Optical Exfiltration of Data via Keyboard LED Status Indicators to IP Cameras

Zheng Zhou, Weiming Zhang, Zichong Yang, and Nenghai Yu

***Abstract*—The ability of the light-emitting diodes (LED) on a keyboard to send data at a rate that is far greater than the human eye can perceive has been fully studied. However, an IP camera can only fetch high-resolution images at a low frame rate. It is unable to act as a sink of the optical covert channel directly. In our paper, a novel form of modulation is proposed to modulate the LEDs on a keyboard. The modulated signal can be received by a nearby IP camera. To verify its validity, we implement a prototype of exfiltration malware. Our experiment shows a significant improvement in the imperceptibility of covert communication. Against the background of the Internet of Things (IoT), it is possible to leak data covertly to IP cameras across air-gapped networks via LED keyboard status indicators.**

***Index Terms*—Air-gapped Networks, Covert Channel, Internet of Things, Light-Emitting Diode, LED indicator, Modulation**

I. Introduction

As a network of physical devices, vehicles, and home appliances, among other items, the Internet of Things (IoT) [1] has developed rapidly in recent years. “For 2020, the installed base of Internet of Things devices is forecast to grow to almost 31 billion worldwide [37].” Further, “267 billion US dollars will be spent on IoT technologies, products, and services [4].” Nevertheless, millions of devices in the IoT have suffered all types of attack from all over the world. Kaspersky Lab reports that “over 63% of devices from which the attacks originated could be identified as DVR(Digital Video Record) services or IP cameras” [22]. An IP camera system that is controlled by attackers is dangerous. The attackers can not only obtain video data but also use the IP camera as the sink of a covert channel.

A covert channel is a well-known way to transmit messages by circumventing security mechanisms. The definition of a covert channel was given by Lampson in 1973 to describe the leakage of data due to abuse of shared resources by processes with different privilege levels [23]. With the development of communication technology, the idea of a covert channel has been extended from a single host to a network. Many types of covert channel have been developed over the past twenty years. Zander et al [40] surveyed covert channels in different network protocols in 2007. To maintain security, almost every top-secret organization uses physical isolation to keep their high-level networks separated from less-secure and public networks. The term for this type of isolation is *air-gapped*.

Are air-gapped networks safe enough? No. Numerous methods for breaching air-gapped networks have been proposed over the last ten years. Infecting air-gapped networks can be accomplished, as demonstrated by incidents such as Stuxnet [21], Agent.Btz [7], and others [8]. There are two directions of data covert transmission: *infiltration* and *exfiltration*. Infiltrations of air-gapped networks include the following:

- Supply Chain Attack [39]: The attacker installed malware on PCs before the users received them.
- Offline Upgrade Attack: The attacker changed the offline upgrade packages before the users copied them onto the air-gapped network.
- Portable Media Storage Attack: The attacker infected the OS of an air-gapped PC by copying a virus or worm to portable media storage devices.

Once the malware has been activated in an air-gapped PC, the next step is to build an air-gapped covert channel through which to leak sensitive data.

Air-gapped covert channels are different from conventional covert channels in hosts and networks. Information can be transmitted reliably via the latter; therefore, the major method of avoiding detection is to use information hiding technology. However, air-gapped covert channels transmit information by building a physical channel directly using electromagnetism, acoustics, thermodynamics, optics, and other factors. The adversaries of such covert channels mainly involve human senses and detection devices rather than technology for information hiding analysis.

Optical covert channels are the most common air-gapped covert channels because of their high covertness and rates. In particular, the Light-Emitting Diodes (LED) that are widely utilized in electrical equipment to indicate device status can always be used to build covert channels.

Loughry and Umphres [28] studied exfiltration via LED indicators in 2002. They divided LED indicators into three classes:

- Class I: Unmodulated LEDs used to indicate the state of the device;
- Class II: Time-modulated LEDs correlated with the activity level of the device; and
- Class III: Modulated LEDs that are strongly correlated with the content of the data being processed.

This work was supported in part by the National Natural Science Foundation of China under grants U1636201 and 61572452.

Z. Zhou, W. Zhang, Z. Yang and N. Yu are with CAS Key Laboratory of Electromagnetic Space Information, University of Science and Technology of China, Hefei, 230026, China.

Corresponding author: Weiming Zhang (Email: zhangwm@ustc.edu.cn)

They found that the TD LED indicators on almost every modem used in those years were in Class III. Even an LED indicator on a DES encryptor leaks plain data. They indicated that although the LEDs in Class II are not as dangerous as those in Class III, they can be modulated to leak significant information and can be used to build covert channels. In contrast, the LEDs in Class I are safer, because they cannot flicker for no reason.

In 2014, Sepetnitsky [35] proposed a covert channel prototype in which data were leaked to the camera in a smart phone via the monitor's power status LED indicator. Guri presented LED-it-GO [17] to leak data via a hard drive LED indicator in 2017. Guri also proposed xLED [16] to leak data via the LED status indicators on routers in 2017.

In Guri's two methods, LED-it-GO and xLED, the LEDs used as the channel source were in Class II. They flicker naturally without causing user suspicion. Nevertheless, Sepetnitsky's prototype may not be sufficient to cope with the covert behavior of a covert channel because the LED indicator he used was in Class I. Unfortunately, the fastest impulse frequency of the monitor power LED is 25 Hz. It is difficult to circumvent the human sense of sight if some data is modulated with OOK at that frequency.

In contrast, in 2002, Loughry et al presented exfiltration via keyboard LED indicators in Appendix A [28]. The impulse frequency reached 150 Hz under Solaris. It is easy to circumvent the human sense of sight at such a high frequency. However, a malicious insider is needed to place a dedicated device nearby.

In our paper, a novel approach to modulating Class I LEDs based on the limits of human vision is proposed. A prototype of an optical covert channel for leaking data from an air-gapped network to an IP camera via the LED status indicators on the keyboard of a PC is built. Our work is based on three facts:

- People cannot see a momentary off during a long on procedure (persistence of vision [6]);
- People cannot distinguish two similar intensities (Weber-Fechner law [5]); and
- People cannot feel flickering at a frequency greater than 60 Hz (flicker fusion threshold [19]).

Then, two similar intensities are used to encode logical '1' and '0'. Covert communication can circumvent the sense of sight of both the people on the scene and the people watching the video.

IP cameras are easy to find in public offices; therefore, no malicious insider is needed. The result of the experiment shows that the effect of covertness is achieved. Our approach can be used in optical covert channels via Class I LED indicators to any receiver at a low sampling frequency. Meanwhile, Sepetnitsky's prototype [35] can also shift OOK into our modulation form to obtain an improvement in the imperceptibility of covert communication.

