Progress In Electromagnetics Research C, Vol. 41, 151–161, 2013

NOVEL METHOD TO DETECT AND RECOVER THE KEYSTROKES OF PS/2 KEYBOARD

Yulei Du*, Yinghua Lu, and Jinling Zhang

School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract—Computer keyboards are often used to transmit confidential data such as passwords. The sensitive information such as keystrokes could be recovered by using the electromagnetic (EM) waves from the electronic components of the keyboard. In this paper, we have investigated the information leakage on the ground line of the PS/2 serial cable due to crosstalk and radiative coupling. The coupling principles are analyzed firstly. And then, through the experiments we found that the signals of keystrokes could leak to the ground line network which could then be detected on the other power outlets whose share the same electric line. Lastly, the eavesdropping experiments demonstrated that the keystrokes could be reproduced on the other places of the ground line network with no trace.

1. INTRODUCTION

At present, more and more information technology equipments (ITEs) are used in our daily activities. Most ITE devices emit unwanted EM noises unintentionally, which can disturb radio communication services and cause electromagnetic interference (EMI) to other ITEs. In order to prevent EMI, the limits that specify the leakage levels for the ITEs [1] have been specified by the International Special Committee on Radio Interference (CISPR). However, the processed confidential information by the ITEs also may be embedded within the EM disturbance, even if the radiation and conduction emission levels are less than the limits. The malicious adversaries can reconstruct the processed date by receiving and analyzing these EM noises [2–11]. In recent years, the information leakage caused by EM radiation and conduction is a hot topic in the field of computer security.

Received 23 April 2013, Accepted 22 June 2013, Scheduled 1 July 2013

* Corresponding author: Yulei Du (dylbupt@gmail.com).

The EM information leakage threat exists because the transmission signals in electronic devices can be obtained maliciously from an analysis of its EM noises. As a typical peripheral of computer, keyboards are often used to transmit sensitive information such as passwords. They have been found to be susceptible to electromagnetic eavesdropping, allowing remote keystroke detection [9–11]. In [9], the author demonstrated that four methods can be used to implement such an attack against a wide variety of keyboards using PS/2, USB, laptop and wireless connections in a range of circumstances. And their best practical attack recovered 95% of the keystrokes of a PS/2 keyboard at a distance up to 20 m, even through walls. The keystrokes can be retrieved not only through EM emanations, but also some other side channels, such as optical reflection [12], acoustic leakage [13–15], and so on. In [12], the exploitation of visual compromising information leaks could be applied to keyboards. In [13], the author discovered that each keystroke produces a unique sound when it is pressed or released and these unique sounds can be applied to recover typed keystrokes with a microphone. This type of attack was improved later [14, 15].

The original display image on the video display unit (VDU) can be reconstructed through analyzing the signals which are obtained by using the current probe from the power leads of the PC [5]. However, whether the keystrokes could be recovered through the conduction emission or not, as far as I know, isn't involved in existing published papers. Therefore, in this paper, we have investigated the information leakage on the ground line of the PS/2 serial cable. The signals of keystrokes can leak to the ground line of the PS/2 serial due to crosstalk and radiative couplings and these couplings are analyzed firstly. Then, through the experiments we found that these signals could transmit to the ground line network via the power outlets. Lastly, the eavesdropping experiments demonstrated that illegal authorizer can recover these keystrokes on the other places of the ground line network without being noticed.

2. THE LEAKAGE PRINCIPLES OF KEYSTROKES

It is not a new research field in detecting and capturing unintentional EM emanation [10]. Generally speaking, there are two kinds of unwanted emission: crosstalk coupling and radiative coupling. Crosstalk coupling requires physical support such as electric wires to transmit EM interferences through the system. And, radiative coupling occurs when a part of the internal circuit acts as an antenna and radiates unintentional EM waves. Through the experiment we have found that the information leakage of keystrokes on the ground line

network is caused by crosstalk coupling and radiative coupling. In the following, we will analyze these two principles.

2.1. Crosstalk Coupling

The PS/2 keyboard is operating the PS/2 protocol which is a bidirectional serial communication based on four wires (data, clock, ground, power supply), as shown in Fig. 1. The PS/2 protocol transmits data in a frame which consists 11 bits, 1 start bit, 8 data bits, 1 optional parity bit and 1 stop bit.

