Covert Data Exfiltration Using Light and Power Channels

Patrick Cronin, Charles Gouert, Dimitris Mouris, Nektarios Georgios Tsoutsos, Chengmo Yang
Department of Electrical and Computer Engineering, University of Delaware
{ptrick, cgouert, jimouris, tsoutsos, chengmo}@udel.edu

***Abstract*—As the Internet of Things (IoT) continues to expand into every facet of our daily lives, security researchers have warned of its myriad security risks. While denial-of-service attacks and privacy violations have been at the forefront of research, covert channel communications remain an important concern. Utilizing a Bluetooth controlled light bulb, we demonstrate three separate covert channels, consisting of current utilization, luminosity and hue. To study the effectiveness of these channels, we implement exfiltration attacks using standard off-the-shelf smart bulbs and RGB LEDs at ranges of up to 160 feet. We analyze the identified channels for throughput, generality and stealthiness, and report transmission speeds of up to 832 bps.**

I. Introduction

For as long as companies have developed proprietary technologies, there have been attackers working to steal that information for financial gain. With the advent of the Internet, corporations were soon besieged by cyber attacks that grew more sophisticated by the day. Moving swiftly to counter such blatant attacks, many companies reinforced their networks and data handling techniques by employing advanced cryptographic methods such as homomorphic encryption [1]. Recent work [2] has shown the ability to run a variety of algorithms on encrypted data, making it much harder for malicious actors to steal data through conventional means [3].

One widely accepted solution to enhance information security is to create self-contained "air-gapped" networks for company data. These networks are separated from the Internet, based on the assumption that adversaries cannot infect a system if they cannot connect to it. As a response to these enhanced countermeasures, attackers have moved to more sophisticated *covert-channel* attacks (e.g., [4]–[6]) where they exfiltrate data over non-conventional channels that are not meant for communication, such as the radio frequency signals emanating from USB drives [7]. The authors in [8] develop malware to exfiltrate data through hard drive activity LEDs using a photodiode and an oscilloscope. Another work exploits an infrared covert channel by implanting an air-gapped computer's keyboard with an infrared module [9].

Recently "smart" products, such as wirelessly-controlled light bulbs, appeared on the market promising automated scheduling and easier building management. Eager to improve the efficiency of their operations, companies and building managers began to adopt these IoT technologies. Nevertheless, as demonstrated in [10], these smart light bulbs could be misused by attackers and could be utilized to covertly send information over long distances via imperceptible modulations of the brightness of light. Sadly, as IoT devices become more prevalent, their security continues to be minimal and attackers continue to exploit them in greater and greater numbers [11].

In this paper, we demonstrate three covert channel strategies for smart light bulbs and analyze their throughput, stealthiness and generality. The three covert exfiltration techniques explored in this paper are summarized below:

- **Light Brightness Modulation:** We modulate and monitor the luminosity of a bulb with a photodiode, encoding logical signals as visibly undetectable brightness changes.
- **Light Color Modulation:** We leverage the color settings of a smart bulb to transmit logical signals via imperceptible color changes. The different color channels (RGB – red, green, blue) can be combined to enhance transmission speed and redundancy.
- **Light Power Consumption:** We modulate the power utilization of a bulb and monitor the circuit current changes in order to exfiltrate a signal.

To increase stealthiness and mitigate timing issues within the covert channels, we employ Manchester encoding [12]. For our demonstration, we use a low power, portable system that can be generically applied to a variety of situations.

The rest of the paper is organized as follows: in Section II we offer a preliminary discussion on threat model, color sensor properties and encoding issues, while in Section III we present our exfiltration methodology, followed by our evaluation in Section IV. Related work is discussed in Section V and our concluding remarks are summarized in Section VI.

II. Preliminaries

This section introduces the threat model and discusses the various components of our exfiltration methodology.

