TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.2, February 2014, pp. 894 ~ 898
DOI: http://dx.doi.org/10.11591/telkomnika.v12i2.4010

Model for Electromagnetic Information Leakage

Mao Jian*, Li Yongmei, Zhang Jiemin, Liu Jinming
Computer Engineering College, Jimei University (JMU), No.183 Yinjiang Rd, Jimei, Xiamen, Fujian, China,
Ph./Fax: +86-592-6182451/6181601
*Corresponding author, e-mail: maojian@jmu.edu.cn

Abstract

Electromagnetic leakage will happen in working information equipments; it could lead to information leakage. In order to discover the nature of information in electromagnetic leakage, this paper combined electromagnetic theory with information theory as an innovative research method. It outlines a systematic model of electromagnetic information leakage, which theoretically describes the process of information leakage, intercept and reproduction based on electromagnetic radiation, and analyzes amount of leakage information with formulas.

Keywords*: electromagnetic leakage, information leakage, model, TEMPEST, data security*

Copyright © 2014 Institute of Advanced Engineering and Science. All rights reserved.

1. Introduction

Electronic information equipment such as computer will inevitably produce electromagnetic radiation. The electromagnetic radio signals have complex spectrum, also carry a lot of useful information [1-7]. So it will cause the leakage of information which is a serious threat to information security. In fact, stealing confidential information from electromagnetic leakage of information equipments has become an important eavesdropping means. Therefore, TEMPEST, as a special research field of information security, gradually aroused the attention of researchers [8-12].

At present, researches about TEMPEST mostly focus on physical phenomenon of electromagnetic radiation based on the theory of electromagnetism, but lack the theoretical explanation for information carried by electromagnetic leakage. Therefore, a systematic model is need for description of electromagnetic information leakage.

2. Cause of Electromagnetic Leakage

2.1. Electromagnetic Radiation

According to Maxwell's equations in electromagnetic theory, time-varying charges or currents in circuits will generate electromagnetic fields. Electric and magnetic fields interact with each other, and propagate away from the circuits to space in form of electromagnetic wave. The process is with energy transmission, which is known as electromagnetic radiation [13].

2.2. Equivalent Antenna

The device which can send or capture Electromagnetic waves is referred to as an antenna. According to its working mode, the antenna can be divided into two categories, transmitting antenna and receiving antenna [13, 14]. Theoretically, all sources of electromagnetic radiation can be looked as transmitting antennas. Some of them are not designed but unintentionally to emit radio signals. We call them equivalent antennas.

An equivalent antenna can be considered as a combination of small radiation elements. These elements are named electric dipoles and magnetic dipoles. They are seen as the basic radiation units.

2.3. Electromagnetic Leakage of Information Equipment

Most information equipments are electronic devices. They need power supply to support their work properly. When information equipment is working, time-varying currents inevitably exist in its circuits. According to Maxwell's equations, electromagnetic waves radiate

Received June 26, 2013; Revised August 23, 2013; Accepted September 19, 2013

out from the circuits. The radio signals are not for the purpose of transmission to launch out, but inadvertently to leak out. This is the cause of electromagnetic leakage in information equipment.

Such as components, parts, wires in information equipment make up the electromagnetic radiation sources. These sources can expressed by electric dipoles and magnetic dipoles, also can be seen as equivalent antennas. Therefore, electromagnetic leakage process can be regarded as equivalent transmitting antenna emits electromagnetic signal into the surrounding space.

3. Modle for Electromagnetic Information Leakage

3.1. Information in The Electromagnetic Signal

Information equipment leaks out electromagnetic signals when it is at work. So the radiated signals reflect the current work condition of the circuit. And there is a certain correlation between the signals and the data been processing by equipment. If intercepted and captured the electromagnetic signals, it is possible to reconstruct processed data and retrieve needed information by analysis technology. Then that will be a serious threat to information security of equipments. It shows that electromagnetic signals leaked from information equipment are carrying information. In other words, information is represented as electromagnetic signal, on the carrier of electromagnetic wave, and leaked out by electromagnetic radiation. We refer to this as electromagnetic information leakage.

The key to explain the nature of electromagnetic information is finding out how to transmit and measure information during the process of electromagnetic leakage, capture and retrieval. As the theory of electromagnetic radiation and propagation, Maxwell's equations and the antenna model explains the principle of the electromagnetic leakage. But that is only the description of objective physical phenomena. Electromagnetic information leakage of information equipment not only presents the physical electromagnetic phenomena, but also contains the processed digital information. Therefore, electromagnetic theory is not enough to explain electromagnetic information leakage. And it is need to refer to information theory for researching the intrinsic relationship between processed information and electromagnetic signal from equipment.

