InkFiltration: Using Inkjet Printers for Acoustic Data Exfiltration from Air-Gapped Networks

JULIAN DE GORTARI BRISENO, AKASH DEEP SINGH, and MANI SRIVASTAVA, University of California, Los Angeles

Printers have become ubiquitous in modern office spaces, and their placement in these spaces been guided more by accessibility than security. Due to the proximity of printers to places with potentially high-stakes information, the possible misuse of these devices is concerning. We present a previously unexplored covert channel that effectively uses the sound generated by printers with inkjet technology to exfiltrate arbitrary sensitive data (unrelated to the apparent content of the document being printed) from an air-gapped network. We also discuss a series of defense techniques that can make these devices invulnerable to covert manipulation.

The proposed covert channel works by malware installed on a computer with access to a printer, injecting certain imperceptible patterns into all documents that applications on the computer send to the printer. These patterns can control the printing process without visibly altering the original content of a document, and generate acoustic signals that a nearby acoustic recording device, such as a smartphone, can capture and decode. To prove and analyze the capabilities of this new covert channel, we carried out tests considering different types of document layouts and distances between the printer and recording device. We achieved a bit error ratio less than 5% and an average bit rate of approximately 0.5 bps across all tested printers at distances up to 4 m, which is sufficient to extract tiny bits of information.

CCS Concepts: • **Security and privacy → Hardware attacks and countermeasures**; *Embedded systems security*; Operating systems security; • **Hardware → Printers;**

Additional Key Words and Phrases: Inkjet printer, covert channel, data exfiltration, air-gap, side-channel attacks

ACM Reference format:
Julian de Gortari Briseno, Akash Deep Singh, and Mani Srivastava. 2022. InkFiltration: Using Inkjet Printers for Acoustic Data Exfiltration from Air-Gapped Networks. *ACM Trans. Priv. Secur.* 25, 2, Article 15 (May 2022), 26 pages.
https://doi.org/10.1145/3510583

The research reported in this paper was sponsored in part by the National Science Foundation (NSF) under award #CNS 1705135, by the CONIX Research Center, one of six centers in JUMP, a Semiconductor Research Corporation (SRC) program sponsored by DARPA, and by the Army Research Laboratory (ARL) under Cooperative Agreement W911NF-17-2-0196. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the ARL, DARPA, NSF, SRC, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation here on.

Author's address: J. D. G. Briseno, A. D. Singh, and M. Srivastava, Networked and Embedded Systems Laboratory, University of California, Los Angeles, USA; emails: julian700@g.ucla.edu, akashdeepsingh@g.ucla.edu, mbs@ucla.edu.

2471-2566/2022/05-ART15
https://doi.org/10.1145/3510583

1 INTRODUCTION

An air-gap is the isolation of an organization's internal network from the external world that blocks Internet access among other things. Air-gaps were previously thought to be the ultimate way of securing a sensitive network; unfortunately, a series of real world attacks have put into doubt even this strategy. For example, as part of supply chain attacks, Brutal Kangaroo [1], ProjectSauron [21], USBFerry [7], Ramsay [28], and Stuxnet [9] have been utilized to infiltrate these isolated networks for nefarious purposes. But extracting information from air-gapped systems, once these are infected, continues to be a challenging task and is the focus of this work. Although increasing efforts have gone into developing security mechanisms to prevent attacks through a network's normal channels, such as traffic monitoring, firewalls, and intrusion detection systems, unintended physical emissions from everyday devices often get overlooked. Consequently, attacks exploiting these vulnerable emanations have emerged, intending to break through traditional defenses. Specifically, through the form of covert channels, data can be infiltrated and exfiltrated to and from air-gapped networks.

All types of physical emissions have been considered in the establishment of out-of-band covert channels: acoustic [11], optical [13], electromagnetic [14], thermal [15], magnetic [19], and vibrational [10]. In practice, most of these channels have considered only one-way communication, either to exfiltrate sensitive information or to infiltrate commands for activating latent malware. Although the main focus on covert channels has been on personal computers, accessory devices connected to these computers can also act as transmission nodes. In particular, malware can harness unintended emanations from accessory devices for attack purposes, as we demonstrate here with inkjet printers. Printers are omnipresent in all kinds of workplaces, such as offices, where their location is selected to be accessible, to facilitate their usage by all employees. Users become habituated to the frequent operation of the printers and the noise they produce without paying attention to specific acoustic patterns. Moreover, because users are not required to constantly monitor the printer's performance, it is common to send print jobs and wait for some time before retrieving the printed pages. All of these facts make a printer an ideal target for developing a covert channel.

We demonstrate how malware can exploit the noise generated by inkjet printers as a covert channel and describe how one can protect against it. To the best of our knowledge, our work is the first to use acoustic emanations from standard inkjet printers for establishing a covert channel. Moreover, the channel is available irrespective of whether an application or a user is actively using the device or not, which is unlike previous attempts at speakerless acoustic covert channels that only work when there is no contention from a potential user [11, 12, 16, 17]. Our proposed attack leverages the fact that inkjet printers are sensitive to the type of graphical objects included in documents and the arrangement of these objects throughout the document (their layout). By introducing certain specific patterns into a document, a deterministic communication channel becomes feasible. An attacker can introduce malware on the computer (e.g., via human vectors or supply chain compromise) that injects these patterns into the documents sent to the printer. A nearby companion device capable of sensing sound (e.g., an infected smartphone) can capture and process the acoustic emissions from the printer to obtain the sensitive data that the attacker seeks to exfiltrate. Any document without images can carry the patterns that we propose. Our approach carefully considers the evidence left behind on the documents by designing the injected patterns to be imperceptible to the human eye.

To validate our idea, we tested seven different inkjet printers. With our recording device at a distance of 4 m, we achieve a **Bit Error Ratio (BER)** lower than 5% and a bit rate of approximately 0.5 bps, which is sufficient to extract tiny bits of information such as passwords. Only one of the printers that we tested appears to mitigate the attack due to its unique design. Finally, we discuss

some possible countermeasures to this type of data exfiltration attack: we implement a color-based filter technique to prevent the successful transmission of information over this covert channel.
Contributions. Our contributions are summarized as follows:

- We propose a first-of-its-kind covert channel designed for inkjet printers. It uses acoustic emissions to exfiltrate sensitive information and exploits human-imperceptible colors to hide any trace of the attack on printed pages. It achieves a BER lower than 5% at up to 4 m in every printer tested.
- We provide a simple framework[1] to discover the modulation parameters needed to exploit any inkjet printer for covert communication without having to delve into the internals of the device. We also show that printers from the same model family share design characteristics, which enable an attacker to use a single set of modulation parameters for all of them, with only minor follow-on tuning needed for specific models.
- We also propose methods that can defend against these types of attacks without human intervention or significant overhead—a filter that can preprocess any document sent to a printer to check for hidden patterns.

The rest of this article is organized as follows. All of the necessary background on printers is presented in Section 2, whereas an overview of the attack and its building blocks is presented in Section 3 and Section 4, respectively. Section 5 details the implementation and the results of our experiments, with a special subsection on how to empirically obtain the parameters needed to attack a printer. We discuss the countermeasures derived from this work in Section 6, whereas limitations of our approach are presented in Section 7. In Section 8, we try to give clear answers to certain key aspects of our work. Finally, related work is presented in Section 9 and our conclusion in Section 10.

2 BACKGROUND

Inkjet printing technology encompasses a series of techniques for the ejection of droplets of ink from a printhead into a substrate. In this section, we will describe more in detail how these printers work to understand the proposed covert channel.

Conventional inkjet technologies are divided into Continuous Inkjet and Drop on Demand: the first one involves the ejection of a stream of continuous liquid whose droplets are directed into a substrate by modulation of an electrostatic field, whereas in the latter each single ink droplet is ejected by a pressure pulse without any subsequent steering of it [31]. Most commercial printers use Drop on Demand technology, and thus we focus in this work on such printers. These printers can dispense ink droplets by either thermal or piezoelectric methods, and they generally come with printheads that are either part of disposable ink cartridges or are meant to last for the entire lifetime of the printer. Finally, inkjet printers can either have movable or stationary printheads. Our work involves, therefore, Drop on Demand inkjet printers with both types of ejection technology and ink containment technology, although stationary printheads are not taken into account, which in reality only a small subset of printers have.

2.1 Anatomy of an Inkjet Printer

Figure 1 shows the components commonly found on an inkjet printer. When printing a document, a paper sheet placed on the paper loading tray is first brought into the printer by the feed mechanism. This mechanism consists of a series of rollers connected through a gear train, whose rotation is

[1]Code is available at https://github.com/nesl/InkFiltration.

