Security Risk: Detection of Compromising Emanations Radiated or Conducted by Display Units

Răzvan Bărtușică[1](✉), Alexandru Boitan[1], Simona Halunga[2],
Mircea Popescu[1], and Valerică Bindar[1,2]

[1] Special Telecommunication Service, 323A, Splaiul Independentei,
060044 Bucharest, Romania
rbartusica@yahoo.com, alexandruboitan@yahoo.com,
bavaly@yahoo.com, mpopescu@sts.ro

[2] Telecommunications Faculty, University Politehnica of Bucharest,
Bd. Iuliu Maniu 1-3, 061071 Bucharest, Romania
simona.halunga@upb.ro

Abstract. In this paper we propose a method of detecting the propagation frequencies of compromising emanations in order to evaluate the risk of eavesdropping the display units. By modulating the video signal with an audio file, we have been able to detect the compromising emanations on the frequencies where the audition occurred. The level of those emanations is an important issue in the process of evaluating the security risk. The higher the level, the higher is the probability of detection and reconstruction of displayed information.

Keywords: Compromising emanation · Emission security · TEMPEST

1 Introduction

In our days, the effort of protecting sensitive information is a critical one. Any form of security incident that involves protected information has a negative impact on the organization that relies on them. Therefore, a series of protective measures, technical and procedural, are needed in order to ensure information security.

One of those measures is known as Emission Security (EMSEC) or Transient Electromagnetic Pulse Emanation Standard (TEMPEST), which represents a set of technical, organizational and procedural measures applied for analysis, investigation and decrease of compromising emissions generated by electronic or electromagnetic equipment processing information, with the purpose of preventing the processed information recovery. Possible sources of compromising emanations can be, but not limited to: power supplies, power amplifiers, microprocessors, internal circuits and wires, keyboards, printers, modems, scanners and display units. This technique had been introduced in early 60 s [1, 2] and has been developed ever since as newer devices appeared on the market. In [3, 4] a number of security limits for compromising emanations have been highlighted for different existing public standards and devices

O. Fratu et al. (Eds.): FABULOUS 2017, LNICST 241, pp. 45–51, 2018.
https://doi.org/10.1007/978-3-319-92213-3_7

and types of attack. Numerous testbeds and methodologies had been developed [5, 6] to evaluate the electromagnetic leakage emanations in different setups and for critical systems, sensitive to electromagnetic threats [7–9, 14]. It has been shown [1, 5, 10, 11] that display units like LCD, LED and old CRT monitors are ones of the most susceptible to eavesdropping due to their mode of operation. Compromising emanations can be processed by averaging since the video signal is periodic with the frame rate, leading to a processing gain of [2]

$$G_P = 10\log_{10}(N). \tag{1}$$

where N is the number of averages, and $N \geq 2$.

2 Compromising Emanation Generation

In this chapter we present the evaluation method, that implies generation of a video *.avi file, that will be repeatedly played and displayed on a LCD monitor. The video file is bearing audio information, encoded in form of horizontal lines, displayed by the frame rate setting of the LCD. Each frame has a number of horizontal lines which represent 256 bit grayscale coded audio samples. Thus, the compromising emanation will be found in radiofrequency spectrum as an amplitude modulation. Then, by AM demodulating, one can recover the audio file encoded in as a video signal.

2.1 Audio File Parameters

The first step is importing an audio file, which has a number of samples N_a and a sampling rate F_s [Hz]. The duration of audio signal is

$$D_a = N_a/F_s\ (s). \tag{2}$$

The samples will be grouped in clusters, corresponding to video display parameters.

2.2 Video Signal Parameters

The LCD has H_{px} horizontal pixels, V_{px} vertical pixels and S_r [Hz] screen refresh rate corresponding to the visible area. The duration of video signal represented by the *.avi file is equal to the duration of the audio file, namely

$$D_v = N_f/S_r\ (s). \tag{3}$$

Where N_f represents the number of frames in the video file.

2.3 Compromising Emanation Encoding

Each video frame contains a number of M audio samples, determined by

$$M = \frac{N_a}{N_f} = \frac{F_s}{S_r}. \tag{4}$$

Because LCD's pixel frequency is larger than the audio file sampling rate by an order of magnitude of 4, the only way to make an image audible is to decrease the pixel frequency by displaying one audio sample on several horizontal video lines. The number of horizontal video lines used to display an audio sample is given by

$$H_l = \frac{V_{px}}{M}. \tag{5}$$

where V_{px} is the number of video lines.