A. Threat Model

A *covert channel* introduces a method of data transfer between two parties (typically a malicious insider and a malicious outsider) over a medium that is not meant for communication. The covert channel attacks demonstrated in this paper are applicable when an attacker is interested in exfiltrating data out of a building, but security policies prevent standard ways of communication with the outside world. Two of the three proposed techniques assume that the attacks could take place in plain sight without being detected, with the

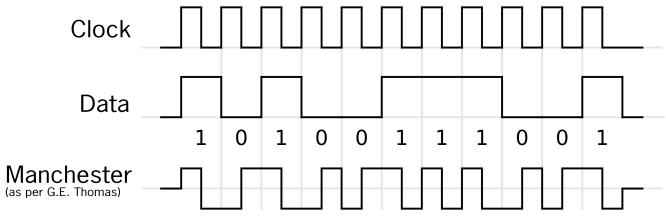

Fig. 1. Manchester Encoding

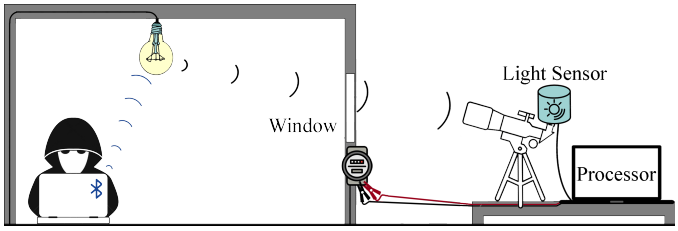

Fig. 2. Overview of our attack environment.

limitation that the attacker has direct sight of a vulnerable light bulb (e.g., from a window). The third attack is meant to take place in a private environment, such as an access-controlled server room, that is devoid of any human presence at the time that the attack is executed. In this case, we assume that the room containing the bulb consists of an electric circuit that is controlled by an external electrical panel.

B. Color Sensors

A color sensor must be employed in order to receive information encoded in small and visually imperceptible changes in hue or luminosity of a smart light bulb. Generally, color sensors use photodiodes to detect light and output current values corresponding to the amount of light detected, which is ultimately fed into an analog-to-digital converter. This converter generates digital codes (e.g., 0 to 255 values) which are determined by the color and intensity of the light with brighter values being represented by higher digital codes. In addition to converting the current values from the photodiode to digital codes, color sensors also employ the notion of *integration time*. This is utilized to allow the sensor to detect very dim light sources where, to generate accurate readings, the sensor must measure the current output of the photodiode for a longer period of time.

C. Manchester Encoding and Timing Issues

The exfiltration channels discussed in this paper rely on a form of encoding known as *Manchester encoding* [12]. In this encoding scheme, every data bit is represented as a logic level transition (e.g., a low to high edge) at the center of each bit period; thus, Manchester encoding requires twice the throughput of conventional data encoding schemes. As depicted in Fig. 1, a low bit is encoded as a transition from low to high, while a high bit is the opposite. This encoding scheme works well for channels that must remain *covert*, as the transitions in the center of the bit period allow the scheme to encode the clock signal along with the data. This requirement is necessary as IoT devices may utilize buffers and low-power microcontrollers to handle communications without real-time guarantees, and thus commands can experience varying and considerable latency, which justifies the need for a self-clocked encoding scheme. Furthermore, if an optical channel is to remain covert, it must be imperceptible to the eye. Indeed, optical channels employ some form of hue or brightness modulation, so a data stream that contains even a few repeated bits may cause the light to stay at a low or high state for an extended period of time, allowing for a noticeable flicker. Manchester encoding, which requires transitions in each bit period, mitigates this issue by guaranteeing that the channel will never remain at one level for too long.

III. Covert Data Exfiltration

We propose three methods of exfiltrating data using smart light bulbs: luminosity, color/hue modulation, and power consumption. An overview of the environment of the three proposed covert channels is illustrated in Fig. 2.

A. Optical Covert Channels

1) Light Brightness Modulation (Luminosity): This attack varies the luminosity of white light by an amount that is imperceptible to the human eye, but can be detected by a color sensor. The marginally brighter and dimmer values are used to represent binary logical levels. An attacker can utilize a compromised device to connect to the smart bulb and quickly vary the luminosity between these values to transmit a message in binary. A color sensor pointed at the bulb can discern the difference between the values, allowing it to decode a message.

