SmartLED: Smartphone-based covert channels leveraging the notification LED

Lorena Gonzalez-Manzano
Computer Security Lab (COSEC)
Universidad Carlos III de Madrid
Spain
lgmanzan@inf.uc3m.es

Sergio Bernardez
Computer Security Lab (COSEC)
Universidad Carlos III de Madrid
Spain
sergio.bernardez@alumnos.uc3m.es

Jose M. de Fuentes
Computer Security Lab (COSEC)
Universidad Carlos III de Madrid
Spain
jfuentes@inf.uc3m.es

***Abstract*—The widespread adoption of smartphones make them essential in daily routines. Thus, they can be used to create a covert channel without raising suspicions. To avoid detection, networkless communications are preferred. In this paper, we propose SmartLED, a mechanism to build covert channels leveraging a widely available smartphone feature – its notification LED. The secret is encoded through LED blinks using Manhattan encoding. SmartLED is assessed in real-world indoor and outdoor scenarios, considering different distances up to 5 meters. Our results show that the best performance is achieved in dark settings – 34.8 s. are needed to exfiltrate a 7-byte password to a distance of 1 m. Remarkably, distance does not cause a great impact on effective transmission time and shorter blinks do not lead to substantially greater transmission errors.**

***Index Terms*—Smartphone, Covert communication, Covert channel, Notification LED**

I. Introduction

Smartphones are rocketing in the last years, reaching a total amount of 3.8 billion worldwide[1]. They serve as a means of communication with other parties, as well as for storing personal information (e.g., pictures, videos, contacts, etc.).

Their permanent, expected presence in all environments make them attractive in order to establish communications that should remain unnoticed. This kind of channels are typically referred to as *covert channels*, and have been extensively researched. A plethora of alternatives exist to build this kind of channels, being the uncommon use of network protocols one of their first examples [1]. Indeed, covert channels are typically used for data exfiltration in well-known threats, such as advanced persistent threats [2].

In the last years, a particular type of covert channels has attracted substantial attention. In essential infrastructures and other corporate environments with highly sensitive information, it is common to have air-gapped systems, that is, computing devices with no network connection. As a result, a great amount of networkless covert channels have been proposed (e.g., [3], [4]).

Given the widespread adoption of smartphones, in this paper we focus on this type of devices for data exfiltration. Indeed, they have already been applied for this purpose in different ways, such as by producing inaudible sounds [5] or vibrations [6]. However, to the best of authors knowledge, no visual covert channel has been built with smartphones.

To address this matter, in this paper we propose SmartLED, a mechanism that uses the notification LED to build a networkless covert channel. This component is already present in most current models, as it visually shows the existence of messages or events that require the user attention. Therefore, it can be used to convey a given secret to an observer. For the sake of illustration, SmartLED may help on exfiltrating sensitive data (e.g., passwords) stored in the smartphone, either intentionally (e.g., disloyal employees) or as a result of an attack (e.g., after infection with a piece of malware).

Since it requires both parties remain in line of sight, a number of associated research questions are devised:

RQ1 Is the notification LED effective for building a covert channel?
RQ2 Is information retrieved affected by the distance to the observer?
RQ3 Is it possible to characterize the impact of the light environmental conditions in the effectiveness?

To address these questions, the contributions of this paper are as follows:

1 We propose SmartLED, a mechanism that leverages the notification LED of a smartphone to build a covert channel.
2 We assess the effectiveness of the channel under different ambient light conditions and observer distances.
3 We release an open-source prototype implementation to foster further research in this direction.

This paper is structured as follows: Related works are introduced in Section II. Section III describes SmartLED, whereas Section IV focuses on its assessment. The countermeasures against the proposed mechanism and its enhancements are discussed in Section V. Finally, Section VI concludes the paper and points out future research directions.

II. Related work

Covert channels are a well-known research topic which has been significantly studied. Their use in networks protocols was one common application [7] and they have been specially applied in air-gapped computers, that is devices isolated from

[1]https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ , last access July 2020

public or insecure networks. In this vein, a wide array of approaches have been proposed – [8] presents a malware to exfiltrate data through cellular GSM frequencies; [9] through the blinking pattern of keyboard LEDs; [3] through electric emissions on power lines; [4] through the magnetic fields of computers, using a smartphone to receive the covert signals with its magnetic sensor; [10] through the speakers of a computer considering acoustic signals emitted from its hard drive; [11] through the LED of a computer hard drive; [12] through blinking infrarred LEDs of computer devices; [13] through LEDs located in network equipments such as switches or routers; [6] through vibrations by controlling the fan speed of a computer; and [14] through the turn of power supplies into speakers by manipulating their internal switching frequency. With the same purpose but not focusing on air-gapped devices, [15] proposes the use of electromagnetic signals as a covert channel between a laptop and a smartphone.

