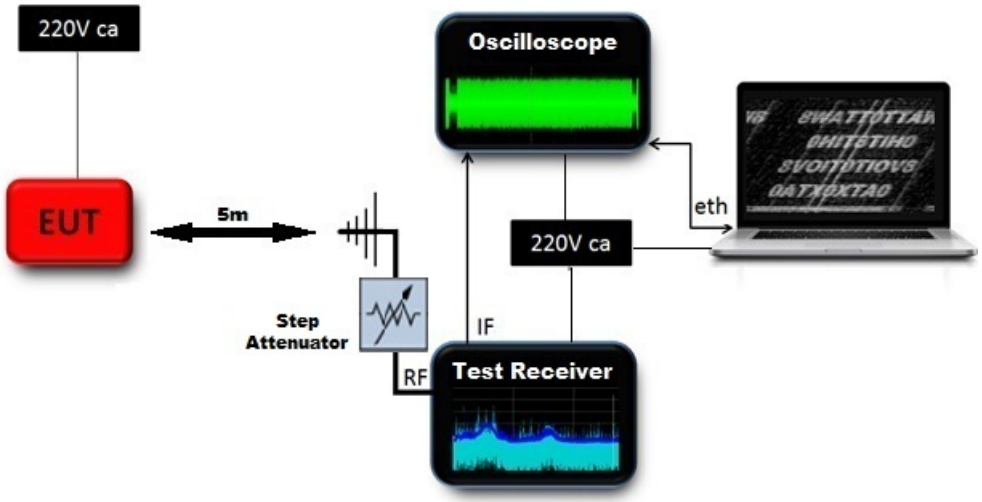

Fig. 2 - The testbed used for the validation

- Radiated compromising emissions (CE)
- Software developed raster application
- Information reconstruction by rastering CE samples

Reference condition:

- raster of full 100MHz acquisition bandwidth
- 0dB attenuation inserted by the step attenuator

Measurement:

- raster of 25MHz sequential selected filter
- 0dB attenuation inserted by the step attenuator

Fig.3 - Raster of full 100MHz acquisition bandwidth

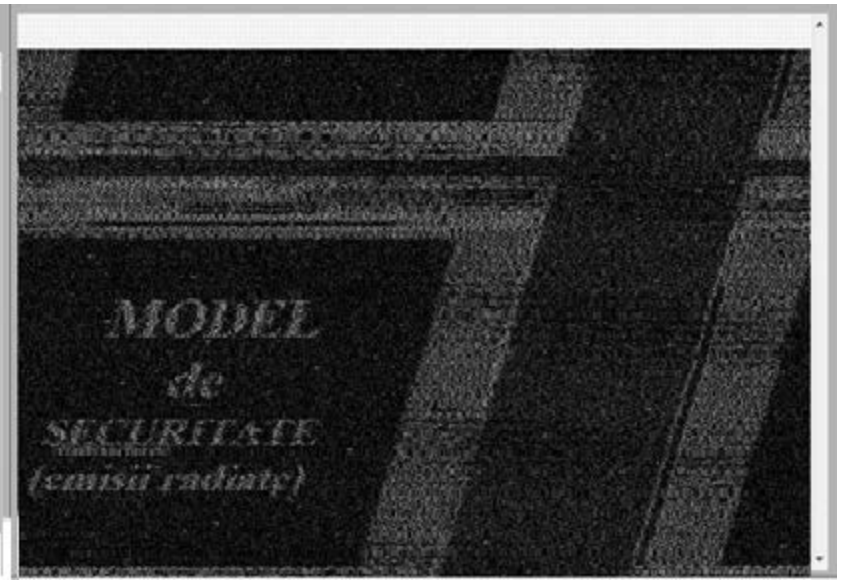

Fig.4 - Raster of 25MHz filter selected bandwidth

By sequential selection of 25MHz filter we obtained an improvement of the reconstructed image, as shown in Fig.4

