Information Leakage Through Electromagnetic Radiation of PS/2 Keyboard

Duc Chinh Bui, The Minh Ngo, Ngoc Vinh Hao Nguyen, Manh Tuan Pham

***Abstract*— Computer keyboards are often used to enter data for a computer system, data could be normal information or confidential information such as password, key. Keyboards use electronic components so they will generate electromagnetic radiation that can reveal information. This article presents the acquisition of electromagnetic emanating from the PS/2 keyboards through different paths (in space, through power line or via LAN cable). After acquisition we develop a program on MATLAB to recover the keystroke signal from data which is obtained in the near field of PS/2 keyboard. The result of this side channel attack is recovered an average of more than 70% of the keystrokes in near field of PS/2 keyboards. Our best attack can recover up to more than 90% of the keystrokes. From this result, we conclude that PS/2 keyboards generate electromagnetic radiations which can cause the loss of information and they are not safe to use when entering confidential information.**

***Tóm tắt*— Bàn phím máy tính thường được sử dụng để nhập dữ liệu đầu vào cho một hệ thống máy tính, các dữ liệu có thể là văn bản thông thường hoặc thông tin cần được bảo mật như mật khẩu hay khóa. Bàn phím sử dụng các linh kiện điện tử, vì thế chúng sẽ gây ra bức xạ điện từ dẫn đến lộ lọt các thông tin khi gõ phím. Bài báo này trình bày về việc thu các tín hiệu bức xạ điện từ phát ra từ bàn phím PS/2 khi gõ phím qua các con đường khác nhau (nhiễu bức xạ trong không gian, nhiễu dẫn trên đường nguồn, qua mạng LAN). Từ đó, nghiên cứu xây dựng một module chương trình trên MATLAB để khôi phục lại tín hiệu gõ phím từ các dữ liệu thu được trong trường gần của bàn phím. Kết quả của cách tấn công trên kênh kề này là khôi phục trung bình được hơn 70% ký tự được gõ trong trường gần của bàn phím PS/2. Trường hợp tốt nhất kết quả có thể lên đến hơn 90% ký tự được gõ. Từ kết quả nghiên cứu trên, nhóm nghiên cứu rút ra kết luận, các loại bàn phím PS/2 đều phát ra các bức xạ điện từ gây mất mát thông tin và không an toàn để sử dụng khi nhập các thông tin cần được bảo mật.**

***Keywords*— Electromagnetic radiation; PS/2 keyboard; acquisition of electromagnetic; recovery keystroke.**

***Từ khóa*— Bức xạ điện từ; bàn phím PS/2; thu bức xạ điện từ; khôi phục tín hiệu gõ phím.**

This manuscript is received June 14, 2019. It is commented on June 17, 2019 and is accepted on June 24, 2019 by the first reviewer. It is commented on June 16, 2019 and is accepted on June 25, 2019 by the second reviewer.

I. INTRODUCTION

Today, with the development of science and technology, information leakage through electromagnetic radiations of electronic devices such as monitors, keyboards, printers... has been published through research works in the world. Those researches indicate that it is possible to recover the original information from electromagnetic radiations with appropriate hardware and software. One component of the computer system that has the highest risk of information leakage is the computer keyboard. Keyboard is an input device of a computer system, used to enter normal information, confidential information or sensitive information. When the keyboard has hardware weaknesses that can be exploited, it will cause loss of information for computer systems regardless of the subsequent security and authentication.

The exploitation of electromagnetic radiation appeared for decades. Research on compromising electromagnetic emanations have been carried out such as radiation detection of Bell 131-B2 devices [8], recovering displayed images on CRT [4], recovery of displayed images on LCD [4], attack on secret keys [9], captures video radiations [12], attack electromagnetic radiation on Elliptic curves cryptographic on FPGA or exploits compromising electromagnetic radiation of the keyboard [8].

With computer keyboards, research in the world has presented different exploitations of leaked information [5] such as through optical radiation [7], video string analysis or using the

keyboard's LED as an auxiliary channel to collect data [3], exploit acoustic radiation to restore keystrokes [2, 11] and especially exploit electromagnetic radiations [4] or conducted radiation noise on the power line [1].

This article presents the acquisition of electromagnetic radiations of PS/2 keyboard in different cases of side channel attacks: the acquisition of radiated signals in space (near field and far field) and the acquisition of conducted disturbances through the power line and over the LAN cable. The obtained data will then be processed by a program on MATLAB to restore the keystroke. This research builds a program based on the Falling Edge Transition technique of the signal to detect the position of the key and based on the characteristics of the keystroke to convert the radiated signal to scancode, then compare it with scancode library to recover the keystroke. The program works well with obtained data in case of capturing radiated signals in near field of the PS/2 keyboard.