2) Light Color Modulation (Hue): Another method to exfiltrate data entails changing the RGB values of the color LEDs inside a smart bulb. It is possible to vary the hue between multiple different values such that the variations are imperceptible. Contrary to the luminosity modulation attack, an RGB light bulb has the ability to vary *up to three color channels* to implement the attack. In our implementation, we utilize both the red and the blue color channels of our smart bulb, while keeping the green at full brightness. This helps to not only disguise the attack but also relieve interference, as the red and blue detectors in a low cost photosensor overlap with the green channel. In fact, using the red and blue channels of our sensor, we are able to decode four different levels per color. Thus, each channel can send two bits per clock period for a total of four bits at once.

B. Power Consumption Covert Channel

Another attack vector incorporates current sensors attached to the electrical circuit on which the smart bulb resides. We assume that the circuit controlling the bulb is connected to an external electrical panel that an attacker has access to. The attacker can then observe modulations to the brightness of the light via the current sensors on the circuit. As most smart bulbs are designed to consume low power (and therefore utilize minimal current), the bulb must undergo larger brightness changes to create visible current fluctuations. Thus, this

channel assumes that the smart bulb resides in an unoccupied room, such as a server room or utility closet. The current value measured when the bulb is powered on and off is assigned to a logical high and a logical low, respectively.

C. Overcoming Timing and Drifting Challenges

Since most smart bulbs utilize some form of Bluetooth or WiFi control system, a communication protocol stack is implemented internally. Such protocols, however, introduce variable latencies so that it is not always possible to ensure that the covert channel will maintain a steady clock rate. To mitigate such clock drifting issues, we encode our signals with Manchester encoding. Specifically, each of the presented channels requires encoding data bits into a form of light or current level. Due to the nature of these covert channels, an attacker would typically not be able to test and synchronize the sender and receiver in the exact conditions under which the attack will take place. As a result, the attacker cannot know the light level or current utilization levels *a priori*, so the decoding method must be able to dynamically adjust the receiver and remove baseline effects from the channel. Notably, Manchester encoding, and its required switching between high and low values in every bit period, provides ample and continuous samples of the high and low values of the channel, allowing dynamic adjustment of the receiver to minimize error rates. Thus, in the interest of increasing the *generality* of these channels, employing Manchester encoding ensures that the receivers can adapt to variable timing and ambient condition changes while avoiding unintentional light flicker.

IV. Experimental Evaluation

A. Experimental Setup

Data Transmitters: The data transmitters utilized in this work are smart LED bulbs that connect with peripheral controllers using wireless communication standards, such as Wi-Fi, Bluetooth Low Energy (BLE) [13], and ZigBee [14]. To implement the sending end of the three covert channels, we obtained a Magic Blue light bulb, RGB LEDs, and a Teensy 3.2 microcontroller board. We investigated two different scenarios: (a) controlling a smartbulb using BLE, and (b) controlling RGB LEDs using the general purpose input/output (GPIO) pins on the Teensy.

Data Receivers: On the receiving side of the first two channels we used a TCS3472 light-to-digital sensor, which can detect subtle changes in light color and intensity, and an additional Teensy 3.6 microcontroller board to decode the covert signals. The recovered data is output as ASCII text. To further increase the range of our channels, we attached the TCS3472 light sensor to a 70mm Telmu telescope pointed at the light bulb. Moreover, we were able to increase the channel effectiveness by leaving the telescope unfocused: If the telescope is properly focused, the bulb would take up a relatively small area of the telescope's field of view, making it difficult for the sensor to discern color differences between the background and the bulb. Conversely, with an unfocused telescope, the bulb light covers more of the field of view so that our sensor was able to discern color changes more accurately. Finally, to implement our power consumption attack, we used two YHDC split-core current transformers that are accurate to ± 1 percent.

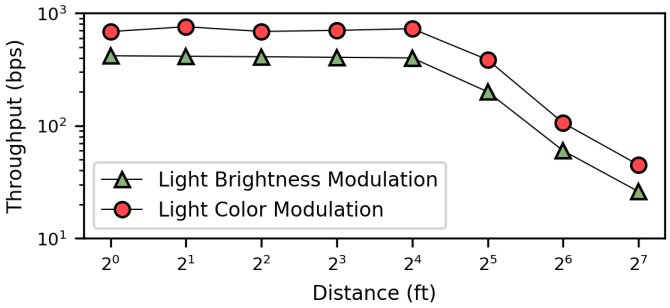

Fig. 3. Throughput of the luminosity and hue covert channels using RGB LEDs and 10W LED array connected to Teensy GPIO pins.