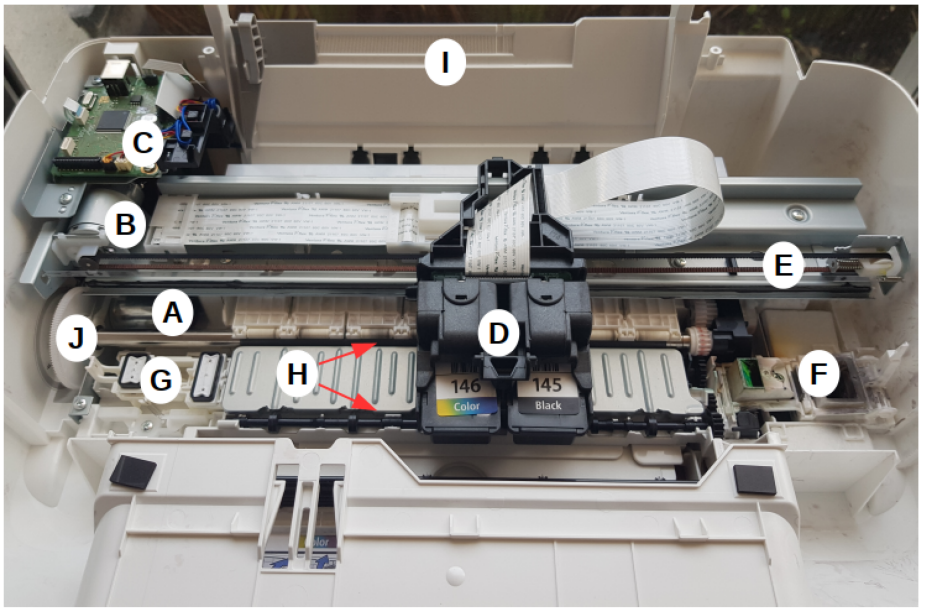

Fig. 1. Components of a Canon Pixma MG2410. (A) DC motor that controls rollers' movement. (B) DC motor that controls printhead movement. (C) Programmable logic controller. (D) Printhead. (E) Timing belt and linear optical encoder stretch across the width of the printer. (F) Excess ink depository. (G) Nozzle caps. (H) Rollers. (I) Loading paper tray. (J) Angular optical encoder attached to the end of one of the rollers.

controlled by a DC motor along with an optical angular encoder. The paper sheet is then advanced into the printer until the first graphical object to be printed is directly below the printhead. The printhead then starts sliding across a metal rail, which spans the width of the printer, by means of a timing belt linked to another DC motor. To regulate the speed and position of the sliding printhead, a transparent plastic strip with fine black bars, located parallel to the printhead's rail, works as a linear optical encoder along with a sensor located in the printhead. Within the printhead, the ejection mechanism expels droplets of ink through each of the hundreds of nozzles that are part of it. When the last graphical object has been printed, the roller mechanism expels the paper sheet from the printer into another paper tray. Excess ink can be removed from the printhead at any time through a series of plastic brushes and two ink compartments located at one end of the printer, whose purpose is to collect the residues of black and color ink. At the other side of the printer, two pads cap the printhead nozzles when not used, so as to avoid ink drying. The printer's actuators are activated and controlled by a microcontroller on a PCB plaque to which all electric components connect. The detailed disassembly of another inkjet printer is shown in the work of Wandel [36].

Depending on the graphical objects present on the document to be printed, the printhead will pass multiple times or just one time through their location; in particular, when dealing with images or fully colored figures, multiple printhead passes will be required to preserve the quality of the graphical objects. Indeed, modern printers implement a dynamic print mode control [20], by which they are able to decide how many passes to do at a given region based on the amount of ink to be ejected. But the exact number of passes the printer is able to do is a fixed quantity predetermined in the design of the device—that is, the printer can only decide whether to do one pass or two passes at a given region, each of which corresponds to what is called a *print mode*, but not more. In the

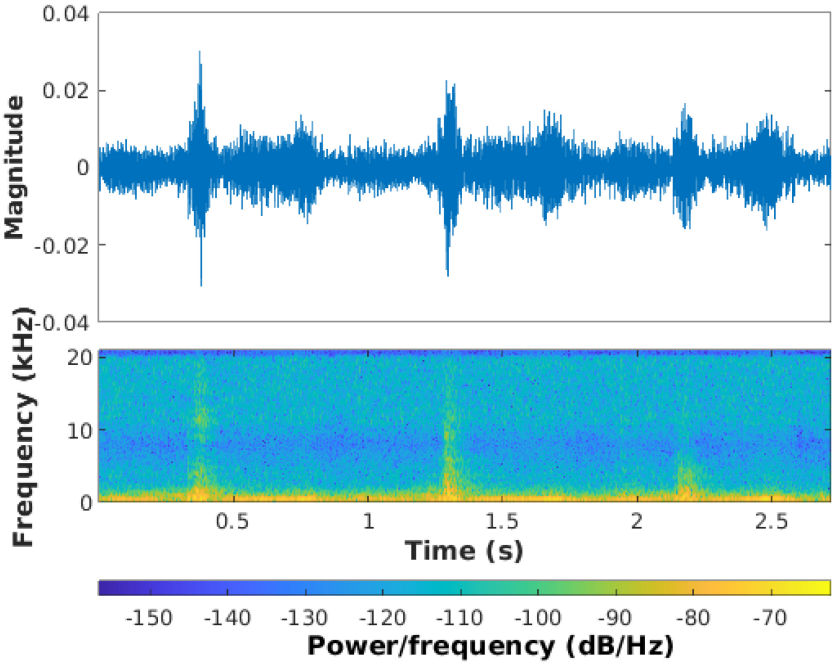

Fig. 2. Acoustic waveform and its respective spectrogram generated by a Canon MG2410 printer in operation.

work of Lee and Allebach [24], the multi-pass mechanism is described by stating that the printer employs a binary mask with a checkerboard pattern to determine in which locations to eject ink droplets in each of the passes to a particular horizontal region. After each pass, the paper feed mechanism will displace the paper by a fraction of the printhead's length so that it then allows the printhead to fill the blank spots left behind, utilizing a new binary mask for this purpose.

The manner in which inkjet printers convert continuous tone images into dot-based images is through the use of halftoning, either by modulating the size of the dots or the frequency in which they appear. The continuous color tones can be emulated as a consequence of the human visual system low-pass filter effect, whereas the individual dots that conform the elements of the documents are blurred out [23]. As white paper is the usual printing medium for printers, bright colors will therefore contain a lower amount of dots than darker ones.

2.2 Printer Acoustics

Throughout our experiments, we identified two highly correlated main sources of noise emitted from inkjet printers that could serve for the purposes of our covert channel: one corresponding to the sliding movement of the printhead and another that matched the rollers' actuation. The noise source we were interested in was the one generated by the roller mechanism, as it proved to produce a louder noise in a pulse-like manner, thus facilitating its reception, than the one generated by the sliding printhead; this difference was consistent across all printers. Figure 2 shows the waveform and spectrum of the acoustical signal we are interested in, a signal whose pulses comprise almost the entirety of the frequency range shown. In our attack, we use these acoustic pulses to transmit data from the infected computer, bandpass filtering the resulting signal to prevent low frequency interference from other printer noise sources and to delimit high-frequency noise from the environment.

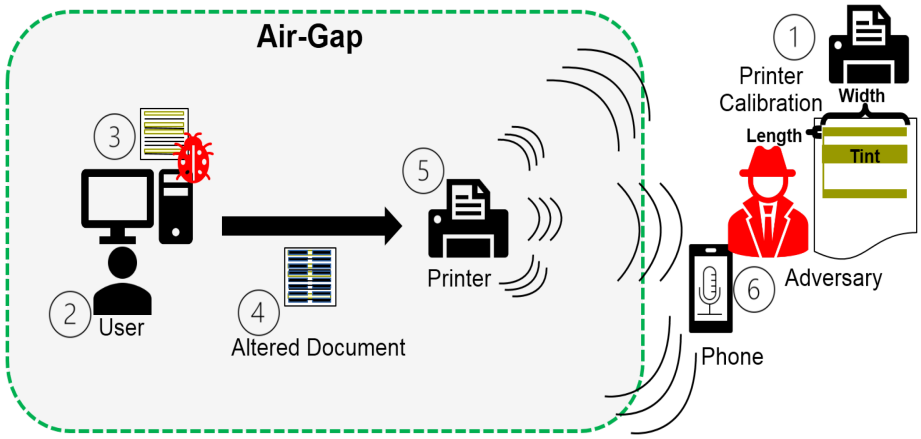

Fig. 3. Proposed attack scenario for establishing the covert channel. The attacker (1) finds information about the type of printers being used and obtains the necessary parameters for exploiting the targeted printer. (2) A trusted user on a pre-infected computer sends a document to print. (3) The malware present on that computer injects particular imperceptible patterns into the document pages. (4) The altered document travels to the printer. (5) The printer produces certain deterministic acoustic emissions depending on the injected patterns. (6) A nearby smartphone records the noise made by the printer.

3 ATTACK OVERVIEW

Figure 3 presents the overall picture of our attack scenario: a trusted user sends a document to print from a computer infected with our malware, which intercepts the print job before it leaves the computer and injects specially constructed imperceptible patterns into the same document. The malware then sends this document to the printer. The manner in which these previously injected patterns are laid out throughout a paper page will affect the printer's operation such that the noise it produces can help establish a communication channel when recorded by a nearby device. For our attack model, the assumption of a situation where a computer with printer access inside the targeted air-gapped network has already been infected with our malware is an assumption consistent with previous works in the field of covert channels (e.g., [11, 12, 16–18, 30, 39]). The feasibility of infecting air-gapped networks has already been proved previously by recent cases like Brutal Kangaroo [1], ProjectSauron [21], USBFerry [7], and Ramsay [28], where malware designed to cross the air-gap by infecting employees' USB drives was used in certain sensitive networks. Perhaps the most studied and publicized instance of this type of malware has been Stuxnet [9], whose initial purpose was to sabotage an industrial control system used for centrifuge operation in an air-gapped facility. We assume in our scenario that the malware has already done privilege escalation and has full permission to tinker with the printer subsystem. The network can either be totally air-gapped or its network traffic may just be heavily monitored, making it difficult to start a connection with a server outside the network without being discovered.

