Reconstruction of Leaked Signal from USB Keyboards

Hyo-Joon Choi, Ho Seong Lee, Dongjoo Sim, and Jong-Gwan Yook
Dept. Electrical and Electronic Engineering
Yonsei University
Seoul, Republic of Korea
jgyook@yonsei.ac.kr

Kyuhong Sim
LIG Nex1
Seongnam, Republic of Korea

***Abstract*—Key information of universal serial bus (USB) keyboards at keystroke can be found by analyzing the electromagnetic emanations from the USB cable. The problem with information security such as eavesdropping arises from these emanations. This paper presents the emission phenomenon according to the signal transmission mechanism of USB keyboards and method of measurement and analysis of the leaked signal. Electromagnetic emanations were measured by the antenna and receiver and analyzed by the several signal processing algorithms.**

Keywords—TEMPEST; universal serial bus (USB) keyboard; electromagnetic emanations; signal reconstruction;

I. Introduction

Recently, the research about analyzing the electromagnetic emanations from input or output devices of the computer which is known as TEMPEST has been continuously progressed. The unintentional radiated emissions inevitably occur when the sensitive personal information such as password is entered through the keyboard. The problem with information security such as eavesdropping or harming hardware by this phenomenon has also been discussed [1]. In 2010, the research about analyzing leaked signal from personal system/2 (PS/2) keyboards was conducted [2]. The recovery technique of radiated signals from not only PS/2 keyboards but also universal serial bus (USB) keyboards is required because the USB keyboards are mainly used in these days. With respect to the USB keyboard, the study about signal reconstruction using matrix scan technique was carried out [3]. But, it is hard to find the original waveform of the radiated signal because it is probabilistic estimation model.

In this paper, the electromagnetic emanations from USB keyboards were measured by antenna and receiver and were analyzed by signal processing algorithms. Finally, the signal reconstruction of keys were accomplished.

II. Radiation Mechanism of USB Keyboards

The signal of USB keyboards which is composed of differential signaling and digital signals is transmitted to the personal computer according to the USB keyboard protocol at keystroke as shown in Fig. 1. The binary code is encoded with non-return-to-zero, inverted (NRZI) method. The packets are composed of start packet, data packet which includes the information of the key, and end packet. The binary code of the key is located at fixed position in the data packet and the scan code of the key is detected by decoding the binary code. The peak electromagnetic emanations are dominantly generated at the transition edge of the digital signals. The scan code of the key is detected by analyzing the waveform of data packet at keystroke.

III. Measurement and Analysis

A. Measurement of Leaked Signal

The electromagnetic emanations are measured by log periodic (LP) antenna which operates from 20 MHz to 3 GHz and the wideband receiver which works from 20 MHz to 3.6 GHz as shown in Fig. 2. The distance between device under test (DUT) and antenna is 15 cm and experiment was conducted in office environment. By the spectrum analysis, it is determined that dominantly radiated emission frequency is 128 MHz. Sampling rate is set to 10 MHz and the number of samples is set to 2 million so that leaked signal can be analyzed from 0 ms to 200 ms. The frequency range of measured signal is from 128 MHz to 133 MHz and the data packet waveform at this frequency range is shown in Fig. 3. The measurement data about key S was shown in this paper and the target keys are 36 keys: alphabet keys and number keys.