However, with the advent of Internet of things (IoT) devices, new approaches appear. For instance, [16] presents a covert channel based on the generation of sound waves imperceptible to human ears to send information to neighbor sensor nodes used for IoT applications. In terms of smartphones, [5] uses Android device speakers to produce an ultrasonic sound that can be retrieved by the microphone of a device with too high frequency for humans. Also in Android, [17] uses a pair of apps to generate an ultrasonic communications bridge in which the the source application has access to the data, the speakers and the local sensor package to send such data. [18] proposes a pair of applications as well – one in the form of a game to modify the status of the system, e.g. motion sensors, by inducing the user to change it voluntarily, and the other one to read performed changes. In [19] an adversary model for data exfiltration in Android devices is proposed. A pair of proof of concepts show the possibility of exfiltrating data through SMS and inaudible audio transmission. Moreover, in [20] the celullar voice stream is used as a new set of covert channel in smartphones. By contrast, in [21] a covert channel applies the reflection of signals from the target device. The impedance of a device's wireless network interface card is controlled to covertly leak sensitive information.

Table I depicts a comparison of related works, analysing the sender, which is the device used to build the covert channel, the receiver and features applied for data transmission. Moreover, for the interest of this paper, the types of light conditions (for visual covert channels) and experimental distances are also specified. Most approaches use computers as sender devices, while five of them apply smartphones [5], [17]–[20] and [21] mobile nodes. By contrast, mobile devices are common receivers, being specially frequent the use of cameras for receiving information from LEDs. Indeed, the LED of assorted devices, like keyboads [9] or routers [13], has been considered for data transmission in covert channels. As a matter of fact, when the LED is the component at stake to build the covert channel, just [11] points out that the system is affected by light conditions specially considering night and daylight. In terms of distances, evaluating systems at different distances in meters is a common practice and when considering long distances, like in [8], a dedicated equipment is applied. However, [11] points out that the computer LED was identified at 20 meters at night but without specifying the type of receiver or given details in this regard. Thus, SmartLED is the first proposal in which the sender is a smartphone using the notification LED as the covert channel feature and in which a comparative analysis of the effects of light conditions is carried out at different distances.

Table I
RELATED WORK

	Sender device	**Receiver device**	**Cover channel feature**	**Light conditions**	**Distance**
[8]	Computer	Mobile phone (not smartphone)	Electromagnetic GSM signals	n/a	1-5.5 m. or +30 m. with dedicated equipment
[3]	Computer, server, IoT device representation (Raspberry Pi 3)	Probe connected to a computer	CPU power consumption	n/a	n/a
[4]	Computer	Smartphone	Magnetic signals	n/a	0-12 cm.
[10]	Computer	Device with audio recording capabilities	Speakers	n/a	1-2 m.
[6]	Computer	Smartphone	Vibrations	n/a	10-160 cm.
[14]	Computer	Moble phone (or smartphone)	Power supplies	n/a	0-2.5 m.
[19]	Smartphone	Computer, server	SMS, inauditable audio	n/a	0.1-6.1 m.
[5]	Smartphone	-	Ultrasonic sound	n/a	6-30 m.
[17]	Smartphone	Smartphone	Ultrasonic bridge between mobile apps	n/a	n/a
[20]	Smartphone	Smartphone	Cellular voice channel	n/a	-
[18]	Smartphone	Smartphone	Game app	n/a	n/a
[15]	Computer	Smartphone	Electromag. signals	n/a	0-14 cm
[21]	Mobile device	Computer	Impedance of a device's wireless network interface card (NIC)	n/a	0.4-2 m.
[16]	Mobile nodes	Mobile nodes	Sound waves imperceptible to human ears	n/a	-
[9]	Computer	Security camera, smartphone	Keyboard LED	Not considered	0-9.5 m.
[11]	Computer	Camera (e.g. drone, security camera…)	Hard drive LED	Night and daylight*	20 m. at night and 3 m., 4 m. and 5 m. in a room in daylight
[12]	Computer	Camera (e.g. smartphone, security camera,…)	Infrarred LEDs	Not considered	1 m.
[13]	Router	Camera/ Optical sensor	Router LED	Not considered	-
SmartLED	**Smartphone**	**Camera (e.g. smartphone)**	**Notification LED**	**Indoor: Darkness / dim light / bright light. Outdoors**	**0.2 m., 1 m., 2 m., 3 m., 5 m.**

* briefly mentioned

III. SMARTLED DESCRIPTION

This Section introduces the proposed mechanism, dubbed SmartLED. For this purpose, Section III-A provides with