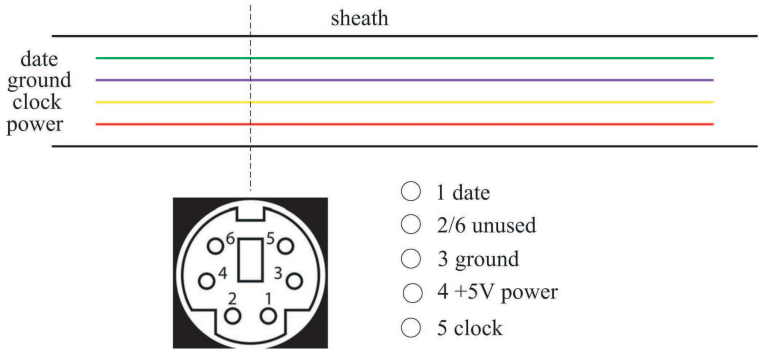

Figure 1. PS/2 serial cables and its port.

As these four wires are very close and not shielded against each other, it is theorized that a fortuitous leakage of information goes from the data wire to the ground wire due to EM coupling. And, the ground wire is routed to the main power adapter ground which is then connected to the power socket and finally the ground line network. This eventually leads to keystrokes leakage to the ground line network which can then be detected on the power outlet itself, including nearby ones sharing the same electric line. A schematic illustrating the coupling from the date wire to the adjacent ground wire is shown in Fig. 2. In Fig. 2, the date wire and ground wire are routed next to each other over ground plane. The date wire is connected to a signal source which is generating the signals of keystrokes at one end and terminated with a load at the other end. The ground wire is terminated with a resistance at the near-end and the signal acquisition device (SAD) at the far-end. The signals of the keystrokes can couple to the ground wire through magnetic-field coupling or electric-field coupling. For example, magnetic-field coupling occurs when magnetic flux lines from the signal source pass through the loop formed by the ground line and

the reference ground. The reference ground is any piece of metal with a direct physical connection to the earth, such as a sink, toilet pipes and so on. Schematically, magnetic-field coupling is represented by a mutual inductance L_m between the two loops. Similarly, a mutual capacitance C_m between the two wires is used to indicate that energy is coupled from the date wire to the ground wire through an electric field.

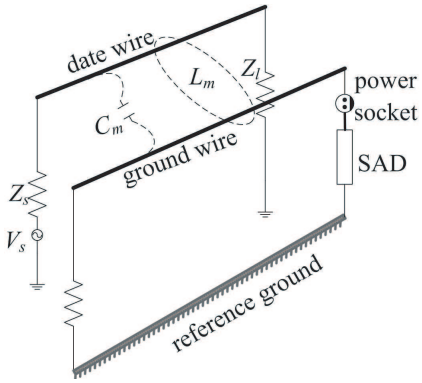

Figure 2. The coupling principle from the date wire to the adjacent ground wire.

The SAD of the Fig. 2 includes three parts, the ground line interface, signal transform device and reference ground interface, which are shown in Fig. 3. The ground line interface and reference ground interface are for connecting the ground line of the power socket to the signal transform device and the signal transform device to the reference ground, respectively. And the function of the signal transform device is for transforming the signals to the specific form which can be used by the following processing circuits. Assuming the coupling between the date wire and ground wire is weakly coupled, the total coupling is a linear combination of contributions due to the inductive and capacitive coupling [16]. As we known, when a frame is sent, the clock is activated at a frequency specific to each keyboard, typically between 10 kHz and 16.7 kHz. Therefore, the date and ground wires of the PS/2 serial cables are electrically short. According to this case, the equivalent circuit model of the ground wire and the reference ground loop which is shown in Fig. 2 can be obtained, as shown in Fig. 4. In Fig. 4, the symbols V_{ind} and I_{cap} represent for the induced voltage due to the inductive coupling and the induced current source due to the capacitive coupling, respectively. And the symbols Z_{gs} and Z_{gl} stand for the

equivalent impedance of the loop ground lines except the portion of coupled part and the SAD, respectively. The induced voltage V_{ind} can be obtained by

$$V_{ind} = -j\omega L_m I_{dateline} \tag{1}$$

where, L_m is the mutual inductance between the date wire and ground wire and $I_{dateline}$ the current on the date wire when the keystroke is pressed on the keyboard. The date and ground wires of the PS/2 serial cables are electrically short, therefore, the self-capacitance and self-inductance can be negligible compared to the source and the load impedances. The voltage on the date wire can be obtained by

$$V_{dateline} = \frac{Z_l V_s}{Z_l + Z_s} \tag{2}$$

Therefore, the induced current source amplitude is given by

$$I_{cap} = j\omega C_m V_{dateline} = j\omega C_m \frac{Z_l V_s}{Z_l + Z_s} \tag{3}$$

where, C_m is the mutual capacitance between the date wire and ground wire. Therefore, the induced voltage V_{ind} and induced current source I_{cap} can generate the current which contains the information of keystrokes on the ground wire and the reference ground loop, as shown in Fig. 4. The keystrokes can then be retrieved through intercepting and analyzing these signals which are obtained by SAD device.

