Parameters optimization filter for signal processing USB keyboard enamation comprimising

Nguyen Ngoc Vinh Hao, Bui Duc Chính, Ngo The Minh

***Abstract*—Computer peripherals such as monitors, keyboards can be targets to exploit information through electromagnetic radiation side chanel attacks. In order to be able to perform these attacks on these devices, it is necessary to use appropriate digital filters to select the frequency band and reduce the effect of noise on the useful radiated signal. The article will introduce the parameter optimization process of the digital filter in recovering keystrokes from the radiated signal of the USB keyboard..**

***Tóm tắt*—Các thiết bị ngoại vi của máy tính như màn hình, bàn phím có thể là mục tiêu để khai thác thông tin rõ thông qua tấn công phân tích bức xạ điện từ trường. Để có thể thực hiện được các tấn công kênh kề này lên các thiết bị này cần sử dụng các bộ lọc số thích hợp để chọn băng tần và làm giảm ảnh hưởng của nhiễu đến tín hiệu có ích thu được. Bài báo sẽ giới thiệu quá trình tối ưu tham số của bộ lọc số trong việc khôi phục phím gõ từ tín hiệu bức xạ của bàn phím USB.**

Keywords*—*Side-channel attack, USB keyboard enamation comprimising, Signal filtering.

Từ khóa*—*Tấn công kênh kề, Bức xạ bàn phím USB, Bộ lọc tín hiệu.

I. INTRODUCTION

Attacks on keyboard radiation of keyboards have been studied by Markus Kuhn since the 2000s [4]. However, Markus only proposed the theoretical method and has not conducted experimental analysis of the keyboard's radiation signal. In 2018 Alexandru Boitan published the results of radiation capture of USB keyboards using Markus Kuhn's correlation method [4]. In 2009 Sylvain Pasini used the keyboard matrix scanning method to find the keystrokes of the USB keyboard [5]. In 2016 Dong-ju Sim, Ho Seong Lee published a number of articles using radiation peak detection technique to analyze keystrokes of USB keyboards [1, 2, 3]

The above studies focus on general introduction of methods used to analyze keyboard keys. However, the effectiveness of the attack on electromagnetic radiation is greatly influenced by the signal processing technique. The objective of the paper is to compare the efficiency of digital filters when dealing with USB keyboard radiation.

This article is divided into 5 main parts. Part I gives a general introduction. Part II conducted the radiation measurement from the USB keyboard. Part III presents the design of a digital filter for processing of radiated signal. Part IV presents the results of using filters in keystroke analysis and the parameter optimization capabilities of those filters. Finally, conclusions and comments are given in the V section.

II. USB KEYBOARD RADIATION MEASUREMENT SETUP

To collect the radiated signal of the USB keyboard, this article uses the measuremen model as shown in figure 1 below:

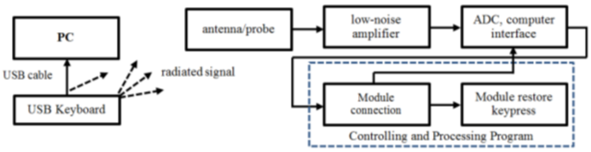


Figure 1. Measurement configuration of USB keyboard enamation comprimising.

To be able to catch radiated signals, it is necessary to have a system of measuring and pre-processing equipment combined with a signal processing program. The hardware system consists of the first three components of model 1 above: the antenna/probe unit, the low-noise amplifier, the ADC (Analog to Digital Converter) and the computer interface. Including the tempest receiver and antenna/transducer set to catch electromagnetic signals from free space. That signal includes USB keyboard radiation and noise. However the USB keyboard used a differential mode signal with a small amplitude, additional low-noise amplifiers are required. Those amplifiers are responsible for enhancing the useful signal at the required frequency ranges. The ADC converts the analog signal into a digital form and then sends it to a signal processing program for analysis.

Based on the model shown in figure 1, the probe is measured at various positions of the keyboard to determine the radiation location as well as the corresponding field strength. Through calculating statistics for USB keyboards, its processing circuit generates electromagnetic radiation related to keystrokes that are processed inside. Thus the position of the signal probe is placed on the microcontroller of the USB keyboard to collect radiation during the operation of the keyboard, see figure 2 below.