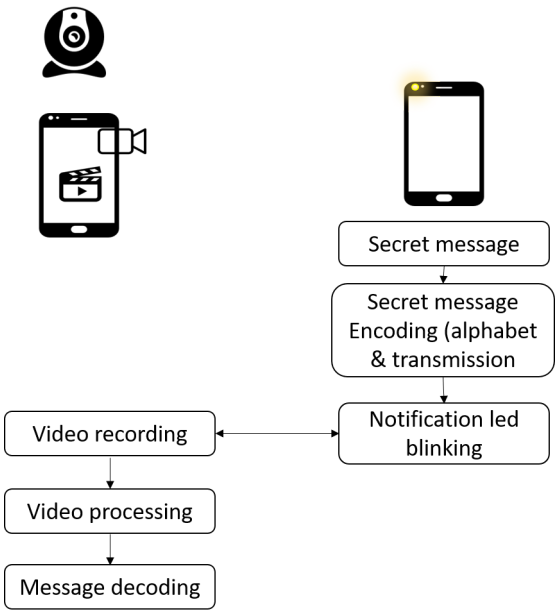

Figure 1. System description

an overview of the mechanism. Afterwards, the user model is shown in Section III-B. The main steps of the secret transmission, namely its preparation, encoding, transmission and receiver processing are introduced in Sections III-C, III-D, III-E and III-F, respectively.

A. Overview

The use of the smartphone notification LED for covert communications involves several steps as depicted in Figure 1. Let us assume a pair of users, one of them owning a smartphone with notification LED (S_{LED}), which will be used to build the covert channel, and the other user owning a camera (C), e.g. in a smartphone, which will be the receiver of transmitted data.

There are two potential use cases for such a communication. On the one hand, to steal data from a smartphone, which is previously infected with regular malware (e.g. [22]) or even one related to an advanced persistent threat (e.g. [23]). On the other hand, to secretly share some information between two participants in a networkless manner.

In any case, the data to be transmitted has to be preprocessed and encoded. Then, S_{LED}'s notification LED blinks accordingly. Once the LED is blinking, C records a video, which is later processed and decoded to get the data at stake.

Along this process the following features should be appropriately tuned as they may reduce SmartLED effectiveness:

- Sender-receiver distance: C has to be located at the right distance from S_{LED}.
- Environmental light conditions: S_{LED} should be located within an appropriate environmental light. Similarly, good conditions are required for C to record the video.
- Blinking features: the intensity and duration of S_{LED}'s blinks should be considered, as it may affect the recording made with C.

B. User model

There are a pair of settings in which SmartLED can be applied, namely intentional and unintentional exfiltration. Each one counts on different parties acting as users:

- Intentional exfiltration: In this case, S_{LED} and C are managed by a pair of (potentially malicious) users who want to share secret information in a place where the use of public networks, e.g., Internet, is not available or is subject to surveillance. This is the case of someone sharing information to another participant in a meeting room, or an insider leaking a secret from a meeting glass-walled room to an outsider. An application to do the exfiltration is installed in S_{LED} and another one for message recovery is installed in C, e.g. in a smartphone.
- Unintentional exfiltration: In this case, the user is a malicious third party different from the smartphone owner. He wants to exfiltrate secret information stored in that device. For this purpose, a malware is installed in S_{LED} to exfiltrate secret data and an application to recover the secret message is installed in C, which is controlled by the attacker. Note that there are assorted ways to install malware on smartphones, such as sending a malicious link to the victim [24] or exploiting the popularity of social networks [25].

Finally, note that people receive lots of notificacions daily [26], namely from emails, chats, etc. and commonly, all of them make the smartphone blink. Analysing the perceptibility of LED notifications, [27] concluded that only a fraction of users noticed LED blinks even when the phone was lying on the table. Going a step forward, [28] determined that LED notifications are easy to be missed. Thus, a smartphone blinking is not considered suspicious at all, though this study considers blinking features for better stealthiness.

C. Message structure

Symbols of the secret message are encoded in 6-bits based on the alphabet presented in Table II, composed of lower letters, numbers and a set of special characters. Note that any kind of alphabet could be used, but this particular one has been set to minimize the amount of transmitted bits without losing the capability to represent typical texts (e.g., phrases, passwords, etc.).

Table II
MESSAGE ALPHABET AND DECIMAL REPRESENTATION

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
p	q	r	s	t	u	v	w	x	y	z	0	1	2	3
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
4	5	6	7	8	9	¡	!	?	¿	;	,	.	:	-
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
_	@	#	$	%	&	/	\	(	)	=	+			
45	46	47	48	49	50	51	52	53	54	55	56			

Message structure	Preamble (8 bits)	Secret message length (8 bits)	Secret message (6-1536 bits)
Alphabet encoding	10101010	00000111(7)	001001(9) 000111(7) 010011(19) 100001(33) 010110(22) 111000(28) 100101(37)
Manchester IEEE 802.3 encoding	01 10 01 10 01 10 01 10	10 10 10 10 10 01 01 01(7)	10 10 01 10 10 01(9) 10 10 10 01 01 01(7) 10 01 10 10 01 01(19) 01 10 10 10 10 01(33) 10 01 10 01 01 10(22) 01 01 01 10 10 10(28) 01 10 10 01 10 01(37)

Figure 2. Message structure and example of encoding 'jht7w2!' Numbers in blue represent decimal values.

