SICE Annual Conference 2012
August 20-23, 2012, Akita University, Akita, Japan

The Effects of PS/2 Keyboard Setup on a Conductive Table on Electromagnetic Information Leakages

Masahiro KINUGAWA[1], Yu-ichi HAYASHI[2], Takaaki MIZUKI[3] and Hideaki SONE[3]

[1] Graduate School of Information Science, Tohoku University, Sendai, Japan
(Tel : +81-22-795-6094; E-mail: kinugawa@s.tohoku.ac.jp)
[2] Research Institute of Electrical Communication, Tohoku University, Sendai, Japan
[3]Cyberscience Center, Tohoku University, Sendai, Japan

Abstract: Recently, it has been shown that electromagnetic emissions from information communication devices emanate internal information. A number of studies have been conducted on measurement methods for information leakage, countermeasure technologies, and the propagation mechanism and acquisition of information via electromagnetic radiation. Some investigations have shown that information leaks through radiated emissions. However, there has been little discussion about the effect of setup environments of information communication devices on information leakages. In this paper, we focus on the distances between a conductive table and the equipment. We focus on distances between a keyboard and a conductive table on EM information leakage and investigate the effects of the setup environment on information leakage via EM fields.

Keywords: EMC, Information Security, EM information leakage, EM measurement, Conducted Emission

1. INTRODUCTION

Keyboards are one of the most popular peripheral devices in order to input data to information communication devices. As the input data contains important information such as passwords, the data should be protected. For example, the important data is protected in the transportation channel by using cryptographic algorithms. On the other hand, there is no protection method applying for data transmission from keyboards to information communication devices and it is known the temporal variations of transmission data cause serious problems of information leakages via electromagnetic (EM) fields [1]. If eavesdroppers receive the EM fields which include the information of key inputs, they can reconstruct the input data at a distance.

According to this issue, previous studies mainly focused reconstruction methods of the information. However, there was not enough discussion of the acquisition capability of leakage information via EM filed from keyboards. When acquisition capability is considered, it is necessary for various parameters which are different according to environments. As one of the major parameters, there are setup environments. The parameters include the target devices with which keyboards are connected, lengths of the cables, places where keyboards are set up, and so on. Although, there parameters were not discussed in previous studies. In this paper, we investigate effects of setup environments of the keyboards on EM information leakages. Especially, we focus on the distance between the keyboards and the conductive table as a parameter related to the places where the keyboards are setup.

2. EM INFORMATION LEAKAGE OF PS/2 KEYBOARD

A PS/2 keyboard consists of a micro-controller unit (MCU) and a key matrix, which is a mechanical switch array. Each key has a unique scan code that consists of at least one byte. The MCU scans the key matrix and finds pressed keys. It then sends assigned scan codes to a PC through a serial bus. This serial bus consists of a data line and a clock line. The data line carries the scan codes bit by bit with positive logic, synchronized with the falling-edge signals on the clock line. The data rate of the bus is between 10 and 16.5 kbit/s depending on the implementation of the keyboard. The data rate of the tested keyboard was approximately 13 kbit/s.

The MCU radiates leaked signals as unintended emissions when it sends the scan codes to the serial bus. The leaked signals include impulse signals which are synchronized with the edges of the data and clock line of the serial bus. This result indicates that the leaked signals leak information of key inputs as scan codes.

The leaked signals propagate as conducted and radiated emissions. In this paper, we focus on propagation of conducted emissions on the cable which is attached to the keyboard. We investigate the relationship between magnitude of the leaked signal and distance between the keyboard and the conductive table.

3. EXPERIMENT

In this experiment, we analyze leaked signals from a PS/2 keyboard. The leaked signals include character information of key inputs. The previous researches on the information leakages of the keyboards mainly focused on radiated emissions. Conducted emissions of the keyboards were not discussed enough. Therefore, this experiment measures the leaked signals from the

PR0001/12/0000- 0060¥400

conducted emissions on the communication cable of the keyboard.

