EM Information Leakage Threat Caused by Low-power IEMI and Hardware Trojan

Yuichi Hayashi

Nara Institute of Science and Technology, 8916-5, Takayama-cho, Ikoma, Nara 630-0192, Japan

Abstract— In conventional electromagnetic (EM) information security, a device that unintentionally radiates EM waves including confidential information inside the device has been targeted as a threat. On the other hand, in this paper, we show that it is possible to cause information leakage through EM waves from potentially leak-free equipment by low-power intentional electromagnetic interference and hardware trojan.

Keywords-EM information security; intentional electromagnetic interference; hardware trojan

I. Introduction

The threat of information leakage through electromagnetic (EM) waves is caused by unintentional EM waves generated from the equipment depending on information processing [1]. For this reason, devices that do not emit EM waves including confidential information were out of the scope of the threat described above. Therefore, in previous studies [1], only devices that potentially leaked were targeted. On the other hand, in this paper, we introduce a new threat to cause information leakage against equipment that does not emit unintentional EM waves including confidential information using low-power intentional electromagnetic interference (IEMI) [2] and hardware trojan (HT) [3].

II. EM Information Leakage Caused by IEMI and HT

In this study, the HT was mounted on the communication line where the target signal was transmitted, and EM wave irradiation was performed on the HT to induce information leakage. The above information leakage can be regarded as caused by a mixer circuit that multiplies the two signals. A mixer circuit multiplies an intercepted signal S_{BB} (t) and a high-frequency signal S_C (t) induced by externally irradiated electromagnetic waves, and generates an amplitude-modulated signal S_{AM} (t) = S_{BB} (t) S_C (t), where S_C (t) is the carrier signal and S_{BB} (t) is the baseband signal. The time change of S_{BB} (t) is radiated outside the device as the amplitude-modulated signal S_{AM} (t) through an unintentional antenna (Fig. 1).

III. EM Information Leakage from Keyboard with HT

In this experiment, we selected the keyboard as a specific target. First, the HT is mounted on the signal line connecting the target keyboard and PC. Then, by using EM waves radiated from the outside, the information inside the device is amplitude-modulated and radiated outside the device. Fig. 2 shows the measurement results. Fig. 2 (a) shows a waveform obtained by tapping the data signal transmitted inside the communication line when "Q" is input. Fig. 2 (b) shows the waveform measured outside the equipment when irradiating the HT with EM waves.

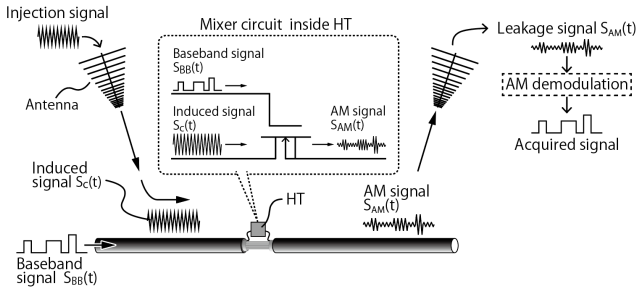

Figure 1 EM information leakage caused by IEMI and HT.

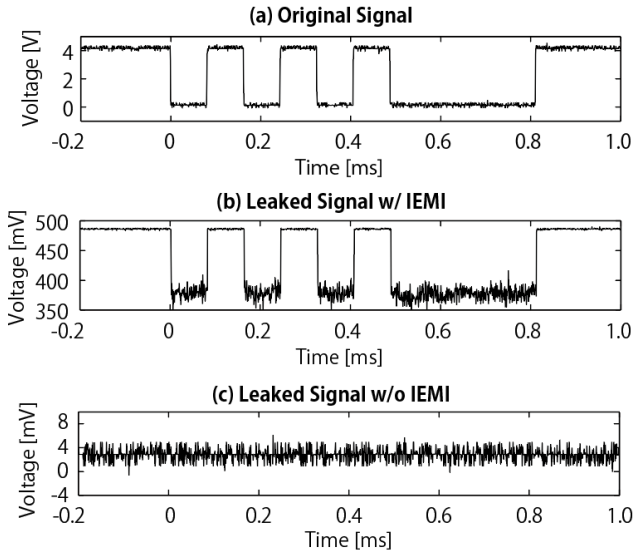

Figure 2 Leakage signals.

Waveforms with time variation similar to those in Fig. 2 (a) are observed, and it can be seen that the input information can be acquired outside the equipment. However, when the EM waves are not irradiated to the HT, the waveform measured outside the device is as shown in Fig. 2 (c), and information leakage does not occur.

The above results show that it is possible to cause information leakage through the EM waves by using IEMI and HT from potentially leak-free equipment.

REFERENCES

[1] Y. Hayashi, et al. (2013). Introduction to the special section on electromagnetic information security. IEEE Transactions on Electromagnetic Compatibility, 55(3), 539-546.

[2] W. A. Radasky, C. E. Baum, & M. W. Wik, (2004). Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI). IEEE Transactions on EMC, 46(3), 314-321.

[3] Tehranipoor, et al. (2010). A survey of hardware trojan taxonomy and detection. IEEE design & test of computers, 27(1).