Study on the Electromagnetic Field Propagation of the PS/2 Signal

Alexandru Mădălin VIZITIU

***Abstract*—The beginning of this century is characterized by the meticulous exploitation of SIGnalINTelligence (SIGINT) techniques, but also by the development and exploitation of COMmunicationsSECurity (COMSEC) techniques. The overcoming of Moore's law [1] on the evolution of the dimensions of electronic components and the need for mobility of computer systems have led to the digitization of services provided by institutions or companies, as well as the existence of electronic equipment available to everyone. Their use often involves the input of sensitive or personal data. This must be done as safely as possible. The sensitive nature of the data entered can turn into a bait that leads to information warfare. The PS/2 protocol, although used since 1987 for communication between peripherals and host devices, can be found nowadays in all notebook or ultrabook devices. Identifying the unintentionally generated electromagnetic signal, how it propagates, detecting sources and configuration the model of the system that generates it are addressed in this article. This paper aims to present a possible method for PS/2 keyboard eavesdropping and also a manner to prevent it. The research was performed using semi anechoic chamber and TEMPEST specific equipment. The novelty of this paper consists in Power Distribution Network (PDN) analysis, which has not been covered in a PS/2 keyboard research. The study can represent the starting point for developing new methods based on artificial intelligence for reconstructing the message inadvertently transmitted by PS/2 keyboard communication.**

***Index Terms*—COMSEC, compromising electromagnetic emissions, electronic warfare, PS2 keyboard, TEMPEST.**

I. Introduction

Any electronic equipment from our surroundings is a source of conducted or radiated electromagnetic emissions that may inadvertently carry information processed by the equipment in question. If these emissions were to be detected and analyzed, it could lead to the reconstruction of the information processed by the circuits of the device from which they originate, in the absence of direct contact.

Each manufacturer of electronic equipment shall subject the product to a series of electromagnetic compatibility (EMC) tests. Their purpose is to establish the possibility of equipment coexistence. The current rules are sufficient to avoid interference between equipment, but they do not guarantee the security of the data transmitted.

The specific techniques and procedures used to prevent information attacks are extremely diverse, but an example of this is the use of the TEMPEST domain (which is part of COMSEC) [2].

TEMPEST (Transient Electromagnetic Pulse Emanation Standard) is the field that deals with the study and investigation of compromising signals in order to establish the appropriate system of communication and data processing for various situations. The purpose of TEMPEST is to prevent eavesdropping, especially given the fact that it is undetectable.

The PS/2 communication protocol was developed in 1987 by IBM and the name comes from "IBM Personal System/2". Although it is a protocol with a low data rate, it is still found on some desktop keyboards, but the importance of its study is due to the fact that the keyboard processor of laptops and notebooks, ubiquitous devices, uses the PS/2 protocol to transmit the key signal to the motherboard. In 1996, the Universal Serial Bus protocol was launched, which, in addition to a higher data rate than the PS/2, also provides plug-and-play communications that the PS/2 cannot achieve.

The PS/2 keyboard leakage studies have been done in the past [3, 4] and the developments of RF equipment allow us to try new methods in detecting unintentionally signals emitted by electronic equipment.

This paper analyzes the signal from a PS/2 keyboard used as equipment under test (EUT) in order to identify some research directions regarding modern eavesdropping methods. It also presents some measurements that reflect an uncommon unintentional emission of some PS/2 keyboards, the construction of the keyboard emissions propagation model and the analysis on the Power Distribution Network (PDN) of this keyboard category.

II. Testbed Setup

In order to identify the electromagnetic radiation that comes strictly from the analyzed EUT, the measurements were performed by placing the keyboard alongside a desktop system previously studied on the test table of a semi-anechoic chamber (SAC). The walls of the room are covered with radio wave absorbers that have the property of occluding electromagnetic radiation so that the used transducer receives only the direct wave from the analyzed object, and not the reflected ones.

The scheme of the test configuration is represented in Fig. 1.

Specific Equipment to this field was used for signal reception: reception system composed of TEMPEST broadband receiver FSET 22 and preset selector FSET Z22, oscilloscope Tektronix MSO 5204B and Rohde & Schwarz (R&S) RTO2002. The transducer used is a biconical R&S HE526 antenna, whose range is between 30 MHz and 200 MHz placed in front of the keyboard at distances from 1.25 m to 5 m. The signal is transmitted to the receiver through the transition panel.