3.2. Modle for Electromagnetic Information Leakage

For information equipment, whether it intentionally sends electromagnetic information to a destination, or unintentionally leaks out electromagnetic information which thus will be intercepted and captured by eavesdropper, all can be abstracted as an information transmission from sender to receiver [15, 16]. So we combine electromagnetic leakage and information transmission theories to build a model for electromagnetic information leakage, as shown in Figure 1.

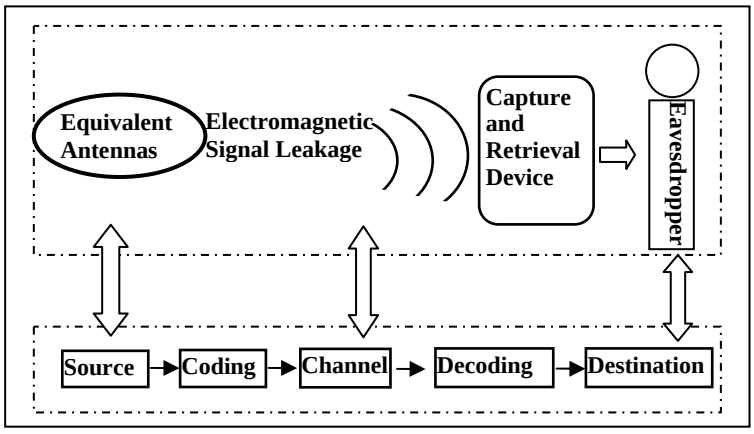

Figure 1. Diagram of Model for Electromagnetic Information Leakage

(a) Source: Sometimes referred to information source, it sends out signal including information. According to the discussion before, the electromagnetic information leakage can be regarded as equivalent antenna to transmit electromagnetic signal carried information to space. The parts caused electromagnetic radiating of information equipment, such as electronic components, connecting wires, can be equivalent to antennas. These equivalent antennas constitute the sources of electromagnetic information leakage.

(b) Channel: Channel is the medium for information transmission, through which information is sent from source to destination. As a source, equivalent antenna send out the information taken the form of electromagnetic radiation. So the physical medium passed by electromagnetic waves can be regarded as a channel. The channel can have many forms: maybe wired medium like wire; also maybe a wireless medium, such as space.

(c) Coding: When information in transmission process, it is usually represented as a signal in certain form. The operation of transforming information into the signal is called coding. Information equipment leakage out information in the form of electromagnetic signal, so captured the electromagnetic signal is not equal to got leaked information. There still need some operations to extract useful information from signals. Therefore, electromagnetic signal can be regarded as coding of information.

(d) Decoding: Decoding is the inverse operation of coding. The process of reconstructing information from the captured electromagnetic signal can be seen as decoding.

(e) Destination: It is the destination of information transmission. As the final receiver at the end of the model, the eavesdropper is the information destination.

4. Discussion for the Model in Ideal Condition

Next to discuss the measurement of electromagnetic information based on leakage model in ideal condition.

4.1. Ideal Condition

Ideal condition refers to the information equipment emits electromagnetic waves out into free space without path loss, also natural and man-made radio noise is nonexistent or ignored. In other word, there is no external noise in the channel. Under this condition, all captured electromagnetic signals can be seen as encoding of electromagnetic information.

Under ideal condition, quantity of leakage information which can be captured only is restricted by two factors: one is signal reception of the eavesdropping device; Second, information reconstruction. Signal reception is implemented by eavesdropping device's receiving antenna. The antenna bandwidth and its internal noise will affect the quality of reception. Information reconstruction can be regard as signal decoding, its essence is to read electromagnetic representation of information and translate the captured electromagnetic signal into useful information. And it is related to the equipment, different equipments need to take different reconstruction methods. For example, Video information rebuilding needs using the frame synchronization technology; keyboard data reconstruction can take advantage of method such as ETT and MST [17]. Ability of the reception is relatively easy to quantify by the parameters of equivalent receiving antenna.

4.2. Electromagnetic Information Leakage In Ideal Condition

According to information theory, an amount of information leakage can be calculated by channel capacity. Under ideal condition, the channel capacity means the maximum transmission rate which eavesdropping device can take to receive information. It can be calculated as follow:

$$C_k = 2 f B \log_2 A[bps] \quad (1)$$

Where C_k is the channel capacity which represents the quality of captured information, B is the receiving antenna bandwidth, A is the coefficient of coding, associated with electromagnetic representation of information. The base of logarithm is to '2', because information is in the form of digital signal in binary code. And f is defined as the coefficient of receiving antenna quality, reflects the receiving efficiency of antenna. It can be calculated as follow:

$$f = 1 + P_S / P_N = 1 + P_S / kTB \tag{2}$$

Where P_S is the input signal power of receiving antenna, P_N is the internal noise power of receiving antenna. For the reason of ideal conditions, the external noise has been ignored, so only the internal antenna noise needs to be discussed. And the internal noise can be equivalently calculated with the antenna noise temperature T and bandwidth B:

$$P_N = kTB \tag{3}$$

Where k is Boltzmann's constant, k = 1.38×10-23 J/K, T is the absolute temperature of the receiving antenna.Additional, we define Fr as the value of receiver noise:

$$F_r = 10\log(P_S / P_N)\left[dB\right] \tag{4}$$

The value of receiver noise can be transformed into noise strength because of relationship of power and field strength.