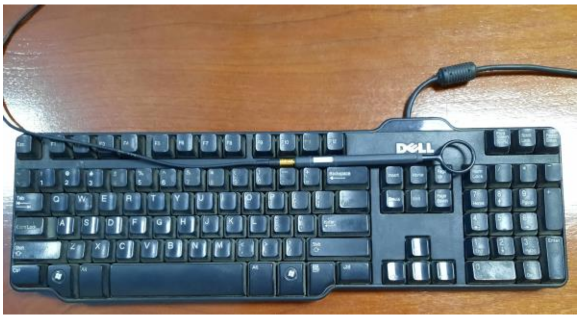


Figure 2. Position of probe on the USB keyboard.

The test uses a HZ-15 probe connected to a 30dB HZ-16 amplifier with the frequency range from 30MHz to 3GHz. The R&S ESR26 receiver acts as an ADC and also communicates with the control computer. The article conducts a test for the Dell SK-8115 USB keyboard.

The method of identifying keystrokes by finding radiation peaks is based on analysis techniques and locates peaks in the radiated signal. The applicability of this method depends on finding the exact position of the peaks corresponding to the radiation of the keystroke signal. Using AMPD (Automatic Multiscale-Based Peak Detection) algorithm for the above radiated signals [1].

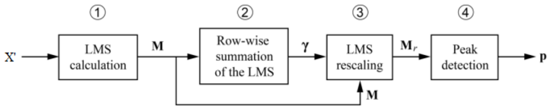
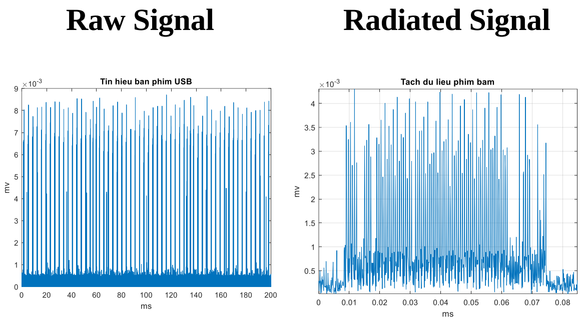


Figure 3. Flowchart of the AMPD algorithm.

The input x is the pre-processed radiated signal, the output P is the signal with the list of detected radiation peaks. Due to the limitation of the paper, we will not go into detail about the operation of the AMPD algorithm. The peak analysis results will then be used to analyze the corresponding scancode of the keystroke. Compare with scancode of USB keyboard to restore keypress.

The results of measuring and recovering radiated signals of some keypress of this keyboard are shown in figure 4:



Scancode = 4 => **Keystroke** “A”

Figure 4. Result of USB keyboard keypress recovery.

The above results of the analysis program are performed with the following measurement setup:

• The program collects 2000000 points of radiated signal samples at a rate of 10Msps, equivalent to a reception time of 200 ms.

• The center frequency is 222MHz for the DELL SK-8115 keyboard.

• Capturing each keystroke (letter and number) and check the accuracy of the recovery program.

Through the above results, it can be confirmed that the Dell SK-8115 USB keyboard has radiation when operating and has the ability to recover keystroke information based on the received radiation.

III. DESIGNING DIGITAL FILTERS USED IN ANALYSIS OF ELECTROMAGNETIC RADIATIONS

As we know the received signal always includes noise from the external environment. By comparing the spectrum of the keystroke and non-keystroke signal, it is possible to identify the signal components and noise components in the background of the received spectrum. Figure 5 below depicts the spectrum of the received raw signal:

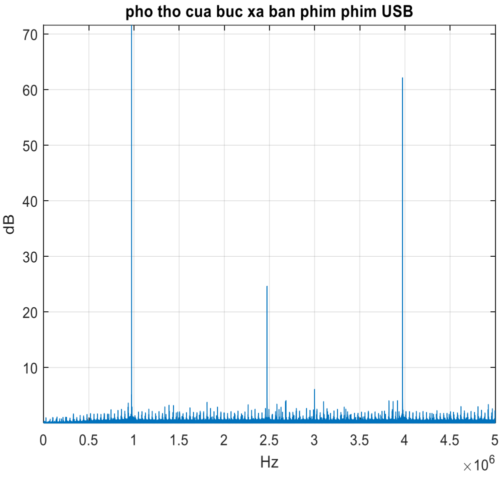


Figure 5. Spectrum of the raw received signal.