The contributions of our research are as follows:

- A novel form of modulation for leaking data from an air-gapped network to an IP camera via keyboard LED indicators is proposed. The existence of this type of covert channel is verified.
- The potential risk of an unmodulated LED status indicator being used to build a covert channel against the background of the IoT is revealed.

The rest of the paper is organized as follows: Related works are described in Section II. The technical background is described in Section III. A prototype is proposed in Section IV. Section V presents and evaluates the results. A new scenario involving a smartphone is discussed in Section VI. Countermeasures are described in Section VII, and our conclusions are drawn in Section VIII.

II. Related Works

Generally, there are mainly four kinds of covert channels that bridge air gaps: *electromagnetic* covert channels, *acoustic* covert channels, *thermal* covert channels and *optical* covert channels.

Kuhn and Anderson [20] proposed a method to transmit information covertly via electromagnetic radiation in 1998. Guri et al introduced AirHopper [11] to leak data from an air-gapped computer to a nearby mobile phone by using an FM radio module in 2014. Guri et al presented GSMem [10] to leak data via electromagnetic radiation generated by computer memory bus in 2015. Guri et al proposed USBee [12] to leak data via electromagnetic radiation generated by a USB cable in 2016. Matyunin et al [30] used a magnetic field sensor in mobile devices to build a covert channel in 2016.

In 2013, Hanspach and Goetz [18] used acoustical devices: speakers and microphones of notebook computers to build a covert channel. Malley et al [32] introduced a covert communication via inaudible sounds in 2014. Lee et al [24] used loud-speakers as acoustical input devices, and built a speaker-to-speaker covert channel in 2015. Guri et al introduced Fansmitter [14] and DiskFiltration [15] to send acoustic signals rather than speakers in 2016.

In 2015, Guri et al introduced BitWhisper [13] to build a bidirectional thermal covert channel with another adjacent PC via heat radiations. Mirsky et al proposed HVACKer [31] to build a unidirectional thermal covert channel from an air conditioning system to an air-gapped network in 2017. The thermal covert channels in the multi-cores CPU has been researched as follows: Mast [29] built a thermal covert channel in multi-cores at a rate of 12.5 bits per second (bps) in 2015. Bartolini [3] studied the capacity of a thermal covert channel in multi-cores in 2016. Selber proposed UnCovert3 [34], a new thermal covert channel in multi-cores at a rate of 20 bps in 2017.

The optical covert channels are the most common to be utilized. Besides LEDs, Shamir [36] presented a covert channel that breaches an air-gapped security system by a light-based printer in 2014. Lopes and Aranha [27] proposed a malicious device to leak data via its flickering infrared LEDs. In 2016, Guri introduced VisiSploit [9], a prototype in which data were leaked via invisible QR-codes in an LCD screen.

III. Technical Background

A. LED

An LED is a two-lead semiconductor light source. It is a p-n junction diode that emits light when activated. When a suitable voltage is applied to the leads, electrons recombine with electron holes within the device, releasing energy in the form of photons. [33]

Currently, most full-size wired keyboards are equipped with three LED indicators. These are 'NumLock', 'CapsLock' and 'ScrollLock' and are arranged horizontally in the upper right corner of the font panel. These LEDs can be controlled by calling the *keybd_event*() function in the Windows API. The function synthesizes a keystroke. A hardware scan code is needed for the key. VK_NUMLOCK, VK_CAPITAL and VK_SCROLL are the codes for the keys NumLock, CapsLock and ScrollLock, respectively. The *GetKeyState*() function is used to obtain an LED's status. It can record the LED's initial status to recover that status after the covert signal has been transmitted.

The advantage of this method is threefold: good compatibility with different versions of Windows; support of both PS/2 and USB interfaces; and no need for administrator privileges. The disadvantage is that the lock status of an LED indicator is changed while the LED is being turned on/off. Therefore, there is interference when the user is typing. Because the method of simulating typing is to send data into the keyboard buffer, the reaction speed of LED indicators can be increased by modifying the Windows Registry keys.

In Linux, there are two methods of turning the LED indicators on/off. The command *setleds* turns the LEDs on/off without changing the lock status. However, superuser privileges are required. On the contrary, the commands *xset* and *numlockx* turn the LEDs on/off without the need for superuser privileges. However, these commands change the lock status of the LED.

Regardless of whether Windows or Linux is used, the kernel privilege is not needed.

B. IP Camera

An IP camera [41], also called a network surveillance camera, is a new type of camera that can access the Internet. The user can control it by manipulating a client panel remotely. With development of optical technology, video coding and networks, the configuration of IP cameras has rapidly increased. MPEG4 encoding with the H.264 standard is used to provide the high resolutions of up to 720p (1280×720) or 1080p (1920×1080). Currently, IP cameras are widely used in normal life.

C. Video Coding

To save storage space, the video data are encoded in accordance with the H.264 standard [38]. During the decoding procedure, the famous free software package *FFmpeg* is used to convert the .mp4 video file to a .rgb video file with the *ffmpeg* command. It is not wise to create a .rgb file that will be too large. Therefore, we handle the .mp4 file with the following steps:

Firstly, the video data encoded in accordance with the H.264 standard is extracted from the .mp4 file.

```
ffmpeg -i input.mp4 -f h264 output.264
```

Secondly, the H.264 video is decoded into YUV format frame by frame. According to [26], this step can be performed using FFmpeg's *avcodec* library.

Finally, the pixel values of the LED indicator are acquired from the YUV data by the LED's position (row and column) in the frame. There are three sample modes of YUV data: YUV444, YUV422 and YUV420. In YUV420, for example, every pixel has a unique Y value, and four adjacent pixels share a set of U and V values, as shown in Table I. Therefore, when the width of the frame is w, the Y offset of pixel (n, m) is $(m-1) \times w + n$, and the offsets in the U and V sequences are both $(\lfloor \frac{m+1}{2} \rfloor - 1) \times \frac{w}{2} + \lfloor \frac{n+1}{2} \rfloor$.

TABLE I
YUV420 SAMPLE

$Y_{11}U_{11}V_{11}$	$Y_{12}U_{11}V_{11}$	$Y_{13}U_{12}V_{12}$	$Y_{14}U_{12}V_{12}$	$\cdots$
$Y_{21}U_{11}V_{11}$	$Y_{22}U_{11}V_{11}$	$Y_{23}U_{12}V_{12}$	$Y_{24}U_{12}V_{12}$	$\cdots$
$Y_{31}U_{21}V_{21}$	$Y_{32}U_{21}V_{21}$	$Y_{33}U_{22}V_{22}$	$Y_{34}U_{22}V_{22}$	$\cdots$
$Y_{41}U_{21}V_{21}$	$Y_{42}U_{21}V_{21}$	$Y_{43}U_{22}V_{22}$	$Y_{44}U_{22}V_{22}$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

IV. ATTACK MODEL

In the attack model, we suppose that the IP camera is compromised by an attacker and that the LED indicators on a keyboard of an air-gapped PC are in the camera's line of sight. We also suppose that malware that controls the LEDs is activated on the PC during a previous infiltration attack.

