Quality Evaluation Model of Information Reconstruction via Electromagnetic Emanation

Zhang zidong*, Yu yuanhui
Computer Engineering College, Jimei University (JMU)
No.183 Yinjiang Rd, 361021 Jimei, Xiamen, Fujian, China, Ph./Fax: +86-592-6182451/6181601
*Corresponding author, e-mail: zdzhang@jmu.edu.cn

Abstract

Electromagnetic emanations from IT device may leak information they process. By analyzing the characteristics of electromagnetic emanations, eavesdropper could reconstruct critical information. Particularly information displayed on monitor faces a serious security risk. Although various electromagnetic information leakage countermeasures have been proposed try to solve the information security problems, their effectiveness evaluations are mostly subjective. The comparison of their efficiency and the evaluation of information reconstruction implementations are challenging issues, no reliable quantitative metric available. From the information theory point of view, this paper presents an evaluation model for assessing monitor information reconstruction through electromagnetic emanations. By a reconstruction experiment, the amount of information leakage and information reconstruction is implemented and analyzed.

***Keywords**: electromagnetic information leakage, information theory, reonstruction evaluation model*

1. Introduction

After Van Eck published his paper in 1985, the risk of information leakage through electromagnetic radiation from a display unit has been widely known. Regarding the leakage channel, a side-channel is an unintended communication channel that leaks some information from a device through a physical media. As far as this paper is concerned, the leakage refers to unintentional electromagnetic information leakage. By analyzing the characteristics of intercepted electromagnetic emanations through measures such as DEMA, averaging technique etc, eavesdroppers may reconstruct critical information, causing information security under serious threat. Among which, the most common cases involve compromising of information displayed on monitors. Although there are various electromagnetic information leakage countermeasures in open literature, very few focused on the quantification of countermeasure effectiveness. Therefore, questions like“How to compare two side-channel attacks?” could not be answered, “which countermeasure is more effective” cannot be determined.

Considering the above-mentioned problem, this paper firstly give an information leakage model to bridge electromagnetic emanations with information theory, and then proposed a reconstruction evaluation model based on information leakage model to quantify the effective of electromagnetic information reconstruction. Thirdly, in section IV an electromagnetic information interception and reconstruction experiment is described and result is analyzed. Lastly, section V draws our conclusion.

2. Information Leakage Metric

Tempest has been a concern regarding computer security in military and government institutions for a long time, which refers to the techniques, investigations, and studies of compromising emanations and their application to eavesdropping, as well as to the information leakage through emanation.

For the past decade, in research field of electromagnetic information security represented by TEMPEST, most based their research on electromagnetic related theory. However, theoretic explanation of the information electromagnetic emanations carries is seldom discussed, especially short of description for electromagnetic information leakage in a

Received August 21, 2013; Revised September 16, 2013; Accepted October 9, 2013

systematic model manner. Essentially, it is the information lies under the form of electromagnetic emanations counts.
Channel Capacity:

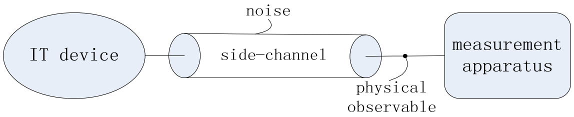


Figure 1. Electromagnetic Information Leakage Through Side-channel.

When there is a communication channel, the maximum amount of information IT device can transmit to receiver is defined as channel capacity, as is illustrated in Figure 1. Side-channel can leak information about the processed data through electromagnetic emanations. According to information theory, Shannon theorem is given in equation(1), where C denotes channel capacity, that is data transmission rate [bps], B denotes the bandwidth, S stands for the power of signal, N is for the power of noise.

$$C = B \times \log_2 \left(1 + \frac{S}{N} \right) \tag{1}$$

As can be seen from Equation (1), there are two ways to increase data transmission rate, one is to raise the transmission bandwidth, the other is to increase S/N ratio. While for the receiver or attacker part, in order to intercept more information, broader receiving frequency and higher S/N ratio are required.

Considering factors such as receiver’s working frequency, antenna’s receiving sensitivity, radiation magnitude of electromagnetic leakage from IT device etc, they all affect the practical channel capacity. So a constraint coefficient k1 is added, thus we proposed electromagnetic information leakage metric as in equation (2), the value of k1 is between 0 and 1, which is determined by the above mentioned factors.

$$C_{k1} = k_1 B \log_2 \left(1 + S / N\right) \tag{2}$$

3. Reconstruction Evaluation Model

After intercepting electromagnetic information leakage, information reconstruction should be followed in order to restore the original data. Reconstruction process is closely correlates with three key aspects, which are the total amount of original information IT device processed, the amount of leaked information, and the amount of intercepted information.