Each transmitted message is composed of a 8-bits preamble, in line with existing works [6]; the size of the secret message in 8-bit format, which corresponds to the amount of symbols of the secret message; and each of the symbols of the secret message in 6-bit format. For instance, the secret message "jht7w2!" is encoded as '9 7 19 33 22 28 37' and Figure 2 presents the message in binary after applying alphabet encoding.

D. Transmission encoding

The secret to be transmitted is translated into S_{LED} blinks. It must be recalled that any LED counts on two possible states, namely activated and deactivated. This opens up the door to multiple encoding types. First of all, the binary encoding is a common solution, setting, for instance, the LED deactivated for transmitting 0 and activated to transmit 1. However, this is not a feasible alternative due to a pair of reasons. On the one hand, we have experimentally determined that the notification LED cannot be continuously activated for a long period of time. Therefore, secrets with sequences of 1's will not be effectively sent. On the other hand, stealthiness would be lost if the notification LED is activated for such a long period.

To overcome these limitations, Manchester encoding is applied in line with other covert channel approaches [11], [13]. This particular encoding uses the transition between two states to transmit each bit. Using the original encoding, by G. E. Thomas, transmitting 0 means a low-to-high signal level transition ('01', LED-OFF; LED-ON) and transmitting 1 from high-to-low ('10', LED-ON; LED-OFF). By contrast, the second convention is proposed in IEEE 802.3 [29] and IEEE 802.4 [30] standards and it is the inverted version of the original one.

Therefore, in SmartLED, once the message is alphabet-encoded the Manchester encoding is applied to be later transmitted. Figure 2 shows the transmission encoding of the secret message 'jht7w2!' following Manchester IEEE 802.3 encoding.

E. Message transmission

Let α be the duration in seconds of each S_{LED} blink. This parameter has to be set with care as it imposes a tradeoff between stealthiness and performance – shorter blinks will lead to better transmission rates but the amount of reception errors may also raise depending on the quality of the receiver camera. Recalling the Manchester encoding, each bit of the message is encoded by a pair of bits ('10' or '01'). Therefore, each bit is transmitted in 2α.

F. Video processing

In the processing of the video recording two general steps are distinguished, the identification of frames, that is images of the video, and their later processing. In this latter step assorted techniques could be applied but, given the need of identifying light points, the use of machine learning algorithms or the management of grayscale images, are common approaches already used, e.g., for traffic light detection [31], [32]. Therefore, SmartLED follows four steps in this regard. First, the video is divided in frames. Second, each image is converted to grayscale. Third, a binary threshold function is applied to distinguish those pixels which are bright and thus, a contour is detected. Finally, the number of contours is identified. Images are compared in terms of contours, assuming that an increase in the number of them corresponds to the activation of the notification LED.

IV. Evaluation

This Section focuses on the assessment of SmartLED. For this purpose, the prototype implementation is firstly described (Section IV-A). Afterwards, the experimental settings and evaluation metrics are introduced in Sections IV-B and IV-C, respectively. The achieved results are presented and discussed in Section IV-D.

A. Prototype implementation

A pair of Android applications have been developed and published in GitHub[2]. In particular, CoverApp has to be installed in S_{LED} whereas RecordApp is a desktop application to be used after the video is recorded. CoverApp consists of an interface in which the S_{LED}'s owner writes the secret message, which is later transmitted through SmartLED. In the case of unintentional exfiltration (recall Section III-B), CoverApp could be replaced by a malware to collect the private data [22].

By contrast, after C records the notification LED of S_{LED}, RecordApp uses OpenCV library[3] to do the video processing. It must be noted that this library provides with primitives to carry out the four steps described in Section III-F.

B. Experimental settings

1) Devices: A pair of devices have been used in the evaluation:

- S_{LED} is an Elephone E7 with Android 7.1.1 and a notification LED.
- C is a Xiaomi Mi Mix 2s with a Sony IMX363 camera of 12 megapixels.

[2]https://github.com/Sergio98bm/SmartLED
[3]https://opencv.org/ , last access July 2020

Figure 3. Experimental setting for indoor dim light

2) Scenarios: Four different scenarios have been applied for evaluation purposes. Considering light intensity, scenarios are the following:

- Indoors-Dark: the scenario is not illuminated in any way.
- Indoors-Dim light: the scenario has some indirect light.
- Indoors-Bright light: the scenario counts on a source of intense light.
- Outdoors-Sun light: the scenario is outside a building, and thus, illuminated by the sun.

For the sake of illustration, Figure 3 shows an indoors-dim light setting.