As shown in Figure 1, sensitive information, such as credit card numbers, passwords, and encryption keys, exfiltrates via the LED indicator of the keyboard on the desk of an office cubicle. The optical signal is fetched by an IP camera hanging from the ceiling of the office. An optical covert channel is built between the LED indicator and the IP camera. Then, the attacker accesses the IP camera via the Internet by manipulating the client panel of the IP camera using the previously obtained user ID and password. An .mp4 video file is obtained by attacker. The YUV data from the LED indicator is obtained after decoding the video file. By demodulating the brightness, the sensitive information is restored.

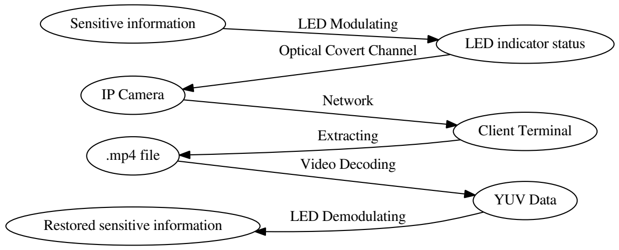

Fig. 1. Flow Diagram for The Prototype

A. Encoding

A normal method of leaking messages is to turn the three LED indicators on a keyboard on/off. The optical signals emitted from the LEDs are received by an IP camera. The video data are stored on a TF card inserted in the camera.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2842116, IEEE Internet of Things Journal

1) Modulation for Various Intensities: The simplest common form of modulation is on-off keying (OOK). The presence of a signal (LED-ON) is used to encode a logical ‘0’, and the absence of a signal (LED-OFF) is used to encode a logical ‘1’, as listed in Table II. OOK can be used for transmissions with high impulse frequencies. When the frequency is up to 150 Hz [28], people do not notice flickering. However, this method is not suitable for low impulse frequencies. Unfortunately, the frame rate of an IP camera is, at most, 15 frames per second (fps). Therefore, we propose a new form of signal modulation that is more suitable for transmitting an optical signal to a receiver at a low sampling frequency without being noticed by human eyes.

TABLE II
MODULATION OF OOK

Logical Bit	LED Status
0	LED-ON
1	LED-OFF

In our approach, one intensity I_0 is used to encode a logical ‘0’, and another similar intensity I_1 is used to encode a logical ‘1’, as listed in Table III. Because there are only two discrete states: ‘on’ and ‘off’ in the brightness of an LED indicator, a novel method is proposed to simulate different intensities by causing the LED to flicker rapidly. The method is described in Figure 2.

TABLE III
MODULATION OF PROPOSED

Logical Bit	Intensity
0	I_0
1	I_1

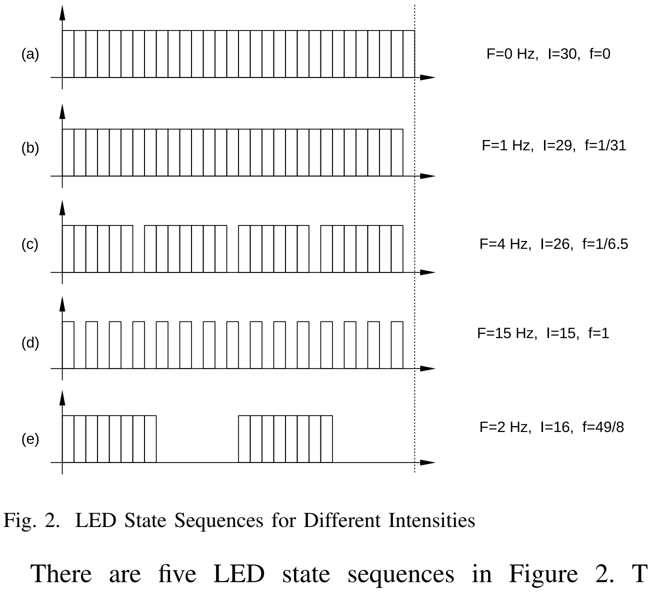

Fig. 2. LED State Sequences for Different Intensities

There are five LED state sequences in Figure 2. The brightness of the LED is shown on the Y-axis, and the X-axis represents time. If there are 30 LED states in a second, then, every state sequence can be supposed to contain some off periods evenly distributed across a long on period (continuous states).

Three indexes are designed to measure every sequence. They are:

- Flicker Frequency (F): The real flickering frequency that can be measured by an optical device. The value is the number of off blocks per unit time. (A group of identical adjacent states make up a block.);
- Intensity (I): The mean brightness per unit time (such as one second). The value is the number of on states per unit time; and
- Flicker Value (f): The feeling of flickering according to the human sense of sight.

The flicker value is given by Equation 1,

$$f = \frac{D_{\text{off}}^2}{D_{\text{on}}} \tag{1}$$

where D_{off} is the average length of off block and D_{on} is the average length of on block.

Then, in Sequence (a), the LED is always on and does not flicker. Therefore, $F = 0$, $I = 30$, and $f = 0$.

In Sequence (b), there is only one off state per unit time. Therefore, $F = 1$, $I = 29$, and $f = \frac{1}{31}$.

In Sequences (c) and (d), there are more off states. Therefore, F and f increase, and I decreases.

In this way, different intensities can be given by setting the number of off states per unit time. Obviously, Sequence (e) is not good for covert transmission. That is why OOK is not a suitable modulation scheme in our scenario. When a long run of ‘1’s follows a long run of ‘0’s, the LED’s flicker value is too high. The user would become aware of this phenomenon.

2) Intensities and Minimum noticeable change: The determination of the two intensities is the key step of the modulation scheme. According to the Weber-Fechner law [5], the minimum noticeable change ΔI depends on the intensity I_0, and $\frac{\Delta I}{I_0}$ is a constant. The constant is found to be $\frac{1}{100}$ by conducting many experiments.

There are 255 intensity levels in video coding. Therefore, if $I_0 = 255$, then $\Delta I = 2.55$. That means I_1 must not lower than 252. This results in a poor signal-to-noise ratio (SNR) for the channel. For a good SNR, the intensity difference $I_0 - I_1$ must greater than ΔI. To minimize the possibility of being noticed, a smooth intensity sequence $\{i_0, i_1, \cdots, i_{n-1}\}$ is designed between two intensities I_0 and I_1 such that $i_m - i_{m+1} < \frac{1}{100}\max\{i_m, i_{m+1}\}$ for any $m \in (0, n-2)$.

For example, i_n can be defined as shown in Equation 2.

$$i_n = 255 \times 0.99^n \tag{2}$$

The values of $\{i_n\}$ are listed in Table IV.