Considering reconstructed information, it not only contains useful information, but also mixed with noise. Particularly, for the displayed information on monitor, it is necessary to reconstruct a clear image so as to read its content, so image quality or legibility is critical. Then come the question: “How to evaluate the quality of reconstructed image quantitatively?” We proposed a information reconstruction evaluation model, it concerns with the following variables: I denotes the amount of original information IT device processed per time unit, for displayed images it can be calculated using equation (4); Ck0 denotes channel capacity of electromagnetic information leakage under ideal condition; Ck1 denotes channel capacity of electromagnetic information leakage with noise; Cr denotes the amount of information intercepted per time unit; Q denotes reconstruction quality. In general, processed original information by IT device will not all leaked out, and the leaked electromagnetic information could not be all intercepted, additionally, compared with ideal condition, under noise environment the channel capacity of electromagnetic information leakage is smaller. Their relationship can be stated as:

$$C_r \le C_{k1} \le C_{k0} \le I$$

The proposed reconstruction evaluation model is given by Equation (4), as for displayed image, value I can be calculated using Equation (3). That is the amount of original information for the processed image is determined by bit depth, display resolution and frame rate. Thus, Q can be extended as Equation (5), because color information is lost within the reconstructed image, value Q actually gives the number of steps in gray scale for reconstructed image, in other words, the greater the Q value is, the more detailed image we can get.

$$I = (bit\ depth) \times (display\ \ resolution\ ) \times (\ framerate\ ) \tag{3}$$

$$Q = \frac{C_r}{I} \tag{4}$$

$$Q = \frac{k_1 B \log_2(1 + S/N)[bps]}{bit\ \ depth\ \ \times display\ \ resolution\ \times\ framerate}[bit] \tag{5}$$

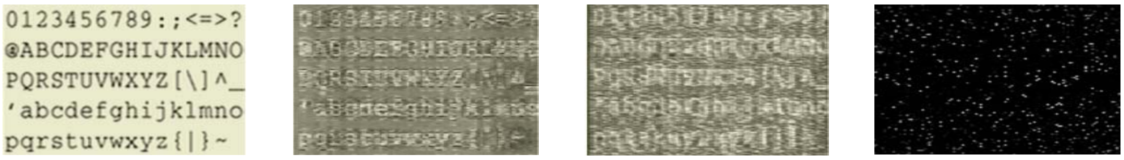
Regarding Equation (4), when Cr ≥ I, that is the amount of intercepted information no less than processed information by IT device, it is theoretically possible to reconstruct the original information; When Cr < I, that is the amount of intercepted information is less than processed information by IT device, in this case information could be easily lost, the possibility of information reconstruction is reduced. There have been report [1] by experiment that when Q is greater than 0.8, a clear image could be reconstructed and when Q is greater than 0.5 but less than 0.8, the reconstructed image is nearly recognizable, in other cases, no clear image can be reconstructed.

4. Experimental Results and Analysis

Various countermeasures for information leakage via electromagnetic emanations have been proposed, they can be classified into three layers: the first is called anti-leakage layer, most realized by hardware means, it aim is to block or reduce electromagnetic radiation; The second is celled anti-intercept layer, its purpose is to make interception more difficult with software methods; The third is celled anti-reconstruction layer, for the cases even most information is intercepted, the original information is still hard to reconstruct.

As in this experiment, in order to test our proposed reconstruction evaluation model, we employed and analyzed a software based countermeasure-tempest fonts, which is developed by Kuhn and Anderson [2]. Because high frequency spectrum among electromagnetic emanations is valuable information that eavesdroppers can use to reconstruct the target display image. Tempest fonts' main idea is to use Fourier transformation as a low-pass filter, removing the top 30% of the horizontal frequency spectrum. Figure 2(a) is the original tempest fonts image employed. We further used a Gaussian filter upon the original image in order to make the image smoother and thus make interception and reconstruction more difficult. Three images (o1、o2、o3) was produced by applying different parameters in Gaussian filter e.g. radius and deviation so as to make the image more gradual changes. Gradual changes in gray scale inhibit strong electromagnetic emanations. The gradation is in the order of o1, o2, o3.

Figure 2(a), (b), (c) are the reconstructed images when Q equals 1.2, 0.8, 0.6 respectively.



(a) Original tempest font image

(b) Reconstruted image Q=1.2

(c) Reconstruted image Q=0.8

(d) Reconstruted image Q=0.6

Figure 2. Original Image and Three Reconstructed Images

As can be seen from Figure 2, when Q>1, it is possible to restore a relatively clear image; when Q=0.8, a partially readable image is obtained; when Q<0.8, the reconstructed image is no readable. There is no case showed a bigger Q corresponding to a less clear image, therefore, we can confirm that the value of Q and the quality of the reconstructed image closely correlated. In this experiment, 0.8 is as the reconstruction threshold for image legibility, it can vary according to the image displayed on monitor and the particular measurement environment.