3) Parameterized features: To analyse the impact of distance in SmartLED, C is located at 20 cm., 1 m., 2 m., 3 m. and 5 m. from S_{LED}. Note that data is collected from smartphones' LEDs, so 5 m. is not only a sensible distance for this type of exfiltration, but also in line with related works. On the other hand, to study the effect of the length of the blink, α is set to 300 ms. and 450 ms. These values have been chosen as 300 ms. is the shortest value that can be configured according to our experiments, and 450 is the one used by default in the considered smartphones. Indeed, these values are chosen as a trade-off between stealthiness and performance because the longer α is set, the longer the time to collect the secret and the higher the possibilities for the victim to notice the exfiltration.

Finally, the secret message *jht7w2!*, which is assumed to be the password, is encoded and sent through the covert channel. Although the experiment could involve more words or sentences, the system is not affected by this issue and results can be generalized to any other secret data.

To ensure the validity of the results, each experiment (i.e., a transmission in a given environment at a given distance with a particular blink duration) has been repeated 5 times. This leads to a total of 170 tests, considering that not all combinations have been successful – for practical reasons, outdoor experiments have been limited to 1 m. In the following, the average results for each setting are reported. For the sake of clarity, the whole set of results are presented in Appendix.

C. Evaluation metrics

There are two main practical issues to be measured in SmartLED, namely the transmission effectiveness and the actual time taken. For this purpose, three indicators are at stake. First, *Bit error rate* is a measure of the effectiveness of the reception after decoding the transmitted data. It corresponds to the ratio between the amount of bits that have errors (E_b) and the total number of bits of the secret message (T_b), see Equation 1.

$$BER = \frac{E_b}{T_b} * 100 \tag{1}$$

As a natural consequence of errors, the secret may have to be sent several times to ensure its correct reception in full. Thus, Retransmission Average Rate (RAR) refers to the amount of times, on average, the message should be retransmitted to be recovered. This is computed considering the inverse of BER following Equation 2.

$$RAR = \lceil \frac{100}{(100 - BER)} \rceil \forall BER! = 0,\ RAR = 0\ otherwise. \tag{2}$$

Concerning performance issues, *Transmission time* (TT) measures the time needed to send a message though the covert channel including its potential retransmissions (Equation 3). It is computed by considering the amount of bits at stake and the number of retransmissions. With respect to the first factor, it is computed by adding 16 bits of the message preamble, the Secret Message size ($|SM|$) and the number of bits of SM, considering that each byte is encoded in 6 bits. Each of these bits takes 2α to be transmitted due to the Manchester encoding. Moreover, it is necessary to retransmit the message RAR+1 times to promote the correct reception. Also, the physical transmission time involves covering the considered distances at light speed, but it is negligible and not considered in TT.

$$TT = (1 + RAR) \times (((16 + |SM| + SM) \times 6) \times 2\alpha) \tag{3}$$

D. Results

For the sake of clarity, each of the research questions will be addressed in a separate subsection, where Table III presents average results in terms of RAR, TT, standard deviation of BER and BER.

1) Feasibility analysis: In order to determine whether SmartLED is suitable for real-world use cases, it is necessary to measure the time taken to exchange the data items at stake. In the case of the proposed secret message (i.e., password), TT is 2.25 and 3.84 minutes for α 300 and 450 ms. respectively, being RAR 3 and 4 and BER 49.57 and 52.66. It must be noted that these results are the global average among all experiments with each α, so they are not representative for any particular distance or environment. Indeed, the particular performance will greatly vary among settings as it will be explained later.

Table III
RESULTS ANALYSIS

	TT (min)	RAR	BER Std. Deviation	BER
α				
300 ms.	2.25	3	13.95	49.57
450 ms.	3.84	4	14.81	52.66
Distance				
20 cm.	2.56	3	13.45	45.35
1 m.	2.51	3	13.11	45.84
2 m.	2.76	3	16.10	49.33
3 m.	3.48	4	11.56	46.58
5 m.	3.00	4	17.96	50.68
Environments				
Indoors-Dark	1.19	1	6.67	2.98
Indoors-Dim light	3.42	4	18.53	69.15
Indoors-Bright light	3.97	5	17.91	70.34
Outdoors-Sun light*	4.42	5	13.97	77.83

*: Up to 1 m.

One important matter is that the effect of α is contrary to our expectations. Our results show that the shorter α is, the better in terms of transmission errors. Although the difference is not substantial, one potential cause is the camera sampling rate. Therefore, more powerful Cs (equipped with better camera or camera lens) could revert this trend.

2) Impact of distance: Our experiments support that the distance has a slight effect on the system accuracy and performance. For the sake of repeatability, the outdoors environment has not been considered herein, because not all distances were considered in that setting (recall Section IV-B3).

In shorter distances, e.g. 20 cm. or 1 m., BER is 45.35 and 45.84 respectively, increasing a little bit in the remaining cases. In 3 m. results are better than closer distances, but the difference in BER is small and no remarkable conclusions are achieved. Nonetheless, in terms of TT the maximum difference between distances is of 0.72 min, being 1 m the best alternative to balance BER and TT. Finally, the most common pattern of the standard deviation shows an increase with the distance.

