Human Interaction and Emerging Technologies (IHIET 2022), Vol. 68, 2022, 233–240
https://doi.org/10.54941/ahfe1002737

Determining Distinctive Features for IT and Medical Devices Hardware Interfaces Based on Compromising Emissions

Rafał Przesmycki and Marek Bugaj

Faculty of Electronics, Military University of Technology, gen. Sylwestra Kaliskiego 2 str., 00-908 Warsaw, Poland

ABSTRACT

The article presents the method of determining the distinctive features for modern IT and medical devices located on the European Un-ion market based on compromising emission. The article describes the method of identifying hardware interfaces of IT or medical devices that uses radiated compromising emission. In addition, the article presents the results of measurements regarding the use of the developed method to identify the USB2.0 serial interface. The developed measurement method can be applied to all hardware interfaces located in the IT and medical devices. But the article focus-es on one of the selected hardware interface - USB2.0.

Keywords: Compromising emission, IT devices, Medical devices, Distinctive features EMC, Hardware interface, PC interface

INTRODUCTION

Generally, energy emitted by any source can depend on frequency (f), time (t) and direction (Φ). Quantity ε can be found as operator describing conversion of energy released in source (which depends only on frequency and time) into space-time-frequency distribution of energy in medium surrounding source. If direction, frequency and time features of source are independent of each other, then its emissivity ε can be presented in the form of product of three functions representing separate characteristics describing frequency, direction and time selectivity of source. With large amount of emission sources working simultaneously the resultant process contains prevailing discrete components with particularly large intensity and electromagnetic background close to noise. Basically, intensity of intentional emission can be estimated on the basis of space-time-frequency distribution of sources, radiated power and other nominal parameters of related devices. Whereas unintentional emission is much more difficult for quantity assessment. Such an example is collocated system in which there are a few sources of electromagnetic emission at the same time.

DISTINCTIVE FEATURES OF HARDWARE INTERFACES IN PC

A co-location system is a system that is an internally compatible system. Such a system can be called a collection of sources of electromagnetic signals and relations between them and their attributes. The relationship between the sources represents their interaction with each other (internal impact) and the impact on the environment (external impact).

By co-locating system, we can name an IT or medical device made up of many electronic components with specific distinctive features. In the case of a co-located system, IT or medical devices cooperate to create the entire system. An example of a co-location system is the central unit of a PC computer, which consists of many IT components, and hardware interfaces placed in one casing creating the entire IT system. Another example of a co-location system is a cardiac monitor with the ability to write data to a USB device using a hardware interface. The cardio monitor is a specialized medical device that is used to monitor the most important vital parameters of the examined person. It is a device containing many components, and hardware interfaces placed in one casing.

Based on the research and the results obtained by the authors, it can be concluded that there is a possibility to identify the hardware interfaces of the IT or medical equipment causing an increase in the emissivity level. Distinctive feature of the work of individual interfaces is its operating frequency and the emissivity level allowing identification of a given hardware interface. Another of such features is the spectrum of radiated emission which is the mapping of the emission of radiated disturbances. These features are the only common features for considered hardware interfaces. Considering the above, it is possible to build a database with distinctive features of hardware interfaces, which will easily support the process of identification of individual hardware interfaces of IT or medical device.

The implementation of the problem of identification of individual hardware interfaces of IT device will contribute to improving the work carried out in the field of protection of information processed in IT systems and the implementation of tasks regulated by the Act on the protection of classified information. In addition, using knowledge about the distinctive features of individual hardware interfaces, it is possible to limit radiated emissions by IT equipment manufacturers at the design stage through additional security.

DETERMINATION OF HARDWARE INTERFACES DISTINCTIVE FEATURES BASED ON COMPROMISING EMISSION

This chapter presents and discusses the developed method for determining the distinctive features hardware interfaces in IT or medical devices. Using the presented method, it is possible to define frequency ranges for particular IT or medical devices that can be used to analyze the possibility identification of IT or medical devices in co-located systems based on radiated compromising emission.