The filter performs the processing of components on the spectrum of the signal. Digital filters are usually described by the following components: adder block, multiplier block and delay block. The adder block has two inputs and one output, its function is to add two input signals together. The multiplier block is an amplifier element that multiplies the input signal by a constant. The delay block implements delaying the input signal by one sample, see figure 5 below [10]:

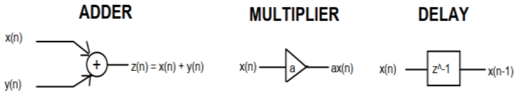


Figure 6. Basic elements of digital filters.

With the above basic blocks, it is possible to build two different basic filter structures. The filter corresponding to these two structures is called: infinite impulse response (IIR - Infinite Impulse Response) and finite impulse response (FIR - Finite Impulse Response).

The LPF (Low Pass Filter) filters used include: LPF FIR and MA (Moving Average). FIR filter is chosen because FIR filter design will be easier in the initial stage. This design slows down the input signal without distorting its phase. In addition, the FIR filter is easy to set up and calculate the FIR in all signal processing software. The MA filter is the most commonly used form of LPF in practical applications. They are optimized to reduce random noise while ensuring the slope of the frequency response function and have good smoothing effect in the time domain. In addition, the MA filter is easy to design by coefficients without taking into account the signal multiplier blocks.

The formula describing the relationship between the output signal, the input signal and the frequency response of the MA filter has the following form:

$$y(n)=\frac{1}{N}\sum_{k=0}^{N-1}x(n-k) \qquad (1)$$

Where: N - the order of the MA filter and is equal to the number of points of the filter. The higher the order of the MA filter, the greater the signal flattening ability. In this paper, we will investigate the MA filter order $N=501\to 2001$ with an increment of 100 steps/time, for example the frequency response of order N = 1001 is as follows :

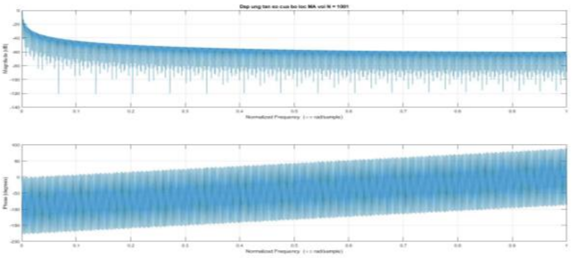


Figure 7. Frequency response of the MA filter with N = 1001.

The radiated signal of the USB keyboard consists of many different frequency components. The characteristics of the low frequency components represent the average energy of the signals transmitted in the keyboard.

It can be understood simply that the larger the keyboard signal is, the lower frequency components in the radiated signal also increase accordingly. The LPF FIR filter will be used to separate these components for the average energy analysis of the USB keyboard signal. Based on the characteristics of the received radiated signal, the parameters of the LPF filter can be selected in the range as follows:

• Sampling frequency: $f_s = 10^6$ Msps. This frequency depends on the the ESR-26 receiver configuration.

• Cutoff frequency: $f_{cutoff} = 0,4 \to 1,2$ MHz. The average energy of the signal when the key is pressed will be higher than the average energy when there is no keystroke. Spectral components in the range $0 \to 0,4$ MHz are characteristic of this energy.

• Bandwidth ripple $A_p = 0,01 \to 0,2$ dB. The passband ripple should be as low as possible to avoid distortion in the frequency range below 0.4 MHz.

• Stopband loss $A_s = 60 \to 100$ dB. This is a relatively good loss commonly used with low-pass filters.

• Degree of filter $N = 60 \to 120$. Selecting this value ensures the necessary slope in the filter's transition band.