The structure of this article consists of 5 parts. Section 1 is a general introduction. Section 2 describes an overview of the electromagnetic radiation of the keyboard. Section 3 describes acquisition method of PS/2 keyboards in different setups. Section 4 describes development a program on MATLAB to restore keystrokes. Section 5 presents results of the measurements of radiated signals in different setups and the results of restoring keystroke in near field. Finally, we conclude the paper.

II. ELECTROMAGNETIC RADIATION OF THE KEYBOARD

Electromagnetic radiation has two types of unintentional radiation: Electromagnetic radiation in space and conducted disturbance transmitted through coupled lines. Electromagnetic radiation in space usually occurs when a part of the electronic or peripheral circuits inside the device acts as an antenna and emanate unintentional electromagnetic wave. Conducted disturbance requires a physical connection such as wire, trace in PCB... to transmit noise through the system [8].

A. The cause of keyboard radiation

Based on the principle of electromagnetic radiation, a change in current causes a change in magnetic field and creates electromagnetic waves propagating into space. The keyboard can generate electromagnetic radiation due to following reasons:

- Connection with the computer: On the data transmission line, the pulse sequences from the keyboard transmitted to the computer which represent typed data from the keyboard.
- Keystroke: Each keystroke is equivalent to closing switch to create a closed current to microprocessor, there is a change in current that creates electromagnetic radiation.
- Pulse sequences move on the data bus of microprocessor.
- Through power lines.

Electromagnetic radiation is usually caused by the types of radiation source in Common Mode (CM) and Differential Mode (DM) [4, 8].

One of the causes of electromagnetic radiation is the current flowing in common mode path. Common mode radiation is the result of undesired internal voltage drops in the electronic circuit which usually occurs due to the CM current flowing back to ground. These voltage drops are not intentionally generated, it is harder to detect and control radiations than differential mode radiation. The CM current flows to the ground due to the unbalanced nature of the circuits that transmit and receive signal. The CM current, that flows in cables and paths, causes electromagnetic radiation from electronic devices onto the power line and other line. External cables or conductor wires is connected to the ground loop act as antennas excited by internal voltage and emit electromagnetic wave in space.

Differential mode radiation is generated by loops formed by electronic components, printed circuit traces, cables... These loops act as small circular antennas and emit electromagnetic radiations. These radiated signals are usually small and do not disturb the whole system but are more dangerous because they carry important information. Differential mode

radiation can be easily avoided by shielding system components or the whole system.

When processors of the keyboard and computer work, they will emit electromagnetic radiations that can contain useful information. If these radiated signals are obtained, they can be used to restore original information. The signal which causes electromagnetic radiation is the signal of intrinsic quartz oscillator. With the PS/2 keyboard, the wires connected to CPU are usually arranged close to each other and are not shielded, so there is a leakage between the data line through the ground line. This ground wire is connected to the PC power supply and then to the power outlet and finally to the power line. This keyboard scancode is leaked and could be detected on the main power. With an appropriate receiver system, this leakage could be captured and used to restore characters which entered into the keyboard [1].

With USB keyboard, the acquisition of electromagnetic radiation becomes more difficult because USB keyboard uses the data transmission line as a pair of differential lines (D + and D-) so the emitted radiation amplitude is small.

B. Radiation frequency range of keyboard

Communication according to PS/2 standard depends on clock signal. With the keyboard, data transmission speed does not need too fast because it depends on the speed of human typing, so the clock rate is usually in the range of 10 kHz - 16,7 kHz. Radiation frequency is the fluctuating frequency of the current (voltage) that generates electromagnetic wave. The period of this fluctuating voltage depends on the clock rate of the pulse sequence. This clock signal is generated by the internal quartz frequency of the keyboard, which is in the range of 4 MHz - 6 MHz. The strongest radiated signal can be up to the order of 30 - 50 harmonics so the radiation range of the keyboard is in the range of 20 MHz - 300 MHz.

III. ACQUISITION OF ELECTROMAGNETIC RADIATION FROM THE KEYBOARD

The method of acquisition presented in this article is used a broadband receiver in combination with a wide-band antenna to scan the whole frequency range of the receiver and determine the keyboard's radiation frequency. Then the receiver frequency is tuned to a specific frequency and demodulate the signal. Narrow-band antennas and filters are used to improve the Signal to Noise Ratio (SNR) of compromising emanations and analysis signal in time domain.

The signal which sent from the PS/2 keyboard to the computer consists of two components: "Clock" and "Data". "Clock" consists of 11 pulses and "Data" is also limited in length of "Clock". When a key is pressed, electromagnetic radiations appear with amplitude and period corresponding to the "Clock" and "Data" signals, which means that they carry useful information that can be used to recover "Clock" and "Data" signals [8].