In order to determine the source of electromagnetic emissions from computer equipment by determining the location of this source in PC central units, this can be done by estimating the degree of test signal content intentionally generated on selected interfaces of the information device in the signal received by the test station as radiated emission. For this we need to know the

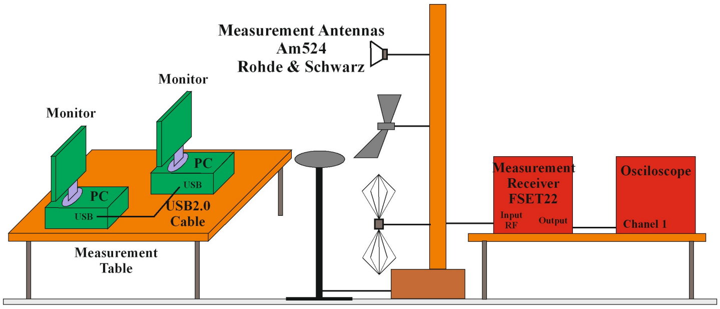

Figure 1: Block diagram of the laboratory stand for measuring compromising emission.

reference signal. A signal generator is activated in the investigated IT or medical device to generate a reference signal at the output of the selected interface of the investigated IT or medical device corresponding to the selected binary information sequence or test image. This gives us the reference signal we are looking for in the radiated spectrum.

The developed method is used to determine the distinctive features of hardware interfaces in PC central units radiated compromising emission (CEM - Compromising Emission Method). With this method, it is possible to determine the distinctive characteristics (spectrum of spectrum components of the signal being analyzed and characteristic binary patterns in the time domain) of the signals occurring at the output of selected time and frequency interfaces corresponding to the specific binary information sequences transmitted by a given interface of a computer device such as a central unit PC. In the present method, as a measuring system used, the system shown in Figure 1.

For each interface, we use the selected binary sequences, selected test images. By receiving antennas, the signal received by the antenna is transmitted through the switching antenna of the antenna to the broadband receiver. At the receiver, the signals are filtered and converted to a lower frequency range. The detection signal is transmitted to the VIDEO output on the receiver and then transferred to the external channel input of the oscilloscope, where it is possible to visualize the received time-domain information, thereby confirming the detection of the test signal at a given frequency.

MEASUREMENT RESULTS

In order to show the practical application of the developed method, an experiment was carried out to measure the radiated compromising emission from the USB 2.0 interface. Measurements were made at a distance of 1 m from an IT or medical device, on which traffic was forced on data lines via the USB 2.0 interface.

The direct effect on the level of individual components of the radio spectrum emission from the USB 2.0 interface received by the infiltration receiver is in the form of a signal path directly on the transmission line. That being so, for analyses aiming at assessment of the possibility of conducting electromagnetic eavesdropping, such a form of binary information sequences was selected which were generated by BTSG (binary testing sequence generator)

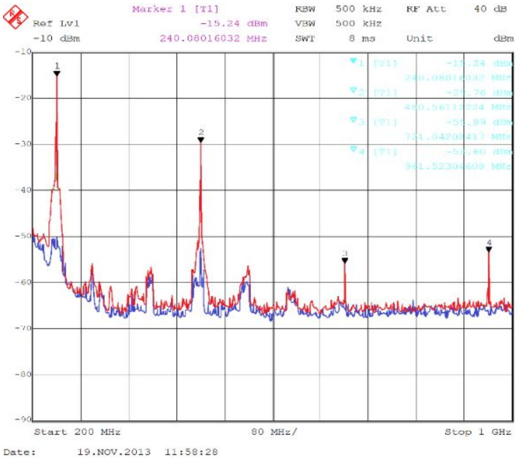

Figure 2: Radiated emission deriving from USB 2.0 interface while the transmission data is OFF (blue color) and while transferring a selected binary sequence of logical zeros (red color) in frequency range 200 MHz– 1 GHz.