The expected gain can be determined as: $\left[G_{filt}\right] = 10 \cdot \log\left(\frac{100MHz}{25MHz}\right) = 6dB$

Compensation of the processing gain: 6dB attenuation, as shown in Figure 6

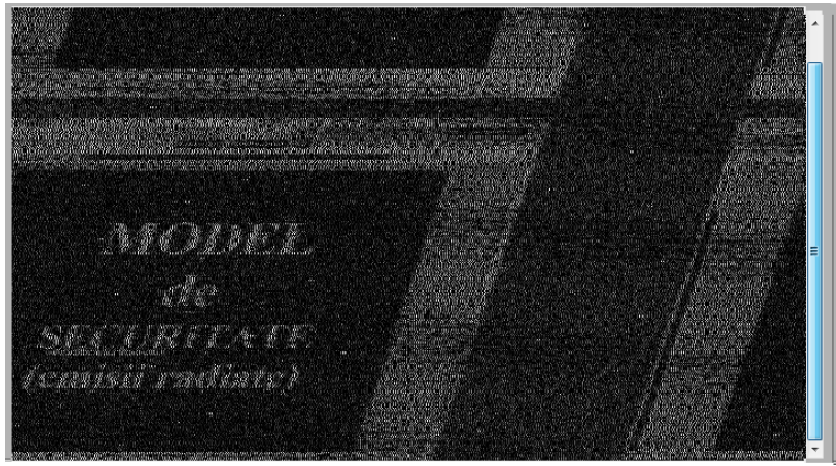

Fig.5 - Raster of 25MHz filter selected bandwidth, 0dB attenuation

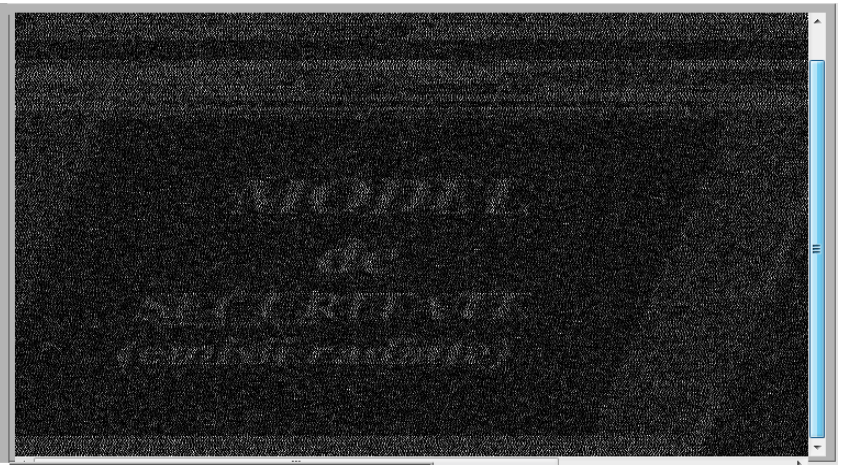

Fig.6 - Raster of 25MHz filter selected bandwidth, **6dB attenuation**

Fig.6 considerations:

- reconstructed information is still visible
- further attenuation should be inserted

Fig.7 considerations:

- increasing the attenuation by 1dB
- the boundary for no visual information obtained at 11dB