To record the printer sound, we assume that the adversary can exploit one of three scenarios: first, the attacker either has the capability to infect an employee's smartphone or other mobile devices that can record audio. Second, in some cases, the printer sound may be recorded through the walls [37], since office walls and cubicles are not soundproof. Third, the attacker may be able to get close enough to the source to record audio using their own device. It is important to note that although the targeted network may be indeed logically air-gapped, this does not mean the physical facilities where the network has been established are entirely isolated from the public.

Finally, the site of the attack is assumed to contain at least one printer with inkjet technology to which the targeted computer is connected.

To mount a successful attack, the adversary needs to *a priori* obtain information about the printer to be used as a covert transmitter. In theory, each printer model requires a particular set of parameters, which characterize the patterns to be injected for successful modulation of the printing process. Those parameters can only be obtained by a series of tests conducted on the target device or another device of a similar model. Therefore, the attacker needs some access to one of these (e.g., the attacker can buy a printer of a similar model, conduct the tests, and obtain the parameters that will also let him attack the targeted printer). Having some knowledge about the models of the printers a targeted organization uses lets the attacker narrow the range of printers among which to search for the parameters. Finding this knowledge is not a difficult task. Inkjet printers rely on either disposable ink cartridges or bottles. Their packaging material, or the used cartridges or bottles themselves, eventually show up when dumpster diving[2] [35]. The numbers that identify the model of these ink cartridges/bottles are more than enough information to reduce the printer search space to a small subset of printer models.

However, as the results in this article demonstrate, knowing only the product line (family) of printers to which the target printer belongs may be sufficient. Printer models that belong to the same family share design characteristics, which means one can use similar modulation parameters for all of them. Thus, the attacker only needs to have a printer that is part of the same product line as the target to obtain the modulation parameters and successfully exploit the latter. Moreover, cartridge models reveal not only compatible printer product lines but also specific compatible printer models. Finally, the number of independent lines of printers that each manufacturer develops is limited, and thus it should not be unfeasible to register the modulation parameters of all product lines for both transmitter and receiver sides. In the case of the receiver, an audio classifier could then be used to automatically detect the type of printer being used when attacking a given facility, and utilize the correct parameters, but we leave this scenario for future work.

4 BUILDING BLOCKS OF INKFILTRATION

The attack introduced in this article can be framed as a communication problem between an unsuspecting victim, in possession of a printer acting as the transmitter, and a recording device utilized by the attacker as a receiver. The communication system exploits the acoustic pulse-like properties of the noise produced by the printers' roller mechanism. In the next subsections, we will detail the operation of this communication system, with an emphasis on the transmitter side, where imperceptible patterns are injected into documents to control the printing process. In the last subsection, we reveal how the pattern injection would be carried out in practice, within the Linux operating system.

4.1 Design of the Injection Patterns

Transmission is done by using imperceptible patterns injected into the documents being printed, which as mentioned before are used to control the printing process. Through the use of a series of very light colored rectangles (imperceptible to the human eye) with different widths imposed on the white background of documents being sent to print, as shown in Figure 4, our objective is to manipulate the frequency at which the printer's roller mechanism activates (i.e., the mechanism that displaces paper sheets inside the printer).

The rectangles we inject into documents are drawn across the horizontal space of a page and are stacked vertically on it. These rectangles are meant to activate a printer's multi-pass mode—

[2]Dumpster diving is the act of going through the trash to find items that one may deem useful.

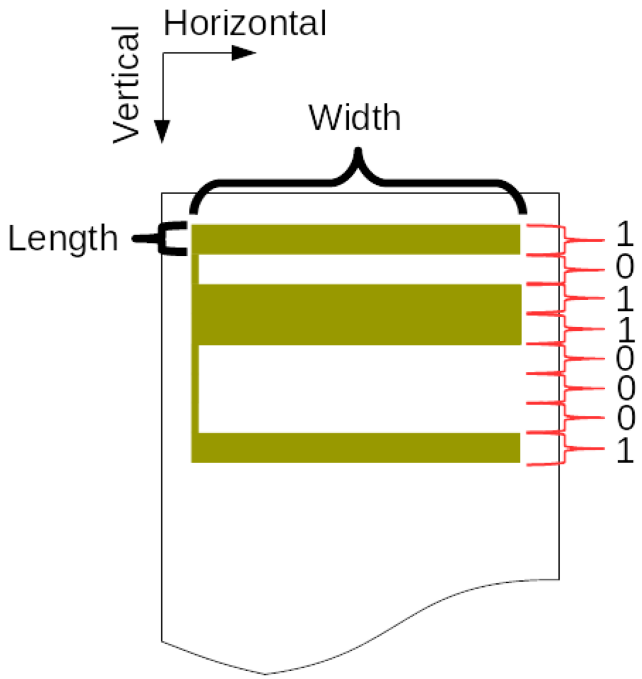

Fig. 4. The imperceptible patterns injected into documents are vertically stacked, and their width changes according to the data transmitted.

that is, the mode that produces the greatest number of printhead passes and roller activations over a given area, which is normally used to ensure densely colored figures keep their details when printed. It is also the mode that generates the least amount of paper displacement for each roller activation. By triggering this mode in text documents, we basically obtain control over the printhead's operation with our injected rectangles, affecting the time the printer takes to complete each of the horizontal areas where the printhead maneuvers. Any overlying text that may be present has minimum influence over the printhead, because of its graphical sparseness, which means the printer can print those segments of text in any of the multiple passes the injected rectangles do require, and not interfere significantly with our modulation, as will be explained in the following.

The timing effect that the injected rectangles cause depends on their size, and thus we define two main spatial properties that characterize these figures, as shown in Figure 4: width and length. First of all, a specific minimum width and length are needed to activate the multi-pass print mode. After determining these minimum parameters, we can subsequently increase the rectangles' width in different proportions to actually modulate the rate at which page displacements are made (i.e., the frequency at which acoustic pulses are produced). The rectangles' minimum length is actually equal to, or a fraction of, the vertical length that the yellow color nozzles occupy on a given printhead. In practice, this means each rectangle will generate exactly one paper displacement if they perfectly occupy all the printable vertical area the printhead can operate at a given moment, which let us maximize the use of a paper's space and produce reliable transitions between rectangles of different width. However, once we assure each rectangle generates a single paper displacement, the way the rectangles' width actually modulates the printing process can be understood with the next example: given two rectangles of the same length, vertically stacked on a blank page and

Fig. 5. A magnified view of two printed letters surrounded by yellow dots.

aligned to the margin closest to the printhead's resting position, if one of the two is wider than the other, it is evident that the printhead will need to go farther away to print the wider rectangle. This will then increase the time period between paper displacements than when printing the rectangle that covers less width of the page.

A third and last factor that controls printheads' speed is the lightness of a figure's color, which affects the total number of ink droplets ejected per area, although this parameter is not that useful for the purpose of our attack, as it can compromise the stealthiness of the operation. It is important to understand that the very light yellow color we use in our rectangles is obtained by sparsely ejecting yellow ink droplets from the printhead, as part of the halftoning process that uses the white paper background to modulate the brightness of colors, an example of which can be seen in Figure 5. By using such a light color, we ensure a human cannot distinguish the patterns from the background. In fact, it is known that the human visual system relies more on luminance contrast than on the absolute levels of luminance, or than on chromatic contrast, for the interpretation of information [38], and the difference in luminance between yellow and white is indeed perceived to be small and hard for humans to see. It is evident then that a very light tint of yellow on a white background will not be detected—an effect that has been previously utilized in the context of printers [29]. If we use darker colors for our injected patterns, we are only making the printhead cover with more ink a given area, which will result in the figures being more noticeable. But the contrary is also true; there is a limit below which we cannot make lighter the color of our rectangles, as the printer stops considering those figures as densely inked, and no change to multi-pass print mode is realized. In practice, the light color utilized in our injected patterns throughout this work was close to this threshold, which in all cases resulted in these patterns being invisible to the authors' sight. Appendix A shows a document page with both a human-visible and a true representation of the injected patterns.

The parameters just mentioned have been described in an isolated way, in the context of blank documents, without other graphical objects interfering. We are now going to explore how these graphical patterns coexist with others introduced by a user. There are two cases we may face: (1) a document with equally dense or more densely inked graphical objects that require multiple passes from the printhead, such as images, and (2) a document with sparser graphical objects, such as text, that usually require only a single pass per horizontal area. Just to be clear, documents can contain both elements, but here we study them separately to understand their effects. First of all, if other dense graphical objects are present, the attacker's modulation may not have any effect.

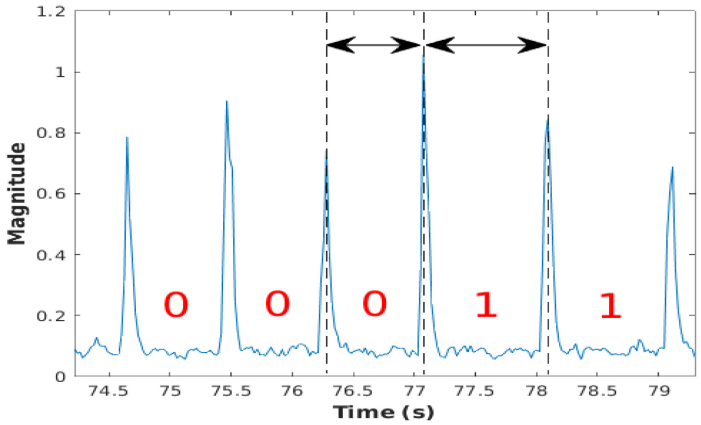

Fig. 6. The acoustical waveform generated by a Canon MG2410 printer, modulated with differential pulse position modulation. In this case, a greater difference in the time between pulses corresponds to a 1 bit, whereas a smaller difference corresponds to a 0 bit.

