Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines

*Cihan Ulaş* [*], *Ulaş Aşık*, *Cantürk Karadeniz*

*TÜBİTAK BİLGEM, Kocaeli, Gebze, Turkey*

ARTICLE INFO

*Article history:*
Received 11 June 2015
Received in revised form 29 January 2016
Accepted 1 February 2016
Available online 10 February 2016

*Keywords:*
Compromising emanations
Information leakages
Printers
TEMPEST
Electromagnetic radiation
Power and signal line conductors

ABSTRACT

In this paper, the emissions of a laser printer are investigated in three media, which are electromagnetic radiation, power line conductors, and signal line conductors. Analysis of Compromising Emanations (CE) of printed data is divided into three parts. First, the candidate frequency points of CE are examined in the frequency domain. Second, the emitted signal is AM-demodulated with the proper bandwidth, and then sampled by a high storage oscilloscope in these frequency points. Third, the collected data are converted to 2 dimensional image by applying signal and image processing techniques. In addition, this study introduces some practical measurement methods to reveal the possible CEs of laser printers. Finally, the procedure of the image reconstruction of CEs of the laser printer data is explained in detail. Experimental studies are carried out in noisy and noiseless environment with four different printers and results show that the proposed method successfully identifies the CE frequency points.

© 2016 Elsevier Ltd. All rights reserved.

## 1. Introduction

Electronic equipment naturally emits electromagnetic (EM) waves during its regular operation, and unintentional intelligence bearing signals may disclose the processed information that might be transmitted, received, or processed by any information processing equipment. If the information is classified as confidential, a serious information security weakness has occurred. There have been many studies on the subject of Compromising Emanations (CE) and information leakages caused by the information technology equipment such as computers, displays units, keyboards, and printers.

Highland and Fåk (1986) mentioned about the computer security risk of electromagnetic radiation in 1967; however, the first detailed open publication about compromising emanation risks was released by a Swedish government committee in 1984 (Beckman, 1984). van Eck (1985) reconstructed Cathode Ray Tubes (CRT) screen information and displayed on a television monitor by using commercial equipment in 1985.

Moreover, information leakages of other computer units and peripherals, such as keyboard, RS232 cable, and laser printers, have been studied in the literature.

Side channel analysis is a common attack method against cryptographic equipment. Examples for such attacks include power analysis, timing attack, electromagnetic and acoustic emanations (Rohatgi, 2006). Most side channel attacks require physical ownership or at least a network connection to the target device. Power analysis methods are divided into two parts, which are Simple Power Analysis and Differential Power Analysis (Kocher et al., 1999). Electromagnetic Analysis uses the similar procedure with the power analysis methods. Instead

[*] *Corresponding author.* Tel.: +90262 648 1882.
*E-mail address:* cihan.ulas@tubitak.gov.tr (C. Ulaş).

http://dx.doi.org/10.1016/j.cose.2016.02.001
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

of measuring power consumptions, they measure the EM currents generated by the target device over time (Quisquater and Samyde, 2001). In this setup, an EM probe, a copper solenoid or a disk magnet, is placed as close as possible to the cryptographic processing element, which can be a microprocessor or an FPGA. The EM attack is first identified by the study of Kocher (1996). Timing Attacks are first proposed by Kocher (1996) on public key algorithms depending on modular exponentiation. Timing attacks are based on the measurements of secret exponent operations on known plaintext under the assumption of known cryptographic protocols.

Keyboards are mostly used as input devices for confidential data such as passwords and text documents entry. Measurements and analyses on compromising emanations of keyboards were started with Han in early 1990s (Fang, 1993). Vuagnoux and Pasini (2009) used an effective method to deal with the keyboard emissions and recovered keyboard entry from a distance around 20 meters with 95% success. Zhang (2010) studied on compromising mechanism of the keyboards and compared the emanations among various keyboard types. The compromising mechanism of PS-2 keyboard was analyzed by Wang and Yu (2011, 2013). Another study about information leakage on the ground line of the PS/2 keyboard was presented in Du et al. (2013). In addition to electromagnetic attacks to keyboards, some studies focus on keyboard acoustic emanations (Asonov and Agrawal, 2004) and dictionary attacks using keyboard acoustic emanations. Keyboard acoustic emanations and the related attacks are based on the recording of the sounds while the user is typing a word. Then the pressed key reconstruction is turned to a classification problem. Smulders (1990) studied the radiation arising from RS232 cables and recovered the processed information successfully. In this study, he recovered the RS-232 data from unshielded RS-232 cable from 7 meters away with short wave radio tuned to 16 MHz. He noticed that signals of a PC modem cable could be recovered by low cost and small size equipment.