Previous researches investigated EM radiations of information communication devices with attached cable. One of the researches [3] indicated effects of surrounding environment on the EM radiations. The environments included distances between the information communication devices and a ground plane. Thus, this experiment measures the leaked signals which are affected by surrounding environments of the keyboards while the distances between the keyboard and a conductive table were altered. Then, this experiment evaluates the information leakage as magnitudes of the conducted emissions by analyzing frequency characteristics of the measured leaked signal.

2.1. Measurement Setup

Geometries of the measurement setup of this experiment are on Fig. 1. The keyboard is secured on a wood board. The wood board is placed at center of an aluminum plate which is the conductive table. Distances *h* between the wood board and the conductive table can be altered. In this experiment, the distances *h* were altered between 15 mm to 150 mm with 10 mm step width.

The measurement system of this experiment is on Fig. 2. A stabilized power supply provides DC 5 V to the keyboard as its power source. The power supply uses batteries to prevent disturbances from outside this measurement system. Pull-up resistors (4.7 kΩ) terminate the each lines of the serial bus of the keyboard. This termination method is defined on the standard specifications of PCs [2]. The signals of the serial bus from the keyboard provide acquisition triggers to the oscilloscope through an optical signal isolator. This optical isolator electrically isolates the serial bus from the measurement equipment. A current probe (Fischer Custom Communications, F-080926-1005-1) probes conducted emissions on the communication cable of the keyboard with non-invasive. This probe is clamped at the keyboard end of the communication cable.

2.2. Measurement of Signal of Information Leaking

A continuously pressed “A” key generates repeated character information as an information source of the leaked signals. The key is pressed with a non-conductive fixture. Fig. 3 shows the measurement result at *h = 15 mm*.

The impulse signals are shown on Fig. 3 as the output of the current probe. One of the impulse signals is enclosed by the dotted line on Fig. 3. The impulse signals are radiated at falling-edge of the clock and the data line. Therefore, the impulses leaks number and positions of the falling-edges as leaked signals. The character information from the leaked signals can be reconstructed by looking up bit patterns corresponding to each character information and word dictionaries [1].

2.3. Analyses of information leakage

This section analyzes magnitudes of the conducted emissions of the leaked signals with frequency-domain techniques. This analysis uses Fast Fourier Transform (FFT) to convert time-domain signals into frequency-domain signals. The time-domain signals (2

