IEICE TRANSACTIONS

on Fundamentals of Electronics, Communications and Computer Sciences

DOI:10.1587/transfun.2024CIP0002

Publicized:2024/09/11

This advance publication article will be replaced by the finalized version after proofreading.

A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY

The Institute of Electronics, Information and Communication Engineers

Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

PAPER *Special Section on Cryptography and Information Security*

Laser-based Covert Channel Attack Using Inaudible Acoustic Leakage from Multilayer Ceramic Capacitors

Kohei DOI[†], ***Nonmember and*** **Takeshi SUGAWARA**[†], ***Member***

SUMMARY We propose a new covert-channel attack that exploits inaudible acoustic leakage from multilayer ceramic capacitors (MLCCs) using a laser Doppler vibrometer (LDV). Malware installed on a victim PC modulates the CPU load by transmitting data bits that induce acoustic noise from an MLCC on the victim PC's motherboard. Unlike conventional attacks that use a microphone to capture such acoustic leakage, we use an LDV aimed at the MLCC to capture the acoustic leakage from the MLCC. Using LDV, instead of microphones, the attacker can exploit inaudible high-frequency signals and penetrate transparent obstacles such as a glass side panel on the victim's PC by shining a laser on the target MLCC. The proposed method requires less privilege compared to conventional covert acoustic channel attacks that require privilege to use IO devices(e.g., loudspeaker, microphone). In addition, the proposed method exploits the acoustic leakage from MLCCs instead of a loudspeaker. Therefore, the proposed method is possible to attack PCs that do not have loudspeaker installed. Compared with conventional LDV-based eavesdropping attacks, the proposed method extends them to MLCC leakage in the covert-channel setting. We experimentally verify the proposed attack by measuring inaudible acoustic leakage from MLCC, induced by modulated CPU load, by using an LDV and evaluating the bitrate.

key words: *Covert Channel, MLCC, Acoustic Side-Channel, Laser Doppler Vibrometer*

1. Introduction

Operating systems check all data accesses and accept or deny them based on an access control list, which is the foundation of information system security. The covert-channel, an alternative information channel usually realized with physical side effects such as timing and sound, is a major threat to such logical access control [1]–[5], [8]. Researchers have been proposing several covert-channels using different physical side effects.

Acoustic noise from computer hardware can contain secret information that is processed by a CPU when electric noise from the CPU is converted to mechanical vibration by electronic components on a motherboard. Multilayer ceramic capacitors (MLCCs) are a major cause of sound generation. Previous works have exploited the acoustic leakage of MLCCs for side-channel cryptanalysis [9] and injection of inaudible voice commands [10].

From the attacker's point of view, a major limitation of MLCC's acoustic leakage is the distance. The sound level from the MLCCs is tiny and decays rapidly as it travels through the air. Furthermore, a chassis surrounding a motherboard efficiently blocks the propagation of the sound.

[†]The author is with the The University of Electro Communications,

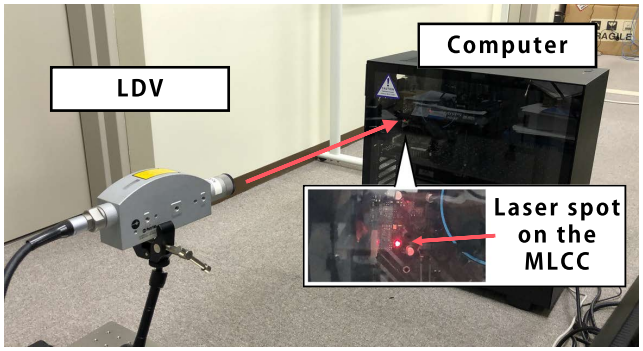

Fig. 1 The experimental setup for measuring vibration of MLCC using the LDV. The laser beam from the LDV is aimed at the target MLCC mounted on the motherboard through a transparent side panel of the chassis.

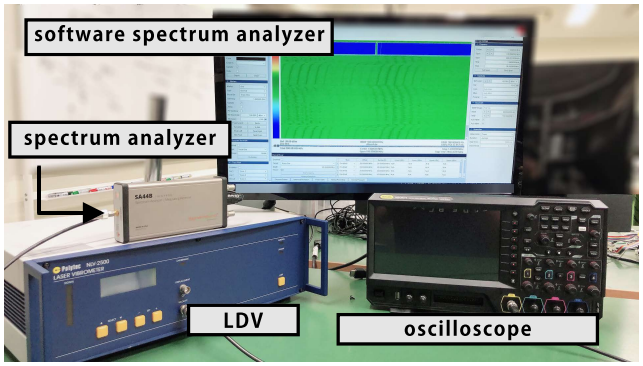

Fig. 2 The signals obtained from the LDV are analyzed using these instruments. Spectrum analyzers and software spectrum analyzers are used in Section 4.1 and Section 4.2 to visualize the signals obtained from the LDV. The oscilloscope is used in Section 5to analyze the signals by receiver.

For example, the attack distances of CapSpeaker [10] and Acoustic Cryptanalysis [9] are limited to about 0.1 and 6 meters, respectively.