Both rectangles and the other densely inked objects, such as images, activate the same multi-pass print mode, but because our rectangles use a very light yellow color that requires less ink than what normal images use, and the latter may occupy the entire width of a page, images will be the ones that effectively control the printhead's speed so that any attempt at modulation will be disrupted.

In the second case, if the graphical objects are sparse and they manage to activate lower priority print modes than the one used by the rectangles, such as normal text, the rectangles will effectively define the speed of the printhead and paper displacements. But depending on how much of a page's width the text covers, it may still add a small offset on the printhead's travel time within a given horizontal space, especially if the rectangle's width is smaller than the text's overall width. Returning to the previous example with the two vertically stacked rectangles of different width, if we now overlay some text on that same page, we can observe that if the width of the bigger rectangle is greater than the text's overall width, then the printhead still needs to go all the way up to the other side of the rectangle, thus preserving the time delay observed in the example before. If the smaller rectangle is of less width than the text, the printhead still needs to travel until the end of the text block, but as the text does not need that much ink, the printhead will pass more rapidly than if it were part of the rectangle, resulting in a small added delay. This means that changing the rectangle's width, even if it is smaller than the text's overall width, will still have an effect on the printhead's travel time.

Overall, this is the intuition behind printer modulation, although there are some caveats with particular printers, as explored in Section 5.

4.2 Transmitter

As our attack is only capable of modifying the differences in timing between subsequent paper displacements, such as acoustic pulses, differential pulse position modulation) was a logical choice to use for encoding bits. We defined two different time periods to establish binary transmission, an example of which can be seen in Figure 6. In our communication system, data is split into packets—the payload size of these packets being dependent on the line of printers to which the targeted device belongs. Each page can be used to transmit a single packet, and besides the payload, each packet includes a 4-bit preamble and a parity bit.

4.3 Receiver

Our receiver processes the modulated acoustic signal by breaking it into overlapping segments of 1 second, but first, a matched filter is utilized to robustly detect the packet's starting point jointly with the bit preamble. Then, for each segment, we bandpass filter the signal in a printer model dependent range, after which we compute the root mean square envelope of the filtered signal over a sliding window. The upper envelope is root mean square normalized and downsampled, and finally the peaks' occurrence in time are calculated based on an empirically determined minimum threshold and minimum distance between peaks. Normalizing the signal before locating the signal's peaks is particularly useful for us, as we can establish the same threshold value to detect peaks irrespective of their absolute values, which vary with the attenuating properties of the channel.

4.4 Infecting the Linux Printer Subsystem

In Linux and macOS operating systems, the **Common Unix Printing System (CUPS)** is the current software tasked with managing the interface between the user's computer and its printers. CUPS uses the PostScript Printer Definition file format (PPD) to describe printers' configuration, and a series of filters translate documents being sent to the printer into a final format understandable to it. Back-end filters are the endpoints to this chain of filters whose purpose is sending the data directly to the printers and other filters performing document format conversions and rasterization. The filters that end up being used are generally determined by the document's MIME format, a list of them defined by the configuration file *mime.types*, and the particular chain of filters assigned for each file format being described on the configuration file *mime.convs*. The CUPS standard print job transfer format passed from being PostScript to **Portable Document Format (PDF)** in 2006, so now all important applications send print jobs in that format [33]. Consequently, our attack is designed to inject the imperceptible patterns into PDF files. PDF became standardized as ISO 32000-1 with version 1.7 in 2008 [2]: it is a device and resolution independent file format, with a structured hierarchy of objects that organizes each pages' content. These features make PDF files perfect for our attack, which requires injecting specific patterns at certain pages in a consistent manner.

In our attack model, the malware with necessary privileges will convert the data bits to exfiltrate into a series of patterns to be injected into the documents whenever they are sent by the user's machine to the inkjet printer. By intercepting the documents before they are processed by the printer's driver or subsequent filters, we can succeed in injecting the patterns. This can be done on CUPS by adding a malicious filter at the beginning of the filter chain used to process documents sent to the printer, or by creating a wrapper for one of the existing filters so that it first calls our malicious code and then executes the original intended code. For example, in the former case, to add a malicious filter at the beginning of the filter chain, one can edit the *mime.types* file so as to create a new MIME type paired with PDF files, removing the original pairing expression from the PDF MIME type. One can then link the malicious filter with the new MIME type by including it in the file *mime.convs*, specifying the malicious filter's ending format as the original PDF MIME type so that the document continues through the normal filter chain. By having control of a CUPS filter, we cannot just inject the patterns into the document, but include a series of checks so as to ensure the document is in the appropriate format—for example, we check if images are present in the document and ignore the pages where those are.

5 EVALUATION

To test our attack, we used seven different printers whose characteristics are shown in Table 1. These printers comprise three of the biggest brands for inkjet printers. We made sure to acquire

Table 1. Characteristics of the Printers Used in Our Experiments

Manufacturer	Product Line	Model	Ink Cartridge Model	Type	Ink Storage Technology
HP	DeskJet	1115	664	Thermal	Cartridge
		2722	64		
	ENVY	7155	67		
		7855			
Canon	Pixma	MG2410	PG-145/CL-146		
		TS202	PG-243/CL-44		
Epson	L	4150	504	Piezoelectric	Ink tank

two printers for every line of printers we included, except we only managed to obtain one Epson printer. The Epson printer had a particular significance in our tests, as it is the only printer that is built with a different technology than the others: it uses a piezoelectric ink ejection method and operates with a permanent ink tank, as opposed to using a thermal ejection mechanism with disposable cartridges.

For our tests, we utilized both Samsung Galaxy S8 and iPhone 7 Plus smartphones as recording devices, choosing a sample rate of 44.1 kHz for each of the recordings. Each test was executed under the following conditions: the designated printer was put on a small table and a recording smartphone was placed on a table nearby. The recordings were carried out in a mostly quiet environment, with direct line of sight between the recording device and the printer. For each test, 50 pages were printed in total, although only 25 pages were printed uninterruptedly at once, as the printer trays in some models could not hold all of the 50 pages at a time. For each printer, a random bit payload was first generated and then translated into a specific pattern to be injected into the pages of the document. The document was sent to print via USB connection to the target printer, from a computer with Ubuntu 18.04 and CUPS 2.2.7. It is important to note that using other methods of connection should not contradict our findings, as the attack is effectively embedded into documents. Last, the essential parameters mentioned in Section 4, which define the behavior of the printing process, were obtained experimentally as shown in Section 5.1.

Because of the small differences between printers of a same product line, we decided to test our covert channel with just one printer per product line. The printers that were selected are the following: HP DeskJet 1115, HP ENVY 7855, Canon Pixma MG2410, and Epson L4150. Hereafter, we refer to them without using their specific series number. That said, in Section 5.2 we do describe the small differences between printers of the same product line that we found when tuning their modulation parameters.

Throughout the rest of this section, we report the performance of our covert channel when measured under three varying conditions: distance between the printer and the smartphone, orientation of the smartphone's microphone, and different levels of noise. We also demonstrate the efficiency of the covert communication system when dealing with various types of text layouts, as summarized in Figure 7. Placeholder text was used in each of these layouts.

5.1 Obtaining the Parameters of the Modulation Schemes

As mentioned in Section 4, the minimum rectangle length is one of the most important parameters needed for this attack to succeed. By applying it, we ensure that each printed rectangle produces only one printer roller activation (i.e., one acoustic pulse), thus letting us use effectively the entire

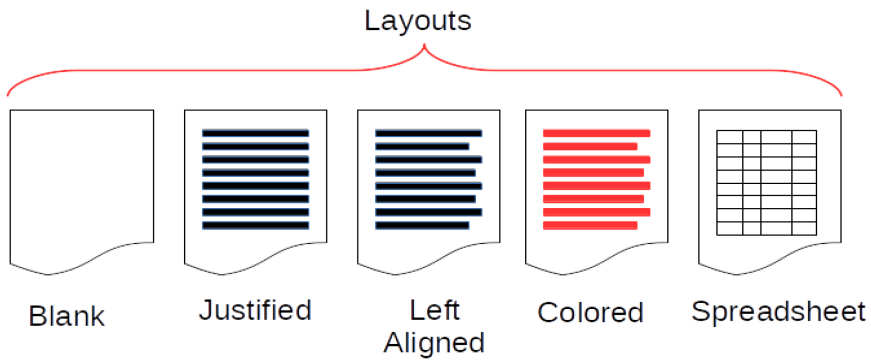

Fig. 7. Five different document layouts were tested to understand the effects of the overlying sparse graphical objects over the injected rectangles.

space of a page. Although theoretically we could obtain the specific rectangle length by measuring the size of the yellow color nozzle columns in a printhead (which would require micrometer accuracy), it is better to use an indirect method that can easily get the exact measurement with no errors. This indirect method consists of a sequence of tests, whereby a rectangle's length is increased in size, until a change in the total number of printer roller activations is produced. The tests are all done in a blank document, where the target rectangle is the only graphical object present. In Figure 8, we give a graphical example of this procedure, and in the next lines, we will describe in detail this simple algorithm. In summary, the steps to be taken are as follows:

(1) Print a rectangle with a short length that only generates a single paper displacement.
(2) Increase the rectangle length until an extra paper displacement is produced.