Kuhn (2003) was very active in the field of electromagnetic emanations. He studied CE of CRT displays, laptop displays, and flat panel displays. He achieved to reconstruct a CRT display image from three meters away (Kuhn, 2003). Then laptop displays and flat panel displays are studied, and target display images are reconstructed successfully (Kuhn, 2005, 2006). In Hidema et al. (2005), laptop displays and LCDs are used as target devices and electromagnetic emanations are taken with a near magnetic field probe and an injection probe. Kuhn (2002) also studied on the optical emanation of CRT displays (Kuhn, 2002). He showed that the optical compromising emanations can be received even after diffuse reflection from a wall. Loughry and Umphress (2002) presented another work related to information leakages on optical emanations. They showed that LED status indicators on data communication devices may carry a modulated optical signal, which is correlated with the processed information. Modems and Internet protocol routers were mentioned as vulnerable to this type attacks.

Printers are also used as output devices for computer systems. Acoustic emanations of printers were studied in 1991, and the letters "W" and "J" were distinguished successfully (Briol, 1991). An attack method has been presented which is based on the recording of the sound of a dot matrix printer processing English text (Backes et al., 2010). Up to 72% of the printed words were recovered and the attack achieved recognition rate up to 95% with the assumption of the knowledge about the text. Tosaka et al. (2006) studied the compromising emanations of laser printers, and they measured the magnetic field of a laser printer in the near field and achieved to reconstruct the printed image. Przesmycki (2014) used some special test patterns to improve the measurements of compromising emanations of monochromatic laser printers. He presented the oscillograms of three lines that are placed on different places of a white sheet.

In this paper, compromising emanations of a laser printer is investigated in the media of power line conductors, signal line conductors, and electric radiation (ER). While most of the studies focus on the measurements of CE in the media of ER, in this study, it is also shown that the risk of information leakages in the media of power and signal lines (like USB) cannot be ruled out. In addition, we introduce a practical approach of searching CE using a conventional spectrum analyzer. It is shown that the configuration of resolution bandwidth, frequency span and the sweep time has to be applied properly. To be able to analyze and detect the CE frequency points more easily, new image patterns are proposed. The reconstruction and visualization of the CE of printer data are explained. Finally, experimental are given in noisy and noiseless environment with four different printers.

In the next section, the operating principle of laser printers and the emission measurement setups in ER, PLC, and SLC are given. In Section 3, the approach for searching compromising emanations and the evaluation of the test patterns are discussed. The image reconstruction method from the CE of the printer emissions is explained in Section 4. Finally, the paper is concluded in Section 5.

## 2. Laser printers and emission measurement setup

In this section, the operating principle of a laser printer and the measurement setups for the compromising emanations in ER, PLC, and SLC media are explained.

### 2.1. *The operating principle of a laser printer*

The monochromatic laser printers are commonly used quick printers that are known for producing high quality print. Although laser printers are based on the interaction of several different technologies including electronics, optics and electrographics, the primary principle in it is static electricity. The block diagram and the printing process are shown in Fig. 1. The formatter receives a print job from the printer interface and processes the data. The formatter separates the print job into image information and instructions that control the printing process.

The image information is converted into a dot image and sent to the laser scanner system in the form of a video signal by the formatter, and the printing process begins. The primary charging roller charges the photosensitive drum with the negative charges. The laser diode emits the laser beam modulated by the video signal sent from the formatter. The laser beam

Download English Version:

https://daneshyari.com/en/article/6884189

Download Persian Version:

https://daneshyari.com/article/6884189

Daneshyari.com