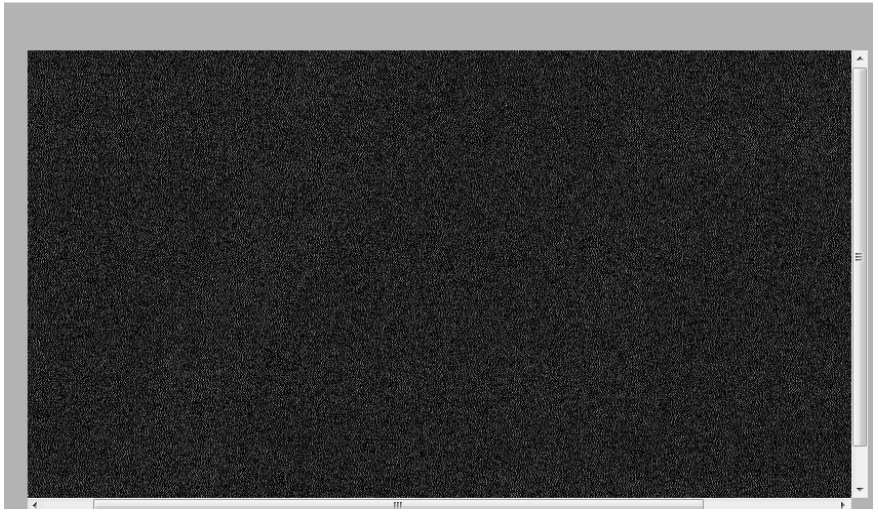

Fig.7 - Raster of 25MHz filter selected bandwidth, **11dB attenuation**

CONCLUSIONS

- **Processing techniques based on improving the SNR should be considered a threat from EMSEC point of view**
- **Compromising emissions represent a high vulnerability of computer systems**
- **Processing techniques such as averaging, filtering and rastering improve eavesdropper's chances to reconstruct sensitive information**
- **Processing gain evaluation should play an important role, as it can be a deciding factor in emission security model**
- **Experimental tests should be constantly performed on different computer systems, starting with design and production stages and continuing on all the lifespan**

REFERENCES

[1] De Meulemeester P, Bontemps L, Scheers B, Vandenbosch GA. Synchronization retrieval and image reconstruction of a video display unit exploiting its compromising emanations. In 2018 International Conference on Military Communications and Information Systems (ICMCIS), IEEE, 1-7 (2018).

[2] Nowosielski L, Wnuk M, Kuźba J. Analysis of Scenarios for It Equipment Location from the Point of View of Electromagnetic Security. In 2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama), IEEE, 1771-1775 (2018).

[3] Niu Y, Li C, Liu Y. A Calculation Method of Multi-Domain Anti-Interference Processing Gain for Wireless Communication System. In 2019 11th International Conference on Wireless Communications and Signal Processing (WCSP), IEEE, 1-6 (2019).

[4] Kubiak I, Przybysz A, Stańczak A. Usefulness of Acoustic Sounds from 3D Printers in an Eavesdropping Process and Reconstruction of Printed Shapes. Electronics, 297 (2020).

[5] Sekiguchi H, Seto S. Measurement of computer RGB signals in conducted emission on power leads. Progress In Electromagnetics Research, 51-64 (2009).

[6] Recommendation ITU-T K.84, “Test methods and guide against information leaks through unintentional electromagnetic emissions”, Telecommunication Standardization Sector of ITU (2011).

[7] A. Boitan, R. Bărtuşică, M. Popescu, B. Valerică, O. Fratu, “Wireless Keyboards Communication Interception - The Balance Between Convenience and Security”, International Conference on Communications (COMM), Bucharest, 539-542, (2018).

[8] M. Popescu, R. Bărtuşică, A. Boitan, S. Halunga, 2017 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.

[9] R. Bărtuşică, M. Popescu, A. Boitan, S. Halunga, “Considerations for Emission Security Risks from the Perspective of Signal Processing Techniques”, International Conference on Communications (COMM), Bucharest, 2018, 535-53 (2018).

[10] R. Bărtușică, A. Boitan, S. Halunga, M. Popescu, V. Bîndar, “Security Risk: Detection of Compromising Emanations Radiated or Conducted by Display Units”, Future Access Enablers for Ubiquitous and Intelligent Infrastructures 45-51. FABULOUS 2017, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 241. Springer, Cham, (2018).

[11] A. Boitan, R. Bărtuşică, S. Halunga, V. Bîndar, “Video signal recovery from the laser printer LCD display, Proc. SPIE 10977, Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies IX, 1097726, (2018).