transmission software operating at PC equipped with a tested USB 2.0 port, which results in maximization of a level of particular components of frequency spectrum of radiated emission. As a result of conducted tests and analyses it was determined that particular components of signal spectrum on USB 2.0 transmission line have maximal levels of particular spectrum components of radiated emission only for binary information sequences generated by BTSG, which after their processing by standard output systems of USB port generate periodic binary stream on transmission line. To force periodic binary stream on transmission line, BTSG should generate binary information sequence which after processing by standard output systems of USB 2.0 port will cause occurrence of periodic binary stream on transmission line. Significant processes of signal processing in USB 2.0 interface, which have influence on a form of binary stream at its output include the process of bit stuffing and NRZI (non-return to zero inverted) linear encoding. Taking into consideration the influence of the above binary stream processing methods on the output of the USB 2.0 port, BTSG application forced the transmission of the binary information stream via the USB interface in the form of zeros logic (0000000000000000) which at the output of the USB port after NRZI encoding gives the binary in the form 0101010101010101.

Figure 2 shows the radiated emission spectrum generated by the USB 2.0 interface when transmitting a data stream consisting of zeros logic. From the above spectrogram, it can be concluded that radiated compromising emission occurs at frequencies; 240 MHz, 480 MHz, 720 MHz and 960 MHz.

In the next part of the experiment, the FSET22 infiltration receiver should be tuned to particular frequencies on which there is radiated compromising emission. Then, a comparative analysis of the signal occurring directly on the transmission line of the USB 2.0 port and its counterpart received by the infiltration receiver was made as radiated emission. For comparative analysis, the signals generated by the USB 2.0 port obtained as a result of measurements at the output of the envelope detector FSET 22 receiver should be used, as

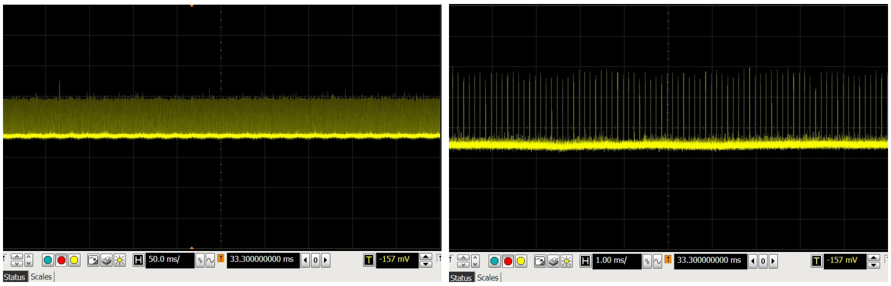

Figure 3: Oscillogram for USB2.0 interface when data transmission is off. The signal received by the antenna for f = 240,00 MHz given from the output VIDEO of the FSET22 receiver.

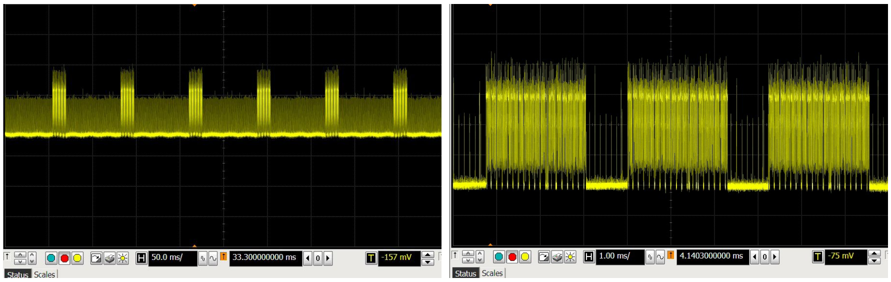

Figure 4: Oscillogram for USB2.0 interface when data transmission is on in the form of binary sequence 00000. The signal received by the antenna for f = 240,00 MHz given from the output VIDEO of the FSET22 receiver.

radiated emission. Exemplary oscillogram showing data off transmission and data on transmission in the form of a binary sequence generated by the BTSG generator consisting of logical zeros are presented in Figure 3 and Figure 4 respectively.