To extend the attack distance, researchers recently started exploring a laser Doppler vibrometer (LDV) that uses a laser beam to remotely measure vibration at the laser spot. Once the vibration is encoded in light, it travels a longer distance. Walker and Saxena showed that an attacker can eavesdrop on human speech by measuring the vibration of environmental objects such as a cup with an LDV [11]. Then, Walker et al. extended the attack by measuring the vibration in the heads of the hard disk drives (HDDs) [12].

This paper further extends the previous attacks by using LDV for a covert-channel by measuring unintentional acous-

Copyright © 2015 The Institute of Electronics, Information and Communication Engineers

tic leakage from MLCCs. Malware installed on the target system induces acoustic noise by modulating the CPU load. Meanwhile, an attacker aims an LDV at the target MLCC mounted on the motherboard through a transparent side panel of the PC chassis, as shown in Figure 1. LDV offers several advantages compared to conventional microphone-based methods [13]:

(1) A wider frequency range.

MLCCs can vibrate at more than 1 MHz, but the sensitivity of microphones is limited to some audible frequency, typically less than 20 kHz.

(2) Object penetration.

The laser light can go through transparent obstacles such as a glass window.

(3) High selectivity.

An LDV measures the vibration at the laser spot, efficiently eliminating environmental noises such as computer case fans.

1.1 Contributions

This paper proposes the LDV-based covert-channel attack[†] and experimentally verifies its feasibility and contains the following key contributions.

- The new covert-channel attack exploits inaudible leakage from MLCCs using an LDV (Section 3).
- Performance comparison with conventional covert-channel attack using microphones (Section 4.2).
- Experimental verification and performance evaluation of the bit rate at different distances (Section 5).
- Discussion of countermeasures and attack improvements (Section 6).

2. Background and Motivation

We briefly summarize conventional work on acoustic leakage and attacks that exploit them.

2.1 Acoustic Side-Channel and MLCC

Acoustic noise from computer hardware can cause critical security problems. For example, Genkin et al. successfully recovered the RSA secret key by measuring such acoustic noise with a microphone [9].

MLCCs are considered as a key electronic component that converts electrical noise, caused by a CPU handling secret information, into mechanical vibration. MLCC is a tiny surface-mounted capacitor shown in Figure 3, which realizes a large capacitance with a small footprint by using layers of dielectric material and is extremely common in computer motherboards.

[†]A video demonstration of the proposed LDV-based covert-channel attack can be found at `https://bit.ly/3IBMfTV`.

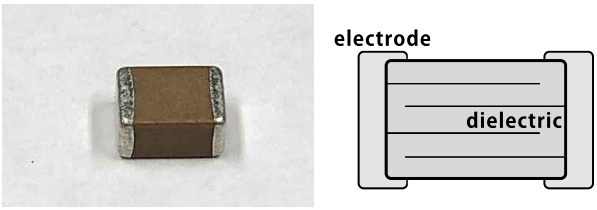

Fig. 3 MLCC appearance (top) and internal structure (bottom). Multiple dielectrics are layered on top of each other, and this thinning and multilayering enables large capacitance despite its small size.

The physical causality behind the voltage-to-sound transduction in MLCCs is explained by the piezoelectric effect, and its basic properties are studied in the non-security context. The dielectric material deforms with voltage across the terminals and causes vibrations on an alternating voltage. The dielectric material quickly responds to voltage changes, and vibration can reach more than 1 MHz [14]. Meanwhile, such high-frequency sound propagates through the air only inefficiently, and the conventional attack that exploits ultrasonic leakage was successful only in 0.1 meters [10].

2.2 Covert-Channel Attack

Covert-channel attacks establish a hidden communication channel through physical side effects, such as system load and data access time, thereby bypassing the logical isolation enforced by a system [1]. The malicious transmitter and receiver in isolated domains cooperatively communicate using the modulation and demodulation methods agreed in advance. The transmitter and receiver are often malwares installed in the target system.

Audible sound and ultrasound are commonly used as covert-channel, and we will discuss them separately in comparison with the proposed method in Section 3.3. The other physical side effects have also been used as a covert channel. Guri et al. transmitted data by modulating CPU load and received the resulting electromagnetic noise with a radio receiver [3]. Similarly, the other work measured the temperature sensor reading, establishing a temperature covert-channel [17], [18], [20]. The optical covert-channel attacks transmit the data by flickering an LED and receiving them with a camera [21]–[24]. Electromagnetic emission [25]–[27], RF signal [28], and vibration [29], [30] are also used for covert-channel attack.

2.3 Laser Doppler Vibrometer (LDV)

An LDV remotely measures vibration by shining a laser on the target object. The light reflected at the target object has a slight frequency shift by the Doppler effect, and an LDV extracts the shift with an interferometer, which can be translated into the vibration at the target object. An LDV has several advantages over microphones. First, an LDV captures high-frequency vibrations as high as a few MHz, which do not travel through the air efficiently and are far beyond the bandwidth of microphones. Second, a reflected

laser beam, carrying information about the vibration at the point of reflection, travels a longer distance compared to an acoustic wave. For the same reason, it penetrates transparent obstacles, such as a glass window, and is not affected by environmental acoustic noise during the path. Walker and Saxena used an LDV to eavesdrop on human speech by measuring environmental objects, such as metal cups [11].

3. Proposed Method

This section explains the threat model and the advantages of the proposed covert-channel attack that measures MLCCs on a PC using an LDV (see Figure 1).