5. Conclusion

Information leakage through electromagnetic emanations causes a serious threat to information security, and various countermeasures have been proposed to try to solve the problem. But the evaluation for countermeasures have long been a challenging issue to be addressed. This paper first introduced the notion of side-channel, described an electromagnetic information leakage metric based on information theory, and then proposed an information reconstruction evaluation model. The main objective is to quantify countermeasure evaluation, make the comparison of various countermeasures possible, facilitates the effectiveness evaluation for information reconstruction via electromagnetic information leakage.

The evaluation model could also be adapted and applied in electromagnetic side-channel cryptanalysis, according to the calculation result, we will be able to determine the necessary number of sampling data, and further get to know the minimum number of samplings for the security evaluation.

References

[1] Hidema Tanaka. *Information Leakage Via Electromagnetic Emanations and Evaluation of Tempest Countermeasures*. ICISS. 2007; LNCS 4812:167–179.

[2] Markus G Kuhn, Ross J Anderson. *Soft Tempest Hidden Data Transmission Using Electromagnetic Emanations. Information Hiding.* 1998; LNCS 1525: 124–142.

[3] Hidema Tanaka, Osamu Takizawa, Akihiro Yamamura. *Evaluation and Improvement of the Tempest Fonts*. WISA 2004; LNCS 3325: 457–469.

[4] Toshihide TOSAKA, Ryo ISHIKAWA. Evaluation of Information Leakage from PC Displays Using Spectrum Analyzers. *The Institute of Electronics, Information and Communication Engineers*. 2007;

[5] Dakshi Agrawal, Bruce Archambeault, Josyula R Rao, Pankaj Rohatgi. *The EM Side–Channel(s)*. CHES 2002; LNCS 2523:29–45.

[6] Takashi Watanabe, Hiroto Nagayoshi, Hiroshi Sako. *A Display Technique for Preventing Electromagnetic Eavesdropping Using Color Mixture Characteristic of Human Eyes*. IH 2008; LNCS 5284:1–14.

[7] H Sekiguchi. Novel Information Leakage Threat For In-Put Operations On Touch Screen Monitors Caused By Electromagnetic Noise And Its Countermeasure Method. *Progress In Electromagnetics Research* . 2012; 36: 399–419.

[8] Markus G Kuhn. *Electromagnetic Eavesdropping Risks of Flat-Panel Displays*. PET 2004; LNCS 3424: 88–107.

[9] Hidema Tanaka. *Information leakage via electromagnetic emanation and effectiveness of averaging technique*. International Conference on Information Security and Assurance. 2008;

[10] Markus G Kuhn. *Security Limits for Compromising Emanations*. CHES 2005; LNCS 3659: 265–279.

[11] TANAKA Hidema, TAKIZAWA Osamu, YAMAMURA Akihiro. A Trial of the Interception of Display Image using Emanation of Electromagnetic Wave. *Journal of the National Institute of Information and Communications Technology.* 2005; 52.

[12] Karine Gandol, Christophe Mourtel, F rancis Olivier. *Electromagnetic Analysis: Concrete Results*. CHES. 2001; 2162 : 251-261.

[13] L Zhu, Y Shi, Y Shi, L Deng, H Shi. Electromagnetic Vector Sensor array parameter estimation method. *TELKOMNIKA Indonesian journal of electrical engineering.* 2013.

[14] AM Fadhil, HM AlSabbagh. Performance Analysis for Bit Error Rate of DS-CDMA Sensor Network Systems with Source Coding. *TELKOMNIKA Indonesian Journal of Electrical Engineering.* 2012.

[15] Li jian. Analog Define the Performance of Oscilloscope. http://www.eepw.com.cn

[16] 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.

[17] 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.

[18] E Biham, A Shamir. Differential Cryptanalysis of DES-like Cryptosystems. *J Cryptology*. 1991; 4(1): 2-21.
[19] E Biham, O Dunkelman, N Keller. *Enhancing Differentiallinear Cryptanalysis. Advances in Cryptology-ASIACRYPT2002:* Proc. 8th International Conference on the Theory and Application of Cryptology and Information Security. LNCS 2501. 2002: 254-266.
[20] P Kocher, J Jaffe, B Jun. *Introduction to Differential Power Analysis and Related Attacks.* Technique Report by Cryptography Research. 1998.
[21] JJ Quisquater, D Samyde. Electromagnetic analysis (EMA): Measures and Countermeasures for Smart Cards. Esmart 2001, LCNS 2140, Springer-Verlag, 2001: 200-210.
[22] Matthews. *Low Cost Attacks on Smart Cards: The Electromagnetic Side-channel.* Next Generation Security Software. 2006.
[23] Paul Kocher, Joshua Jaffe, Benjamin Jun. Dierential Power Analysis. CRYPTO’99, 1999; LNCS 1666: 388-397.
[24] U.S. CNSS (the Committee on National Security Systems). Index of National Security Systems Issuances. 2012
[25] TEMPEST standards overview, http://www.sst.com