According to the previous discussion, the captured quantity of information leakage is determined by A and f in ideal condition. A is related with the type of equipment and method of decoding. If A is confirmed, along with the increase of f, more information can be eavesdropped. And f is determined by receiving antenna's internal noise SNR.

5. Conclusion

This paper proposed a model to express electromagnetic information leakage based on the combination of electromagnetic radiation theory and information transmission principle. The model has clarified the nature of the electromagnetic information, and described the essence of electromagnetic information leakage. It may be a theoretical guiding for the research of electromagnetic information leakage and protection, also will be helpful to ensure the information security of electronic equipment.

References

[1] W van Eck. *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?* Computers & Security, 1985; 4: 269–286.
[2] Markus G Kuhn. *Security Limits for Compromising Emanations.* Cryptographic Hardware and Embedded Systems, LNCS 3659, Springer. 2005: 265–279.
[3] Markus G Kuhn, RJ Anderson. *Soft tempest: Hidden data transmission using electromagnetic emanations.* In Information Hiding, Second International Workshop1998 Proceedings, LNCS 1525. Springer. 1998: 124–142.
[4] H Tanaka, O Takizawa, A Yamamura. *Evaluation and Improvement of the Tempest Fonts.* In Information Security Applications, 5th International Workshop WISA, LNCS 3325, Springer. 2004: 457–469.
[5] H Tanaka. *Information leakage via electromagnetic emanationsand evaluation of tempest countermeasures*. Third International Conference on Information Systems Security, LNCS 4812, Springer. 2007: 167–179.
[6] Ikematsu Taishi, Hayashi Yu-ichi, Mizuki Takaaki, Homma Naofumi, Aoki Takafumi, Sone Hideaki. *Suppression of information leakage from electronic devices based on SNR*. Electromagnetic Compatibility (EMC), IEEE International Symposium. 2011.
[7] Kinugawa M, Hayashi YI, Mizuki T, Sone H. *Information Leakage from the Unintentional Emissions of an Integrated RC Cscillator.* Electromagnetic Compatibility of Integrated Circuits (EMC Compo), 8th Workshop. 2011.
[8] Mao Jian, Li Yongmei, Liu Min. *Research for Data Erasure Based on EEPROM*. The 5th International Conference on Computer Science & Education. 2010: 1377-1379.
[9] Liu Jinming, Mao Jian, Li Yongmei. *Designing Eraser of Secret Information in EEPROM*. 5th International Conference on Computer Science & Education. 2010.
[10] Zhang Jiemin, Li Yongmei. *The Study of The Standards Architecture and The Standards Attributes Based on EMC Standards and TEMPEST Standards in Computer System.* The 8th International Conference on Computer Science & Education, in Colombo, Sri Lanka. 2013.

[11] Jurong Hu, Xuning Zhu, Long Chen. Electromagnetic Environment and Target Simulator for Radar Test. *TELKOMNIKA Indonesia Journal of Electrical Engineering*. 2013; 11(7): 3699-3703.
[12] Jianbo Yao, Tao Zhang. Biometric Cryptosystem Based Energy Attack Analysis*. TELKOMNIKA Indonesia Journal of Electrical Engineering*. 2013; 10(5).
[13] Robert RG Yang, Thomas TY Wong. *Electromagnetic Fields and Waves.* Higher Education Press. 2006: 353-399.
[14] T Tominaga, M Masugi. *Overview of Electromagnetic Wave Security Guidelines.* ITU-T/SG5, TD143. 2005: 1-11.
[15] CE Shannon. *A mathematical theory of communication*. The Bell System Technical Journal. 1948; 27: 623–656.
[16] Rodger E Ziemer, William H Tranter. *Principle of Communications Systems, Modulation and Noise.* Higher Education Press. 2003: 524-564.
[17] Karine Gandol, Christophe Mourtel, Francis Olivier. *Electromagnetic Analysis: Concrete Results*. Cryptographic Hardware and Embedded Systems. 2162 of Lecture Notes in Computer Science. 2001.