A. M. VIZITIU is with the Special Communications Service, Bucharest, Romania, Ph.D. student at the Doctoral School of Electronics, Telecommunications & Information Technology, "Politehnica" University of Bucharest, Romania (e-mail: vizitiuamadalin@gmail.com).

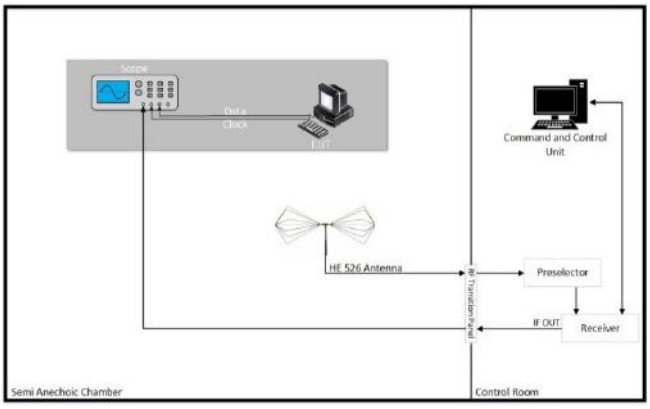


Figure 1. Testbed setup

The keyboard that is the subject of this study is a commercial keyboard that uses the PS/2 protocol to transmit data to the computer system.

III. PS/2 Signal Measurements

The PS/2 communication protocol implies the transmission of data at a rate of 7 ÷ 12 kbps, the existence of a clock signal with a frequency of 10÷16.7 kHz, and, in the case of a keyboard, at a single press of a key, the key signal is transmitted once every 30 ms to the I/O port of the motherboard of a host device [5].

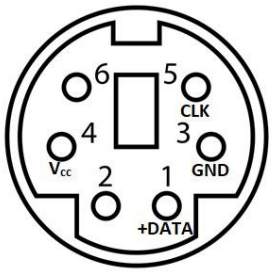


Figure 2. PS/2 plug pins configuration

Following the measurements, the signal corresponding to pressing a key is present on different frequencies.

In order to facilitate the understanding of the signal propagation mode, in the following figures we present some waveform captions on the 92.4 MHz frequency at which the signal-to-noise ratio facilitates the visualization and the analysis of the compromising signal.

The capture presented in Fig. 3 shows that the signal corresponding to the electromagnetic emission of the EUT can be associated according to the duration of the key packet with the signal obtained by galvanic probing of the keyboard circuits.

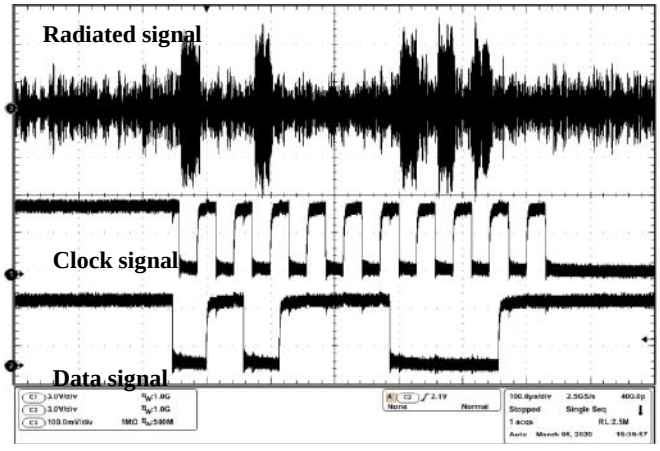
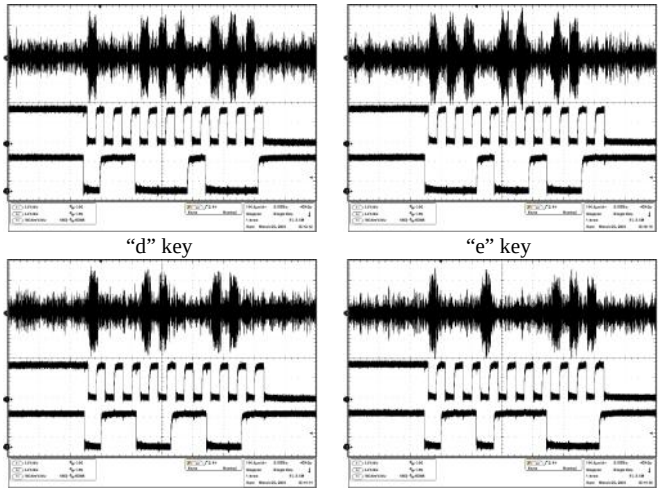


Figure 3. "w" key signal analysis

The analysis of several keys led to the elaboration of the mathematical model presented in chapter IV of this paper.