Very often evaluation of spectrum itself is insufficient due to difficulties resulting from rating of appearing signals at particular frequencies. Because of that it is necessary to use other methods consisting in the use of more advanced measuring devices. Anyway in most cases qualification of emissions occurs with the use of visual method. It should be remembered though that in doubtful cases or in such ones where visual assessment is impossible evaluation methods based on digital methods of processing of recorded signals are used.

The analyzed waveforms and their spectra were obtained as a result of measurements carried out on a laboratory stand, whose block diagram is shown in Figure 1.

Identification is a process or a result of processes of identifying a particular object with other object. It may include distinguishing common features, capturing similarities between a tested object and other objects of the same category, estimating values of observed parameters of a particular object. Using any methods of signal identification of compromising emission requires determination of distinctive features characteristic for model information signals and determination of a similarity degree of those features for analogous parameters of tested signals.

In order to assess the degree of penetration of the electromagnetic information from the USB 2.0 interface, calculate the degree of similarity between the signal generated by the USB 2.0 port, obtained by the measurement of the output envelope detector of FSET22 receiver, received as radiated emissions and the measured signal directly to the transmission line. As a measure of the degree of similarity can be used intercorrelation function and cross-correlation coefficient.

Intercorrelation function $R_{xy}(\tau)$ of two random signals x(t) and y(t) is characterized by the interdependence of one random signal from second random signal value and is determined by the following relation:

$$R_{xy}(\tau) = \lim_{T\to\infty} \int_0^T x(t)y(t+\tau)\,dt \qquad (1)$$

Cross-correlation coefficient is described as a measure of interdependence. It characterizes to what extent one variable is similar to the other. He answers the question of how big the relationship and its intensity is between them. Cross-correlation coefficient is determined using the following relationships:

$$\rho_{xy} = \frac{C_{xy}}{\sigma_x \sigma_y} \qquad (2)$$

where:

C_{xy} is the covariance of x and y variables,

∂_x, ∂_y standard deviations of x and y variables.

Both the intercorrelation function and cross-correlation coefficient can be used to detect the signal hidden in the noise. In particular, when we have a noiseless copy of the signal generated on the transmission line of the USB 2.0 port as a result of the transmission of information bits generated by the BTSG to be detected. Then the intercorrelation function or cross-correlation coefficient between the noisy signal decoded by the infiltration receiver and saved a copy of the signal present on the transmission line it possible to assess the degree of penetration of the electromagnetic information. This fact allows to assess the degree of electromagnetic penetration of information from the USB 2.0 interface.

CONCLUSION

The article presents and discusses the developed method for determining the features of distinctive hardware interfaces in PC central units using radiated compromising emission. Using the presented method, it is possible to extract distinctive features for hardware interfaces that can be used to analyze the identification of IT devices in co-location systems based on radiated emission.

The developed measurement method can be applied to all hardware interfaces located in the central units of the PC. The article focuses on one of the selected hardware interface - USB2.0.

From the presented waveforms of the radiated emission signals for the USB 2.0 interface, it can be seen that these signals have a clear relationship with the content of the transmitted binary sequences, and thus have the character of the compromising emission signals. Time waveforms identify the form of the content of the transmitted information. On the basis of the oscillogram obtained on the interface's transmission lines and their spectrograms obtained with the use of the spectrum analyzer and oscilloscope obtained as a result of measurements, it can be stated that: by selecting the pattern transmitted binary sequence in the test computing device can shape the character of the time course of signal transmission lines for USB 2.0 in such a way that it can be easily identified on the oscillogram.

The use of the USB 2.0 interface to transfer data poses a major threat to electromagnetic infiltration, which negates the possibility of its usefulness in the devices used for processing classified information without the use of additional security.

The intercorrelation function and the cross-correlation coefficient between the signal recorded at the output of the envelope detector infiltration receiver (FSET 22), as an radiated emission, and a signal registered directly on the transmission line USB 2.0 interface, can be successfully used as a measure of similarity between these signals during testing information devices equipped with USB 2.0 interface to assess the possibility of carrying out electromagnetic infiltration.