The difficult problem when capturing electromagnetic radiation of the keyboard is optimization and balance between the acquisition time and the sample rate because the memory of receiver is limited. With a high sampling rate, the full spectrum of signal will be obtained but it will consume memory, i.e. if the memory capacity is fixed, the acquisition time will be shorter. If the sampling rate is reduced, the acquisition time will be increased but the signal may be incomplete.

The experiments below use a personal computer that connects to different types of PS/2 keyboards. For security reasons, this article will not provide the brand name and model of the keyboard. The setup diagram is shown below.

Experimental setup

- Keyboard: Use five PS/2 keyboards from three different brands.
- Antenna: A set of antennas including a Loop antenna, a Biconical antenna, a Log - Periodic antenna and a Horn antenna, the set of antenna has frequency range from 10 kHz to 18 GHz.
- Near field probe set: HZ-15 near field probe set with frequency range from 30 MHz to 3 GHz and HZ-16 preamplifier with frequency range from 100 kHz to 3 GHz.
- Spectrum analyzer: ESR test receiver and spectrum analyzer with frequency range from 10 Hz to 26,5 GHz, bandwidth from 10 Hz to 10 MHz, internal preamplifier of 20dB with frequency range from 1 kHz to 7 GHz.

The experiments are set as follows:

- Case 1: Measure electromagnetic radiation in near field.

Experimental setup for measuring radiated signal from PS/2 keyboard in near field is shown in Fig.1.

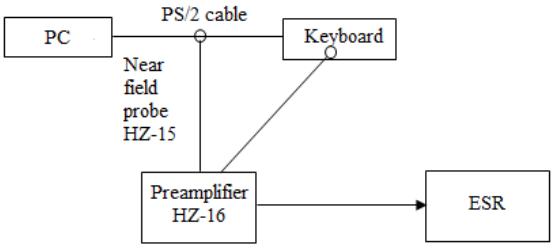

Fig.1. Model measurement of radiated signal from PS/2 keyboard in near field

This experiment will use the near field probe set HZ-15 to measure radiated signals on PS/2 cable or around PS/2 keyboard in near field and use HZ-16 preamplifier to amplify signal and transmit obtained signal to ESR receiver.

- Case 2: Measure electromagnetic radiation in far field

Experimental setup of measuring radiated signal from PS/2 keyboard in far field is shown in Fig.2.

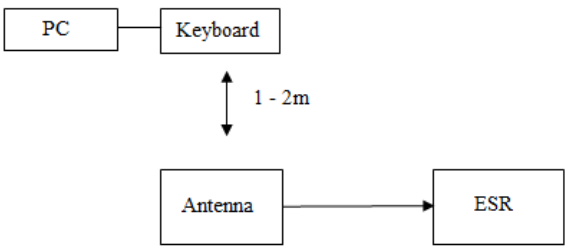

Fig.2. Model measurement of radiated signal from PS/2 keyboard in far field

This experiment will perform acquisition of electromagnetic radiations from PS/2 keyboard by using a Biconical antenna (20MHz ÷ 300MHz) and the ESR receiver.

- Case 3: Measure conducted disturbance through power line

Experimental setup of measuring conducted disturbances from PS/2 keyboard through power line is shown in Fig.3.

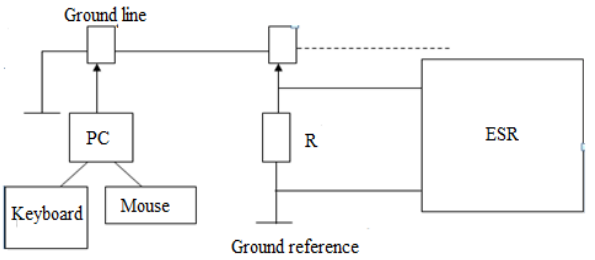

Fig.3. Model measurement of conducted disturbance from PS/2 keyboard through power line

This experiment will perform acquisition of conducted disturbance by an appropriate R resistor and connect directly to the ground line of computer, then obtained data will be transmitted to the ESR receiver.

- Case 4: Measure conducted disturbance over LAN cable

Experimental setup of measuring conducted disturbance from PS/2 keyboard over LAN cable is shown in Fig.4.

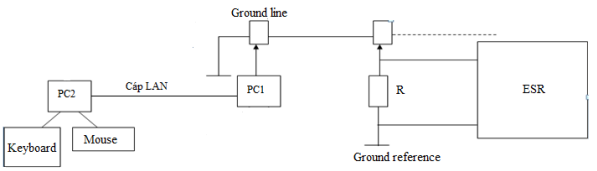

Fig.4. Model measurement of conducted disturbance from PS/2 keyboard over LAN cable

This experiment will perform acquisition of conducted disturbance by an appropriate R resistor and connect directly to the ground line of computer 1, computer 1 connects to computer 2 via LAN cable and performs keystroke on computer 2, then obtained data will be transmitted to ESR receiver.