All in all, it must be noted that the increase in distance does not lead to the same increase in TT. Thus, while the distance grows in a factor of 25 (from 20 cm. to 5 m.), TT only increases by a factor of 1.17 (from 2.56 min. to 3 min).

3) Impact of light conditions: SmartLED is highly impacted by environmental conditions. This is observed in all settings, even considering that the maximum distance for outdoors settings has been 1 m.

While in a dark environment BER is 2.98 and most of the message could be retrieved even without a single retransmission, other environments are more challenging and require higher RAR. When the environmental light is brighter, results get worse, as BER is 69.15 in "Indoors-Dim light" and 70.34 in "Indoors-Bright light", getting to 77.83 in "Outdoors-Sun light" and TT goes from 3.42 to 4.42 min.

As a result, if SmartLED is used in bright environments, RAR increases up to 5 in some cases and it has a dramatic impact on TT. A similar trend is observed in the standard deviation of BER, as it increases around to 18. Therefore, the effect of light is not only a reduction in SmartLED effectiveness, but also an increase in the uncertainty of the success of each execution.

4) Discussion: Based on our findings, SmartLED is heavily affected by the environmental settings at stake. Thus, in what comes to the light conditions, a set of conclusions can be drawn:

- In a "indoor-dark" environment the system works remarkably well in 1 m. or less. For larger distances SmartLED works slightly worse. Indeed, the system works well even considering the standard deviation. Besides, BER differences are less than in other environments.
- In "indoor-dim light" the best behaviour corresponds to shorter distances, 1 m or less.
- The system is significantly resistant to distance variations in "indoor-bright light".
- In "outdoor-sun light" smaller α are preferable.

Concerning distances, the shorter, the better, though results show that the impact is not proportional to the distance. This is not a highly differentiating factor, as least considering 5 m. as the greatest distance. However, using a better camera may lead to better and more consistent results across different distances, even beyond the ones considered herein.

Moreover, SmartLED is appropriate to exfiltrate short messages, such as passwords, as longer ones increase TT and the system may become impractical. Around 3.04 min, on average, are required for exfiltrating a 7-bytes word and thus, the system is not ready to work on an immediacy bases. For the sake of illustration, a typical SMS (140 characters) would require around 8 minutes with α 300 ms., which might not be practical. In any case, SmartLED has been shown to be suitable for indoor dark environments, in which promising performance rates (around 1 min. with very low BER) have been achieved.

Finally, in comparison with related works dealing with LEDs, SmartlLED improves BER results of [9] and [13] in "dark" environments, while the remaining works cannot be compared in this regard. Moreover, [9] and [13] do not compare and analyse different environmental settings. On the other hand, SmartLED achieves bit rates of 0.15 and 0.23 bits/s for α 300 and 450 respectively. Although they are smaller than other proposals (i.e. [9] and [13]), it must be recalled that the management of smartphone LEDs in Android impose practical limits that restrict the available choices for α. Moreover, as pointed out in Section IV-B, data exfiltration should be carried out in an stealthy way, so α should be kept within common limits.

V. COUNTERMEASURES AND ENHANCEMENTS

A pair of different types of countermeasures against the use of SmartLED are identified, namely hard and soft ones, as follows:

- Hard countermeasure: a barrier between the transmitter and received device, S_{LED} and C in this case, is the most effective countermeasure. In this way data exfiltration

would be infeasible. In a real setting this would refer to the existence of a dark wall, a person or any other object between S_{LED} and C.

- Soft countermeasure: the modification of environmental features may decrease the system effectiveness, as transmitted data could be altered or even lost. One possible alternative is to use another light point, e.g. flashlight, to confuse the system. Moreover, specially focused on the 'unintentional exfiltration', the use of a polarized filter to change the intensity of the notification LED would make data exfiltration more difficult.

A pair of enhacements can be considered in the current design of SmartLED. On the one hand, the message could be encrypted. Stream ciphers (such as ChaCha20 [33]) are appropriate alternatives. They could be applied without impacting the message length or performance to a great extent, for instance, using ChaCha20 270.72 MB/s are encrypted in a i386 processor[4]. On the other hand, when retransmissions are required, specially in bright environments where RAR is higher, the inclusion of integrity checks would help in the message recovery allowing the identification of incorrect bits.

VI. Conclusion and future research issues

Nowadays, smartphones are present in daily routines in modern societies. Thus, their use for sharing information is regarded as normal. In this paper, a mechanism (dubbed SmartLED) to build a covert communication with an external observer has been proposed. SmartLED leverages the notification LED that is currently present in most smartphones. Therefore, it does not require any data connection between both parties. Its effectiveness under different ambient light conditions and observer distances has been characterized. Thus, it has been shown to be effective to convey short messages such as passwords in dark environments. Moreover, the impact of the type of ambient light is significantly greater than the observer distance – SmartLED has been shown to perform similarly until 5 m.

