Optical, Acoustic and Electromagnetic Vulnerability Detection for Information Security

W B Liu\textsuperscript{1,2,3}*, P Z Fan\textsuperscript{1}, M H Wang\textsuperscript{2}, Y K Li\textsuperscript{3} and J F Ding\textsuperscript{2,3}

\textsuperscript{1}School of Information Science and Technology, SouthWest Jiaotong University, Sichuan, China
\textsuperscript{2}The 30th Research Institute of China Electronics Technology Group Corporation, Sichuan, China
\textsuperscript{3}China Electronics Technologies Cyber Security Co. Ltd., Sichuan, China

*Corresponding author’s e-mail: bingge389@sina.com

Abstract. The information interaction between the air-gapped internal network and the external Internet is only possible through authorized and strictly controlled methods. Attackers make use of the vulnerability to transmit information covertly by software-stimulated signals leakage, which vary from optical, acoustic to electromagnetic, so we need to find the vulnerabilities and protect them from malicious exploitation. In this paper, a simple and active method to detect these vulnerabilities is presented from an optical point of view, that is, the Light Emitting Diode (LED) status indicator and screen backlight are controlled to send information by frequency shift keying (FSK) or amplitude shift keying (ASK). An improved receiver is designed for acquisition of optical signals, and the vulnerability detection methods are unified for acoustic and electromagnetic vulnerability. The target signal is easily distinguished from the noise signal by the time-frequency domain characteristics, the hidden testing information is recovered by simple modulation methods, and the mechanism of compromising emanation from digital signal is revealed. Several hidden features such as harmonics and intermodulation have been investigated, which can be used to detect optical, acoustic and electromagnetic vulnerability quickly.

Keywords: Air-gapped network, Optical Vulnerability, Electromagnetic Information Leakage

1. Introduction

With the development of information technology, computers have many input/output functions based on multiple data interfaces. Side channel or covert channel will appear along with these interfaces in the form of acoustic, optical or electromagnetic leakage signal.

LED and other visible light devices have the functions of lighting or indication, and can be attacked by malicious code to send modulated information which can’t be detected by human eyes. Fans or speakers in computers can be controlled to send covert acoustic signals. Electrical devices, such as digital processors, will emanate electromagnetic side channel signals from the connected power lines or inner bus in processing state. These intentional or unintentional activities will bring great information security risks to the air-gapped networks, which are physically isolated from Internet. Many researchers have found new threats to bridge the air-gapped networks with Internet in recent years, especially using inner interfaces in computers to transmit covert signals to the outside.
Different from conventional vulnerability, we conclude the threat of constructing covert electromagnetic channels as electromagnetic vulnerability, which can be extended to include optical and acoustic vulnerabilities [1]. We can use both active and passive detection methods to find the vulnerabilities.

The main contributions of this paper are as follows:

- By generating modulated optical signals on the computer using software, two covert channels are demonstrated, i.e. the LED indicator covert channel by FSK, and the LED screen backlight covert channel by ASK. For both covert channels, signals are received with suitable sensors, and information are extracted by the proposed detecting methods.
- By changing the state of the processors or output interfaces periodically, many signal emanation sources and transmission channels can be detected more quickly and distinguished more clearly, based on our proposed active method for vulnerability detection.
- The characteristics of the leaked digital signals and the covert behavior have been discovered from time domain, frequency domain, including the number of harmonics, the variation of signal strength, etc.
- The combined passive and active method processes of constructing an optical, acoustic and electromagnetic vulnerability detection platform are suggested.

In this paper, a novel active method to quickly find the covert channels is proposed, which is based on using software to generate modulated signal which can’t be detected by human. In this research, we provide a active process to detect optical vulnerability, and test the hard disk indicator signal and screen backlight signal, then several acoustic and electromagnetic examples are tested, after that a platform for detecting various optical, acoustic and electromagnetic vulnerabilities is constructed.

2. Related Work

In 1998, Markus G. Kuhn introduced the techniques of soft tempest, which enable the software on a computer to control the screen electromagnetic emission. Malicious code can generate screen leakage signal with amplitude modulation (AM) characteristics and optimize the transmission distance, receiver cost and covertness [2]. Many years later, Alenka Zajic verified that both active and passive electromagnetic side/covert-channel attacks on many computer systems are possible, and hidden information can be extracted from the state identification of different operations or activities [3].

Mordechai Guri et al. have found many new covert channels, such as data exfiltration from air-gapped computers over Global System for Mobile Communication (GSM) frequencies, magnetic channels, and optical channels [4][5][6]. Optical covert channels use sources such as computer screens, hard driver LED, keyboard LED and router LEDs. The optical signals can be modulated by sensitive information, which are invisible to users. Researchers have also been looking for intentional or even unintentional ways to modulate signals by other signals, and the way to inject information to target systems through their sensors [7][8].

The above studies mainly analyse the threat from the perspective of attack methods, but not from the perspective of information security and vulnerability detection. Compared to the traditional host or network vulnerability detection, there is a lack of optical, acoustic and electromagnetic vulnerability detection, especially the lack of active detection method. This is what we try to solve and described in this paper.