IV. KEYSTROKE SIGNAL RECOVERY PROGRAM

Recovering keystroke from radiated signal of keyboard is a complex problem that requires a combination of techniques, each of which exploits one aspect of the radiated signal. Recovering keystroke based on obtained signal use detection techniques such as: Falling edge transition technique, Generalized transition technique, Modulation technique, Matrix scan technique and use trigger to detect and use feature extraction to identify keystroke. The method of acquisition and recovery in best condition has an accuracy of up to 95% [8].

With PS/2 keyboard, when a key is pressed, the keyboard sends a packet of scancode

information to the computer. The communication protocol of PS/2 keyboard is a bidirectional serial protocol, based on four wires: VCC (5V), ground, Data and Clock. For each byte of scancode, the keyboard sends an 11 bits data frame with a Clock frequency between 10 kHz to 16,7 kHz. The 11 bits correspond to a bit 0 (start bit), 8 bits for the scancode of pressed key, an odd parity check bit on the byte of scancode and a bit 1 (stop bit). Our keystroke signal recovery program is built on the Falling edge transition technique.

A. The Falling edge transition technique

The Falling edge transition technique based on property that the duration of the rising side (2µs) is longer than the duration of falling edge (200ns) of Clock signal and Data signal of PS/2 keyboard [8]. Thus, the electromagnetic radiation of a falling edge should be much more powerful and has a higher maximum frequency than a rising edge. The electromagnetic radiation of the keyboard is the combination of Data and Clock signals. Therefore, the detection of electromagnetic radiation is a combination of these two signals. However, the falling edges of Data and Clock are not superposed, so it is easily to separate the falling edges of Data and Clock. The falling edges of the Clock signal is always fixed and the falling edges of the Data signal depends on the scancode of pressed key, so it is possible to accurately identify 11 falling edges with equal spacing of the Clock signal and the falling edge of Data signal in the obtained signal (Fig.5).

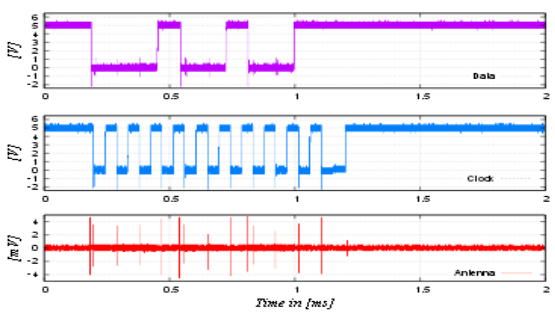

Fig.5. Data signal, Clock signal and radiated signal of PS/2 keyboard when key E is pressed [8]

When key E is pressed in Fig.5, we can clearly distinguish 11 falling edges of the Clock signal and 3 falling edges of the Data signal. Assuming the definition of falling edge trace as "2" when there are radiated peaks of Data and Clock signal and "1" when there is only a radiated peak of Clock. The falling edge trace of key E is "21112112111". Table 1 shows the falling edge trace of letter keys of PS/2 keyboard.

TABLE 1. THE FALLING EDGE TRACE OF LETTER KEYS

Trace	Possible letter keys
21111121111	a
21121112111	b, d, h, j, m, x
21211112111	c, n
21112112111	e, g
21121212111	f, v
21121111211	i, k
21121211211	l
21112111211	o
21211211211	p
21212121111	q
21211212111	r, space
21121121111	s, z
21111212111	t
21111112111	u
21211121111	w
21212112111	y

However, one thing to note that only the falling edges are detected, collisions occur during the recovery keystroke process when two keys or more have the same trace, such as both key C (scancode "21") and key N (scancode "31") have falling edge trace are "21111112111". But even when a collision occurs, the falling edge technique also limited the set of possible pressed key. For example, if a password includes 8 letters, the number of possible passwords is $26^8 \sim 2^{37}$. With the falling edge technique, the biggest number of possible passwords is $6^8 \sim 2^{20}$ when the letters in the password belong to a group of 6 letters ("b", "d", "h", "j", "m", "x"), but in reality, this case rarely happens. Thus, the average result is only about 2^{10}, much lower than the 2^{37}.

B. Keystroke signal recovery program for electromagnetic radiation of keyboard

Based on the falling edge technique mentioned above and analysed characteristics of scancode such as the first bit is bit 0 (start), the last bit is bit 1 (stop), bit 1 always has a larger amplitude than the bit 0... we built a program on MATLAB to recover the keystroke signal from obtained electromagnetic radiations of the PS/2 keyboard with the block diagram of the acquisition and recovery process is shown in Fig.6.