3.1 Threat Model

The attacker has a transmitter running on the victim's computer through malware. The attacker installs malware on victim's computer without network connectivity via USB storage [39], [40]. Previous research has shown that the attacker can compromise air-gapped networks in the same way [5], [22], [28]. The transmitter generates acoustic leakage by changing the CPU load with transmitting bits. As such, the transmitter does not need special privileges, such as access to IO devices. As a precondition of the function of malware to achieve these conditions, malware must be able to access confidential information, and manipulate CPU load.

The attacker receives the transmitted data by remotely measuring the modulated acoustic leakage using an LDV. The attacker needs a line of sight to the target electronic components, such as MLCCs, on the target machine. The attacker can stay in the other room or building, as long as the line of sight is available. The attacker knows the location of an MLCC that generates acoustic leakage in the target PC. The attacker can easily achieve this by profiling the same motherboard/PC model purchased on the market. This requirement is satisfied with the target machine with a transparent side panel, as shown in Figure 1. Once this requirement is satisfied, the LDV-based attack can be performed from greater distances compared to conventional covert-channel attacks.

3.2 Attack Senario

Attack scenario is classified into two phases same as previous work [5].

(1) Infection phase

The victim machine is compromised by malware. Malware can infiltrate devices without network connection via USB storage devices.

This phase starts with the assumption that the attacker has identified the victim machine, and the identification of the victim machine must be satisfied using other methods outside the scope of this paper, such as social engineering. Such assumptions are common in covert-channel attack research [5], [22], [28]. For example, Stuxnet is malware infection of a specific machine in an air-gapped network [39].

(2) Exfiltration phase

The infiltrated malware collects confidential information, and modulates and transmits the confidential information using acoustic leakage generated by MLCC. An attacker in another space (another room, building, etc.) remotely measures the acoustic leakage from the MLCC using LDV to recover confidential information.

3.3 Comparison to Previous Approaches

(1) Comparison with general malware attacks

Confidential information can be stolen over the network using malware. On the other hand, covert-channel attack research generally focuses on air-gapped networks. Therefore, it is not possible to use a normal network (Ethernet, Wifi, etc) to exfiltration confidential information from the victim's machine. The advantage of the proposed method as a malware attack is that physical phenomena such as sound, light, and electromagnetic waves can be used to exfiltrate information beyond the air-gapped network.

(2) Comparison with previous covert-channel attacks

The proposed attack has several advantages over the previous covert-channel attacks. Table 1 compares the channel type, the signal source, the signal receiver, if the attack is noticeable by a nearby user, and the ability to penetrate obstacles.

Several attacks exploit sound as a covert channel. In particular, researchers have been conducting stealthy attacks using inaudible sound, i.e., ultrasound beyond 20 kHz [3], [7], [15], [19] and infrasound in 16–24 Hz [30]. As a drawback, these attacks need a speaker to generate inaudible sound, and PCs in a shared office typically have audio devices muted or no speakers.

Addressing the issues, the other papers pursue no-speaker attacks by turning several computer components into a sound emitter, e.g., hard disk drives (HDDs) [16] CD/DVD drives [4], and cooling fans [8]. However, as a drawback, these attacks generate audible sound and thus are noticeable by nearby human operators.

The other methods achieve no-speaker and inaudible attacks. Power-Supplay [5] generates ultrasound by changing the load to a power supply unit, but the sound generated is weak and easily blocked by obstacles. Meanwhile, AiR-ViBeR [6] exploited inaudible vibration. However, the receiver needs a mechanical coupling, e.g., a smartphone placed on the same desk, and a long-distance attack is impossible.

Another approach is the optical covert channel attack using LEDs [21], [22]. These attacks are advantageous because light can easily penetrate transparent obstacles. However, the attack needs GPIO access and an LED connected to it. Moreover, the flickering LED can be noticed by nearby human operators.

Table 1 Comparison with existing covert channels. The columns show the channel type, the signal source, the signal receiver, the noticeability by a nearby user, the ability to penetrate obstacles, the resistance of noise, max attack distance, and restriction.

Ref.	Channel	Source	Reciever	Speaker?	Audible/ Visible?	Obstacle?	Noise?	Distance	Restriction
MOSQUITO [3]	Ultrasound	Speaker	Speaker	Yes	No	No	Yes	8 m	same room
GAIROSCOPE [7]	Ultrasound	Speaker	Gyroscope	Yes	No	No	Yes	8 m	same room
Guri et al. [15]	Ultrasound	Speaker	Speaker	Yes	No	No	Yes	3 m	same room
Deshotels [19]	Ultrasound	Speaker	Microphone	Yes	No	Yes	Yes	1.5 m	same device
Matyunin et al. [30]	Infrasound	Speaker	Accelerometer	Yes	No	No	–	0.5 m	same surface
Diskfiltration [16]	Audible Sound	HDD	Microphone	No	Yes	No	Yes	2 m	same room
CD-LEAK [4]	Audible Sound	CD/DVD drive	Microphone	No	Yes	No	–	8 m	same room
Fansmitter [8]	Audible Sound	PC fans	Microphone	No	Yes	No	Yes	8 m	same room
Power-Supplay [5]	Ultrasound	Power-supply	Microphone	No	No	No	–	6 m	same room
AiR-ViBeR [6]	Vibration	PC fans	Accelerometer	No	No	—	Yes	1.6 m	same surface
LaserShark [21]	Light	LED, Laser	LED, Photodetector	No	Yes	Yes	–	25 m	line of sight
xLED [22]	Light	LED	Camera, Photodetector	No	Yes	Yes	–	–	line of sight
Ours	Ultrasound	MLCC	LDV	No	No	Yes	–	1.5 m	line of sight