B. Experimental Results

1) Magic Blue Smart Bulb: To evaluate our method in a realistic situation, the Magic Blue smart bulb was tested for all three channels. In both the brightness and hue modulation channels, the Magic Blue achieved data rates of up to 20 bps at close range and about 5 bps at ranges up to 75 feet. The relatively small transmission rate was in attributed to the control stack of the Magic Blue, which begins to drop control packets once more than 40 packets are sent per second. At long ranges, the integration time of the color sensor has to be increased such that it can discern changes in the relatively dim 4.5W Magic Blue bulb. This increase in integration time lowers the data rate to 5 bps.

With regards to the current modulation channel, we were able to achieve data rates of up to 20 bps, demonstrating that current utilization of the smart bulb can effectively encode information. Although the power consumption of a single light bulb is not significant, it is highly possible that the isolated room would have more than just one bulb and therefore the consumption would be perceived by our sensors. Same as before, the control stack of the bulb is the limiting factor of the date rate.

2) Maximum Throughput Experiments: To better examine the capabilities of the proposed covert channels, two more data transmitters are tested. The first is a group of RGB LEDs connected directly to a Teensy microcontroller board. These LEDs could be varied at rates approaching 1KHz, which removes the aforementioned control stack throughput limitation. The second transmitter uses a 10W 3-by-3 LED array that allows testing our brightness modulation scheme at longer ranges. Table I summarizes the maximum data rates.

In testing the RGB LEDs directly connected to the microcontroller, we confirmed that it is possible to vary the red and blue channels simultaneously, allowing for the creation of two parallel channels. While red and blue can also be varied simultaneously on the Magic Blue, the plastic diffuser of the bulb does not fully blend these colors, so the dual channel approach is not possible with that bulb. Furthermore, as it is possible to vary the microcontroller LEDs faster,

TABLE I
MAXIMUM BIT-RATE AND DISTANCE FOR THE THREE CHANNELS USING BOTH THE MAGIC BLUE SMART BULB AND THE LEDS.

Covert Channel	Maximum Bit-rate		Maximum Distance	
	Light-bulb	LEDs	Light-bulb	LEDs
Luminosity	20 bps.	416 bps.	75 ft.	160 ft.
Hue	20 bps.	832 bps.	75 ft.	160 ft.
Power	20 bps.	N/A	N/A	N/A

we can generate four levels on each channel without them being perceptible, which effectively allows the transmission of 4 bits per clock period. Recall that Manchester encoding requires up to two level transitions per bit transmission, so the effective data rates are halved. In our experiments, we observed maximum transmission rates of 832 bps.

A similar result is achieved in experiments with the 10W LED array. By avoiding the control rate limitations of the Magic Blue bulb, it is possible to vary the array between 4 values imperceptibly, thus transmitting 2 bits at a time. In this case, we observe maximum transmission rates of 416 bps.

Fig. 3 illustrates the relationship between distance and data rate. As the telescope moves farther from the bulb, the corresponding field of view increases and the brightness perceived by the color sensor decreases. This necessitates an increase of the sensor integration time, which decreases the maximum observable transition rate. Overall, we are able to achieve covert data exfiltration of 52 bps at a distance of 160 feet.

V. RELATED WORK

Carrara and Adams performed experiments with acoustic covert channels in air-gapped networks achieving a covert ultrasonic attack with a bit rate of 230 bps at a distance of up to 11 meters [15]. Our proposed system can achieve higher data rates, and can be executed at much farther distances. The authors of [4] present an undetectable optical covert channel that uses LCD screens by embedding data within images. A thermal covert channel called BitWhisper is proposed in [16], which allows data to be exfiltrated from one computer to another; this channel has a data rate of only 1-8 bits per hour and both computers must be positioned close together.