In the first step, we are forcing the printer to feed in a paper sheet, make a single printhead pass on it, and then eject it immediately. Because the rectangle length is too small and does not need that much ink, the printer will be just using a single-pass mode for the covered area. It is not until the second step that the multi-pass print mode, reserved for densely inked figures, is finally activated, as the rectangle's length will be sufficiently large enough to surpass the limit between print modes. In some printers, the transition between print modes will be reflected by two paper displacements, but in others, the transition may instead produce a greater number of paper displacements (e.g., from zero to three). We refer to the specific rectangle length that produces this transition as the *transition* length. Increasing the size of the rectangle by a constant value hereafter will generate only single extra paper displacements—a constant value that is different from the *transition* length, and which we call the *modulation* length. Increasing the rectangle length by this quantity n times will result in n printer roller activations.

If our goal is binary modulation, as it is in this work, we can design the rectangles such that one of them covers the entire horizontal area of a page, whereas the other one has its width reduced to cover the least amount of horizontal space possible without changing the multi-pass print mode into a single-pass print mode. Finally, the exact yellow tint to be used for the rectangles is found by iterating over brightness values until a change in the print mode is noticed, which is usually when the rectangles stop being visible. The minimum rectangle length ensures that at the border of each rectangle a new paper displacement is produced, but the behavior elicited by a rectangle's width may not be what is expected when facing bit transitions. Specifically, a rectangle covering all of a page's width stacked vertically with a rectangle covering only a part of it may not trigger the expected behavior—that is, the wide rectangle may dominate and the printhead will operate

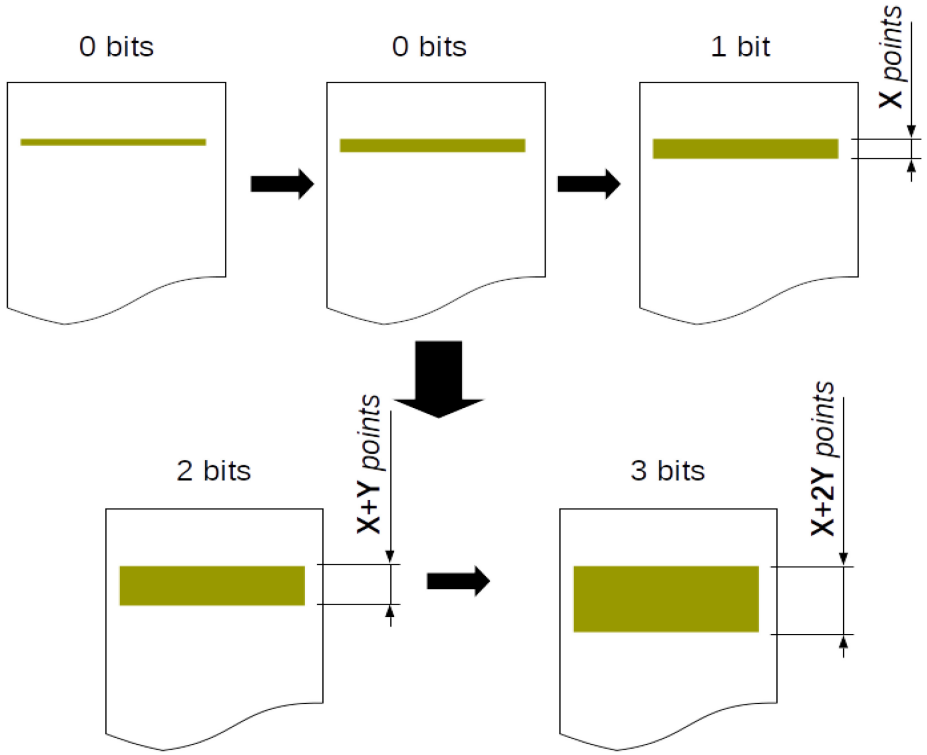

Fig. 8. To obtain the injected rectangles' minimum length for a given printer, we start with a short length that does not activate the multi-pass print mode. We then increase it until a change is noticed. *X* corresponds to the *transition* length, whereas *Y* corresponds to the *modulation* length. At the top of each document, we represent the number of bits that would be possible to transmit.

as if printing in both cases two wide rectangles, and thus no modulation will occur. This may be because of some small overlapping area between rectangles or some imprecision on the printing mechanism. Nevertheless, fixing this problem just requires inserting some buffering (extra rectangles with small width) when making transitions between rectangles of different width. In practice, we also make each rectangle be double the minimum length needed to produce a printer roller activation, which provides us with some robustness.

Table 2 presents some of the results we obtained with respect to the main parameters and performance metrics. It is important to note that the number of payload bits per page we define in that table is a practical estimate, not the theoretical maximum, given the constraints we found when executing the experiments. Our payload bits per page metric is limited, first by the total vertical area of a paper page, which coupled with the injected rectangle's minimum length establish a hard limit on the total number of rectangles that may be printed. But as a matter of fact, the printer also introduces document margins beyond which the device does not operate, which further limits the total space to be exploited on a page, although to be fair these margins are normally close to the pages' edges. The next three factors also constrain the total number of bits per page: each rectangle in our implementation occupies two times the minimum size, padding is used at the beginning and end of pages to isolate acoustic pulses from the initial and ending noises produced by the printer, and finally a part of a page's bottom may be left unused. This last constraint is necessary because in some printers, as the page progresses through the printer and the printing process approaches its

Table 2. Attack Design Parameters and Performance Metrics for Each Printer

Printer	Minimum Rectangle Length	Payload Bits per Page	Net Bit Rate	Max. Bandwidth	Bandwidth Efficiency
HP DeskJet	0.40 cm	11	0.53 bps	6.32 Hz	0.08 bit/s/Hz
HP ENVY	1.40 cm	11	0.80 bps	6.27 Hz	0.13 bit/s/Hz
Canon Pixma	0.68 cm	9	0.28 bps	2.85 Hz	0.10 bit/s/Hz
Epson L	0.82 cm	9	0.42 bps	1.02 Hz	0.41 bit/s/Hz

end, the amplitude of the acoustic pulses decay, as some of the printer rollers stop having contact with the page, and thus we avoid the bottom area to not compromise the communication range of the covert channel.

Because the printing process is a relatively slow procedure, the net bit rate is not that high, but it can still serve to exfiltrate small bits of sensitive information. In Table 2, maximum bandwidth refers to the theoretical maximum bit rate we could obtain if we used all the capabilities of the injected patterns (i.e., if we could mix dark yellow colored rectangles that cover all the horizontal area of a page with almost invisible rectangles that occupy a tiny fraction of that same area). By combining different quantities of color brightness levels and rectangle lengths on a blank paper to achieve multi-level modulation, ideally we could reach those maximum rates. But because we are constrained by the light yellow tint, which should be invisible to human sight, and by any overlying text that may be in place, it is difficult to achieve the theoretical maximum. Finally, the observed time differences between printer roller activations are sometimes not that consistent, which would therefore make our attempt at multi-level modulation even more error prone when coupled with the other constraints. In Table 2, we show how much of the theoretical maximum bandwidth our attacks use.

5.2 Variance Across Lines of Printers

Based on our experiments, we found that printers of the same manufacturer share many characteristics such that an attacker only needs to know a printer of the same product line to exploit another. Although printers within a line are divided by specific series (e.g., HP ENVY 7800 series and 7100 series), we found that for the purposes of our attack these differences were almost insignificant. In particular, for the two printers of the HP ENVY product line (i.e., 7155 and 7855), we found no modification was needed on the modulation parameters. Thus, if an attacker characterizes one of these, the extracted parameters will work for both printers. The other pairs of printers that belong to distinct product lines do not share this convenience—first of all because they use different ink cartridge models, as can be seen in Table 1. As ink cartridges may produce different tints for the same color values on a document depending on their model, it is expected that the attacker will need some recalibration to obtain again the exact yellow tint that hides the injected rectangles. Another difference we found on the Canon Pixma and HP DeskJet printers is that the *transition* length is of different size, although this is not a serious problem because the attacker can select the greatest of them and use it for both printers of a specific product line. For Canon Pixma printers, we did find that besides the previously mentioned differences, the amount of buffering between bit transitions does change by a small factor.

Unfortunately, although no other parameter change was apparently needed for the HP DeskJet 2722, with respect to the 1115 model used as the baseline, the fact is that this printer model seems to apply a type of rate-limiting mechanism that directly affects the malicious modulation. In our experiments, we found that large sequences of rectangles with a small width, which should increase the rate of paper displacements, were instead printed at a slower rate, both in text and blank docu-

Table 3. Distance vs. BER Results

Printer	Distance							
	Facing Printer				180° from Printer			
	50 cm	2 m	4 m	8 m	50 cm	2 m	4 m	8 m
HP DeskJet	3.82%	3.45%	4.18%	30.91%	4.36%	6.73%	26.73%	72.00%
HP ENVY	2.91%	2.00%	2.18%	2.73%	3.64%	5.64%	10.36%	18.73%
Canon Pixma	2.22%	2.89%	2.00%	5.56%	3.11%	2.00%	3.11%	52.44%
Epson L	3.56%	2.89%	3.56%	22.89%	3.11%	4.44%	4.89%	26.22%

ments, thus making our modulation ineffective. Indeed, this particular printer model inadvertently deploys a defense against our attack by homogenizing the printing process, an effect that clearly has an impact in its overall performance. Compared with the HP DeskJet 1115 results shown in Table 3, a BER of approximately 20% (against a BER of 3.82%) was the minimum we could obtain with the HP DeskJet 2722 when printing a document with left-aligned black text at 50 cm. What we did observe is that if the rectangles are instead filled with black color, our modulation may be possible in this printer, but clearly any attempt at stealth fails immediately.