3. Optical vulnerability detection

3.1. Optical vulnerability detection process

Taking optical signal leakage and active detection as an example, we introduce the typical process of vulnerability detection as depicted in Fig.1. First, we choose a target which can be programmed by computer software to emit light, such as computer LED lights which can be programmed indirectly, and display screens which can be programmed directly. Then, we choose a sensor that can be used to receive the optical signal and a platform for processing the optical signal. Thirdly, we check whether
some characteristics of the transmitted signal can be detected by the receiver. Finally, we check whether the modulated test data can be recovered. The difference between the passive method and the active method depends on whether the leaked signal is intentionally emitted.

![Diagram](image1.png)

**Fig. 1 Optical vulnerability detection method using active method**

### 3.2. Optical sensor selection

Many types of optical sensors can detect light illumination. We firstly select Cross Domain Development Kit (XDK) device made by Bosch, and it has a built-in digital light sensor MAX44009, as showed in Fig. 2(a). It can be used to sense the illuminance of the environment, and the detected values can be sent to computers it connected. But we find that the sensor has low sampling rate and amplitude resolution from the detected values, so it can’t be used to provide a transmitting rate more than 10 bits per seconds (bps).

In order to achieve a higher transmission rate, an optimization is made for the receiver. The system is depicted in Fig. 2(b). We select a simple optical sensor with a photoresistor or photodiode whose function is to convert optical signals into electrical signals. Its analog output connected to the microphone input of computer’s integrated sound card which has a default 44100Hz analog to digital conversion (A/D) sampling rate, so the analysis bandwidth is up to 22.1kHz. The time-frequency domain features are depicted in receiver software through calculations. Both hard disk LED indicator flashing light and LED screen backlight can be detected use this method, and the results will be demonstrated in the following two sections in this paper.

![Diagram](image2.png)

**Fig. 2 Sensor connected to a computer to analyze the optical signal from LED screen or indicator**

### 3.3. LED indicator vulnerability detection

As depicted in Fig. 3, we select Thinkpad X230 as a target computer which has two LED indicators under the screen.

![Images](image3.png)

**Fig. 3 Different states of the LED indicator**
The left LED is a Wi-Fi indicator, it shows the state of whether the wireless network is connected. The right LED shows the data transfer state of the hard disk, which means if it is reading or writing the hard disk. If the reading or writing is periodic, the indicator signal will leak out the corresponding frequency.

We use this method to actively construct a FSK electrical signal by software, and it will reflect to the optical signal of the LED indicator. As referenced in [2][3], repeated activity in computers has certain operation period and can be used as a carrier. Such as the readfile activity, it has a period $T_0$ shown in Fig. 4. It will act as a carrier frequency $f_0 = 1/T_0$, and it may have many harmonics because it is a kind of digital signal. We can use some simple code to control the duration of activity A (readfile for example) and activity B (be silence for example), here they both have a duration for half of the period $T_1$. For example, if $T_1$ is 1ms, then both Activity A and Activity B has a duration of 0.5ms, and there will be a frequency $f_1 = 1000$Hz generated, and the carrier frequency $f_0$ will be modulated by $f_1$. We use this kind of modulation specially for construction of leakaged digital signal and vulnerability detection. Here we can tune the central frequency of the receiver to $f_1$ or its harmonics, and use amplitude demodulation to retrieve $T_1$ in baseband, so we also regard it as an amplitude modulation.

If we change $f_1$ according to bits need to be transmit, then a simple FSK modulation is formed. Here we use Fast Fourier Transform (FFT) size as 4096, then the frequency resolution is $44100/4096 = 10.77$Hz. And we use the 60th, 70th, and 80th FFT point which stand for 646Hz, 754Hz, 861Hz correspondingly for information transmitting and easily for demodulation. More frequencies can be selected, and many efficient modulation schemes can be chosen, but they are not the main topics of this paper, here we only take feasibility and simplicity into consider for detecting.

As the time-frequency feature of received signals dipicted in Fig. 5, several frequencies are used in baseband. 646Hz is used for transmitting message head and tail, 754Hz for bit 0, 861Hz for bit 1, and the duration of one bit is 0.1s. Then the transmitted data ‘0011010100110101’ has a time-frequency presentation and FSK is obvious. We successfully retrieved the information after the detection of the above frequencies and corresponding duration time. In fact, time diversity is achieved by repeated transmission to ensure that the target information can be received succesfully.

### 3.4. LED screen vulnerability detection
The brightness of LED screen for computer is usually controlled by Pulse Width Modulation (PWM) in which duty cycle is used. The larger the duty cycle, the brighter the screen. Signals with different duty cycle have different strength for harmonics. For example, the portable computer Thinkpad X230 has a 220Hz fundamental wave and many harmonic waves, as shown in Fig. 6(a) and Fig. 6(b).

We can use the light+ or light- function key in the keyboard to increase or decrease the brightness by changing the PWM duty cycle, where some harmonics of the 220Hz frequency show an On-Off Keying (OOK) change. But this function can’t be easily and smoothly controlled by user software.