In [17], Guri at al. present a covert channel between a smart phone with an FM radio receiver and a computer infected with malware. In this case, the computer produces FM signals using electromagnetic radiation from the video display adapter. This approach is able to achieve a data rate of up to 60 bits per second, but the phone must be positioned within 1-7 meters of the infected computer. Another work exploits an infrared covert channel by implanting an air-gapped computer's keyboard with an infrared module, achieving up to 2.62 bits per second [9]. Finally, the covert channel in [8] can exfiltrate data using the hard disk drive activity LEDs at speeds of up to 4000 bits per second via on/off keying; however, such on/off keying of the drive LED is easily detectable by humans.

VI. CONCLUSION

We have proposed and tested three covert methods of exfiltrating data using smart light bulbs and LEDs, including color and brightness modulation, and current measurement. To ensure data recovery and overcome potential protocol latencies, our approach employs Manchester encoding. We are able to achieve a maximum bit rate of 832 bps with a covert channel based on light hue at relatively close distances, and maintain transmission rates of up to 52 bps at a distance of 160 feet.

ACKNOWLEDGMENTS

This work was partially supported by the NSF CNS-1513130 and the ONR N00014-18-1-2886 grants.

REFERENCES

[1] N. G. Tsoutsos and M. Maniatakos, "The HEROIC framework: Encrypted computation without shared keys," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 875–888, 2015.

[2] D. Mouris, N. G. Tsoutsos, and M. Maniatakos, "TERMinator Suite: Benchmarking privacy-preserving architectures," *IEEE Computer Architecture Letters*, vol. 17, no. 2, pp. 122–125, 2018.

[3] N. G. Tsoutsos, C. Konstantinou, and M. Maniatakos, "Advanced techniques for designing stealthy hardware Trojans," in *Proceedings of the 51st Annual Design Automation Conference*. ACM, 2014, pp. 1–4.

[4] M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "An optical covert-channel to leak data through an air-gap," in *Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 642–649.

[5] A. Giani, V. H. Berk, and G. V. Cybenko, "Data exfiltration and covert channels," in *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V*, vol. 6201. International Society for Optics and Photonics, 2006, p. 620103.

[6] P. Cronin and C. Yang, "A Fetching Tale: Covert Communication with the Hardware Prefetcher," in *IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*, 2019, pp. 101–110.

[7] M. Guri, M. Monitz, and Y. Elovici, "USBee: air-gap covert-channel via electromagnetic emission from USB," in *Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 264–268.

[8] M. Guri, B. Zadov, E. Atias, and Y. Elovici, "LED-it-GO: Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED," *ArXiv e-print 1702.06715*, Feb. 2017.

[9] Z. Zhou, W. Zhang, and N. Yu, "IREXF: Data Exfiltration from Air-gapped Networks by Infrared Remote Control Signals," *ArXiv e-prints*, Jan. 2018.

[10] E. Ronen and A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights," in *IEEE European Symposium on Security and Privacy (EuroS&P)*, March 2016, pp. 3–12.

[11] Z. Doffman, "Cyberattacks On IoT Devices Surge 300% In 2019, 'Measured In Billions'," Sep 2019. [Online]. Available: www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/

[12] V. Lalitha and S. Kathiravan, "A Review of Manchester, Miller, and FM0 Encoding Techniques," *Smart Computing Review*, vol. 4, no. 6, pp. 481–490, Dec 2014.

[13] C. Gomez, J. Oller, and J. Paradells, "Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology," *Sensors*, vol. 12, no. 9, pp. 11 734–11 753, 2012.

[14] P. Kinney *et al.*, "Zigbee technology: Wireless control that simply works," in *Communications Design Conference*, vol. 2, 2003, pp. 1–7.

[15] B. Carrara and C. Adams, "On acoustic covert channels between air-gapped systems," in *Foundations and Practice of Security*, F. Cuppens, J. Garcia-Alfaro, N. Zincir Heywood, and P. W. L. Fong, Eds. Cham: Springer International Publishing, 2015, pp. 3–16.

[16] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "BitWhisper: Covert Signaling Channel between Air-Gapped Computers Using Thermal Manipulations," in *IEEE Computer Security Foundations Symposium*, July 2015, pp. 276–289.

[17] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *International Conference on Malicious and Unwanted Software: The Americas (MALWARE)*. IEEE, Oct 2014, pp. 58–67.