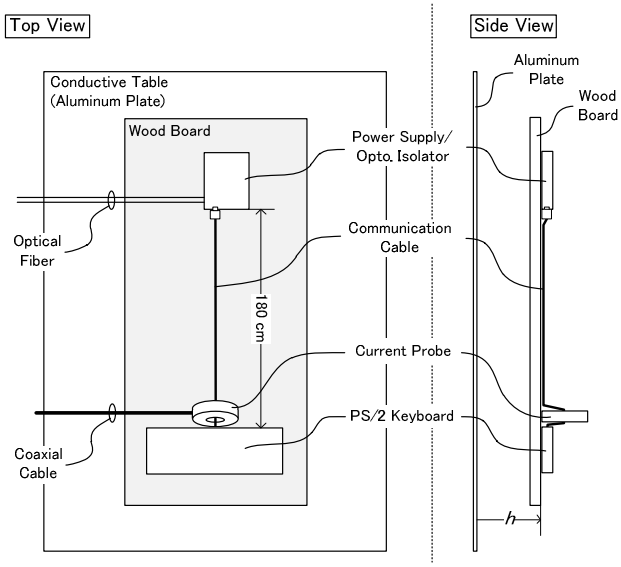

Figure.1 Setup of Measurement Target

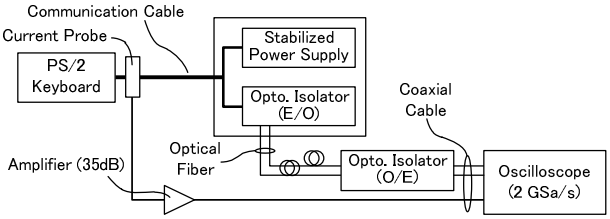

Figure.2 Setup of Measurement System

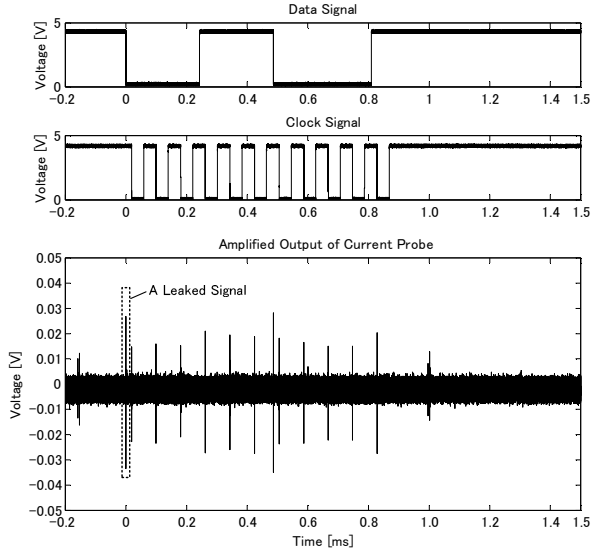

Figure.3 Serial Signal and Signal of Leaking Information

GSa/s) are divided into 4.096 μs (8192 samples) to analyze impulse signals one-by-one. The frequency range of this analysis is between 150 kHz and 30 MHz, which is the specific frequency range of conductive emissions. Fig. 4 shows analyzed time-domain signals of a background noise and a leaked signal and the frequency spectrum of these time-domain signals at h = *15 mm*. This result shows increasing magnitudes of the spectrum between 5 MHz and 30 MHz. The maximum change of the increasing magnitudes is 15 dB at 30 MHz.

Next analysis analyzes variations of the frequency spectrums while h is altered. In the result, the frequency spectrums of the back ground noises show no variation. However, the frequency spectrums of the leaked signals show increasing magnitudes of the spectrums while h is decreased.

Fig. 5 shows averages of the frequency spectrums of the leaked signals between 5 MHz and 30 MHz. Fig. 6 shows magnitudes of the frequency spectrums of the leaked signals at 30 MHz. The result of Fig. 5 indicates increasing of conductive emission while h is decreased. At 30 MHz, changes of the frequency spectrum indicate a maximum increasing magnitude which is 15 dB.

4. EFFECTS OF CONDUCTIVE TABLE ON ELECTROMAGNETIC INFORMATION LEAKAGES

The results of the experiment indicate that the conductive emissions of leaked signals increase while the distance between the keyboard and the conductive table is decreased, and there is no variation on background noise. A cause of the results is capacitive couplings among the keyboard, the communication cable and the conductive table [3]. These capacitive couplings become close couplings while the distance is decreased. This phenomena increase the conductive emissions cause the information leakages.

From viewpoints of the EM information security, eavesdroppers can reconstruct the character information at a large distance from the keyboards when the conductive emission is increased due to higher clarities of the leaked signals on cables connected to the keyboards. Especially, information leakages from the power lines [4] become a serious issue of the EM information security because most information communication devices require power lines.

5. CONCLUSION

To discuss the effects of the setup environment on information leakage via EM fields, we focused on distances between a keyboard and a conductive table on EM information leakage.