Instead, we actively use a software-controlled method, which use windows system API SetBrightness() to set the backlight brightness parameter value from 0 to 255. Binary data ‘0011010100110101’ is transmitted repeatedly and the brightness is set 0-80 and 95-100 separately, where brightness variation between 0 to 80 is obvious to naked eye, and the brightness variation between 95 and 100 is almost invisible to the naked eye. The time-frequency features extracted from the receiver are present in Fig. 6(a) and Fig. 6(b) correspondingly. We focus on the strength of 220Hz, which acts as a harmonic frequency of backlight, and the strength varies from time as depicted in Fig. 6(c). The average value of the maximum and minimum strength over a period of time is used as a dynamic threshold to make the bit 0-1 decision, and it is found that the binary data can be extracted correctly by this approach in the receiver at a 1 meter distance from the transmitter. The larger the variation range of the transmitter’s brightness, the farther the receiving distance.

![Fig. 6 Features of screen backlight signal at the receiver](image_url)
4. Common vulnerability detection process exploration

Acoustic and electromagnetic vulnerability can be detected using similar methods as optical vulnerability detection. Fig. 7(a) shows that the rotation of the CPU fan causes the computer to vibrate, and the two signals interact to produce amplitude modulation. Fig. 7(b) shows that the carrier signal and baseband FSK signal with rich harmonics can be stimulated and radiate in the form of electromagnetic waveform by signal level control in lines.

![Inter-modulated acoustic signal](image1)

(a) inter-modulated acoustic signal  
(b) baseband of electromagnetic signal

Fig. 7 Features of acoustic and electromagnetic vulnerability

From the above findings and the detection methods of optical, acoustic and electromagnetic vulnerability, the recommended common detection processes are depicted in Fig. 8. Both active detection and passive detection processes are illustrated. Both exfiltration and infiltration directions have been taken into consider. The vulnerability detection platform and many new applications can be explored by the processes.

From the process, we can see that the passive detection mainly detects the existing leakage signals, while the active detection proposed by us is to detect the potential leakage sources and transmission channels to determine whether they can be used by malware.

![Active and passive vulnerability detection process](image2)

Active detection process  
- Select a optical, acoustic, or electromagnetic transmitter source  
- Test if a carrier can be produced with certain frequency  
- Test if other signals will be stimulated or carried by the carrier  
- Test if the carrier can be modulated by information through GOK, FSK, ASK, etc.  
- Make a security assessment through receiving distance, retrieved information, frequency harmonics range, etc.

Passive detection process  
- Test if it has a clock signal leakage, and if the clock signal act as a carrier  
- Test if there are intermodulated signals, and if there are harmonic waves with the same features  
- Test if different activities have responding leaked signals with different features  
- Test if the leaked signals have unique features and can act as fingerprint of the source  
- Test if the signals with information can infiltrate into receivers in target devices

Fig. 8 Active and passive vulnerability detection process

5. Conclusions

Information leakage is verified by covert transmission using software to stimulate optical signals. An active detection method which use simple modulation schemes is recommended to find the
vulnerabilities rapidly. During the vulnerability detection process, testing information is carried covertly and retrieved through the transmitter-receiver cooperation using a communication model, and typical characteristics of the leaked digital signals are analyzed from time-frequency domain. An optical, acoustic and electromagnetic vulnerability detection process is proposed to construct a platform, which not only detects whether the leakage signal carries information through feature analysis, but also detects whether there are potential leakages through our proposed active method.

References
[1] Liu W B, Ding J F, Kou Y F, et al. Research on electromagnetic vulnerability of air-gapped network, High Power Laser and Practicle Beams, Vol. 13, No.10, Oct. 2019, pp.103215-1 - 103215-5.
[2] Kuhn M G, Anderson R J, Soft tempest : Hidden data transmission using electromagnetic emanations, Information Hiding 1998, LNCS 1525, pp. 124-142.
[3] Zajic A, and Prvulovic M, Experimental Demonstration of Electromagnetic Information Leakage from Modern Processor-Memory Systems, IEEE Transactions on Electromagnetic Compatibility, Vol. 56, No. 4, August 2014, pp.885-893.
[4] Guri M, Kachlon A, Hasson O, et al, 2015. GSMem: data exfiltration from air-gapped computers over GSM frequencies. 24th USENIX Security Symposium (USENIX Security 15), pp. 849-864.
[5] Guri M, Zadov B, Daidakulov A, et al. xLED: Covert Data Exfiltration from Air-Gapped Networks via Switch and Router LEDs. 2018 16th Annual Conference on Privacy, Security and Trust (PST).
[6] Guri M, Bykhovsky B and Elovici Y, Brightness: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness, 2019 12th CMI Conference on Cybersecurity and Privacy (CMI).
[7] Nassi B, Pirutin Y, Shamir A, et al, Lamphone: Real-Time Passive Sound Recovery from Light Bulb Vibrations. Information on https://www.nassiben.com/lamphone.
[8] Ding J F, Liu W B, Wang M H, et al. Threat Analysis of Computer Information Leakage in Intermodulation of Acoustic, Optical and Electromagnetic Signals, Communications Technology, Vol. 52, No.4, Apr. 2019, pp:967-970.