TABLE IV
A SMOOTH SEQUENCE OF INTENSITY VALUES

$I_0 = i_0$	i_1	i_2	$\cdots$	i_8	$i_9 = I_1$
255.0	252.45	249.96	$\cdots$	232.95	230.62

When the change in intensity is smooth, the computer user hardly notices the change in the LED’s intensity because it does not flicker. To decrease the chance of user perception further, the slope of the LED’s intensity transition curve must be limited to a small range. That means a long time between bits is needed.

B. Decoding

As we mentioned in the section on modulation, two intensities are used to modulate the data. Naturally, we can demodulate the signal by distinguishing two different intensities. The median value of $\{Y_i\}$ in the video data is regarded as a threshold in Equation 3.

$$H = \frac{\max\{Y_i\} + \min\{Y_i\}}{2} \tag{3}$$

The means $\{M_i\}$ and the variances $\{V_i\}$ of the video data for each unit time can be calculated.

According to the principle of optical radiation, every mean corresponds to an I value of a sequence in unit time, as previously described. Then, the bits of information can be judged by comparing the means $\{M_i\}$ with the threshold H.

The variance of the Y values $\{V_i\}$ in the video data for each unit time also represents the amount of dither in the signal. It can be used to judge the reliability of the demodulation.

C. Effective Distance

The effective distance is an essential index of a camera's ability to fetch the optical signal of the LED indicators. The ability of a camera is determined by its frame resolution and electronic sensitivity. In terms of distance, there is an upper bound to the availability of the message to a certain camera. Three factors influence the upper bound on the effective distance:

1) Ambient Brightness: LED indicators are only used to represent keyboard statuses; therefore, the brightness of an LED indicator is always low. When the ambient brightness is too high, the brightness status of an LED can hardly be distinguished in the video. In contrast, when the ambient brightness is low enough, the status of an LED is quite obvious in a video.

Nevertheless, in our experiments, we find that when the camera is close to the keyboard, i.e., within 2 meters (m), a certain intensity of ambient brightness can reduce the noise in an MPEG-4 video, and the capacity of the channel is increased.

2) Emission Angle and Distance: The emission angle of an LED indicator is defined here as the angle between the direction of the LED's emission and the direction of the camera.

IP cameras on surveillance duty are always hanging from the ceiling. The distance between the desktop and the ceiling is constant. Therefore, the longer the distance from the LED indicator to the camera is, the larger the emission angle is, and the weaker the intensity of the signal is. The relationship between the emission angle and the distance is described in Figure 3, where $\angle$UZX is the angle between the keyboard surface and the desktop. According to the state of the keyboard's feet, $\angle$UZX has two fixed values. Taking a Logitech K120 keyboard as an example, the values of $\angle$UZX are $1.1353328°$ and $6.9474259°$.

In general, an LED's emission direction is perpendicular to the surface of the keyboard. That is, XB $\perp$ XZ, then $\angle$UZX $=$ $\angle$AXB. Suppose J is an arbitrary point on line AB. Then, we obtain the relation expression between the emission angle $\angle$JXB and the distance $|$XJ$|$ in Equation 4,

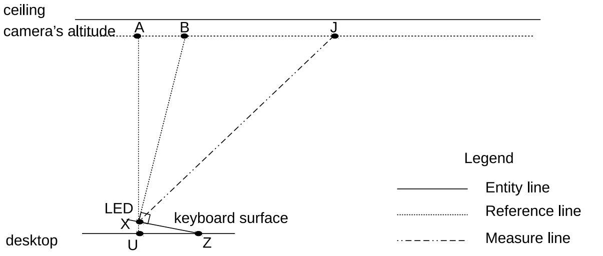

Fig. 3. Relationship between Emission Angle and Distance

$$\angle\text{JXB} = \arccos\left(\frac{|\text{XA}|}{|\text{XJ}|}\right) - \angle\text{AXB} \tag{4}$$

where $\angle\text{AXB} = \angle\text{UZX}$ is known and $|\text{XA}|$ can be measured.

3) Distance and Brightness: A geometrical model of the relationship between the LED indicator and the camera is described in Figure 4. In this figure, piont Y is the camera lens, and line segment ON is the LED indicator surface in the direction of change.

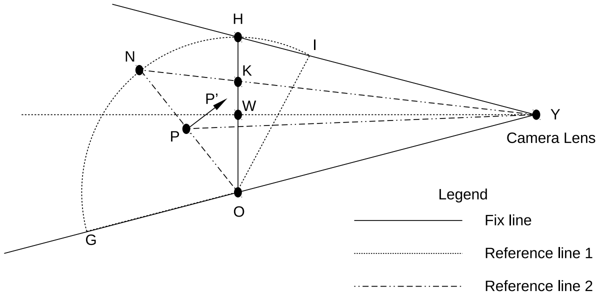

Fig. 4. Relationship between Emission Angle and Effective Shine Area

Because $\frac{|\text{OY}|}{|\text{ON}|} \approx 1000$, $\angle\text{HOY} = \arccos\left(\frac{|\text{OH}|}{2|\text{OY}|}\right) = \arccos\left(\frac{|\text{ON}|}{2|\text{OY}|}\right)$ is approximately $90°$. Therefore, a simplified model is described in Figure 5. In this figure, point O is one side of the LED indicator, and point N is the other side. Changing the emission angle from $0°$ to $90°$ moves N on arc GH. Point K is N's projection in the camera direction. Then, $|\text{KO}|$ represents the LED's effective shine area in the projection plane. We obtain the relation between the emission angle and the effective shine area given in Equation 5,

$$|\text{KO}| = |\text{ON}| \cos(\angle\text{HON}) \tag{5}$$

where $\angle$HON is equal to the emission angle.

Furthermore, the brightness in the video is related not only to the effective shine area but also to the distance between the LED indicator and the camera. Then, the relation between the

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/JIOT.2018.2842116, IEEE Internet of Things Journal

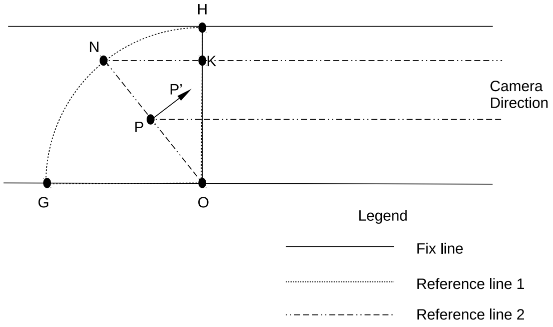

Fig. 5. Simplified Relationship between Emission Angle and Effective Shine Area

brightness and the influencing factors is as shown in Equation 6,

$$B = \beta \frac{|\mathrm{ON}| \cos(\angle \mathrm{HON})}{\left(\frac{|\mathrm{OY}|}{y}\right)^2} \tag{6}$$

where β is a constant coefficient, y is the initial reference distance, a non-zero value, and $|\mathrm{ON}|$ is the length of the LED indicator in the direction of change.