In contrast to the above attacks, the transmitter in our attack does not need any privileges, including access to IO devices; the proposed method simply changes the CPU load from a user space. MLCC generates ultrasonic sound beyond 100 kHz which is inaudible to human ears. The laser-based measurement using an LDV enables penetration of transparent obstacles, such as a glass window. The proposed attack also extends the LDV-based eavesdropping attack [11] to a new threat model (covert channel attack) and a new target (inaudible and high-frequency sound from MLCC).

4. Preliminary experiments

In this section, we conduct basic experiments on MLCC acoustic leakage using LDV. These measurements will verify that the LDV can measure vibration and manipulate acoustic leakage from MLCCs, and confirm that the covert-channel can be established using these measurements.

4.1 Preliminary experiments 1: Relationship between MLCC acoustic noise and CPU utilization

We first verify the feasibility of the attack by measuring an MLCC with an LDV under different CPU loads.

(1) Setup.

We use the setup shown in Figure 1. LDV (Polytec NLV-2500) aims at an MLCC mounted on the target motherboard (ASRock H610M-HDV/M.2 [31]) from 0.3 meters away. The sensitivity of the LDV is 10 mm/s/V. A spectrum analyzer (SignalHound SA44B [32]) and its companion software (SignalHound Spike) analyze and visualize the signals from LDV. The spectrum analyzer runs in real-time mode with a center frequency of 100 kHz, a span of 200 kHz, and the resolution bandwidth (RBW) and the video bandwidth (VBW) both at 100 Hz. The target machine runs a program that periodically changes CPU utilization between 0 and 100% every second.

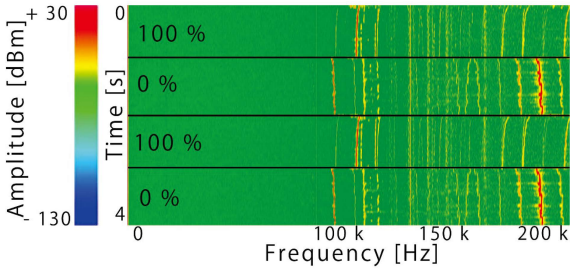

Fig. 4 Relationship between CPU utilization and acoustic noise from MLCC. The horizontal lines highlights the changes in the CPU load.Letters 100% and 0% indicate when CPU usage is 100 % and when it is 0 %.

(2) Result.

Figure 4 shows the spectrogram between 0–200 kHz during the experiments. The horizontal and vertical axes are frequency and time, respectively. The intervals with different CPU loads are highlighted with horizontal lines. Figure 4 clearly shows that the spectral pattern significantly changes with CPU utilization. After a preliminary exploration, we chose the narrow frequency band around 100 kHz for our covert-channel, considering the following two points. First, the target frequency should be stable during the target CPU load. For example, the band around 200 kHz is contaminated with slight frequency shifts, which is unfavorable for a covert-channel. Second, the band should be isolated from the surrounding changes. The band around 180 kHz falls in this category, which interferes with neighboring bands. Although CPU-dependent frequency shifts are observed in higher frequency bands, they are relatively unstable and suffer from the above problems.

4.2 Preliminary experiments 2: Effect of glass on LDV and microphone measurements

Next, we verify LDV's advantage by putting a transparent obstacle in between the sound source and the attacker over a microphone by measuring a speaker by putting a glass panel in between.

(1) Setup.

This experiment measures a speaker (Union Team Limited NA202C) making a 10 kHz tone driven by a function generator (Instek's MFG-2120MA [33]). We measure the speaker with either an LDV or a microphone, during which we insert a glass window in between. The LDV is aimed at the speaker. Meanwhile, we used a microphone (Focusrite Scarlett Studio CM25 MkII [34]) with an audio interface (Focusrite Scarlett [34]) and analyzed the signals with a spectrum analyzer. In both measurements, the distance between the MLCC and the microphone or LDV is 0.3 m, and the glass is placed approximately 0.15 m between the MLCC and the microphone or LDV. Experiments have empirically confirmed that the position of the glass has little effect on the measurement of acoustic leakage from the MLCC. The spectra are measured in real-time mode where the center frequency is 10 kHz, the span is 20 kHz, and RBW and VBW are both 100 Hz.

(2) Result.