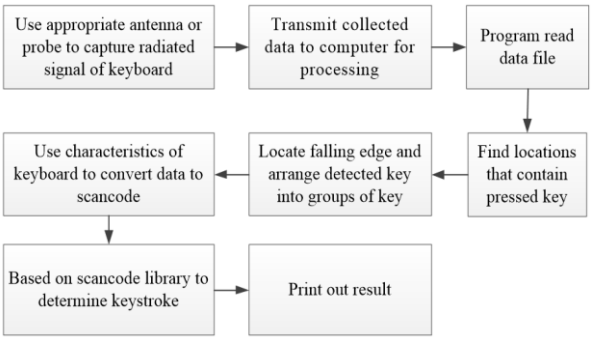

Fig.6. Diagram of capture and recover keystrokes process

The process of capturing and recovery keystroke includes following steps:

- First, use the antenna system or probe with appropriate sensitivity and in combination with the spectrum analyzer to capture radiated signal of keyboard.
- Then, collected data will be saved and transmitted to the computer for processing.
- MATLAB program for recovery keystroke will read data file in fixed-length frame. Use threshold to eliminate noise and find data locations that contain pressed keys.
- Locate the falling edge and arrange the detected keys into groups of keys (see Table 1).
- Use the characteristics of the keyboard scancode (bit 1 or bit 0) to convert keystroke data to scancode.
- Compare the transferred scancode with the keyboard's scancode library to determine the keystroke and print out the result.

The algorithm flowchart of capturing and recovery keystrokes process is shown in Fig.7.

Flowchart in Fig.7 includes the following steps:

1. Initiate the connection between the computer and the receiver via LAN cable.

2. Set up the necessary parameters of the measurement:

- Center frequency.
- Sample rate.
- Time of acquisition.
- Trigger.

3. The program will wait until the receiver completes the settings and send a notification to computer.

4. When the receiver is ready, the program will send a request to start measuring and wait for the receiver to respond.

5. When the receiver has completed a measurement, a notification will be sent and computer will read the measurement data in the receiver memory.

6. When data is available, the program will perform analysis and display the result on the screen.

7. After completing the data analysis, the program can continue measuring (go back to step 4) or stop.

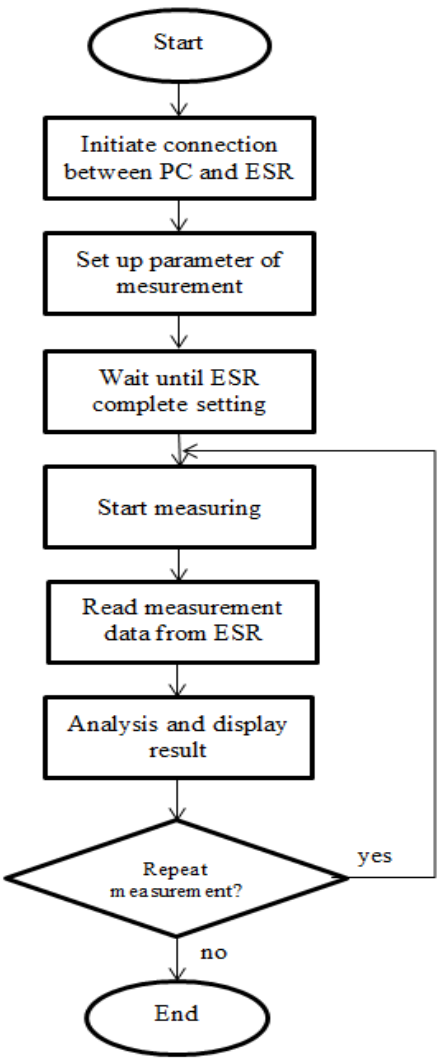

Fig.7. Algorithm flowchart of capturing and restoring keystrokes process

Note that the time of acquisition or the number of samples collected per frame must be large enough to contain all pulses of a keystroke. In order to minimize the amount of redundant data collected, the collection method only focuses on data frames that contain keystroke by using trigger. In principle, the clock is always high when there is no data transmitted between the keyboard and the computer, so the first clock pulse is always changing the state from 1 to 0, which means appearing a falling edge. Based on the above rule, the program selects trigger so that receiver starts from the first clock pulse of keystroke pulse sequence.

The algorithm flowchart of analyzing obtained data process in Fig.8.

Flowchart in Fig.8 includes the following steps:

Step 1. From receiver memory, the program checks to see if there is enough data for analysis. If not, exit program or else, analysis will be executed.

Step 2. From the data block, read out N data samples. N is defined so that it can contain no more than 1 pulse of clock.