All things considered, results demonstrate that lines of printers do share modulation parameters. Whether other mechanisms are in place is another story. In particular, results obtained from the HP ENVY printers tell us that testing a printer from the same product line, and one that uses the same ink cartridge/bottle models, is enough to find the specific modulation parameters of the target printer.

5.3 Distance and Receiver Orientation

To test the robustness of our covert channel with respect to distance and the orientation of our smartphone receiver, a series of tests were carried out to measure the overall BER, with the results shown in Table 3. For these tests, a 50-page document with left-aligned blocks of text and 12-point Arial font was used, except for the HP ENVY printers, where blank documents were used for convenience (i.e., to save ink), as we did not observe any significant performance difference with respect to text documents. Four different distances between the printer and receiver were considered: 50 cm, 2 m, 4 m, and 8 m. Smartphones' MEMS microphones have been shown previously to be sensitive to the angles of incidence of the incoming acoustic signals, especially as the frequency of the signal increases [8], so two different orientations were tested when laying a smartphone flat on a table: having the microphone face the noise source and having the microphone facing 180° away from the noise source. BER was calculated using the Hamming distance between the actual received payload and the transmitted one.

From the results shown in Table 3, we can note that at 50 cm and until 4 m we can achieve in all cases a BER lower than 5%, when the smartphone's microphone is facing the noise source. When the smartphone is not facing the printer, at 4 m we find that printers from the HP DeskJet product line, and to a small degree from the HP ENVY line, may start suffering in performance. At 8 m, only the HP ENVY and Canon Pixma printers still maintain a low BER. Results show that the smartphone's orientation does affect performance, but it is only really apparent after a certain distance from the printer. The variation in BER with distance seems to be roughly correlated to the power of the noise produced by the printers, and similar results can be obtained when testing the robustness of the covert channel to noise. By adding Gaussian noise to the original recordings at 50 cm from the printer, and varying the signal-to-noise ratio, we can obtain a better

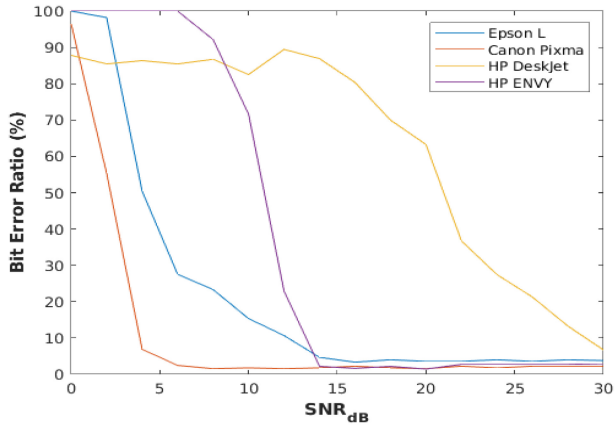

Fig. 9. BER according to the signal-to-noise ratio of the signal.

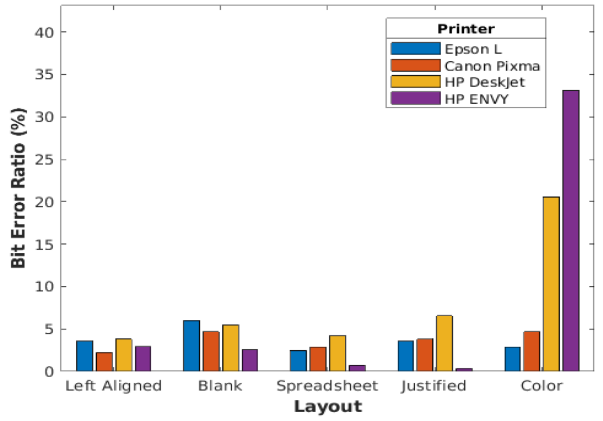

Fig. 10. BER according to the layout used on different printers.

characterization of the communication system, with the results shown in Figure 9. It is clear that the HP DeskJet printer is the one that suffers the most in performance with increasing noise and increasing distance. Qualitatively speaking, it is also the printer whose rollers produce the faintest sounds. With respect to the other printers, it is important to note that a factor that influences their robustness toward noise is related to the receiver parameters—that is, receiver frequency range, amplitude threshold, and smoothing window, all of which differ with respect to the product line.

5.4 Changing the Documents' Layout

Five different layouts were utilized to test the impact of the overlying text on the printing process. Figure 10 shows the results that were obtained at 50 cm from the source. Although we are aware that the number of layouts found on existing documents can be infinitely large, we selected the layouts shown in Figure 7 to test particular attributes found on documents that could affect the attacker's modulation. The chosen layouts were the following: a document with left-aligned 12-point black Arial text, another one with the same type of text but with justified alignment, and

a third one exactly the same as the first one but with red as the text's color; we also included a spreadsheet-type document with a table covering all the pages and, finally, a blank document. The left-aligned text document served as the baseline. This document had the particularity of including lines of text that covered a different amount of the width of a page, which we thought could affect the modulation. This is because, as we described in Section 4, when text overlays our injected rectangles and these rectangles cover less horizontal space than the text width, a small time offset may appear on the time measurements that depends on that same text width. The document with justified text was used to test if any improvement could be seen by making the width of the text constant. The document with a table was used just to test whether lines instead of text could affect the modulation, especially the vertical lines that leave no space between contiguous rows of a page. The document with red-colored text was used to test whether utilizing the same yellow color for the text (as red is a combination of yellow and magenta) would somehow interfere with the modulation. Finally, a blank document was used to test the modulation when facing considerable blank spaces on text documents.

The layout had no significant effect on the acoustic modulation except for a few cases, as can be observed in Figure 10. In particular, when using the colored text layout with HP DeskJet and HP ENVY printers, the BER increases considerably. This was discovered to be a consequence of the fact that these lines of printers introduce an intermediate print mode between the single-pass mode used for black text and the multi-pass mode used for images, which interferes with our modulation. This intermediate print mode is used specifically for sparsely colored graphical objects, which is what the colored text represents. As this type of text requires greater detail than normal black text and it encompasses the width of a page, the narrower injected rectangles will stop producing the fast printhead travel times, and modulation will be disrupted. This effect is not only seen in colored layouts but also when including any text that is not perfectly black, as shades of gray are in practice done with colored input.

A second point of interest with these layouts is with respect to blank documents. As blank documents do not include any text, this means that rectangles with a small width will produce an even faster printer roller activation (paper displacement) than would occur in text documents, because now the printhead does not need to always travel through all the width of a page. For the Epson, Canon, and HP ENVY printers this is not an issue, but for the HP DeskJet printers, the problem is that both wide rectangles and rectangles with smaller width produce a faster response in the printhead travel time that enters into conflict with the original receiver parameters. This means that if the receiver uses the same parameters as those used for text documents (i.e., the time period ranges associated with a 1-bit or 0-bit), the attacker will find that an overlap occurs with the actual time periods produced by the wide and narrow rectangles in the blank documents. A separate set of receiver parameters for blank and text documents is needed in this case, which means that for HP DeskJet printers, there may be problems when combining text with large spaces unless proper action in the receiver is taken.

6 COUNTERMEASURES

The attack presented in this article is designed to work as covertly as possible; however, the reality is that it still leaves some physical evidence on printed documents. The traces left are not visible to humans in normal light conditions, so supplementary equipment is needed to check if a document has been injected with the attack patterns designed here. Thus, we present two ways of detecting if a computer is using our covert channel: (1) by pointing a blue LED into the suspected paper pages, the clusters of tiny dots become visible as black-colored dots, basically as a consequence of yellow being the complementary color of blue (i.e., the blue light is absorbed completely by the

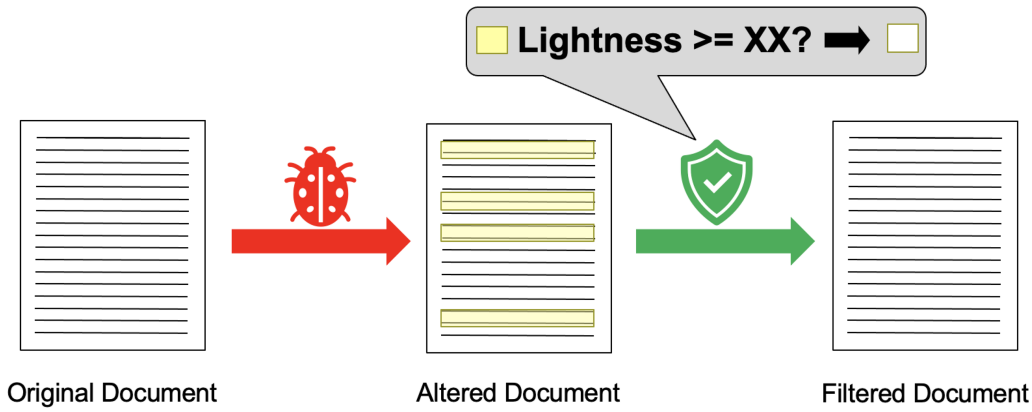

Fig. 11. The proposed defense sanitizes any document that passes through the printer's filter chain, removing very light yellow tints that are injected by the malware.

dots); (2) by using a high-resolution scanner (>600 dpi) to scan the document, clusters of tiny dots will be visible when closely inspecting the resulting digital image [6]. However, these measures may require some special efforts that may not be practical or scalable. That is why we enumerate two methods for making the covert channel ineffective.