Figures 5-(a) and 5-(b) show the spectrograms of the microphone and the LDV measurements, respectively. We place and then remove the glass window during the continuous measurement, and the corresponding time slots are separated with the horizontal lines. The 10 kHz tone signal is highlighted with black rectangles. The results clearly show that the LDV measurement is mostly unaffected by the glass window because the laser beam simply penetrates it. Meanwhile, the microphone measurement shows that the 10 kHz tone is blocked by the glass window; the peak power at 10 kHz decreases by 84% with the glass. The result clearly shows that LDV is advantageous when there is a transparent obstacle between the attacker and the victim machine. †

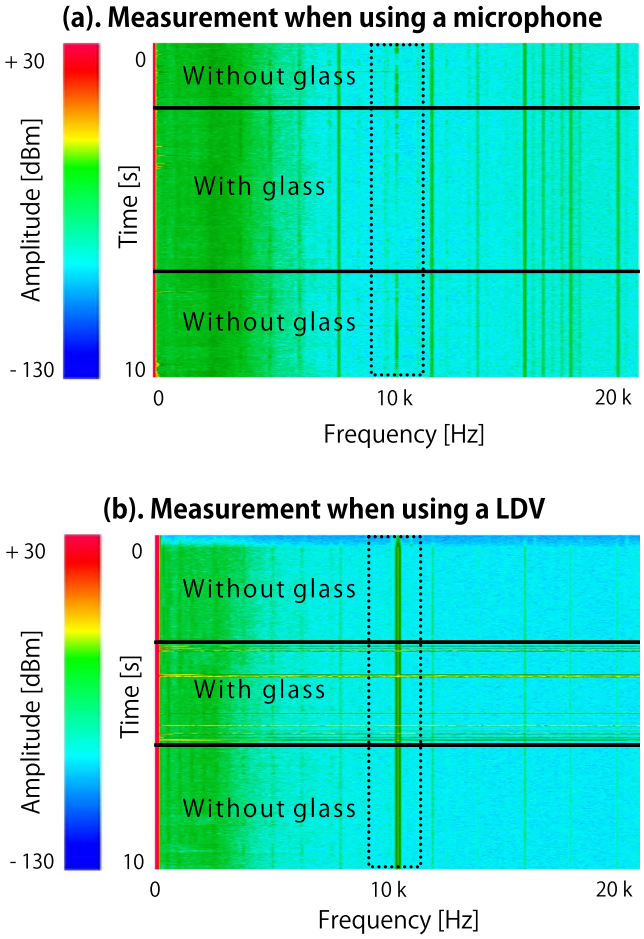

Fig. 5 The Influence of Glass on Microphones and LDV. Measured 10 kHz from a speaker and confirmed the difference in measurement results when glass was placed in between. In the case of the microphone (a), the signal is attenuated in the section where the glass is placed, while in the case of the LDV (b), the measurement is not affected by the glass.

5. Evaluation of Covert-Channel Attack

We verify the proposed covert-channel attack and evaluate its performance in terms of bit rate and attack range.

5.1 Attack Feasibility

(1) Setup.

We verify the attack feasibility using the same setup as in Section 4.1 but with some important changes. First, the victim machine runs the program in Algorithm 1, which changes the CPU load every n second. This n determines the bit rate, and we use $n = 0.5$, i.e., 2 bps, for this particular experiment. Second, we capture the LDV signals using an oscilloscope (RIGOL MSO5074 [35]) instead of a spectrum analyzer. The oscilloscope captures the time domain signals for 50 seconds with 500 kSa/s sampling rate. The transmitter in Algorithm 1 sends the ASCII string `capacitor` which is converted to byte string with the synchronization symbols, namely `1111110000` and `0000111111`, before and after the string. As a result, $N_m = 88$ bits are transmitted in total.

(2) Data analysis.

We demodulate the received signals based on the previous study [19], as illustrated in Figure 6. We first obtain a spectrogram with the short-time Fourier transform (STFT), i.e. a two-dimensional array indexed by frequency and time. We extract the subarray for the 107.4 ± 0.9 kHz band identified in the preliminary experiment in Section 4.1. The moving aver-

†In the demo video (`https://bit.ly/3IBMfTV`), the obstacle is a transparent side panel in the PC case; the attack is successful with an additional glass window, but it is omitted for the simplicity of the setup.

Algorithm 1 Programs to manipulate CPU utilization

Require: N bits of message: $a_0, \ldots, a_{N-1} \in \{0, 1\}$
Require: Time duration: n.
  for $j = 0$ to $N - 1$ **do**
    if $a_j = 0$ **then**
      Sleep for n seconds
    else
      Run 12 processes for n seconds
    end if
  end for

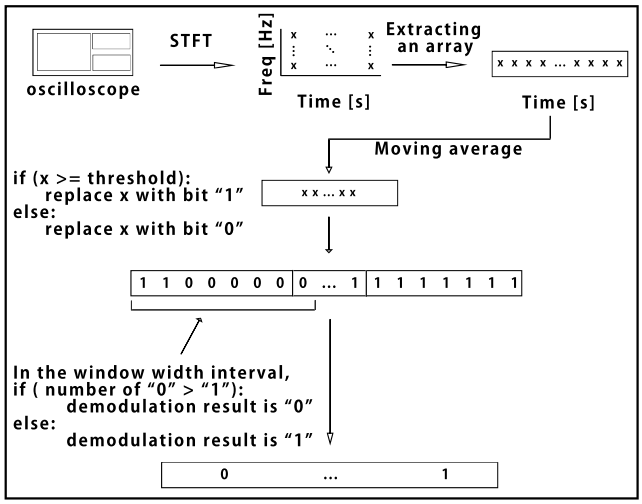

Fig. 6 A method for demodulating the modulation signals obtained from LDV. The signals collected by an oscilloscope is processed by the STFT method and the 100 kHz spectrum is extracted. and a moving average method. The bit value is determined using a pre-profiled threshold value.

age is applied to the subarray to reduce measurement noise. The bit values are finally recovered by sampling the resulting trace with a certain timing and threshold determined for the target bit rate.