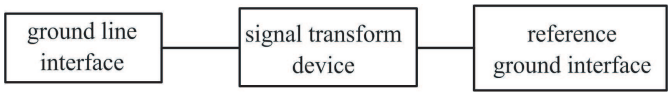

Figure 3. The structure of SAD.

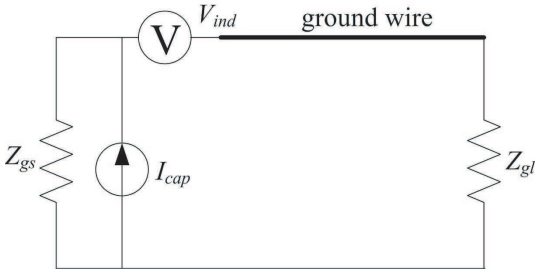

Figure 4. The equivalent circuit model of the ground wire and the reference ground loop.

2.2. Radiative Coupling

In electromagnetic compatibility (EMC) field, there are usually two types of radiation source: differential mode and common mode. Differential-mode radiation is generated by loops formed by electric components, printed circuit traces, etc.. These loops act as small circular antennas and eventually radiate. Common-mode radiation is the result of undesired internal voltage drops in the circuit which usually appear in the ground loop. Because these voltage drops are not intentionally created by the system, it is generally harder to detect and control common-mode radiations than differential-mode radiations. In [17], the author demonstrated that the EMI was mainly caused by common mode source. Therefore, the radiation emissions from the PS/2 keyboard are mainly caused by common mode source.

Radiative coupling occurs when a part of the internal circuit acts as an antenna and radiates unintentional EM waves. From the eavesdropper's point of view, the EM emanations can be divided to two board categories: direct emanations and indirect emanations [9]. In this paper, we only consider the direct emanation from the PS/2 keyboard. Direct emanations result from intentional current flows. Many of these consist of short bursts of current with sharp rising edges which result in emanations observable over a wide frequency band. In the PS/2 keyboard, the date is encoded with logic states, generally

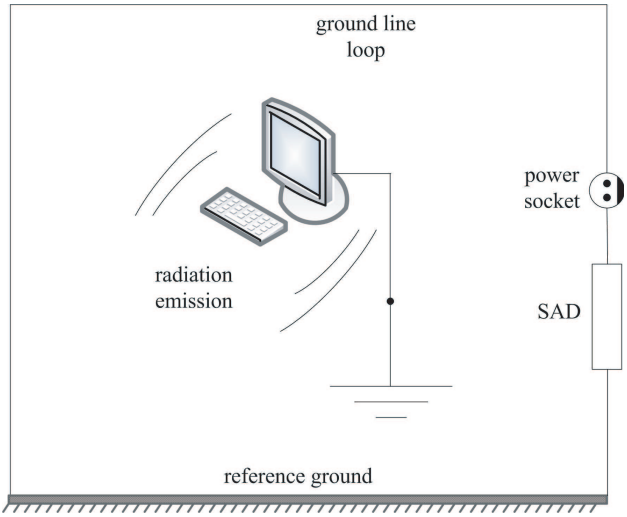

Figure 5. The information leakage due to the radiative coupling.

described by short burst of square waves with sharp rising and falling edges. During the transition time between two states, EM waves are eventually emitted at a maximum frequency related to the duration of the rise or fall time. Therefore, when the key is pressed in the PS/2 keyboard, the EM waves which contain the information of keystrokes are emitted directly from the date wire transmitting sensitive date.

The radiation emission due to the direct emanations which contain the information of keystrokes can induce the current on the ground line loop. The malicious adversaries can reconstruct the keystroke information by receiving and analyzing these conduction emissions on the ground line loop with no trace. The radiative coupling principle is shown in Fig. 5.