There are three research questions that remain open. First, adapting SmartLED for scenarios in which both sender and receiver are in motion. Second, assessing the improvement of leveraging the LED light color (which is variable in some smartphones) to convey a greater amount of information. Last but not least, the impact of visual interferences (which is a practical countermeasure) on the effectiveness of the mechanism is other open issue to analyse.

Acknowledgements

This work was supported by MINECO grant TIN2016-79095-C2-2-R (SMOG-DEV), PID2019-111429RB-C21 (ODIO), P2018/TCS4566 (CYNAMON-CM) funded with European FEDER funds and CAVTIONS-CM-UC3M funded by UC3M and the Government of Madrid (CAM).

Appendix

Table IV presents all experimental results.

[4]https://bearssl.org/speed.html , last access July 2020

Table IV
Experimental results

α	Environment	Distance	BER - number of experiments 1	2	3	4	5	Average RAR	Average TT (ms)
300	Dark	20cm	0	0	0	0	0	0	34800
		1m	0	0	0	0	0	0	34800
		2m	0	0	0	0	72.81	2	104400
		3m	0	0	0	0	0	0	34800
		5m	0	0	0	0	0	0	34800
	Dim light	20cm	73.69	48.03	44.74	81.58	49.13	3	139200
		1m	97.37	60.53	92.77	57.02	58.55	4	174000
		2m	55.27	78.08	71.06	88.6	76.22	4	174000
		3m	78.08	91.23	53.51	65.79	55.27	4	174000
		5m	79.83	55.27	86.85	98.25	79.83	6	243600
	Bright light	20cm	42.11	92.99	63.16	57.9	93.86	4	174000
		1m	64.92	82.46	56.2	62.29	98.25	4	174000
		2m	43.86	82.46	68.43	42.99	73.69	3	139200
		3m	45.62	47.37	37.72	73.69	34.22	2	104400
		5m	50.88	64.92	56.15	96.5	79.83	4	174000
	Sun light	20cm	84.22	88.6	89.48	71.06	52.64	5	208800
		1m	57.9	89.48	68.43	58.78	91.23	4	174000
450	Dark	20cm	0	0	0	0	0	0	52200
		1m	0	0	0	0	0	0	52200
		2m	0	0	0	0	0	0	52200
		3m	0	1.75	0	0	0	2	156600
		5m	0	74.57	0	0	0	2	156600
	Dim light	20cm	97.37	57.1	48.25	61.41	87.72	4	261000
		1m	45.62	54.39	53.51	90.36	50.88	3	208800
		2m	63.16	59.65	45.62	89.48	74.57	3	208800
		3m	95.62	91.23	43.86	96.5	43.86	4	261000
		5m	97.37	56.15	54.39	44.74	78.08	3	208800
	Bright light	20cm	87.72	51.76	49.13	87.72	85.09	4	261000
		1m	40.36	50.88	75.44	91.23	92.11	4	261000
		2m	92.99	89.48	78.95	49.13	83.33	5	313200
		3m	83.33	86.85	76.32	97.37	98.25	9	522000
		5m	85.97	86.85	87.72	48.25	57.9	4	261000
	Sun light	20cm	88.6	84.22	71.93	83.33	85	6	365400
		1m	83	48.25	91.23	78.08	91.23	5	313200

References

[1] S. Zander, G. Armitage, and P. Branch, "A survey of covert channels and countermeasures in computer network protocols," *IEEE Communications Surveys & Tutorials*, vol. 9, no. 3, pp. 44–57, 2007.

[2] PaloAlto, *OilRig Targets Middle Eastern Telecommunications Organization and Adds Novel C2 Channel with Steganography to Its Inventory*. PaloAlto Networks, 2020.

[3] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "Powerhammer: Exfiltrating data from air-gapped computers through power lines," *arXiv preprint arXiv:1804.04014*, 2018.

[4] M. Guri, A. Daidakulov, and Y. Elovici, "Magneto: Covert channel between air-gapped systems and nearby smartphones via cpu-generated magnetic fields," *arXiv preprint arXiv:1802.02317*, 2018.

[5] L. Deshotels, "Inaudible sound as a covert channel in mobile devices," in *8th {USENIX} Workshop on Offensive Technologies ({WOOT} 14)*, 2014.

[6] M. Guri, "Air-viber: Exfiltrating data from air-gapped computers via covert surface vibrations," *arXiv preprint arXiv:2004.06195*, 2020.

[7] K. Ahsan, "Covert channel analysis and data hiding in tcp/ip," *Canada, University of Toronto*, 2002.

[8] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "Gsmem: Data exfiltration from air-gapped computers over {GSM} frequencies," in *24th {USENIX} Security Symposium ({USENIX} Security 15)*, 2015, pp. 849–864.