D. Channel Capacity

According to the Nyquist-Shannon sampling theorem, if the sampling frequency of the receiver is f, the maximum impulse frequency of the transmitter is $\frac{f}{2}$. The frame rate of most normal cameras currently on the market is 25 fps. The frame rate of the camera in a high-end smartphone can be 60 fps or higher. However, a high frame rate and a high resolution are mutually restricted. For example, the frame rate of most IP camera is 25 fps at 720p but 15 fps at 1080p. In surveillance for security, there is no tendency to increase the frame rate of IP cameras. Therefore, there is an upper bound on the transmission speed.

The rolling shutter effect in many CMOS cameras can be used to record time-varying information sent from a high impulse frequency LED [25]. This means that the channel's throughput can be greater than the frame rate of the camera. Nevertheless, several hundreds of pixels of LED height are needed to extend the channel throughput. There are only 4 pixels of LED height in a distance of 2.54 m. Therefore, the rolling shutter effect cannot be exploited in our scenario.

E. Covertness

According to the persistence of vision [6], a single slight change of 50 microseconds (ms) is not sensible by human vision. This feature can help us hide turn-off behavior within 40 ms in an LED indicator that is always on. For humans, the maximal fusion frequency is up to 60 Hz at very high illumination intensities [19]. By conducting experiments, we find that a 20 ms turn-off behavior can hardly be observed even the LED is stared at continuously. When the duration of the off state is 20 to 50 ms, a tiny dither in the brightness of LED can be seen during careful observation.

Moreover, the covertnesses of the three LED indicators on the keyboard are different. Normal computer users would suspect something wrong with their computers if they noticed LED indicator turning for no reason, even when they notice a tiny flash in the brightness of an LED. Our only choice is to set the LED indicator to always on to leak data covertly.

Of the three LED indicators, NumLock is always on after Windows has booted on most computers. Therefore, NumLock is most suitable for leaking covert messages, except on computers in the finance department, where the number pads are used all the time. ScrollLock is another suitable key because the function of screen rolling is too old for current OSes. If ScrollLock could remain on after Windows boots, exfiltration would not catch the attention of the user. On the contrary, the function of CapsLock is always used input text messages such as ID number, password etc. Therefore the exfiltration would make user anxious when CapsLock turns on.

F. Comparison with modified OOK

When the impulse frequency is so low that the turn-off behavior can be identified with human vision, it is natural to optimize and to make the behavior less detectable. A normal way is to turn on for a long duration before turning off. Then, the message before modulation can be encoded as shown in Table V.

TABLE V
ENCODING BEFORE OOK

Plain Bit	Codeword
0	0
1	$\underbrace{0\cdots01}_{\lvert\mathrm{Enc}(1)\rvert}$

Then, the channel rate R_{OOK} and the flicker value f_{OOK} can be derived as shown in Equation 7 and Equation 8,

$$R_{\mathrm{OOK}} = \frac{2F}{|\mathrm{Enc}(1)| + 1} \tag{7}$$

$$f_{\mathrm{OOK}} = \frac{1}{|\mathrm{Enc}(1)|} \tag{8}$$

where F is the impulse frequency and $|\mathrm{Enc}(1)|$ is the length of the codeword for the bit '1'.

Additionally, the channel rate $R_{\mathrm{Prop.}}$ and the flicker value $f_{\mathrm{Prop.}}$ with $F_{I_0} = 0$ can be derived as shown in Equation 9 and Equation 10,

$$R_{\mathrm{Prop.}} = F_{I_1} \tag{9}$$

$$f_{\mathrm{Prop.}} = \frac{1}{\frac{2F}{F_{I_1}} - 0.5} \tag{10}$$

A comparison of the flicker values is given in Figure 6 for $F = 25$, as in Sepetnitsky's prototype [35]. The figure shows that the latter flicker values are always lower than those for OOK.

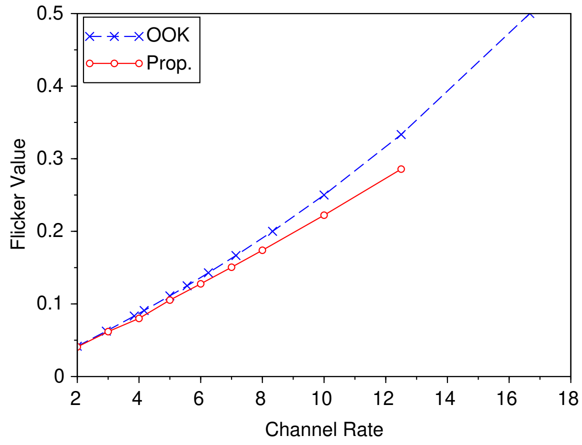

Fig. 6. Flicker Value Comparison with Modified OOK

V. Results and Evaluations

A. Experimental Setting

An open-plan office serves as the experimental environment. This is a common environment for most businesses and research organizations. The keyboard that leaks data is located on the desk of an office cubicle. The IP camera is hanging from the ceiling of the office. A survey of the experimental environment is shown in Figure 7.

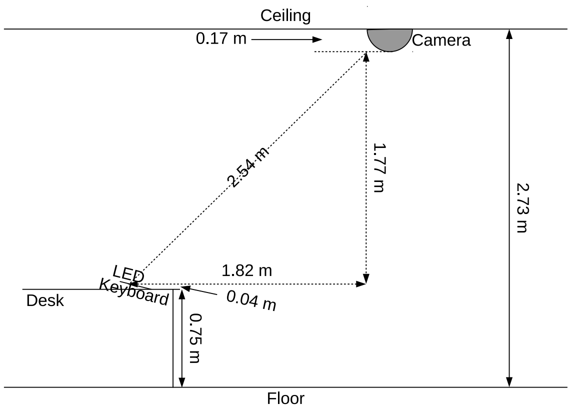

Fig. 7. Survey of the Experimental Environment

The configurations of the personal computer and the IP camera are shown in Table VI and Table VII.

TABLE VI
Configuration of Personal Computer

Module	Configuration
CPU	Intel Core i5-4590 CPU 3.30GHz
Motherboard	ASUS B85-PLUS R2.0
RAM	8GB
Hard Disk	SEAGATE Desktop HDD 500G
Keyboard	Logitech K120 HID USB

TABLE VII
Configuration of IP Camera

Module	Configuration
Resolution	1920×1080 and 640×352
Video Encoding	H264MANINPROFLE, JPEG Snapshot
Wireless Network	IEEE 802.11b/g/n 2.4GHz
Focus	5 times optical zoom, 3.6-12mm
Aperture value	F2.0

In our experiments, $\angle UZX = 6.9474259°$ (the angle between the keyboard surface and the desktop) and $|XA| = 1.77$ m (the vertical distance between the LED and the camera) in Figure 3. A list of emission angles and distances is given in Table VIII. We see that the emission angle increases observably for distances from 2.54 m to 5.08 m. This means that the camera receives a quick drop in brightness when the emission angle increases.