3. EAVESDROPPING EXPERIMENT

The information of keystrokes leaking to the ground line network is caused by crosstalk coupling and radiative coupling. When these signals which contain the information of keystrokes are intercepted on the other places of the ground line network, the illegal authorizer can reproduce these keystrokes with no trace. Therefore, it can cause big threats to the information security. In order to verify whether the information of keystrokes can be recovered on the ground line network or not, the eavesdropping experiment is conducted. The system configuration is shown in Fig. 6. In Fig. 6, the target PC has a PS/2 keyboard, and the target connects the power socket via the power cable. Another outlet which is in the adjacent room connects the

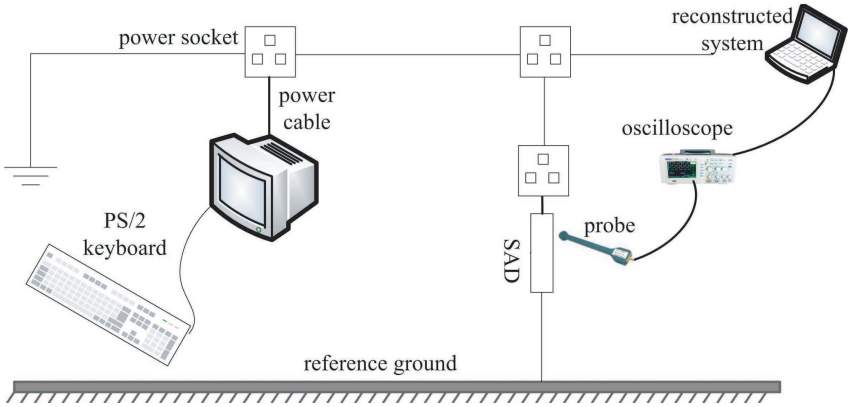

Figure 6. The eavesdropping experiment for PS/2 keyboard.

reference ground via the SAD. In here, the heating pipe is chosen to be the reference ground. The heating pipe doesn't contain the electrical system noises and can be used for improving the measurement. And in addition, all the power sockets in this building share the same electric grid. The SAD outputs the signals to the oscilloscope via the probe. The voltage potential difference between the ground line of the power socket and the heating pipe is detected by the probe and these signals are transmitted to the oscilloscope in real time. The oscilloscope used in this experiment is Tektronix TDS5054B and the sampling rate is 500 M samples per second. Eventually, the keystrokes are reproduced in the reconstructed system through some signal processing and decoding.

When a key is pressed, released or held down, the keyboard sends a packet of information known as a scan code to the computer. The scan code is bound to a physical button on the keyboard, and it does not represent the character printed on that key. For instance, the scan code of b is 0×32 if we consider the American layout keyboard. When the letter b is pressed in the PS/2 keyboard, the signals is obtained by the oscilloscope on the ground line is shown in Fig. 7. In Fig. 7, the blue part represents the leakage signals on the ground line.

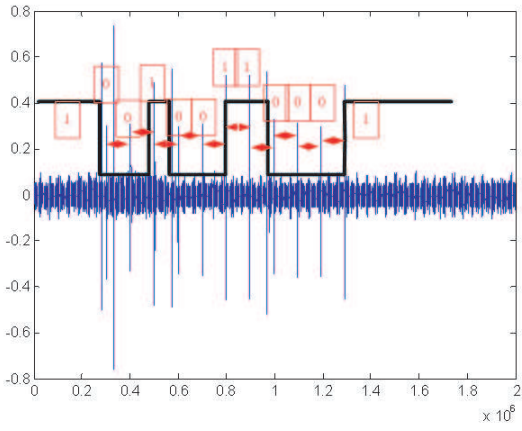

Figure 7. The leakage keystrokes signals and decoded.

According to the principle of the PS/2 keyboard, the logic states given by data and clock signals in the keyboard are usually generated by an open collector coupled to a pull-up resistor. The particularity of this system is that the duration of the falling edge is significantly shorter than the duration of the rising edge. Thus, the compromising

emanation from the falling edge should be much more powerful than the rising edge. Hence, the compromising emanation detected which is shown in blue part of the Fig. 7 is the combination of both clock and data signals. In addition, from the testing we have found that the energy of the peaks generated by the falling edges of the clock signal is not constant. And, the clock peaks are higher when the state of data signal is high.

Therefore, based on the PS/2 communication protocol and some findings which are indicated above the date signals can be obtained through the reconstructed system, and the decoded date signal is shown in black lines part of the Fig. 7. Therefore, the bits of the transmitting date in a frame are shown in red parts of the Fig. 7. And these bits are |0|01001100|0|1|. So, the letter b can be reproduced at another outlet in the adjacent room without being noticed. This type of eavesdropping poses a serious threat to the information security. To avoid the leakage of information coupled to the ground line in PS/2 keyboard, there may be some protected means to be carried out. For example, enlarging the distance between the ground line and the date line in PS/2 serial cable, adding some shielding between two lines to avoid crosstalk, and also can add a low pass filter between the personal computer and the power socket to prevent the conductive emissions propagating to ground line network. The effectiveness of these methods and some other methods will be researched in our future work.