[9] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "Ctrl-alt-led: Leaking data from air-gapped computers via keyboard leds," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1. IEEE, 2019, pp. 801–810.

[10] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise ('diskfiltration')," in *European symposium on research in computer security*. Springer, 2017, pp. 98–115.

[11] M. Guri, B. Zadov, and Y. Elovici, "Led-it-go: Leaking (a lot of) data from air-gapped computers via the (small) hard drive led," in *International conference on detection of intrusions and malware, and vulnerability assessment*. Springer, 2017, pp. 161–184.

[12] A. C. Lopes and D. F. Aranha, "Platform-agnostic low-intrusion optical data exfiltration." in *ICISSP*, 2017, pp. 474–480.

[13] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xled: Covert data exfiltration from air-gapped networks via switch and router leds," in *2018 16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2018, pp. 1–12.

[14] M. Guri, "Power-supplay: Leaking data from air-gapped systems by turning the power-supplies into speakers," *arXiv preprint arXiv:2005.00395*, 2020.

[15] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors," in *2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC)*. IEEE, 2016, pp. 525–532.

[16] J. E. Coyac-Torres, M. E. Rivero-Angeles, and E. Aguirre-Anaya, "Cognitive radio based system for best effort communications in sound-based covert channel for iot environments," *Mobile Networks and Applications*, pp. 1–12, 2020.

[17] K. Block, S. Narain, and G. Noubir, "An autonomic and permissionless android covert channel," in *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2017, pp. 184–194.

[18] W. Qi, Y. Xu, W. Ding, Y. Jiang, J. Wang, and K. Lu, "Privacy leaks when you play games: A novel user-behavior-based covert channel on smartphones," in *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*. IEEE, 2015, pp. 201–211.

[19] Q. Do, B. Martini, and K.-K. R. Choo, "Exfiltrating data from android devices," *Computers & Security*, vol. 48, pp. 74–91, 2015.

[20] B. Aloraini, D. Johnson, B. Stackpole, and S. Mishra, "A new covert channel over cellular voice channel in smartphones," *arXiv preprint arXiv:1504.05647*, 2015.

[21] Z. Yang, Q. Huang, and Q. Zhang, "Nicscatter: Backscatter as a covert channel in mobile devices," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, 2017, pp. 356–367.

[22] R. Schlegel, K. Zhang, X.-y. Zhou, M. Intwala, A. Kapadia, and X. Wang, "Soundcomber: A stealthy and context-aware sound trojan for smartphones." in *NDSS*, vol. 11, 2011, pp. 17–33.

[23] L. O'Donnell, "Android spyware variant snoops on whatsapp, telegram messages," https://threatpost.com/new-android-spyware-whatsapp-telegram/159694/, Tech. Rep., 2020.

[24] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Computers & Security*, vol. 73, pp. 519–544, 2018.

[25] M. R. Faghani and U. T. Nguyen, "Socellbot: a new botnet design to infect smartphones via online social networking," in *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering (CCECE)*. IEEE, 2012, pp. 1–5.

[26] M. Pielot, K. Church, and R. De Oliveira, "An in-situ study of mobile phone notifications," in *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*, 2014, pp. 233–242.

[27] A. Exler, C. Dinse, Z. Günes, N. Hammoud, S. Mattes, and M. Beigl, "Investigating the perceptibility different notification types on smartphones depending on the smartphone position," in *Proceedings of the 2017 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2017 ACM International Symposium on Wearable Computers*, 2017, pp. 970–976.

[28] A. Komninos, J. Besharat, V. Stefanis, G. Gogoulou, and J. Garofalakis, "Assessing the perceptibility of smartphone notifications in smart lighting spaces," *Journal of Ambient Intelligence and Smart Environments*, vol. 11, no. 3, pp. 277–297, 2019.

[29] IEEE, "Ieee std 802.3-2018 (revision of ieee std 802.3-2015)," vol. 8457469, pp. 1–5600, 2018.

[30] P. Montuschi, L. Ciminiera, and A. Valenzano, "Time characteristics of ieee 802.4 token bus protocol," *IEE Proceedings E (Computers and Digital Techniques)*, vol. 139, no. 1, pp. 81–87, 1992.

[31] S.-H. Lee, J.-H. Kim, Y.-J. Lim, and J. Lim, "Traffic light detection and recognition based on haar-like features," in *2018 International Conference on Electronics, Information, and Communication (ICEIC)*. IEEE, 2018, pp. 1–4.

[32] R. De Charette and F. Nashashibi, "Traffic light recognition using image processing compared to learning processes," in *2009 IEEE/RSJ International Conference on Intelligent Robots and Systems*. IEEE, 2009, pp. 333–338.

[33] A. Langley, W. Chang, N. Mavrogiannopoulos, J. Strombergson, and S. Josefsson, "Chacha20-poly1305 cipher suites for transport layer security (tls)," *RFC 7905*, no. 10, 2016.