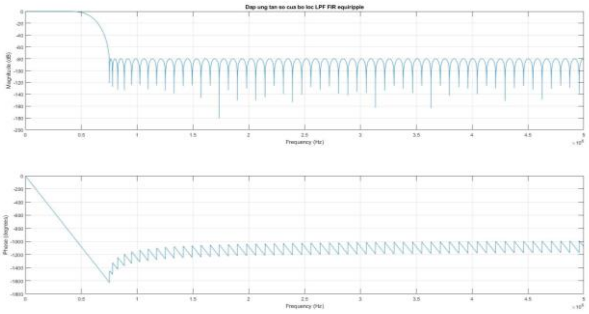


Figure 8. Frequency response of an LPF FIR filter.

According to documents [1, 2, 3] and from experimental results, it is found that these spectral components are concentrated at mid frequencies in the range of 1.5 MHz; 3 MHz; 4.5 MHz… after the radiated signal has been converted to the baseband. With DSP System Toolbox to design BF filters can use designfilt function. Thus, to separate and integrate these useful spectral components, it is necessary to use a BF FIR bandpass filter around the 3MHz center frequency with the following parameters:

• Sampling frequency: $f_s = 10^6$ Msps. Similar to the LPF filter this frequency depends on the setup of the ESR-26 receiver.

• Lower cut-off frequency: $f_{cutoff1} = 1,48;\ 2,98;\ 4,48$ MHz; cutoff frequency above $f_{cutoff1} = 1,52;\ 3,02; 4,52$ MHz. Spectral components in the 0.04 MHz band around the center frequency carry information about the data of the keystroke [1].

• The passband and stopband ripple calculated by Matlab depend on the definition of the passivation depending on the cutoff frequencies and the order of the filter.

• Degree of filter $N = 60 \to 120$. Selecting this value ensures the necessary slope in the filter's transition band

The optimal parameter value of the filter will be selected through running the allowable range. The analysis program evaluates the keystroke recognition results to find the optimal value for the filters.

IV. RESULTS OF ANALYZING KEYPRESS WITH DIFFERENT DIGITAL FILTERS

It is possible through the experimental method to choose the optimal parameter value for these filters. The program flowchart to determine the optimal value for the filter parameters designed in Part III has the form shown in figure 9 below:

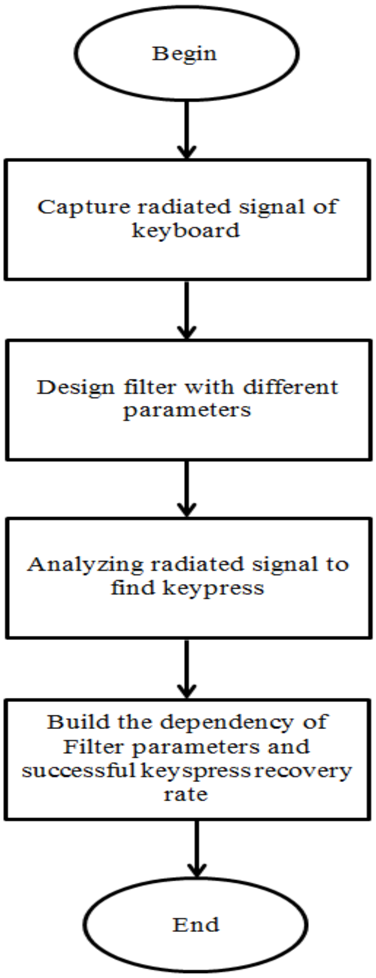

Begin
Capture radiated signal of keyboard
Design filter with different parameters
Analyzing radiated signal to find keypress
Build the dependency of Filter parameters and successful keyspress recovery rate
End

Figure 9. Flowchart of the program to choose the optimal value of the filter.

Using the above method, it is possible to calculate the successful keyspress recovery rate depending on the order of the MA filter with the form shown in figure 9 below:

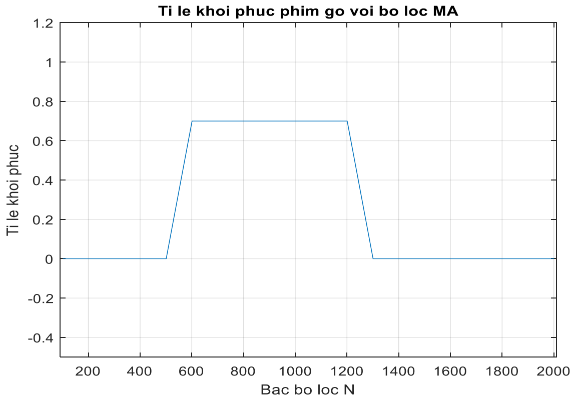


Figure 10. Relationship of keypress recovery rate and MA filter order.