(3) Result.

Figure 7 shows a trace after moving average where the horizontal and vertical axes are time and amplitude, respectively. The vertical lines highlight the moment the bit value changes. The result shows that the regions for `0` and 1 are clearly separable, and the covert-channel is successfully established.

5.2 Bit rate evaluation

We finally evaluate the performance of the covert-channel by measuring the bit rate and the bit error rate (BER) at different distances between the LDV and the victim computer. We repeat the experiment in Section 5.1 by decreasing n in Algorithm 1, i.e., the bit rate, from 10 to 150. During the experiments, we record the BER $\epsilon = N_e/N_m$ where N_e and N_m are the number of error and message bits. We conduct the above experiment by changing the distance between the LDV and the computer to 0.5, 1.0, and 1.5 meters. For each setting, we make three identical measurements and obtain the average between them.

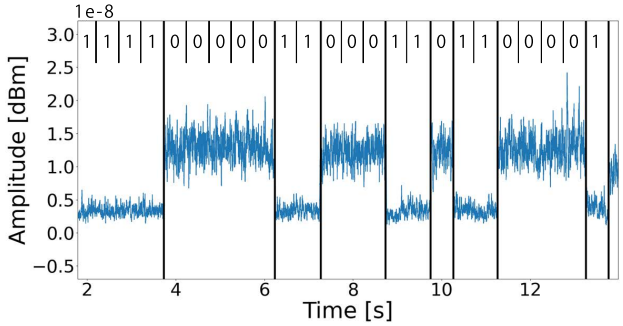

Fig. 7 Demodulated Bit string. The sender sends the ASCII string `capacitor` and sync code. The preamble and postamble are `11110000` and `00001111`, respectively.

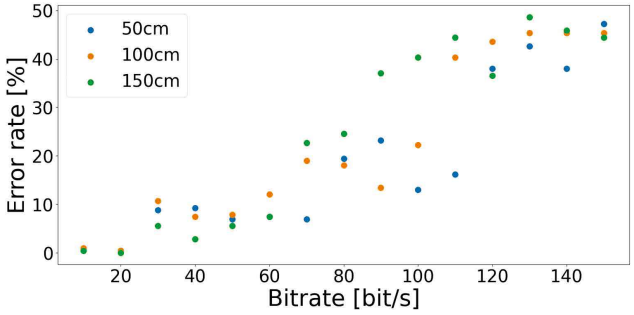

Fig. 8 Experiments on the distance and bit rate. The vertical axis and the horizontal axis represent the BER and the bit rate respectively. Experiments were conducted by varying the bit rate for each distance. It can be seen that as the bit rate increases, the BER also increases.

(1) Result.

Figure 8 compares the bit rate and the BER in a scatter plot. The horizontal and vertical axes are bit rate and BER, respectively. The results with 0.5, 1.0, and 1.5 meters distances are shown with the blue, orange, and green dots, respectively. The bit rate impacts BER. BER approaches 50% around 120 bps wherein the received signals are indistinguishable from a random bit sequence. This performance is better than the RF covert-channel attack ODINI [2] which achieves 40 bps and BER 10% at 1.5 meters. Meanwhile, the acoustic covert-channel attack MOSQUITO [3] achieves 166 bps and BER 1% at 3.0 meters, which is better than ours, although there is no glass window in between.

Although BER degrades as distance increases, the impact is relatively minor compared to the bit rate. Meanwhile, focusing becomes more challenging as the distance increases with our LDV (Polytec NLV-2500) using its default optics. The distance of 1.5 meters is in between the conventional LDV-based attack; the works [11] and [12] measured up to 3 and 0.3 meters, respectively. Extending the LDV with better optics or using a long-range LDV [13] can further extend the distance.

6. Discussion

Finally, we discuss possible countermeasures and further

attack improvements.

6.1 Countermeasures

(1) Reducing acoustic leakage.

A straightforward countermeasure is to use electronic components that generate less acoustic noise. Electrolytic or film capacitors cannot be a viable alternative due to their sizes and prices [10]. Another approach is to control acoustic noise at design time. However, the acoustic leakage from each electronic component is not usually characterized. and the electronic noise that drives them is usually hard to predict.

There are several implementation techniques to reduce the acoustic noise of MLCCs, which can be effective countermeasures against the covert-channel. For example, Murata proposes to attach a metallic foot, thereby suppressing the distortion on the substrate that causes acoustic leakage [36]. Similarly, EDN proposes to symmetrically layout MLCCs on a target power line so that vibration from each MLCC cancels out with each other [37].

(2) Blocking the line of sight.

We can prevent the attack by blocking the line of sight between the LDV and the target MLCC. Computers handling sensitive information should avoid a PC case with a non-transparent side panel.

(3) Detecting anomalies.

The victims can detect the abnormal CPU utilization pattern as the covert-channel attack. The abnormal CPU utilization patterns that appear during the covert-channel attack can be used as a detective countermeasure.