It can be noticed the existence of a signal associated with a keystroke for all characters entered by the keyboard user, some of which are shown in Fig. 4 [6].

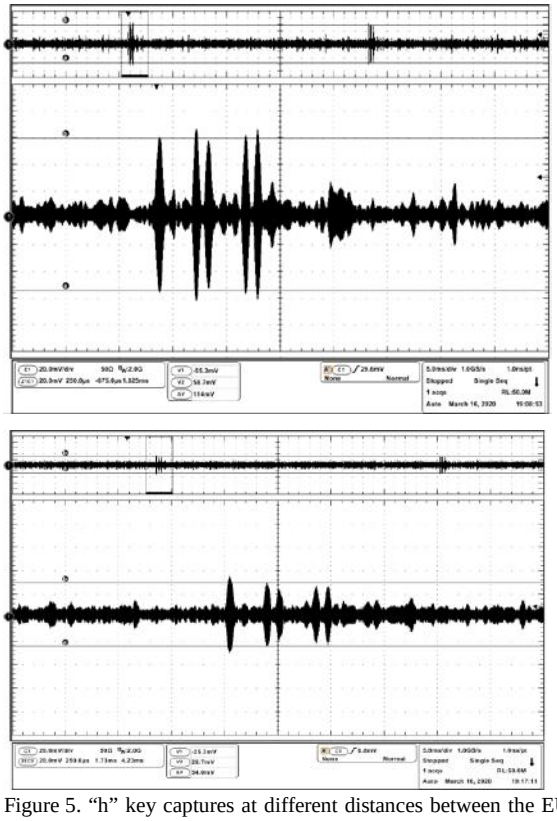


"d" key "e" key

"h" key "j" key

Figure 4. "d", "e", "h", "j" keys signal analysis

To establish how much a user could be exposed to keystroke eavesdropping attack, measurements were made by positioning the receiving antenna at different distances [7]. Fig. 5 shows the captures made with the reception at a distance of 1.25 m, respectively 5 m from the keyboard. After analyzing the signals in Fig. 5 we conclude that the signal can be captured even from distances beyond the perimeter of a space that serves as an office or even outside a building, indeed, depending on the attenuation of its walls. The signal level even allows the realization of a visual correlation, but inefficient in terms of time required, in order to correctly identify the key entered by the user.



"h" key signal, EUT-HE526 distance = 1.25 m

"h" key signal, EUT-HE526 distance = 5 m

Figure 5. "h" key captures at different distances between the EUT and the TRANSDUCER

IV. Analytic Model of Compromising Emanation

In the TEMPEST domain most of the times the compromising signal corresponds to the increasing and / or decreasing fronts of the transitions of the data signal conveyed by the studied equipment.

Analyzing the signal obtained by galvanically probing the data line of the EUT and comparing it with the signal received from the radiation it generated we initially notice only a match for the data packet duration. This led to the creation of a database with the signals obtained from the radiation corresponding to several alpha-numeric keys of the studied keyboard. By adding to the analysis the clock signal on the PS/2 bus, we established the way in which the received signal is associated with a key entered by a user. It corresponds to the function (1) in which $s[n]$ represent the signal received with the TEMPEST system, $c[n]$ is the clock signal and $x[n]$ is the data signal

$$s[n]=\begin{cases}1, & c[n]=x[n]=0\\ 0, & \text{otherwise}\end{cases} \quad (1)$$

The block diagram of the system that would allow obtaining the compromising signal received from the studied keyboard is highlighted in Fig. 6, where $s(t)$ is the modulating signal obtained at the output of the digital-to-analog converter (DAC), f_p is carrier signal (and its frequencies correspond to frequencies where the PS/2 leakage signal is detected, e.g. 92.4 MHz), $n(t)$ is the noise from the channel and $y(t)$ is the radiated signal.