ACKNOWLEDGMENT

This work was financed by Military University of Technology under research project UGB-22-741/2022 on "Electrical parameters measurement of solid materials using the reflection and the free space method in the millimeter band".

REFERENCES

F. G. Awan, N. M. Sheikh, S. A. Qureshi, A. Ali – "A Generic Model for the Classification of Radiation Emission Data in Electromagnetic Compatibility Measurement", Radio and Wireless Symposium, 2008, ISBN: 978-1-4244-1462-8,

Fang Han, Changsheng Shi, Deyun Lin, Guoding Li, – "Measurement of radiated emission from PC computer system", CH3044-5/91/0000-0208 $01. OO 0 1991 IEEE, str. 209 – 210.

I. Kubiak, "Influence of the Method of Colors on Levels of Electromagnetic Emissions From Video Standards," in *IEEE Transactions on Electromagnetic Compatibility*, vol. 61, no. 4, pp. 1129-1137, Aug. 2019. doi: 10.1109/TEMC.2018.2881304

L. Dong, H. Yue, Y. Yang, H. Xiao and S. Wang, "Emission Signal Analysis Based on Conventional and Modified Wavelet Cross-Correlation," *2009 2nd International Congress on Image and Signal Processing*, Tianjin, 2009, pp. 1–4. doi: 10.1109/CISP.2009.5301182

L. Wang and B. Yu – "Research on the Compromising Electromagnetic Emanations of PS/2 Keyboard", American Journal of Engineering and Technology Research Vol. 11 Issu.. pp 663-668 Sept. 2011,

Markus G. Kuhn – "Compromising emanations: eavesdropping risks of computer displays", Technical Report Number 577, 2003,

P. De Meulemeester, L. Bontemps, B. Scheers and G. A. E. Vandenbosch, "Synchronization retrieval and image reconstruction of a video display unit exploiting its compromising emanations," *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, Warsaw, 2018, pp. 1–7. doi:10.1109/ICMCIS.2018.8398727

R. Przesmycki and L. Nowosielski, "USB 3.0 interface in the process of electromagnetic infiltration," *2016 Progress in Electromagnetic Research Symposium (PIERS)*, Shanghai, 2016, pp. 1019–1023. doi: 10.1109/PIERS.2016.7734569

R. Przesmycki and M. Bugaj, "Analysis the identification process of information interfaces based on radiated emissions and database," *2016 Progress in Electromagnetic Research Symposium (PIERS)*, Shanghai, 2016, pp. 1033–1037. doi: 10.1109/PIERS.2016.7734572,

R. Przesmycki, M. Bugaj, L. Nowosielski and M. Wnuk, "Implementation a database of hardware interfaces for information devices in the identifying process based on radiated emissions," *2016 International Symposium on Electromagnetic Compatibility - EMC EUROPE*, Wroclaw, 2016, pp. 701–706. doi: 10.1109/EMCEurope.2016.7739192,

Rafał Przesmycki Measurement and Analysis of Compromising Emanation for Laser Printer, Guangzhou, China, PIERS Proceedings 2014, str. 2661-2665, ISSN 1559-9450,

Rafał Przesmycki, Leszek Nowosielski Analiza czułości współczesnych systemów odbiorczych w wybranych środowiskach elektromagnetycznych, Przegląd Telekomunikacyjny, ISSN 1230-3496, NR 8-9/2014, str: 971–977.

Vuagnoux M. Pasini S. – "An improved technique to discover compromising electromagnetic emanations", Electromagnetic Compatibility (EMC) 2010 IEEE International Symposium on Digital Object Identifier pp. 121-126 2010,

Zhenfei S., Donglin S., Fei D., Duval F. Louis A. – "A Novel Electromagnetic Radiated Emission Source Identification Methodology", 2010 Asia-Pacific International Symposium on Electromagnetic Compatibility, April 12 - 16, 2010, Beijing, China, 978-1-4244-5623-9/10/$26.00 ©2010 IEEE, str 645 - 648,