Step 3. Find falling edge in those N data samples (radiated impulse detection). If not, go back to step 1 and read the next N data samples, if there is a falling edge then go to step 4.

Step 4. When appearing a falling edge, the program will read the next N1 samples, N1 will include the entire data of a keystroke. N1 is determined based on the keyboard's clock frequency and the receiver sample rate.

Step 5. Find the remaining falling edges positions in the N1 samples.

Step 6. Based on the searching results for the position of falling edges, divide the keystroke into the key group according to Table 1 for falling edge traces.

Step 7. Based on the characteristics of the keyboard scancode to recover scancode of the keystroke.

Step 8. Compare the scancode results with the scancode library and display the results on the screen. Then go back to Step 1.

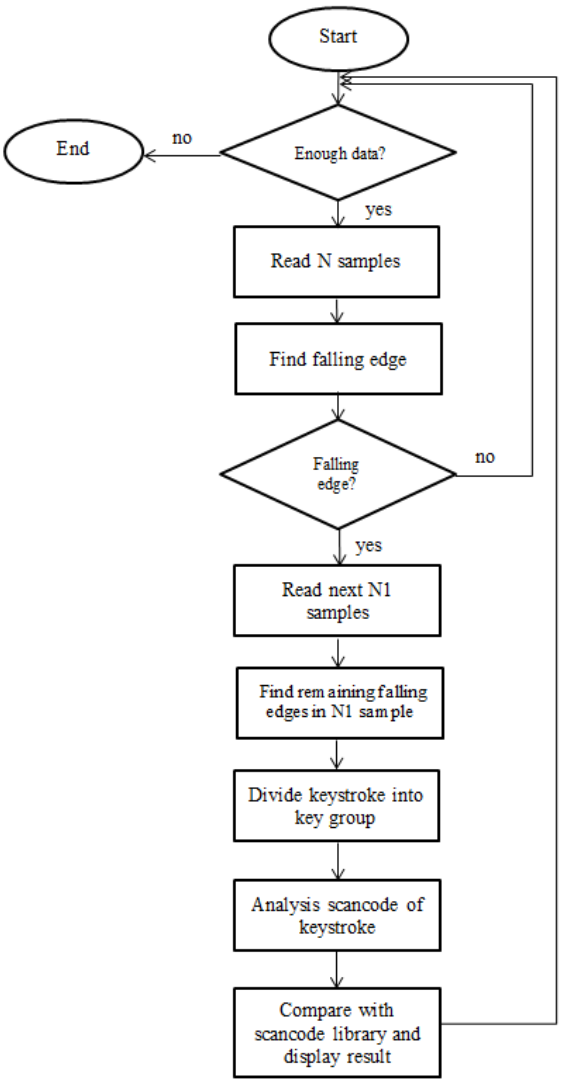

Fig.8. Algorithm flowchart of analyzing radiatied signal process

V. EXPERIMENTAL RESULTS

The experiments capture radiated signal as described in Part III with 4 different cases. The results are shown in Fig.9 to Fig.12.