The final step is to convert the audio samples, represented by vector A into a raster-type video stream, represented by matrices, according to values above.

$$A = [a_1\, a_2\, a_3 \ldots a_M \ldots a_{N_a - 1}\, a_{N_a}]. \tag{6}$$

The audio samples are 8-bit encoded in order to obtain 256 grayscale values in order to obtain a video frame, as follows

$$\begin{aligned} &Frame\ \#1 \quad \begin{bmatrix} a_1 & \ldots & a_1 \\ \ldots & & \\ a_M & \ldots & a_M \end{bmatrix}, \quad Frame\ \#2 \quad \begin{bmatrix} a_{M+1} & \ldots & a_{M+1} \\ \ldots & & \\ a_{2M} & \ldots & a_{2M} \end{bmatrix}, \\ &Frame\ \#N_f \quad \begin{bmatrix} a_{N_a - M} & \ldots & a_{N_a - M} \\ \ldots & & \\ a_{N_a} & \ldots & a_{N_a} \end{bmatrix}. \end{aligned} \tag{7}$$

3 Method Validation and Information Recovery

In order to check the efficiency of the method, an experimental testbed has been built, consisting of:

- LCD monitor, as the equipment under test with screen resolution of 1024 by 768 pixels and a refresh rate of 60 Hz [15]
- Log-periodic antenna, for wideband reception
- Test receiver, with AM demodulation and intermediate frequency output
- Oscilloscope, connected to the IF output of the receiver, in order to visualize the waveform on the frequency where the compromising emanation is present
- Speakers, used for audio detection of compromising emanations during the frequency sweep performed by the test receiver.

The experimental setup block diagram is presented in Fig. 1. By sweeping the spectrum and using AF demodulation option on the test receiver, we were able to detect the frequencies where the compromising emanation was identified. The tests were performed under different conditions, using several LCDs at distances between 3 and 30 meters, in line of sight or obstructed by concrete walls.

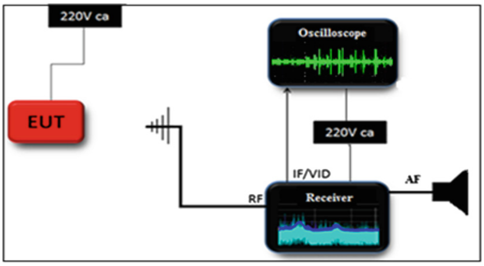

Fig. 1. The test setup used in the experiment. EUT represents different LCDs.

Next, to view the waveform and validate the method, we used the intermediate frequency output of the receiver connected to the scope input. We found that the waveforms visualized on the scope are correlated to the video frames displayed on the LCD, on those frequencies where the audition was possible.

The received frequency spectrum, presented in Fig. 2, contains several emissions, some of those being generated by the LCDs as spurious emissions. The compromising emanation of interest is marked in Fig. 2, at the frequency of 649.35 MHz.

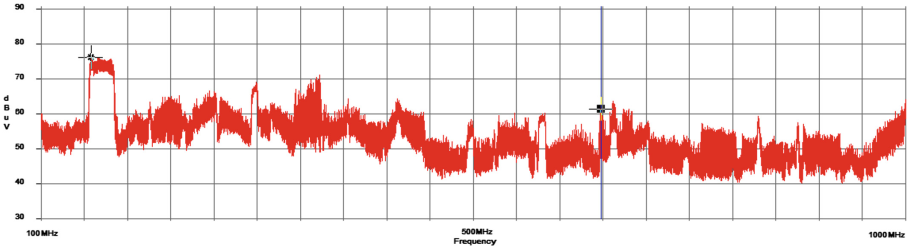

Fig. 2. Frequency spectrum. The marked frequency represents one detection.

Compromising emissions can be found on several frequencies, with different amplitude levels and audio quality. In this study the highest level and clearest audio recognition have been taken into consideration. On the other hand, different configurations of the testing scenario might lead to compromising emanations which are masked under the noise and interference, making it possible for the eavesdropper to recover information if he possesses a high quality receiver and strong signal processing capabilities.

One important parameter used for reducing the amount of received noise and increasing the frequency resolution is the resolution bandwidth, RBW. Thus the receiving sensitivity can be calculated as:

$$R_S = -174 + 10\log_{10}(RBW/Hz) + [NF]_{dBm} + [SNR]_{dBm} + [P_{att}]_{dBm} \quad (dBm). \tag{8}$$

where −174 is the thermal noise expressed in dBm, *RBW* is the bandpass filter of the receiver on the intermediate frequency path, *NF* is receiver noise figure, *SNR* is signal to noise ratio and P_{att} is the sum of antenna factor and cable loss, expressed in dB. By reducing RBW, the power of received noise decreases, compromising emanations can be separated from adjacent interferences making detection possible. Using a range of RBWs instead of a single one offers a higher confidence for our method.

The final step of validation is the visual correlation between displayed frames and received signal. To accomplish that we compared one video frame with corresponding waveform triggered on the oscilloscope. The amplitude and duration of each transition in oscilloscope waveform correspond with the intensity and thickness of displayed horizontal lines, as shown in Figs. 3 and 4.