6.2 Improved attack

(1) Invisible attacks.

Our LDV (Polytec NLV-2500) uses a HeNe laser that emits visible red light at 633 nm, as shown in Figure 1, and people around the victim machine potentially notice the laser spot and detect the attack. First, the color and intensity of LDV's laser spot look similar to typical red LEDs on motherboards, and noticing it without precaution will be difficult. However, users might disable such LEDs to prevent covert-channels based on LEDs [21], [22], making the proposed attack more noticeable. In such a case, an attacker can use an LDV using the invisible wavelength instead [38]. Such an advanced LDV also has a visible laser for aiming, which can be easily blocked during the attack.

(2) Higher data rate.

The bit rate and BER are determined by SNR, which can be improved with better aiming and optics. Also, channel selection has room for further improvement because we choose a particular narrow band, and other CPU-load-dependent changes are simply ignored (see Figure 4). In addition, replacing the basic ASK modulation with more advanced ones can further improve the performance. Meanwhile, In addition, an error-correction scheme will be necessary to use the covert-channel at a higher bit rate.

7. Conclusion and Future Works

In this paper, we show that a new covert-channel attack can be achieved by using an LDV to measure acoustic leakage from MLCCs implemented in the computer. This attack is achieved by controlling the acoustic noise of MLCCs by manipulating CPU utilization and measuring the acoustic noise using an LDV. Our attack achieves 100 bps with 10% BER in 1.0 meters away.

Further experiment is needed for a longer-range attack using better optics. The choice of a target band and the signal processing have room for further improvement. Reducing the attack cost is another challenge because LDVs are generally expensive as they are scientific instruments. Meanwhile, efficient countermeasures such as leakage suppression, need a better understanding of MLCC acoustic leakage.

In addition, it is known that acoustic leakage also occurs from silicon capacitors [41]. Therefore, searching for the source of acoustic leakage can extend the attack scenario.

Acknowledgement

This work was supported by JSPS KAKENHI Grant Number 21K11884 and 22H00519.

References

[1] B. Lampson, "A Note on the confinement problem," Communications of the ACM, vol. 16, issue 10, pp. 613-615, 1973.
[2] M. Guri, B. Zadov, and Y. Elovici, "ODINI: escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," TIFS '20, vol. 15, pp. 1190-1203, 2020
[3] M. Guri, Y Solewicz, A Daidakulov, and Y Elovici, "MOSQUITO: covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker Communication," DCS '18, 2018
[4] M. Guri, "CD-LEAK: Leaking secrets from audioless air-gapped computers using covert acoustic signals from CD/DVD drives" in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 808–816., 2020
[5] M. Guri, "Power-supplay: Leaking sensitive data from air-gapped, audio-gapped systems by turning the power supplies into speakers," IEEE Transactions on Dependable and Secure Computing, 2021.
[6] M. Guri, "AiR-ViBeR: Exfiltrating Data from Air-Gapped Computers via Covert Surface ViBrAtIoNs," CoRR, 2020
[7] M. Guri, "GAIROSCOPE: Leaking Data from Air-Gapped Computers to Nearby Smartphones using Speakers-to-Gyro Communication," 2021 18th International Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, pp. 1-10, 2021
[8] M. Guri, Y. Solewicz, and Y. Elovici, "Fansmitter: Acoustic data exfiltration from air-Gapped computers via fans noise," Comput. Secur. 91, 2020
[9] D. Genkin, A. Shamir, and E. Tromer, "Acoustic cryptanalysis," Journal of Cryptology, vol. 30, issue 2, pp. 392-443, 2017.
[10] X. Ji, J. Zhang, S. Jiang, J. Li, and W. Xu, "CapSpeaker: injecting voices to microphones via capacitors," CCS'21, pp. 1915-1929, 2021.
[11] P. Walker and N. Saxena, "Laser meager listener: a scientific exploration of laser-based speech eavesdropping in commercial user