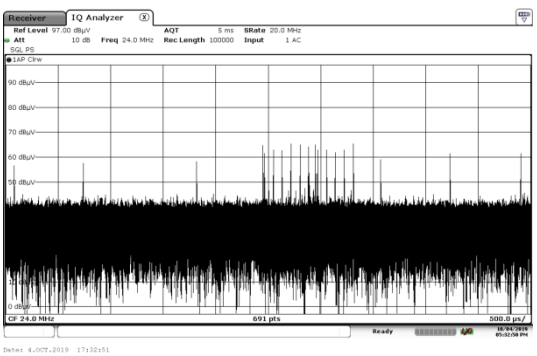

Fig.9. Radiated signal of key A is captured in near field

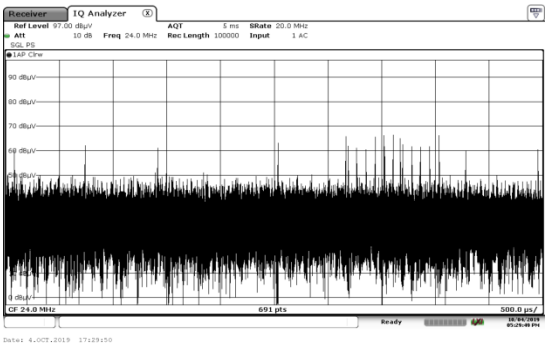

Fig.10. Radiated signal of key H is captured in far field

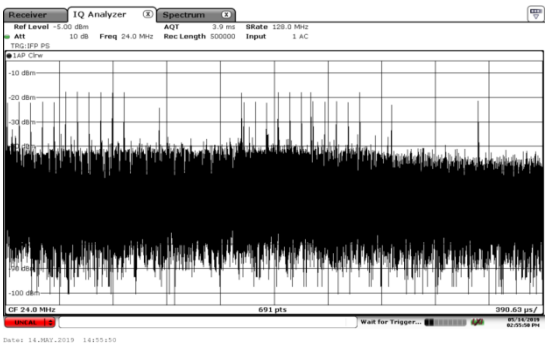

Fig.11. Radiated signal of key A is captured through the power line

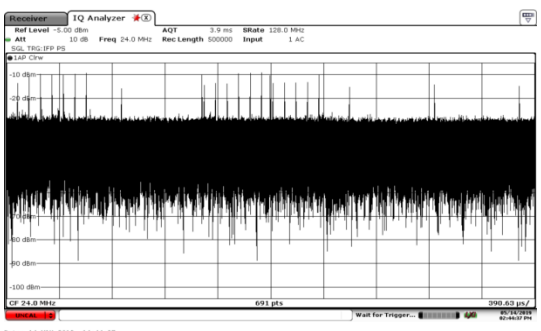

Fig.12. Radiated signal of key A is captured over LAN cable

The above test results show that the PS/2 keyboard emits electromagnetic radiations and these radiated signals can be obtained in different cases such as in far field, near field, conducted disturbance through power line and over LAN cable. Test cases have been successful on different PS/2 keyboards with different radiation amplitude and the scancode pattern does not change. The radiated frequency range of PS/2 keyboards is from 20MHz to 300MHz. In particular, the amplitude of radiation when receiving in near field is 20-30dB higher than the background noise and can clearly distinguish the signal pulses (bit 1 and 0), making the recovery process easier. For the remaining cases, the radiation amplitude is 10-15dB higher than the background noise, in addition the background noise is irregular, so restoring the keystroke signal is more complicated in near field. Our program is currently experimenting with the results of obtained signal in near field.

The obtained data in near field is processed in program presented in Part IV to perform recovery keystroke. The results are shown in Fig.13 with the keystroke sequence of "vien khoa hoc cong nghe mat ma". This example results in a true 26/30 keystroke ~ 86,67%.

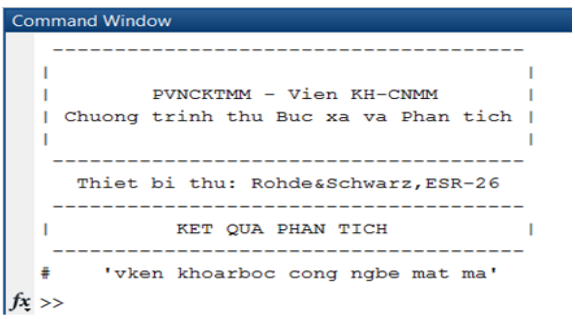

Fig.13. Results of running program

Based on a number of tests, as shown in Table 2, the results show that the program can recover averaged more than 70% of keystrokes. In the best cases of background noise as well as amplitude of the radiated signal, the result can up to 90% of keystrokes. With the case of Vietnamese typing with Vietkey or Unikey, the signal transmitted from the keyboard to the computer remains the same. Therefore, we can still recover the original text. From the above test results, it can be confirmed that PS/2 keyboards have a high risk of leaking information, that can cause the loss of important data and unsuitable for high security systems.

TABLE 2. EXPERIMENTAL RESULTS OF RECOVERY KEYSTROKE

Keystroke	**Recovered keystroke**	**Tỷ lệ**
abcdefghijklmn	amchefghijilmn	11/14 ~ 79%
conghoaxahoi	conghoaxahoi	12/12 ~ 100%
vienkhcnmm	vienkhcnmm	10/10 ~ 100%
cong hoa xa hoi chu nghia viet nam	cong hoa xa joi nhurnghiarvigt nam	26/31 ~ 84%
vien khoa hoc cong nghe mat ma	vienrkboa joc nongrnehe mat ja	23/30 ~ 76%

hello good morning	hgllo gooh morning	16/18 ~ 89%
bùi đức chính	buif jhuwcs nhinbs	14/18 ~78%
demo thu ban phim co day	dgmo thu ban phim co day	22/23 ~ 96%

Future studies are being carried out by us regarding restoring other cases of PS/2 keyboards, such as eliminating the increase of noise and amplifying the radiated signals. In addition, we are also studying methods of capturing radiated signals of other keyboards such as USB keyboard, wireless keyboard and Laptop keyboard. This requires improving the acquisition process by using preamplifiers as well as testing in environments with low background noise such as semi-anechoic chamber. The initial results of these studies are relatively positive, but the results are not comprehensive so we do not present in this article.

