Introduction to a Special Session on EMC and Information Security

Yu-ichi Hayashi [#1], Jong-Gwan Yook [#2]
[#1] *Tohoku Gakuin University,* [#2] *Yonsei Univserity*

Abstract— **This paper introduces the special section on EMC and Information Security. As information security becomes more important every day, safeguarding security at the physical level is as important as at the higher levels. In recent years, instrumentation has become cheaper and more precise, computation has become faster, and storage capacity has increased. With these changes, the threat has increased of advanced attacks that were previously too difficult to carry out, not just in the military and diplomatic fields but also for general-use commercial manufactured goods. This special session focuses on the problem of reduced security concerning electromagnetic waves (electromagnetic information security), which has made attack detection particularly difficult at the physical level. As well as introducing the mechanisms of these information leaks and countermeasures, this session presents the latest research trends.**

***Keywords*— electromagnetic information security, TEMPEST, electromagnetic interference, side-channel attacks**

I. INTRODUCTION

In advanced information societies, information leakage and communication disruptions associated with telecommunication devices have a strong impact on social and economic activities and security technology that can ensure the security and reliability of such devices are becoming increasingly important. One of the main reasons for information leakage is unintentional or intentional radiation of EM fields from communication devices. Such radiation, referred to as "EM information leakage", can even be in the form of weak EM fields emitted from devices that are compliant with existing public standards.

The problem of information leaks via electromagnetic radiation first came to be clearly known in the military and diplomatic spheres in the second half of the 1950s, principally in the US project codenamed TEMPEST. Information surveillance attacks using electromagnetic radiation were widely believed to only be realistically possible at the military level using expensive and difficult-to-obtain devices; they did not become a threat to general-use manufactured goods until later on.

This threat has, in recent years, expanded from the military sphere to general-use manufactured goods because instrumentation has become cheaper and more precise, computation has become faster, and storage capacity has increased. As a result, electromagnetic waves can now be measured at low cost for extended periods of time. Further, it has become easy to carry out processes such as statistical processing on the obtained data.

Specifically, the following threats concerning leaks via electromagnetic radiation have been clearly identified: information on the screen of a desktop or notebook personal computer (PC) [1,2], information on the screen of a device such as a tablet or phone [3], information for business purposes calculated inside the CPU of a PC [4], information output from a printer [5], keyboard input key information [6], and secret key information in devices that are processing passwords [7].

Addressing the above issue, this special session aims to promote and accumulate research on the security of ICT devices, equipment and systems associated with the research field of EMC. Topics in this special session include acquisition, measurement, and analysis techniques for information leakage from information and communication devices via EM fields; modeling and simulation techniques for evaluation of EM information leakage; countermeasures against attacks based on EM information leakage.

II. MECHANISMS OF ELECTROMAGNETIC RADIATION INFORMATION LEAKS

Information leaks via electromagnetic waves result from the time-variable generation of electromagnetic radiation from electronic signals created and transmitted to the device. This radiation varies depending on the data being processed by the equipment. Generally, electromagnetic radiation produced by telecommunication devices is limited by electromagnetic compatibility. However, information leaks via electromagnetic radiation can occur even with weak signals that do not exceed the standard electromagnetic wave strength because such leaks are caused by the data-dependent waveforms of emitted electromagnetic waves.

Figure 1 illustrates how information is leaked via electromagnetic waves. When the integrated circuit (IC) that is the leak source processes data, the signals that contain the information are composed of different frequencies, which correspond to different components of the waveform, depending on the data being processed. High-frequency content is then transmitted via electromagnetic conductors to a part that acts as an antenna within the device and radiates into the surrounding space according to the frequency response of the antenna.

The component acting as an antenna may be the trace patterns on the circuit board, conductors in the device housing,

or a cable connected to the device. Electromagnetic radiation is conducted and emitted because these parts unintentionally act as antennas.

Information can be acquired directly from PC monitors by this method. The color and contrast of pixels in PC monitors are represented as combinations of RGB (red, green, blue) voltage signals, which change continuously. Figure 2 shows an image of a display connected to a PC. When black characters are displayed on a white background, the voltage signals are turned on and off by the shapes of the characters. A specific set of on/off signals is transmitted to the PC depending on the display images and characters. During signal switching, transient currents appear for a short period. These transient currents can be regarded as "information signals" containing the display information, and its high-frequency components are emitted through a component in the device acting as an antenna. The same information can be conducted via communication and power cables attached to the device.