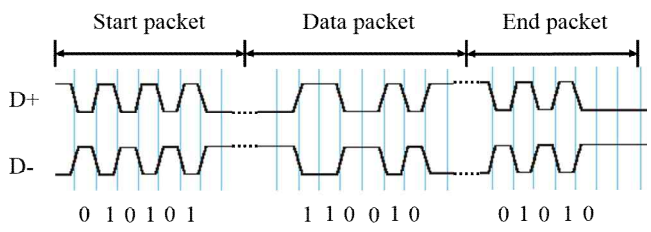

Fig. 1. USB Keyboard Protocol

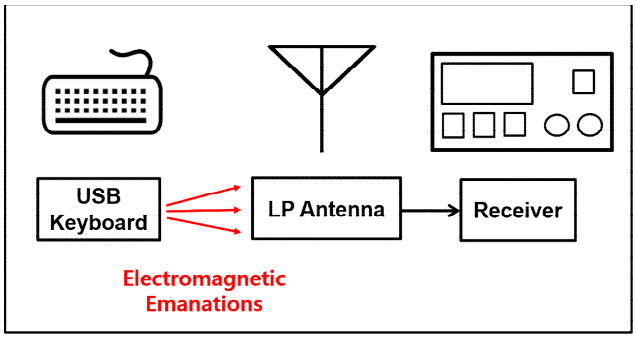

Fig 2. Experimental Setup

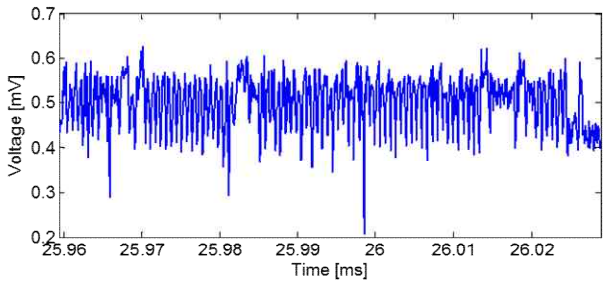

Fig. 3. Data Packet of Measured Signal

B. *Analysis of Leaked Signal*

Measured electromagnetic emanations are analyzed by signal processing algorithms for signal reconstruction as shown in Fig. 4. To find the position of data packet of the key, band-pass filtering is processed at the frequency range from 128 MHz to 128.4 MHz and the data packet of band-pass filtered signal at this frequency range is shown is Fig. 5. Negative peak detection is used in order to find the binary code of the key. To find the effective negative peak, the voltage threshold level is set, which is from 0.9 to 0.92 times the average value of measured signal. Since the data rate of USB keyboard is 1.5 Mbps, a minimum interval of effective negative peaks is from 0.6 μs to 0.7 μs. The binary code of the key is figured out by allocating binary bit to the effective negative peaks. The first bit can be either 0 or 1 because the relationship between the adjacent two bits determines whether it accords with the original scan code of the key or not. As a result of allocating binary bits which changes at every effective negative peaks, the binary bits from 32nd bit to 40th bit are the binary code of the key. By decoding this binary code using NRZI method, 01101000 is found and this data is accordance with the original scan code of the key S as shown in Fig. 6. In the same way, signal reconstruction of the other keys were also accomplished.

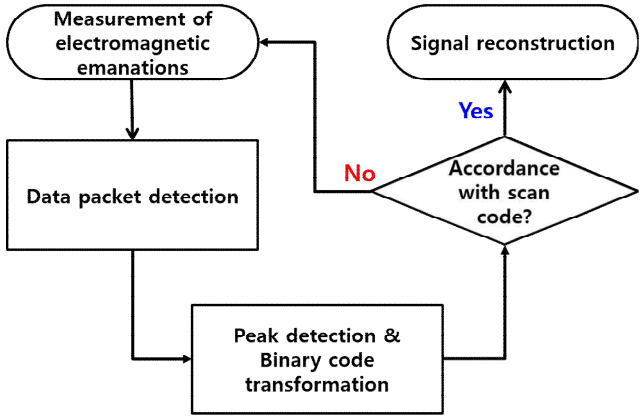

Fig. 4. Flowchart of signal processing algorithm

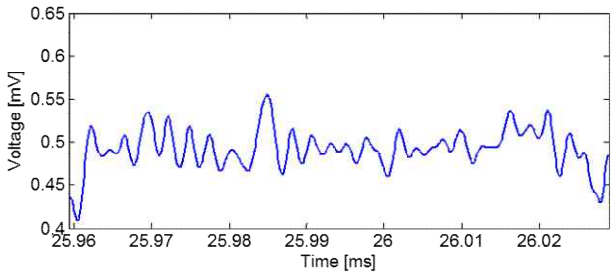

Fig. 5. Data Packet of Band-pass Filtered Signal

IV. Conclusion

In this paper, the electromagnetic emanations from USB keyboard were measured by LP antenna and receiver, and analyzed by the signal processing algorithms for information recovery. As the center frequency was set to 128 MHz and sampling rate was set to 10 MHz, the leaked signal at the frequency range from 128 MHz to 133 MHz was received by the receiver. In order to find the position of data packet of the key, band-pass filtering at the frequency range from 128 MHz to 128.4 MHz was conducted. By processing peak detection, it was shown that the analyzed data in the measured signal was accordance with the scan code of the key and the signal reconstruction of 32 keys among 36 keys were accomplished.

Acknowledgement

"This work has been supported by LIG Nex1 under the contract UC140011ED"

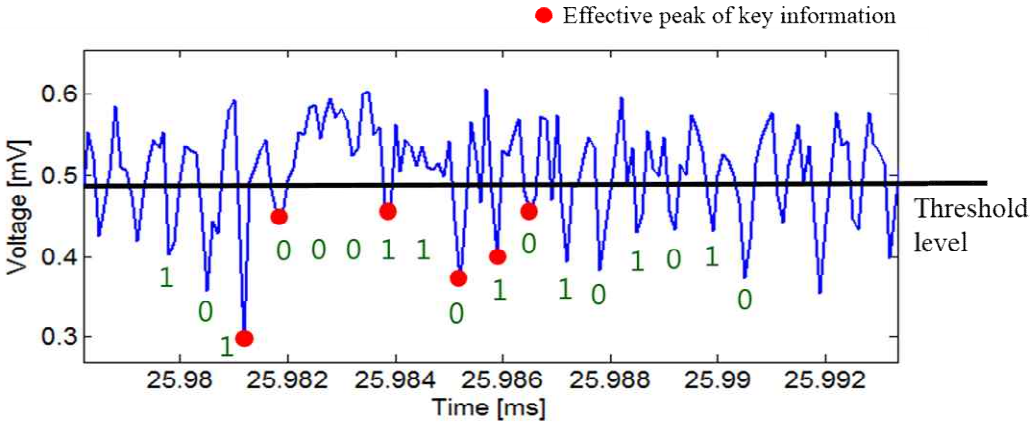

Fig . 6. Binary Code of key S

REFERENCES

[1] Yasunao Suzuki, Masao Masugi, Kimihiro Tajima, and Hiroshi Yamane, "Countermeasures to Prevent Eavesdropping on Unintentional Emanations from Personal Computers," NTT Technical Review, vol.6, no.10, Oct. 2008.

[2] Ho Seong Lee, Dong-Joo Sim, Kyuhong Sim, and Jong-Gwan Yook, "Analysis of the Compromising Electromagnetic Emanations of PS/2 Keyboards," in *Asia Electromagnetics Symposium (ASIAEM) 2015*, Aug. 2015.

[3] Vuagnoux, Martin, and Sylvian Pasini, "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," *USEMIX Security Symposium*, 2009.