TABLE VIII
Emitting Angles and Distances

	Exp.1	Exp.2	Exp.3	Exp.4
Distance	2.54 m	3.27 m	4.02 m	5.08 m
Angle	38.877°	50.2814°	56.9296°	62.6616°

B. Results

1) Distance, Emission Angle and Brightness: Two graphs relating the distance and the emission angle and the distance and the brightness are made with $y = 1.77$ m (the vertical distance between the LED and the camera), $\beta = 1$ (the constant coefficient in Equation 6) and $|ON| = 1$ (the length of the LED indicator in the direction of change) in Figure 8 and Figure 9. The figure shows that the brightness captured by the camera at a distance of 4 m is only approximately 10% of the brightness at 1.77 m.

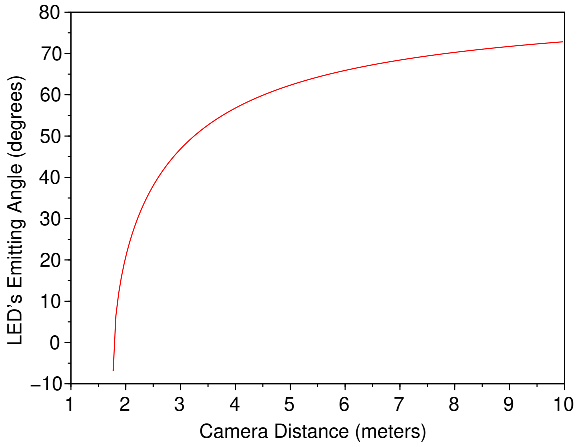

Fig. 8. Relationship between Distance and Emission Angle

2) Bit Error Rate: Several experiments were conducted with different distances and various ambient brightness. The bit error rates (BER) obtained for our covert channel are listed

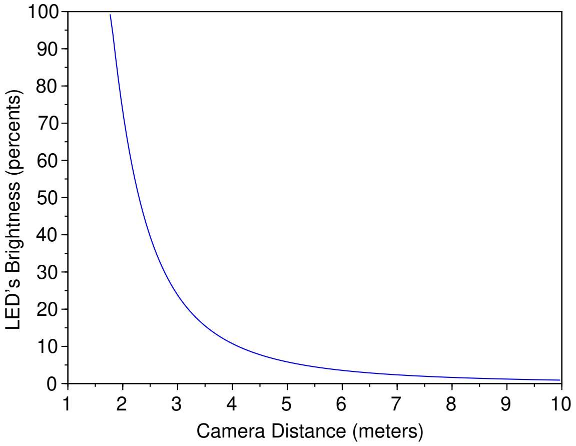

Fig. 9. Relationship between Distance and Brightness

in Table IX. The results show that the BER increases with the distance but does not have a linear relationship with the ambient brightness. When the distance is 2.54 m, the BER is usually less than 10%. When the distance is 3.27 m, the BER is usually less than 25%.

TABLE IX
BIT ERROR RATES(%) WITH DIFFERENT DISTANCES AND VARIOUS AMBIENT BRIGHTNESS

	2.54 m	3.27 m	4.02 m	5.08 m
100 LUX	0.39	3.13	26.17	38.67
200 LUX	15.63	1.95	35.55	37.89
300 LUX	0	27.73	30.08	33.98
400 LUX	0	23.05	26.17	37.11
500 LUX	0	14.06	37.89	33.20
600 LUX	10.16	6.64	33.20	41.41
700 LUX	4.30	10.94	28.13	41.41
800 LUX	0	16.80	24.61	44.92
900 LUX	16.02	10.55	30.08	38.28
1000 LUX	5.47	42.19	30.86	41.41
1100 LUX	1.17	10.55	39.84	42.58
1200 LUX	8.98	23.38	39.84	39.06

C. Evaluation

1) User Perception: To verify the covertness of the channel, we invited 20 students in our laboratory to participate in double-blind experiments. All the participants are between the ages of 22 and 27. They have their best visual sensitivities currently. Meanwhile, all experiments were conducted between 9 am and 10 am when people are most awake during the whole day.

In our experiments, the impulse frequency used to control the LED was 400 Hz. There were 400 LED states per second. We used 20 adjacent states to create one intensity. Therefore, 20 intensities could be simulated per second. The first 5 intensities and the last 5 intensities per second were used to form a smooth intensity sequence. The middle 10 intensities were used to transmit a bit with intensity I_0 or I_1. All the intensities are listed in Table X.

TABLE X
SMOOTH SEQUENCE OF INTENSITY VALUES IN EXPERIMENTS

$I_0 = i_0$	i_1	i_2	i_3	i_4	i_5	i_6	i_7	i_8	$i_9 = I_1$
20	19	19	18	18	17	17	16	16	15

Experiments for each participant were conducted for 5 times. For each time, the computer either transmitted bit string ‘0101010101’ via the LED, or did nothing in 10 seconds. The actions of the computer were recorded on the disk. Therefore, the experimenter did not know the real answers until all the experiments were finished.

Participants observed the intensity fluctuation of the LED indicator and gave scores. Shown in Figure 10, the score is between 0 to 4, where 0 represents that the participant feels no sense of the intensity fluctuation completely and 4 represents that the intensity fluctuation can be seen clearly.

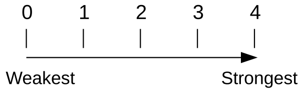

Fig. 10. Perception Scores for Intensity Fluctuation of LED

The average observation distance for the 20 participants was 0.588 m. And the average ambient brightness was 887.75 LUX. The computer had transmitted the bit string for 48 times and had idled for 52 times. The aggregates score for the transmission was 129, and the average score was 2.69; The aggregates score for the idle was 106, and the average score was 2.04. Experimental results show that this form of modulation is difficult to identify using human vision.

2) Throughput: According to the previous analysis, the throughput of the channel is 1 bps to ensure smooth variance between two different bit intensities. Improvement of the throughput is not feasible in practice because human eyes are very sensitive to flickers of 1 Hz to 15 Hz. [2]

3) Upper Bound on the Effective Distance: In Table IX, the BER is greater than 33% while the distance reaches 5 m. According to the channel capacity formula, we know that when the transition probability $p = \frac{1}{3}$, the capacity $C = 1 - H(p) = 0.081704166 < \frac{1}{12}$. That means we need more than 12 bits of data to transmit 1 bit of information correctly. It is impossible to build a reliable channel under such conditions. Additionally, Figure 9 shows that the brightness captured by a camera at a distance of 5 m is only approximately 5.76% of the brightness at 1.77 m. Therefore, 5 m can be considered an upper bound on the effective distance to build a covert channel with the current experimental devices.