This method is also applicable to cryptographic devices, in which case it is referred to as simple electromagnetic analysis (SEMA) [8]. When a cryptographic device performs two operations (A and B) depending on a secret key, attackers identify the difference between the EM traces of A and B within a single execution step and subsequently estimate the secret key from the sequence pattern (Fig.3). In general, SEMA is suitable for public-key ciphers, which require a large number of computations for calculating each bit of the secret key. For example, the RSA cryptosystem [9], which is one of the most popular public-key ciphers, performs encryption and decryption by simple modular exponentiation. The typical exponentiation algorithm performs multiplication and squaring sequentially by the bit pattern of the exponent corresponding to the secret key. Thus, the key bit pattern can be derived by analyzing when the difference between multiplication and squaring operations appears in an EM trace.

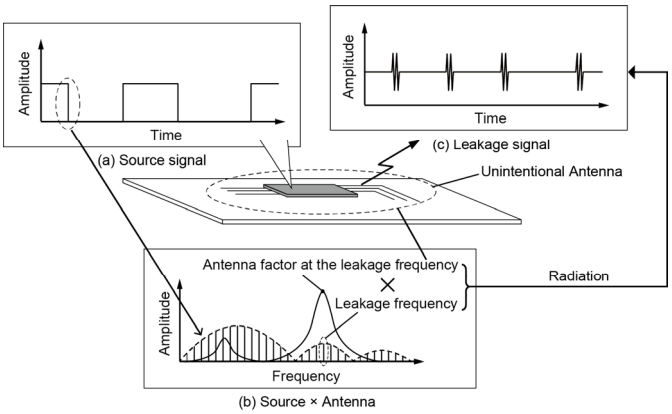

Fig.1 Model of EM information leakage

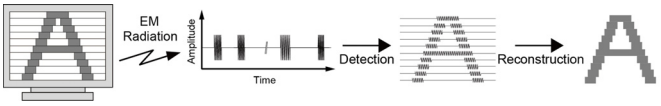

Fig.2 EM information leakage from a display

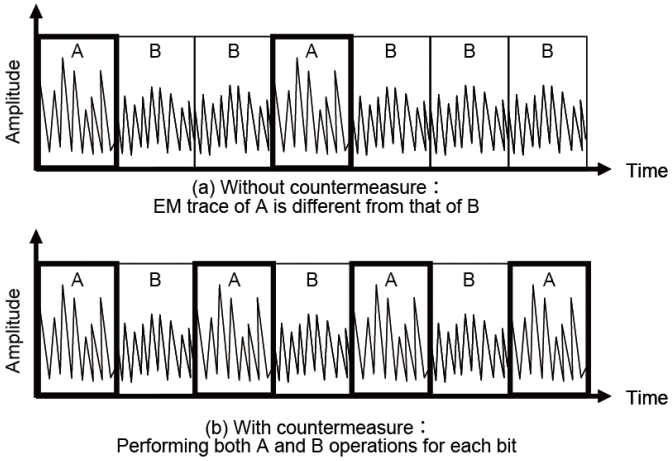

Fig.3 EM information leakage from a cryptographic device

REFERENCES

[1] M.G. Kuhn, "Compromising emanations of LCD TV sets," IEEE International Symposium on Electromagnetic Compatibility, pp. 931-936, Long Beach, California, USA, August, 2011.

[2] T. L. Song, Y. R. Jeong and J. G. Yook, "Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR," IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 2, pp. 164-172.

[3] Y. Hayashi, N. Homma, M. Miura, T. Aoki, H. Sone, "A threat for tablet PCs in public space: remote visualization of screen images using EM emanation," 21st ACM Conference on Computer and Communications Security (CCS'14), pp. 954-965, Scottsdale, Arizona, USA, November, 2014.

[4] A. Zajic and M. Prvulovic, "Experimental demonstration of electromagnetic information leakage from modern processor-memory systems," IEEE Transaction on Electromagnetic Compatibility, vol.56, no.4, pp.885–892, March, 2014.

[5] T. Tosaka, K. Taira, Y. Yamanaka, A. Nishikata, M. Hattori, "Feasibility study for reconstruction of information from near field observations of the magnetic field of laser printer," 17th International Zurich Symposium on Electromagnetic Compatibility, 2006. EMC-Zurich 2006, pp.630-633, Singapore, February, 2006.

[6] M. Vuagnoux and S. Pasini, "An improved technique to discover compromising electromagnetic emanations," IEEE International Symposium on Electromagnetic Compatibility, pp.121-126, Fort Lauderdale, FL, USA, July 2010.

[7] D. Agrawal, B. Archambeault, R. Rao, and P. Rohatgi, "The EM Sidechannel(s)," CHES 2002, Lecture Notes in Computer Science, pp. 29-45, San Francisco, CA, August, 2002.

[8] J. Quisquater and D. Samyde, "Electromagnetic analysis (EMA): Measures and counter-measures for smart cards," E-Smart 2001, Lecture Notes in Computer Science, no. 2140, pp. 200-210, Sep. 2001.

[9] R.L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM 21, pp. 120-126, 1978.