4. CONCLUSION

The information of keystrokes can leak to the ground line network due to the crosstalk coupling and radiative coupling. As the date wire and ground wire are very close and not shielded against each other, the information of keystrokes goes from the date wire to the ground wire due to the crosstalk coupling. Then, these signals eventually leak to the ground line network through the main power adapter ground and several power sockets. And, the information leakage of keystrokes can also be caused by the direct emanations from the date wire. The eavesdropping experiment demonstrates that the signals of keystrokes indeed leak to the ground line network which can be detected on the other power outlets whose share the same electric line.

ACKNOWLEDGMENT

This work was supported by National Natural Science Foundation of China under Grants No. 61072136, 61171051.

REFERENCES

1. CISPR 22-Edition 5.2, "Information technology equipment–radio disturbance characteristics–limits and methods of measurement," International Electro-technical Commission (IEC), 2006.
2. Tosaka, T., Y. Yamanaka, and K. Fukunaga, "Method for determining whether or not information is contained in electromagnetic disturbance radiated from a PC display," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 53, No. 2, 318–324, 2011.
3. Kuhn, M. G., "Compromising emanations: Eavesdropping risks of computer displays," Technical Report 577, Computer Laboratory, University of Cambridge, 2003.
4. Van Eck, W., "Electromagnetic radiation from video display units: An eavesdropping risk?," *Computers & Security*, Vol. 4, No. 4, 269–286, 1985.
5. Sekiguchi, H. and S. Seto, "Measurement of computer RGB signals in conducted emission on power leads," *Progress In Electromagnetics Research C*, Vol. 7, 51–64, 2009.
6. Du, Y. L., Y. H. Lu, F. Mo, and N. Zhang, "A method for choosing the best frequency range for receiving the electromagnetic compromising emanations from a PC display," *Journal of Beijing University of Posts and Telecommunications*, Vol. 36, No. 1, 54–58, 2013.
7. Du, Y. L., Y. H. Lu, J. L. Zhang, and Q. Cui, "Estimation of eavesdropping distance from conducted emission on network cable of a PC," *2012 6th Asia-Pacific Conference on Environmental Electromagnetics (CEEM)*, 347–350, Beijing, China, Nov. 6–9, 2012.
8. Hayashi, Y. I., N. Homma, T. Mizuki, et al., "Efficient evaluation of EM radiation associated with information leakage from cryptographic devices," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 55, No. 99, 1–9, 2012.
9. Vuagnoux, M. and S. Pasini, "Compromising electromagnetic emanations of wired and wireless keyboards," *The 18th USENIX Security Symposium*, 1–16, 2009.
10. Vuagnoux, M. and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," *Proc. 2010 IEEE Int. Symp. EMC*, Florida, USA, Jul. 2010.
11. Wang, L. T. and B. Yu, "Research on the compromising electromagnetic emanations of PS/2 keyboard," *Proceedings of the 2012 International Conference on Communication, Electronics*

and Automation Engineering, 23–29, Springer, Berlin, Heidelberg, 2013.

12. Backes, M., M. Durmuth, and D. Unruh, "Compromising reflections-or-how to read lcd monitors around the corner," *IEEE Symposium on Security and Privacy (2008)*, 158–169, Oakland, CA, 2008.
13. Asonov, D. and R. Agrawal, "Keyboard acoustic emanations," *Proceedings. 2004 IEEE Symposium on Security and Privacy*, 3–11, IEEE Computer Society, May 9–12, 2004.
14. Berger, Y., A. Wool, and A. Yeredor, "Dictionary attacks using keyboard acoustic emanations," *ACM Conference on Computer and Communications Security (2006)*, 245–254, New York, USA, 2006.
15. Zhang, L., F. Zhou, and J. D. Tygar, "Keyboard acoustic emanations revisited," *ACM Conference on Computer and Communications Security (2005)*, 373–382, New York, USA, 2005.
16. Paul, C. R., *Introduction to Electromagnetic Compatibility*, Wiley, New York, 1992.
17. Paul, C. R., "A comparison of the contribution of common-mode and differential-mode currents in radiated emission," *IEEE Transactions on Electromagnetic Compatibility*, Vol. 31, No. 2, 189–1936, 1989.