The success rate of keypress recovery depends on the order of the FIR LPF filter, as shown in figure 11 below:

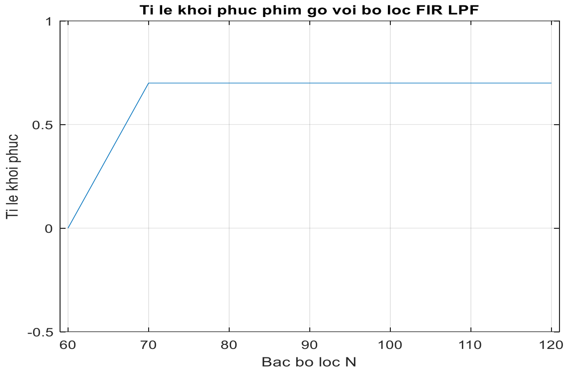


Figure 11. Relationship of keypress recovery rate and LPF filter order.

The successful keystroke recovery rate depends on the order of the FIR BF filter, as shown in figure 12 below:

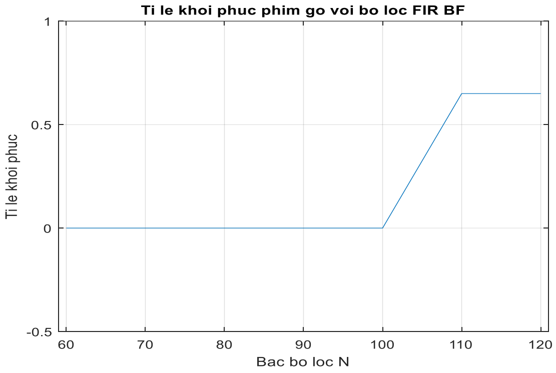


Figure 12. keypress recovery rate and BF filter order.

Through the keypress analysis results, it can be seen that the order of MA filter has the optimal value range from 600 to approximately 1200. LPF filter needs at least order N > 70 or higher, the recovery rate will reach 70%. For a BF filter it is necessary to use N > 110 or more for a recovery rate of approximately 70%.

V. CONCLUSION

The article presented the process of performing electromagnetic radiation measurement for the DELL SK-8115 USB keyboard. Through the received radiated signal, it is analyzed and restored to the corresponding keypress. The article also uses experiments to find the dependence of the basic parameters of the filters on the successful recovery rate. From there, it is possible to choose the optimal value of the filters when restoring keypress. Selecting the optimal value increases the USB keyboard's keystroke recovery success rate, approximately 70% with of the R&S HZ-15 probe.

REFERENCES

[29] Dong-ju Sim, Ho Seong Lee, Jong-Gwan Yook, Kyuhong Sim, "*Measurement And Analysis Of The Compromising Electromagnetic Emanations From USB Keyboard*", Asia-Pacific International Symposium on Electromagnetic Compatibility, 2016.

[30] Hyo-Joon Choi, Ho Seong Lee, Dong-ju Sim, "*Reconstruction Of Leaked Signal From USB Keyboards*", IEEE, 2016.

[31] Dong-ju Sim, Ho Seong Lee, Jong-Gwan Yook, "*Measurement and Analysis Of The Compromising Electromagnetic Emanations from USB Keyboard*", 7th Asia Pacific International Symposium on EMC.

[32] Alexandru Boitan, Razvan Bărtușică, "*Compromising Electromagnetic Emanations of Wired USB Keyboards*", Future Access Enablers for Ubiquitous and Intelligent Infrastructures, 2018.

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

ABOUT THE AUTHORS

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.

Recent research direction: Field of electromagnetic compatibility. Currently, he is working on cryptography analysis through side channels.

Duc Bui Chinh

Workplace: Institute of Cryptographic Science and Technology, University of Electro-Communications Japan.

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.

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

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.

Recent research direction: Field of electromagnetic compatibility, include solutions to ensure EMC for electronic devices and research about EMC standar