VI. CONCLUSION

The keyboard is an input component of a computer system, so if it is attacked, security of the system becomes insignificant. This article has proven the risk of information leakage through electromagnetic radiations of PS/2 keyboard. The article also presented the successful acquisition of electromagnetic radiations from PS/2 keyboard with cases of electromagnetic radiation in near field, far field and conducted disturbance through the power line and over LAN cable. Result of the keystroke recovery program can achieve an average of 70% of the keystrokes and up to more than 90% of keystrokes in the best case. With PS/2 keyboard, it is difficult to improve the hardware to avoid attacks as when improving the errors of software or operating system with patches. Therefore, for a high security computer system, keyboards with lower electromagnetic radiation leakage should be used and tested before being use in practice as well as applying some techniques to reduce electromagnetic radiation, such as using filters, shielding or generate noise.

ACKNOWLEDGMENT

This work was supported by Institute of Cryptographic Science and Technology, Viet Nam.

REFERENCES

[1]. Andrea Barisan Daniele Bianco, "Side Channel Attacks Using Optical Sampling of Mechanical Energy and Power Line Leakage", Copyright Inverse Path Ltd, 2009.

[2]. Asonov, D., and Agrawal, R., "Keyboard Acoustic Emanations", In IEEE Symposium on Security and Privacy, 2004.

[3]. Blzarotti, D., Cova, M., and Vigna, G., "Clearshot: Eavesdropping on keyboard input from video", In IEEE Symposium on Security and Privacy, 2008.

[4]. Kuhn, M. G., "Compromising Emanations: Eavesdropping risks of Computer Displays", Technical Report, 2003.

[5]. John V. Monaco, "SoK: Keylogging Side Channels", IEEE Symposium on Security and Privacy, 2018.

[6]. Lizhuang, Fengzhou, J. D. Tygar, "Keyboard Acoustic Emanations Revisited", In Proceedings of the 12th ACM Conference on Computer and Communications Security, November 2005.

[7]. Loughry, J., and Umphress, D. A., "Information leakage from optical emanations", ACM Trans. Inf. Syst. Secur, 2002.

[8]. Martin Vuagnoux, Sylvain Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards", Security and Cryptography Laboratory, 2007-2009.

[9]. Smulders, P., "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables", Computers and Security, 1990.

[10]. Tuttlebee, W., "Software Defined Radio: Enabling Technologies", John Wiley and Sons, England, 2003.

[11]. Tzipora Halevi, Nitesh Saxena, "Keyboard acoustic side channel attacks: exploring realistic and security-sensitive scenarios", International Journal of Information Security, Springer, 2014.

[12]. Van Eck, W., "Electronagmetic radiation from video Display Units: An eavesdropping risk?", Comput. Secur, 198.

ABOUT THE AUTHOR

M.Sc. Duc Chinh Bui

Workplace: Institute of Cryptographic Science and Technology, Vietnam Government Information Security Commission.

Email: ducchinh1108@gmail.com

Education: Received the Degree of Engineer in Electronics and Telecommunication Engineering in 2013 and the Degree of Master of Enginerring in Electronics Engineering in 2016 from the School of Electronics and Telecommunications, Hanoi University of Science and Technology, Vietnam.

Research today: Field of electromagnetic compatibility, include solutions to ensure EMC for electronic devices and exploit information leakage through side channels.

M.Sc. The Minh Ngo

Workplace: Institute of Cryptographic Science and Technology, Vietnam Government Information Security Commission.

Email: ntminh1963@yahoo.com

Education: Received the Degree of Engineer from Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Hungary, in 1987. Received the Degree of Master of Engineering from Academy of Cryptography Techniques, Vietnam, in 2005.

Research today: Field of electromagnetic compatibility, include solutions to ensure EMC for electronic devices and research about EMC standards.

Ngoc Vinh Hao Nguyen

Workplace: Institute of Cryptographic Science and Technology, Vietnam Government Information Security Commission.

Email: nnvh89@gmail.com

Education: Received the Degree of Engineer and Master in Aerospace Radio-Electronic System from Karkov Aviation University, Ukraine, in 2013 and 2015 respectively.

Research today: Field of electromagnetic compatibility. Currently, he is working on cryptography analysis through side channels.

M.Sc. Manh Tuan Pham

Workplace: 129 Company Limited, Vietnam Government Information Security Commission.

Email: tuanpm.129@gmail.com

Education: Received the Degree of Engineer from Posts and Telecommunications Institute of Technology, Vietnam, in 2003. Received the Degree of Master from Military Technical Academy, Vietnam, in 2008. Received the Degree of Doctor of Physolophy from Posts and Telecommunications Institute of Technology, Vietnam, in 2017.

Research today: design and implement cryptographic algorithms on hardware; overall study of security solutions for voice and video data on different media environments.