VI. DISCUSSION

The cameras on smartphones are currently the most common optical receivers. To study the performance of data exfiltration through an LED, another scenario is proposed: We suppose that in a company with strict management, all employees operate their computers only with keyboards and mice. Exporting data is forbidden by a technical method, such as switching to a read-only CDROM, disabling USB storage devices, locking the configuration of network adapters, or spying on screen contents. Therefore, an employee must build an air-gapped covert channel to export information from the air-gapped network. Now, the role of the employee is that of a malicious insider throughout the security system. Because of the existence of a malicious insider, it is not necessary to compromise an IP camera, and there is no need to circumvent human vision either. The only thing that should be taken into account is the throughput of the covert channel.

Now, the frame rate of a high-end smartphone can be up to 60 fps. According to the Nyquist-Shannon sampling theorem, the throughput of an LED can be 30 bps. Therefore, the flickering of three LEDs can be used directly to form an optical channel with a throughput of 90 bps. Furthermore, exploiting the rolling shutter effect of a CMOS camera [25] can double the throughput to 180 bps with a mirror that clones the LEDs on the different heights of the CMOS sensitive plate.

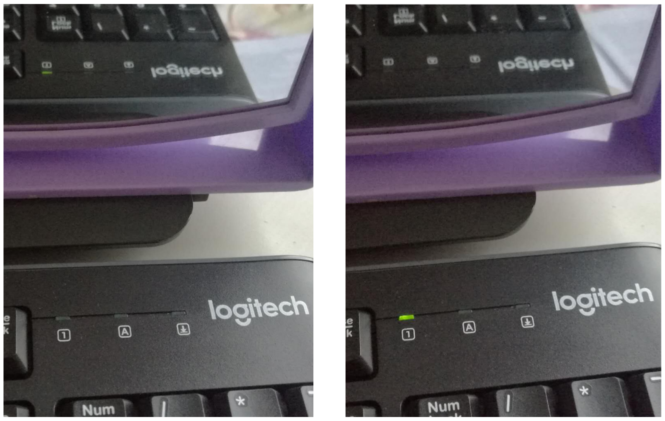

Fig. 11. Rolling Shutter Effect of a CMOS Camera

The rolling shutter effect is shown in Figure 11. The two photographs in the figure look strange because the brightness of the NumLock LED is quite different on either side of the mirror. Because of the delay in every row on CMOS camera's sensitive plate, the status of the LED in the mirror can be obtained much earlier than the status of the real one. Both photos are taken with an exposure of 1/400 second.

VII. Countermeasures

The countermeasures can be divided into two types: procedural countermeasures and technical countermeasures.

Procedural countermeasures involve banning cameras from offices, covering the LEDs, cutting off the LEDs' feet and shielding windows. Any banning policy requires constant supervision to ensure that there are no exceptions. Covering the LEDs or cutting off their feet is easy to do but inconveniences users without any indication. In addition, armored glass is used for walls in many office spaces. A surveillance camera can also receive optical signals through the glass of the windows or walls. Thus, it is necessary to shield them.

Technical countermeasures involve LED status monitoring with software or optical methods and LED status confusion with software. Detecting malware is a common job for security software. Then, an LED status watchdog can be used to identify abuses. One cost is that CPU resources are occupied, which slows down the OS. Detecting the abuse of LEDs using an outside sensor without giving any information to the attacker is a perfect method. This method always obtains a high percentage of success if the hardware meets the necessary conditions. However, the existence of a covert channel is a low probability event. Therefore, it remains difficult to detect this type of attack. We note that only one covert channel can be established at a time. Therefore, we can actively confuse the LED status to avoid the real risk.

The list of all countermeasures is summarized in Table XI.

TABLE XI
Cost and Effect of Countermeasures

Countermeasure	Cost	Effect	Shortcomings
Banning cameras from office	High	Good	Need for supervision
Covering LEDs	Low	Good	Inconvenience to user
Cutting off LEDs' feet	Low	Good	Inconvenience to user
Shielding windows	High	Good	Change surrounding brightness
Monitoring software	Low	Good	Occupy CPU resources
Optical monitoring	High	Normal	Difficult to detect
Status confusing	Low	Good	Occupy CPU resources

VIII. Conclusions

The use of a novel form of signal modulation of status LEDs to build an optical covert channel was proposed in this paper. Using this form of modulation, a Class I LED indicator can leak covert signals with a good chance of avoiding detection by human vision. An attack model was given to build a covert communication channel with a normal IP camera by turning the LED on/off. The existence of this type of covert channel was verified. A potential risk of an unmodulated LED status indicator being used to build a covert channel against the background of the IoT was revealed. Furthermore, the form of modulation and the corresponding demodulation method were designed and optimized. Then, the efficiency and covertness were estimated. The upper bound on the effective distance was obtained through both theoretical calculation and experimental observation. A new scenario involving a smartphone was discussed. Finally, countermeasures were given by considering the conditions necessary for the existence of this type of covert channel.

References

[1] Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Computer Networks*, 54(15):2787 – 2805, 2010.

[2] Peter G. J. Barten. Contrast sensitivity of the human eye and its effects on image quality. *Technische Universiteitndhoven*, 1999.

[3] Davide B Bartolini, Philipp Miedl, and Lothar Thiele. On the capacity of thermal covert channels in multicores. In *Proceedings of the Eleventh European Conference on Computer Systems*, page 24. ACM, 2016.

[4] Louis Columbus. Internet of things market to reach $267b by 2020. https://www.forbes.com/sites/louiscolumbus/2017/01/29/internet-of-things-market-to-reach-267b-by-2020/#39038c66609b, 2017. [Online; accessed 30-September-2017].

[5] Gustav Theodor Fechner, Helmut E Adler, Davis H Howes, and Edwin Garrigues Boring. Elements of psychophysics. *Psychological Bulletin*, 1966.

[6] E. Bruce Goldstein. *Cognitive Psychology: Connecting Mind, Research and Everyday Experience*. Wadsworth Cengage Learning, 2007.

[7] Alexander Gostev. Agent.btz: a source of inspiration? https://securelist.com/agent-btz-a-source-of-inspiration/58551/, 2014. [Online; accessed 9-Apirl-2018].

[8] GReAT. A fanny equation: I am your father, stuxnet. https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/, 2015. [Online; accessed 9-Apirl-2018].

[9] Mordechai Guri, Ofer Hasson, Gabi Kedma, and Yuval Elovici. An optical covert-channel to leak data through an air-gap. In *Privacy, Security and Trust*, 2016.