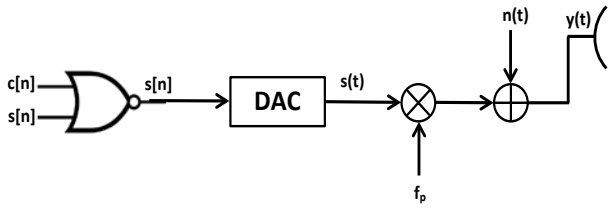


Figure 6. The block diagram of the radio transmitter

Establishing the transmitter block diagram results in a logical model of the EUT and describes its level of knowledge.

The model thus obtained can be implemented using an SDR that simulates the EUT. Using the keyboard and SDR at the same time, the latter configured to transmit a signal similar to that of a keystroke, may deceive an attempt to intercept the device. This method of protecting the signal carried by a particular device is called “spoofing”.

V. The Source of Compromising Emission

Regarding a first possible source of radiation generated by the keyboard used, this could be the conductor from the keyboard controller to the PS/2 port of the computer system. This can be explained by taking into account (2), which establishes the dependency between the wavelength, λ_0, corresponding to the resonant frequency of a conductor and its length, l_0, which is usual

$$l_0=\frac{\lambda_0}{2}. \quad (2)$$

In practice, through measurements, it is found that in the case of the studied keyboard, the cable length has the effect only of attenuating the signal level, not influencing the frequency on which it will be emitted. The usual length of the keyboard cable is 120 cm and this length has nothing to do with the wavelength of PS/2 signals.

PDN (Power Distribution Network) is considered one of the sources of system disruptions [8]. Analyzing this subject from the perspective of I/O ports and currents flowing through the system circuits, it is established that there are variations in the voltage that supplies that circuit, V_{cc}, corresponding to the transitions of the data signal processed by that circuit.

Using the oscilloscope it is observed that variations $\Delta V_{cc} = 500$ mV appear (Fig. 7 and Fig. 9) and that these variations are found in the spectrum of this signal by the presence of harmonics in different ranges (Fig. 9). Because the study was due by the TEMPEST view point and conducted emissions have been received on higher frequencies, the figure presents the spectrum from DC to 400 MHz.

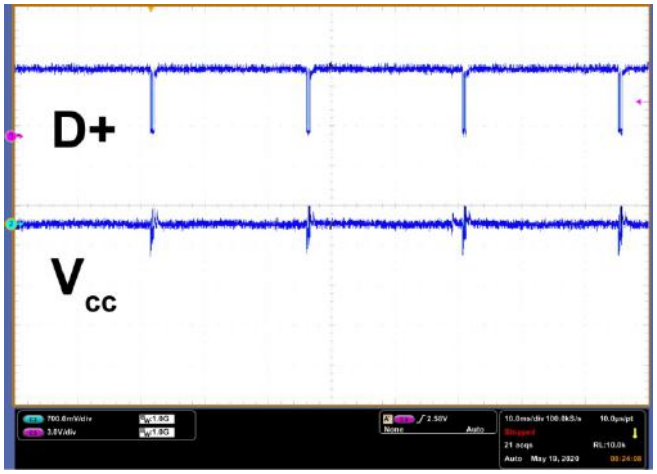


Figure 7. Waveforms corresponding to the data line and supply voltage, V_{cc}, for 4 PS/2 keys

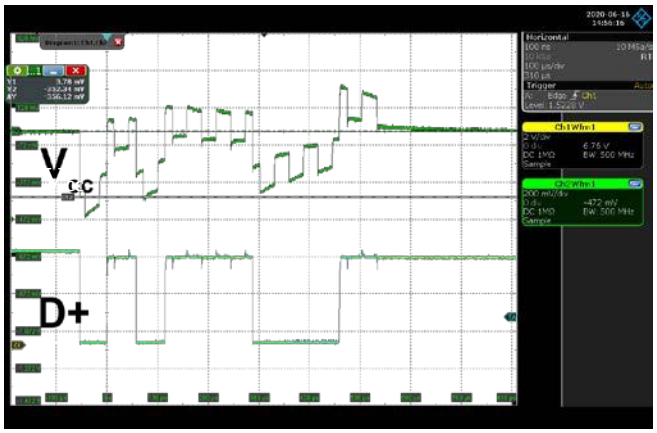


Figure 8. Analysis of supply voltage variations, V_{cc}, and data line, D+, for pressing a key

Interestingly, not all of these harmonics will modulate to the rhythm of the modulating signal, but only some of them. The key signal will be more or less affected by the noise on these harmonics, depending on their place in the spectrum.