In one method, a naive solution is to simply fill all pages sent to print with the same light yellow colored rectangles that are used for covert transmission. This will force the printer to always be in the multi-pass print mode, and make the printhead travel across the entire width of the page at each paper displacement, effectively homogenizing the printing process. Only visible images would then have an effect on the printing process, as these require a more careful printing process. Although humans would not be able to distinguish the yellow background, yellow ink may still deplete at a slightly faster rate than normal. There are some methods we can use to optimize the ink usage for these rectangles, but the reality is that making the printer always operate in multi-pass mode may inflict a terrible loss on time performance. As can be seen in Table 4, in the context of our attack, always activating the multi-pass print mode can significantly increase the time it takes for printers to operate on a page—sometimes more than double the normal time.

A second method that is a more pragmatic approach is simply to disable yellow tints lighter than a certain threshold, which when crossed would automatically convert the color to white, so the printer does not try to print any apparently invisible figure. This would be inconsequential for printing, as the yellow tints we use are imperceptible to human beings and one cannot distinguish them from the white background of paper pages. Even in colored pages, because the ink used in printers has some transparency and applying it on those type of pages results instead on darker patches of color that are also difficult to see, there is no need to enable support for very light yellow tints. Checking for these colors should be very easy to implement at any level of the printer system so that any attack that wishes to modulate the printer's acoustic emanations necessarily needs to use darker colors, which are totally visible and would defeat the purposes of the attack. Our particular implementation installs itself on the same printer's filter chain that is originally leveraged by the malware, but it needs to be placed after it in the filter chain so that any change the malware does is automatically neutralized by our defense mechanism, as can be seen in Figure 11. Similar to how the malware operates, our benign filter checks every content stream of any PDF file sent to the printer and then sets to white the arguments to any color instruction that uses a yellow color lighter than a certain threshold. All tests made with each printer were successful. Last, it is clear that any malware that installs itself deeper into the filter chain will require a defense

Table 4. Time Duration of the Printing Process for a Normal Text Document vs. Time Duration of the Printing Process for an Altered Text Document

Printer	Time Duration	
	Normal	Altered
HP DeskJet	13.45 s	20.69 s
HP ENVY	7.75 s	13.76 s
Canon Pixma	33.45 s	32.22 s
Epson L	8.01 s	21.54 s

mechanism that is installed even deeper, until any defense will need to be implemented at the firmware level of the printer. We leave this implementation for future work.

More elaborate countermeasures could be based on the time it takes for the printer to print certain documents, or even one could consider the frequency of sounds made during the printing process according to the graphical object being printed. For example, text documents without images should not take that much to print in normal conditions and should produce pulses with a certain frequency. Previous work in 3D printing has employed sound signatures to validate that the printed object is not being sabotaged [5]. From the manufacturer's perspective, homogenizing the printing process to produce constant sounds irrespective of the type of document might prevent this type of attack, but it would entail a huge performance cost as printing would take a lot more of time. A more effortless way of dealing with this problem would be simply producing artificial noise so as to mask the noise generated by the printer, or just restricting access to the printer by moving it to a monitored soundproof room. By using a monochrome inkjet printer instead, it would be obvious when the documents are intervened, as the yellow color would be converted into grayscale, rendering visible the injected stripes. At the level of computer software, creating a checksum for each of the CUPS filters could prevent any kind of modification of the filter chain, although control over the implementation of new filters should be also monitored.

7 LIMITATIONS

Overall, the greatest limitation in the design of the covert channel presented in this article is its ineffectiveness when dealing with documents containing densely colored figures, which by nature of their design capture control of the printhead and make our imperceptible rectangles ineffective. Although we could vary the color brightness in the images themselves instead of introducing our patterns, the problem is that the magnitude of the changes need to be significant to produce an effect on the printing process, defeating the stealthiness of the attack. Another significant limitation is the sensitivity that some lines of printers may have with respect to document layouts. Although all seem to work with plain text documents, as was shown in Section 5, acoustic modulation on HP DeskJet printers may not be effective for two reasons: (1) if the documents contain sparsely colored graphical objects that cover a substantial part of a page (a constraint also seen in HP Envy printers) or (2) if we mix large spaces with text. Furthermore, we found that the HP DeskJet 2722 model particularly seems to mitigate our attack by limiting the effect of rectangles with a small width on the printing speed. Thus, the success of the attack may be dependent on the ability of the attacker to obtain a printer with the same product line or model as the targeted one, in which to first test the parameters for the covert communication channel. Future work should try to note how many lines of printers are agnostic or not to document layouts, and how many printers have a rate-limiting mechanism like the one implemented by the HP DeskJet 2722.

With regard to the distance from the printer one can place the receiver without any performance loss, it was noticed that as distance increased, error rates did as well but by different magnitudes depending on the type of printer. To test the effect of walls in the recording capabilities of our receiver, we performed a set of short experiments where we found that although printers operating in a closed room can be heard perfectly from outside the room, it was impossible for us to record the acoustic signals with the microphone of the smartphone we used. Only when we placed that same smartphone on the space between the door and the floor did we manage to capture the signal without significant errors. This may be conducive to using more powerful microphones in future work to substantially extend the range of our covert channel, although this would make it more difficult to maintain stealthiness. Noise is another factor to be considered when using the covert channel introduced in this work, as it can clearly impact the performance of it, as seen in Section 5.3. Future work may need to test the covert channel with noise from real world settings and not only with artificially added Gaussian noise, as in this work.

Finally, testing laser printers to see if they can be manipulated with imperceptible patterns like the ones shown in this article would amplify an attacker's range of operation and would make exploitable almost all printers actually used in office settings. Implementing our attack on computers with operating systems other than Linux is also left for future work.

8 DISCUSSION

Q1: How usable is the covert communication system described in this article when compared with other speakerless acoustic covert channels? First of all, InkFiltration does not necessarily rely on any technology that is in the process of being phased out, like hard disk drives being slowly replaced by Solid State Drives (SSDs), CD/DVD drives that are simply falling into disuse along with the storage format they support, or fans being simply removed in fanless personal computers. In contrast, inkjet printing is not only still relevant for paper printing but also has become more important in the field of electronics manufacturing [26]. Moreover, InkFiltration does not compete with the user for access to the exploited device—that is, it does not need the CPU, fan, CD/DVD, or hard disk to be idle. Our attack can operate successfully whether or not a user is using the printer. Only images and colored text in some printers can present problems. This means that either injecting a payload into user's documents or printing blank documents with this payload is an effective way of exfiltrating information. In addition, the covert channel presented in this article can almost perfectly camouflage inside an office environment, as the attack employs the normal capabilities of printers (i.e., no abnormal sounds are produced that could alert a user). Finally, as mentioned before, printers are ubiquitous in offices, which means that these devices end up being shared by many users and are required to be placed on accessible locations, contrary to personal computers, whose approach by non-users may raise suspicions.

Q2: Does this attack require an in-depth knowledge of the printer and its hardware? No, the process of obtaining the parameters is simple—it only requires the attacker to do a series of tests from its computer, as described in Section 5.1; there is no need to delve into the electrical or mechanical design of the printer. In fact, once the attacker knows the product line to which the printer belongs, the modulation parameters can be extracted from other printers from the same product line, and some further tuning may just be necessary depending on the ink model the printer uses.

Q3: How do noise and distance affect the performance of the printer? As printers differ on their design, the power of the acoustic signals may vary, and thus they may be more susceptible to noise or spatial decay, as shown in Section 5.3. That said, the receiver parameters also influence this, as different lines of printers may need their acoustic signals to be processed at distinct ranges of frequency, and their pulses may require different thresholds to be applied.

9 RELATED WORK

Covert channels that use acoustic emanations from personal computers to exfiltrate information have been the particular subject of previous research. For example, by alternately turning speakers and headphones connected to a computer into input and output devices via jack retasking, a covert two-way communication channel can be established at the ultrasound level [18]. But on more constrained settings with speakerless computers, leveraging mechanical components' noise-generating capabilities, like in the case of CD/DVD drive noise [11], fan noise [16], and hard disk drive noise [17] or exploiting the noise produced by vibrations from electrical components in a switch-mode power supply [12] have all provided reliable results. These covert channels rely mostly on computers' internal components and require a degree of control over the targeted device's emissions, contrary to our covert channel that can work either when the printer is being used by a user or when it is not being actively used. There has also been certain work on cyber-physical systems in this domain, in which control signals driving physical instrumentation are altered to produce specific acoustic signals without significantly affecting the closed-loop system [22], although this work has only been evaluated with the help of a testbed emulating the targeted industrial control system.