[10] Mordechai Guri, Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Yuval Elovici. Gsmem: data exfiltration from air-gapped computers over gsm frequencies. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 849–864, 2015.

[11] Mordechai Guri, Gabi Kedma, Assaf Kachlon, and Yuval Elovici. Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies. In *2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*, pages 58–67. IEEE, 2014.

[12] Mordechai Guri, Matan Monitz, and Yuval Elovici. Usbee: Air-gap covert-channel via electromagnetic emission from usb. In *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, pages 264–268. IEEE, 2016.

[13] Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici. Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations. In *IEEE 28th Computer Security Foundations Symposium (CSF), 2015*, pages 276–289. IEEE, 2015.

[14] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici. Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers. *arXiv preprint arXiv:1606.05915*, 2016.

[15] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici. *Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise ('DiskFiltration')*, pages 98–115. Springer International Publishing, Cham, 2017.

[16] Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici. xled: Covert data exfiltration from air-gapped networks via router leds. *arXiv preprint arXiv:1706.01140*, 2017.

[17] Mordechai Guri, Boris Zadov, and Yuval Elovici. *LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED*, pages 161–184. Springer International Publishing, Cham, 2017.

[18] Michael Hanspach and Michael Goetz. On covert acoustical mesh networks in air. *Journal of Communications*, 8(11):758–767, 2013.

[19] S Hecht and S Shlaer. Intermittent stimulation by light : V. the relation between intensity and critical frequency for different parts of the spectrum. *Journal of General Physiology*, 19(6):965, 1936.

[20] Markus G Kuhn and Ross J Anderson. Soft tempest: Hidden data transmission using electromagnetic emanations. In *International Workshop on Information Hiding*, pages 124–142. Springer, 1998.

[21] David Kushner. The real story of stuxnet. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet, 2013. [Online; accessed 9-Apirl-2018].

[22] Vladimir Kuskov, Mikhail Kuzin, Yaroslav Shmelev, Denis Makrushin, and Igor Grachev. Honeypots and the internet of things. https://securelist.com/honeypots-and-the-internet-of-things/78751/, 2017. [Online; accessed 30-September-2017].

[23] Butler W. Lampson. A note on the confinement problem. *Commun. ACM*, 16(10):613–615, October 1973.

[24] Eunchong Lee, Hyunsoo Kim, and Ji Won Yoon. Various threat models to circumvent air-gapped systems for preventing network attack. In *International Workshop on Information Security Applications(WISA)*, pages 187–199. Springer, 2015.

[25] Hui Yu Lee, Hao Min Lin, Yu Lin Wei, Hsin I Wu, Hsin Mu Tsai, and Ching Ju Lin. Rollinglight: Enabling line-of-sight light-to-camera communications. In *International Conference on Mobile Systems, Applications, and Services*, pages 167–180, 2015.

[26] X. Lei, X. Jiang, and C. Wang. Design and implementation of a real-time video stream analysis system based on ffmpeg. In *2013 Fourth World Congress on Software Engineering*, pages 212–216, Dec 2013.

[27] Arthur Costa Lopes and Diego F Aranha. Platform-agnostic low-intrusion optical data exfiltration. In *International Conference on Information Systems Security & Privacy(ICISSP)*, pages 474–480, 2017.

[28] Joe Loughry and David A. Umphress. Information leakage from optical emanations. *ACM Trans. Inf. Syst. Secur.*, 5(3):262–289, August 2002.

[29] Ramya Jayaram Masti, Devendra Rai, Aanjhan Ranganathan, Christian Müller, Lothar Thiele, and Srdjan Capkun. Thermal covert channels on multi-core platforms. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 865–880, 2015.

[30] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser. Covert channels using mobile device's magnetic field sensors. In *Asia and South Pacific Design Automation Conference*, pages 525–532, 2016.

[31] Y. Mirsky, M. Guri, and Y. Elovici. Hvacker: Bridging the air-gap by manipulating the environment temperature. *Magdeburger Journal zur Sicherheitsforschung*, 14:815–829, August 2017. Retrieved August 18, 2017.

[32] Samuel Joseph OMalley and Kim-Kwang Raymond Choo. Bridging the air gap: Inaudible data exfiltration by insiders. 2014.

[33] E. F. Schubert. *Light-Emitting Diodes*. Cambridge University Press, 2003.

[34] Mirko Selber and Prof Dr Lothar Thiele. Uncovert3: Covert channel attacks on commercial multicore systems. 2017.

[35] V. Sepetnitsky, M. Guri, and Y. Elovici. Exfiltration of information from air-gapped machines using monitor's led indicator. In *2014 IEEE Joint Intelligence and Security Informatics Conference*, pages 264–267, Sept 2014.

[36] Adi Shamir. Light-based printer attack overcomes air-gapped computer security. https://www.scmagazineuk.com/light-based-printer-attack-overcomes-air-gapped-computer-security/article/541140/, 2014. UK, SG SC Magazine,[Online; accessed 18-September-2017].

[37] Statista. Internet of things - number of connected devices worldwide 2015-2025. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, 2016. [Online; accessed 30-September-2017].

[38] Joint Video Team. Draft itu-t recommendation and final draft international standard of joint video specification. 2013.

[39] Luca Urciuoli, Toni Mnnist, Juha Hintsa, and Tamanna Khan. Supply chain cyber security potential threats. 29:51–68, 2013.

[40] S. Zander, G. Armitage, and P. Branch. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys Tutorials*, 9(3):44–57, Third 2007.

[41] L. Zhang, S. Ruan, M. Zhang, and C. Liu. Method of video capture port design for ip camera. In *Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series*, volume 6357 of *procspie*, page 63573R, nov 2006.

Zheng Zhou received his B.S. degree and M.S. degree in 2001 and 2007 respectively from Information Engineering University, Zhengzhou, China. He is now pursuing the Ph.D. degree in University of Science and Technology of China. His research interests include steganography, covert channels and cyberspace security.

Weiming Zhang received his M.S. degree and Ph.D. degree in 2002 and 2005 respectively from Information Engineering University, Zhengzhou, China. Currently, he is a professor with University of Science and Technology of China. His research interests include multimedia security, information hiding, and privacy protection.

Zichong Yang received his B.S. degree in 2014 from University of Electronic Science and Technology of China, Chengdu, China. He is now pursuing the M.S. degree in University of Science and Technology of China. His research interests include network security and steganography.

Nenghai Yu received his B.S. degree in 1987 from Nanjing University of Posts and Telecommunications, M.E. degree in 1992 from Tsinghua University and Ph.D. degree in 2004 from University of Science and Technology of China, where he is currently a professor. His research interests include multimedia security, multimedia information retrieval, video processing, information hiding and security, privacy and reliability in cloud computing.