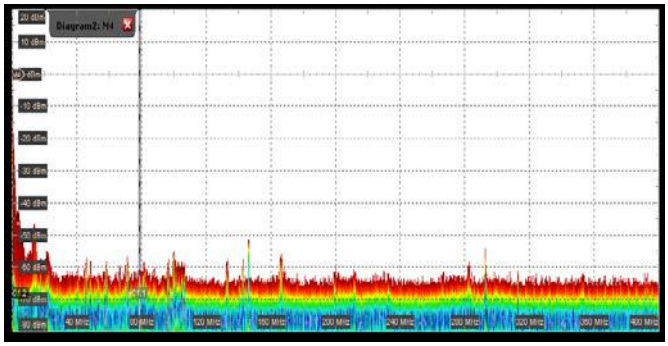


Figure 9. Signal spectrum of V_{cc}

Therefore, PDN analysis may be key in identifying a possible cause of how the key signal is found in the electromagnetic spectrum.

VI. CONCLUSIONS

Based on analysis and procedures presented we conclude that the studied equipment inadvertently generates electromagnetic radiation, and a signal of a compromising nature is also found. At the same time, through this paper we can notice that the signal-to-noise ratio is favorable for the recognition of a key pressed from the electromagnetic signature that produces its transmission to the information processing device.

The study presents a new approach on detecting PS/2 keyboard leakage signal with its unintentional model of construct. The article also shows how PDN analysis on PS/2 keyboards can contribute to detect the carrier which can modulate the D+ signal.

A database containing the compromising signal corresponding to each key of the studied equipment will lead to studying of the possibility of applying algorithms that use artificial intelligence in order to automatically detect the key and the "message" entered by a user. One challenge is to use these algorithms in real time, not an offline processing of the compromising signal. The operator's activity can be streamlined by developing a solution that leads to a reduction in time and effort.

Artificial intelligence, along with current techniques for the analysis and detection of electromagnetic emissions, can lead to new analysis techniques in a short time and with high accuracy. They can also be used in other applications for acquiring and processing signals in various engineering fields.

Although the PS/2 standard is quite old, it is still used today not only for the communication of desktop keyboards, but also for the communication of all laptops, equipment found in the logistics of any military or civilian structure. Knowing the model of the system at the output of which we obtain the signal radiated by the analyzed keyboard, but especially its physical implementation can be an effective means of defense in the electronic war in which we take part. With the help of this system, it is possible to mislead the opponent with regard to the information entered by the users of a system specified above, as well as its confusion with regard to the equipment used in unfavorable premises from the TEMPEST point of view.

REFERENCES

[1] D. C. Brock, G. E. Moore, *Understanding Moore's Law: Four Decades of Innovation*, Pennsylvania, Philadelphia: Chemical Heritage Press, 2006.

[2] C. I. Vizitiu, *Electronic warfare. Theoretical fundaments*, Military Technical Academy Publishing House, Bucharest, Romania, 2011.

[3] C. D. Bui, M. T. Ngo, H. N. V. Nguyen, T. M. Pham, "Information leakage through electromagnetic radiation of PS/2 Keyboard", *Journal of Science and Technology on Information Security*, vol. 10, no. 2, 2020. doi:10.54654/isj.v10i2.67

[4] X. Rognean, G. Roșu, A. Boitan, B. Trip, V. Butnariu, "Study of Compromising Emisions of PS/2 Keyboards by Correlative Methods", *Rev. Roum. Des. Sci. Tech. Ser. Electrotech. Energetique*, vol. 65, 2020.

[5] *Personal System/2 Hardware Interface Technical Reference – Architectures*, IBM, 1990.

[6] L. D. Smith and E. Bogatin, *Principles of Power Integrity for PDN Design: Robust and Cost Effective Design for High Speed Digital Products*, Teledyne LeCroy, New York, U.S., 2021.

[7] M. Vuagnoux, S. Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards", *SSYM'09, Proc. 18th Conf. on USENIX Security Symposium*, Aug. 2009, pp. 1–16 Berkeley, U.S., 2009.

[8] D. Yu-Lei, L Yinghua, and Z. Jinling, "Novel Method to Detect and Recover the Keystrokes of PS/2 Keyboard", PIER C, 2013, pp. 151-161. doi:10.2528/PIERC13042302