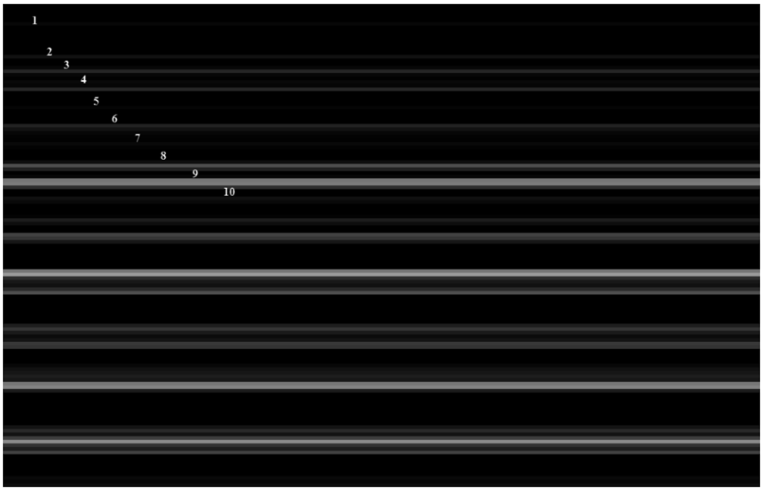

Fig. 3. Video frame displayed on the LCD. Audio samples are marked 1 to 10.

4 Conclusions

The method presented in this paper can be considered a fast solution for detecting compromising emanations from display units like LCD, LED and CRT monitors, using even a low cost wideband AM receiver.

The main advantage of this method is that it can be used in sites, to verify the conformity of installation process with emission security regulations, where display units operate as a part of a system and can’t be moved or replaced by other display units. The disadvantage is that it is limited only to detection of compromising emanations and is not able to not measure their level, according to emission security regulations.

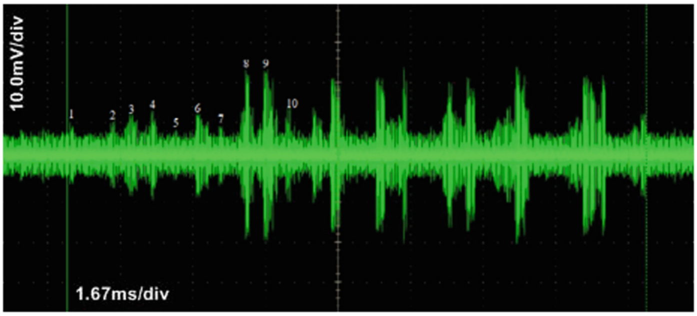

Fig. 4. Oscilloscope waveform. Detected audio samples are marked 1 to 10.

Information reconstruction by receiving and processing emissions generated by electronic equipment is a security risk and should be treated accordingly. The threat increases with the development of high performance Software Defined Radios that can be found on the market, which are becoming more affordable as the time passes.

Protective measures should be complex but also cost effective, starting with procedural measures which control operating conditions, software solutions like filtering displayed information and hardware measures like electromagnetic shielding and filtering [12, 13].

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

References

1. Kuhn, M.G.: Compromising emanations: eavesdropping risks of computer displays, Technical report (2003). http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-577.pdf
2. Kuhn, M.G.: Security limits for compromising emanations. In: Rao, J.R., Sunar, B. (eds.) CHES 2005. LNCS, vol. 3659, pp. 265–279. Springer, Heidelberg (2005). https://doi.org/10.1007/11545262_20
3. Kuhn, M.G.: Eavesdropping attacks on computer displays. Inf. Secur. Summit, 24–25 (2006). Prague
4. Kuhn, M.G.: Compromising emanations of LCD TV sets. IEEE Trans. Electromagn. Compat. **55**, 564–570 (2013)
5. Katamreddy, S.: Experimental testbed for electromagnetic analysis doctoral dissertation. George Mason University (2016)
6. Kasmi, C., Esteves, J.L., Armstrong, K.: EMC/EMI and functional safety, methodology to characterize effects of interferences on devices. In: IEEE 2016 Asia-Pacific International Symposium on Electromagnetic Compatibility (APEMC), vol. 1, pp. 1178–1180 (2016)
7. 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

8. Jian, M., Jinming, L.: Information leakage from computer based on electromagnetic radiation. Control Intell. Syst. **43**(2) (2016)
9. Van Eck, W.: Electromagnetic radiation from video display units: an eavesdropping risk? Comput. Secur. **4**(4), 269–286 (1985)
10. Sekiguchi, H., Seto, S.: Measurement of radiated computer RGB signals. Prog. Electromagn. Res. C **7**, 1–12 (2009)
11. Bîndar, V., Popescu, M., Craciunescu, R.: Aspects of electromagnetic compatibility as a support for communication security based on TEMPEST evaluation. In: 2014 10th International Conference on Communications (COMM), Bucharest, pp. 1–4 (2014)
12. ITU-T K.84: test methods and guide against information leaks through unintentional electromagnetic emissions (2011)
13. ITU-T K.87: guide for the application of electromagnetic security requirements (2016)
14. https://www.sans.org/reading-room/whitepapers/privacy/introduction-tempest-981. Accessed Apr 2017
15. http://tinyvga.com/vga-timing. Accessed Apr 2017