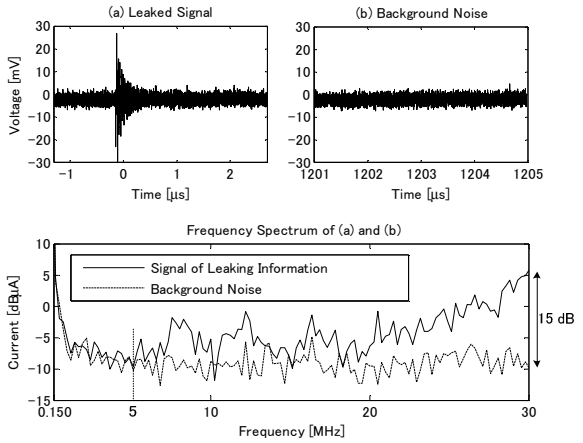

Figure.4 Characteristics of Signal of Leaking Information

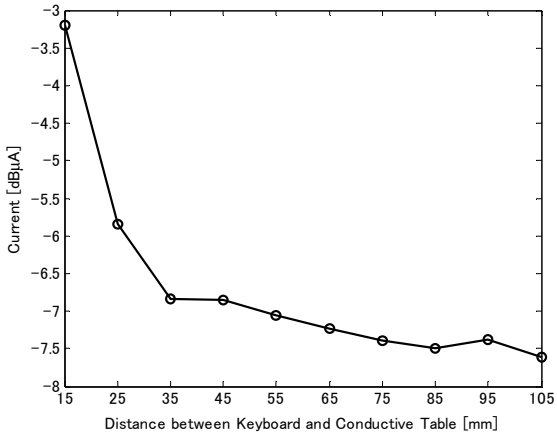

Figure.5 Averaged Conducted Emission (5 – 30 MHz)

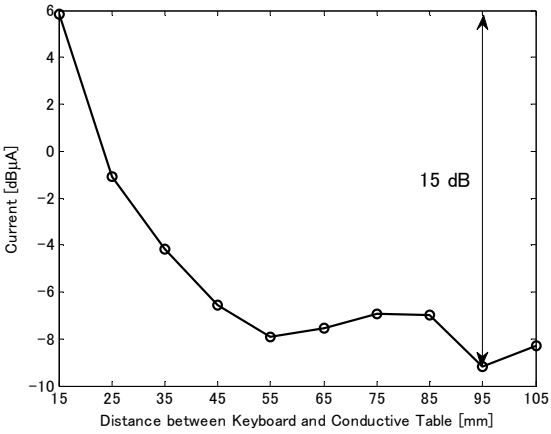

Figure.6 Conducted Emission at 30 MHz

Conductive emissions of leaked signal are increased due to the coupling between the keyboard and the conductive table. Then, the acquisition of information is improved at the specific frequency range of conductive emissions. Furthermore while the keyboard is close to the conductive table, ratios of the leaked signals to the background noises increase. Thus, this result shows the change in the setup environment causes the

increasing risk of the information leakage. This type of information leakage constitutes a real threat in many peripheral electrical devices with attached cables.

To provide a secure and safe environment for information communication devices, electromagnetic compatibility (EMC) countermeasures in order to reduce unintentional emission are necessary for the design of many peripheral electrical devices with attached cables. In addition to these standard countermeasures, we also need to discuss a new tamper-resistance capability to prevent information leakage from the view of both EMC and information security.

REFERENCES

[1] M. Vuagnoux and S. Pasini "Compromising Electromagnetic Emanations of Wired and Wireless Keyboards," 18th USENIX Security Symposium, 2009.

[2] *OADG Technical Reference (Hardware)*, OADG, Tokyo, 2000.

[3] K. Morimitsu, N. Song, Y. Toyota, K. Iokibe and R. Koga, "Modeling and Identification of Common-mode System in Cable Interconnection between Transmitter and Receiver Pairs," *IEICE Technical Report, EMCJ*, Vol. 110, No. 300, pp. 33-38, 2010.

[4] M. Kinugawa, Y. Hayashi, T. Mizuki and H. Sone, "Measurement of the Effect of Ungrounded Power Cables on Compromising Electromagnetic Emanation," *IEICE Transactions on Communications*, Vol. J93-B, No. 11, pp. 1559-1561, 2010.