space," EuroS&P '22, pp. 537-554, 2022.
[12] P. Walker, S. Saini, S. Anand, T. Halevi, and N. Saxena, "Hearing check failed: using laser vibrometry to analyze the potential for hard disk drives to eavesdrop speech vibrations," ASIA CCS '22, pp. 67-81, 2022.
[13] Y. Deng, "Long range standoff speaker identification using laser doppler vibrometer," BTAS '16, pp. 1-6, 2016
[14] B. Ko, S. Jeong, Y. Ahn, K. Park, N. Park, and Y. Park, "Analysis of the correlation between acoustic noise and vibration generated by a multi-Layer ceramic capacitor," Microsyst Technol, vol. 20, issue 8-9, pp. 1671-1677, 2014.
[15] M. Guri, Y. A. Solewicz, and Y. Elovici, "Speaker-to-speaker covert ultrasonic communication," JISA'20, 51, 2020
[16] M. Guri, Y. A. Solewicz, A. Daidakulov, and Y. Elovici. "Acoustic data exfiltration from speakerlessair-gapped computers via covert hard-drivenoise ('DiskFiltration')," ESORICS'17, pp. 98–115, 2017
[17] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "BitWhisper: Covert signaling channel between air-gapped computers using thermal manipulation," In Proc. of the IEEE Computer Security Foundations Symposium, 2015
[18] M. Guri, "HOTSPOT: Crossing the air-gap between isolated pcs and nearby smartphones using temperature," EISIC'19, pages 94–100, 2019
[19] L. Deshotels, "Inaudible sound as a covert channel in mobile devices," WOOT'14, 2014.
[20] R. Masti, D. Rai, A. Ranganathan, C. Müller, L. Thiele, and S. Capkun, "Thermal covert channels on multi-core platforms," SEC'15, 2022, pp. 865-880, 2015
[21] N. Kühnapfel, S. Preußler, M. Noppel, T. Schneider, K. Rieck, and C. Wressnegger, "LaserShark: establishing fast, bidirectional communication into air-gapped systems," ACSAC '21, pp. 796–811, 2021
[22] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xLED: covert data exfiltration from air-gapped networks via switch and router LEDs," PST '18, pp. 1-12, 2018
[23] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "CTRL-ALT-LED: Leaking data from air-gappedcomputers via keyboard leds," COMPSAC'19, pp. 801–810, 2019
[24] M. Guri, B. Zadov, and Y. Elovici, "Led-it-go: Leaking (a lot of) datafrom air-gapped computers via the (small)hard drive led," DIMVA'17, pages 161–184, 2017
[25] M. Guri, M. Monitz, and Y. Elovici, "USBee: Air-gap covert-channel via electromagnetic emission from usb," PST'16, 2016
[26] M. Guri, "Air-Gap Electromagnetic Covert Channel," IEEE Transactions on Dependable and Secure Computing, 2023
[27] M. Guri, "Near Field Air-Gap Covert Channel Attack," TrustCom'22, pp. 490–497, 2022,
[28] M. Guri, "SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables," PST'22, pp. 1–10, 2022
[29] M. Guri, "Exfiltrating data from air-gapped computers via ViBrAtIoNs," Future Generation Computer Systems, vol. 122, pp. 69–81, 2021
[30] N. Matyunin, Y. Wang, and S. Katzenbiesser, "Vibrational covert channels using low-frequency acoustic signals," IH&MMSec'19, pp. 31-36, 2019.
[31] ASRock Inc., "H610M-HDVM.2, "https://download.asrock.com/Manual/H610M-HDVM.2.pdf, 2021, accessed Mar. 12. 2024.
[32] SignalHound, "USB-SA44B Spectrum Analyzer, "https://signalhound.com/sigdownloads/datasheets/SA44B_sellsheet-Spring-2021.pdf, 2021, accessed Mar. 12. 2024.
[33] Good Will Instrument Co., Ltd., "Multi-Channel Function Generator MFG-2000 Series User Manual," https://www.yildirimelektronik.com/dokuman/GW%20INSTEK%20MFG%20Serisi%20Kullan%C4%B1m%20K%C4%B1lavuzu.pdf, 20211, accessed Mar. 12. 2024.
[34] Focusrite, "Scarlett 2i2 Studio User Guide," https://fael-downloads-prod.focusrite.com/customer/prod/downloads/Scarlett%202i2%20Studio%203rd%20Gen%20User%20Guide%20V2.pdf, 20211, accessed Mar. 12. 2024.
[35] RIGOL Technologies, Inc., "MSO5000 Series Digital Oscilloscope," https://jpmall.rigol.com/item-downfile.html?file=%2Ffiles%2F202210%2F07%2F42075c88098903615d30bec763f76baed761a5b2.pdf, 20191, accessed Mar. 12. 2024.
[36] Murata Manufacturing Co., "CeramicCapacitor KRM series," https://www.murata.com/en-us/products/capacitor/ceramiccapacitor/overview/lineup/smd/krm, 2021
[37] EDN, "Reducing MLCCs' piezoelectric effects and audible noise," https://www.edn.com/reducing-mlccs-piezoelectric-effects-and-audible-noise/, 2012
[38] Polytec GmbH, "RSV-150 remote sensing vibrometer," https://www.polytec.com/us/vibrometry/products/special-application-vibrometers/rsv-150-remote-sensing-vibrometer, 2022
[39] R. Langner, "Stuxnet: Dissecting a Cyberwarfare Weapon," in IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, May-June 2011, doi: 10.1109/MSP.2011.67.
[40] Mordechai Guri. 2021. USBCulprit: USB-borne Air-Gap Malware. In Proceedings of the 2021 European Interdisciplinary Cybersecurity Conference (EICC '21). Association for Computing Machinery, New York, NY, USA, 7–13.
[41] Kohei Doi and Takeshi Sugawara. 2022. Poster: Inaudible Acoustic Noise from Silicon Capacitors for Voice-Command Injection. In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security (CCS '22). Association for Computing Machinery, New York, NY, USA, 3339–3341.

Kohei Doi received B.S.C. from The University of Electro-Communications, Tokyo in 2022. He is currently a Master student at The University of Electro-Communications, Tokyo, since 2022. His research interest involves hardware security and side-channel attack.

Takeshi Sugawara received Ph.D. from Tohoku University, Sendai in 2011. He joined Mitsubishi Electric Corporation in 2011 and involved in R&D of embedded systems security. He is currently an Associate Professor at The University of Electro-Communications, Tokyo, since 2017. His research interest involves hardware and embedded systems security, lightweight cryptography, and side-channel attack.