To the best of our knowledge, the covert transmission system detailed in this article is the first one to be designed for printers. Regarding printers' unintended emanations, Backes et al. [4] revealed how a dot matrix printer's acoustic emissions could be leveraged to recover the text being printed. Laser printer emanations have also been investigated before, with results indicating that electromagnetic emissions can be leveraged in the same way to reconstruct the document being printed [34]. In the realm of additive technologies, also known as 3D printing, acoustic emanations have been utilized previously to re-create the G-codes used for prototype design in fused deposition modeling [3]. Capturing both acoustic emanations and magnetic emanations with a smartphone from this type of printer has also been done previously to recover the G-codes [32]. Altering the compiler that generates these G-codes so as to modify the printing process to maximize the leakage information, a procedure similar in nature to the way we modify documents to establish a deterministic communication channel, has been done in the work of Chhetri et al. [27].

Some research has instead focused on the printers' acoustic emissions for the purpose of defending the printing process from sabotage, producing a digital signature that can be compared with further printings of the same object and can detect changes in particular G-codes [5]. The only previous work found to exploit printers' capabilities to establish a covert channel is that of Nassi et al. [25], where it is shown that by using a multi-function printer, one can establish a duplex channel by exploiting the optical characteristics of an integrated scanner. By transmitting data through an optical source when the scanner is operating, and receiving an acknowledgment by capturing the scanner's optical output with a camera, one can establish the communication system. But this covert channel does not exploit the emanations of a printer as such—it only makes use of its integrated scanner.

As our attack is based on injecting patterns that are imperceptible to humans into documents, it is worth mentioning some previous research on this realm. The Electronic Frontier Foundation revealed in 2005 that manufacturers of laser printers had been using imperceptible tiny yellow dots arranged in grids as watermarks, for each of the documents printed by those type of devices [29]. Specifically, the tracking mechanism they discovered encoded the serial number of the printer in use, as well as the date and time of the printing process. Inspired by these revelations, Briffa et al. [6] explored a way to create a similar tracking system for inkjet printers, based as well on the use of yellow dots. As can be seen, injecting imperceptible patterns into printed documents is nothing new, and its stealthiness has been demonstrated before, but the purpose for which we used them in this work may definitely be new.

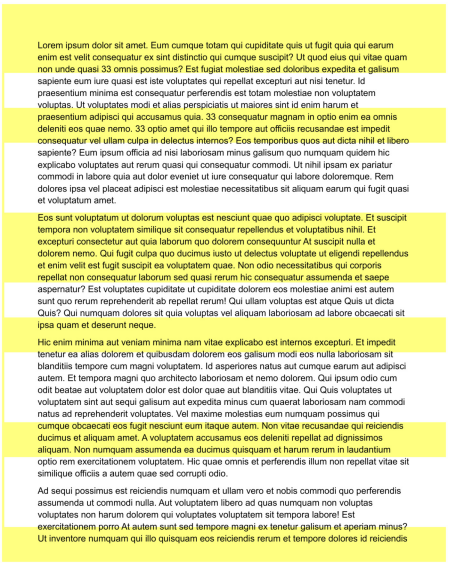

Fig. 12. Document page that shows how the injected patterns would be seen if their color were visible to human beings.

10 CONCLUSION

As has been described throughout this article, since printers are omnipresent in places of work, they can pose a grave danger to organizations if left unmonitored. Acoustic emissions can be used as a means to exfiltrate sensitive information from internal computer networks. As a result, organizations and individuals need to constantly monitor these devices for any unexpected behavior. Since these devices may be on an air-gapped network, it is not possible to keep them secure with over-the-air updates, and hence the onus to protect them lies completely on the individual or organization owning them.

In this work, we present a new type of acoustic covert channel attack that targets inkjet printers. To achieve this, a relationship was first discovered that linked the layout of graphical objects in a document with the noise generated by a printer. We exploited this relationship by injecting special imperceptible patterns into all documents being sent to print, thus modulating the printing process in such a way that a deterministic communication channel was established using the acoustic emanations. We also found that lines of printers share design characteristics that allow us to use a single set of attack parameters for all of them, with small alterations needed in some cases. Finally, we evaluated the attack with seven printers by testing the communication range of the covert channel and robustness toward document layouts and noise. The results reveal that on average, a receiver close to the printer, up to 4 m, will achieve a BER lower than 5%. We also propose a set of defense techniques that may lessen the danger these devices represent, but further attack vectors may arise that consider other types of emanations.

APPENDIX

A SAMPLE OF A DOCUMENT PAGE WITH INJECTED PATTERNS

In Figures 12 and 13 of this appendix, we show a sample page of a PDF document with injected patterns. The difference is that Figure 12 shows how these patterns would be seen if they were totally human visible, whereas Figure 13 shows the patterns with the actual color used in the

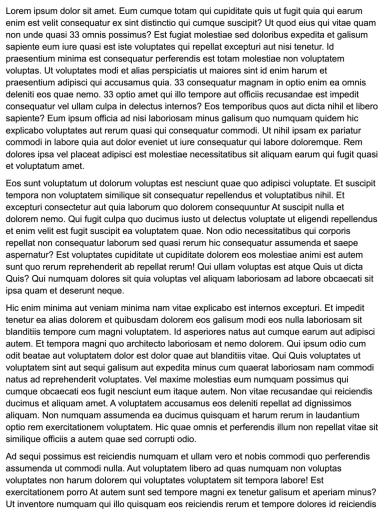

Fig. 13. Document page that shows how the injected patterns would actually be seen.

attack. It is necessary to emphasize that the correspondence between the color observed on a PDF document and on a printed page are not exact—that is, although patterns may appear somewhat visible on a PDF page, on a printed page they may be totally invisible.

REFERENCES

[1] WikiLeaks. 2016. Brutal Kangaroo—Drifting Deadline v1.2: User Guide. Retrieved October 11, 2020 from https://wikileaks.org/vault7/document/Brutal_Kangaroo-DriftingDeadline-V1_2-User_Guide/.

[2] Adobe Systems Inc. 2008. *Document Management—Portable Document Format—Part 1: PDF 1.7.* Adobe Systems Inc. https://www.adobe.com/content/dam/acom/en/devnet/pdf/PDF32000_2008.pdf.

[3] M. A. Al Faruque, S. R. Chhetri, A. Canedo, and J. Wan. 2016. Acoustic side-channel attacks on additive manufacturing systems. In *Proceedings of the 2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS'16)*. 1–10.

[4] Michael Backes, Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, and Caroline Sporleder. 2010. Acoustic side-channel attacks on printers. In *Proceedings of the 19th USENIX Conference on Security (USENIX Security'10)*. USA, 20.

[5] S. Belikovetsky, Y. A. Solewicz, M. Yampolskiy, J. Toh, and Y. Elovici. 2019. Digital audio signature for 3D printing integrity. *IEEE Transactions on Information Forensics and Security* 14, 5 (2019), 1127–1141.

[6] J. A. Briffa, C. Culnane, and H. Treharne. 2010. Imperceptible printer dot watermarking for binary documents. In *Optics, Photonics, and Digital Technologies for Multimedia Applications*, Peter Schelkens, Touradj Ebrahimi, Gabriel Cristóbal, Frédéric Truchetet, and Pasi Saarikko (Eds.), Vol. 7723. International Society for Optics and Photonics, SPIE, 166–174. https://doi.org/10.1117/12.854708

[7] Joey Chen. 2020. Tropic Trooper's USBferry Targets Air-Gapped Networks. Retrieved October 2, 2020 from https://www.trendmicro.com/en_us/research/20/e/tropic-troopers-back-usbferry-attack-targets-air-gapped-environments.html.

[8] I. Djurek, T. Grubeša, and N. Orlić. 2019. Measurements of analog MEMS microphones. In *Proceedings of the 2019 2nd International Colloquium on Smart Grid Metrology (SMAGRIMET'19)*. 1–4.

[9] Nicolas Falliere, Liam O. Murchu, and Eric Chien. 2011. *W32.Stuxnet Dossier*. Technical Report. Symantec. https://www.wired.com/images_blogs/threatlevel/2011/02/Symantec-Stuxnet-Update-Feb-2011.pdf.

[10] Mordechai Guri. 2020. AiR-ViBeR: Exfiltrating data from air-gapped computers via covert surface ViBrAtIoNs. arXiv:2004.06195 [cs.CR].

[11] M. Guri. 2020. CD-LEAK: Leaking secrets from audioless air-gapped computers using covert acoustic signals from CD/DVD drives. In *Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC'20)*. 808–816.

[12] Mordechai Guri. 2020. POWER-SUPPLaY: Leaking data from air-gapped systems by turning the power-supplies into speakers. arXiv:2005.00395 [cs.CR].

[13] M. Guri, O. Hasson, G. Kedma, and Y. Elovici. 2016. An optical covert-channel to leak data through an air-gap. In *Proceedings of the 2016 14th Annual Conference on Privacy, Security, and Trust (PST'16)*. 642–649.

[14] M. Guri, M. Monitz, and Y. Elovici. 2016. USBee: Air-gap covert-channel via electromagnetic emission from USB. In *Proceedings of the 2016 14th Annual Conference on Privacy, Security, and Trust (PST'16)*. 264–268.

[15] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici. 2015. BitWhisper: Covert signaling channel between air-gapped computers using thermal manipulations. In *Proceedings of the 2015 IEEE 28th Computer Security Foundations Symposium*. 276–289.

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

[17] Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici. 2017. Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise ('DiskFiltration'). In *Computer Security—ESORICS 2017*, Simon N. Foley, Dieter Gollmann, and Einar Snekkenes (Eds.). International, Cham, Switzerland, 98–115.

[18] M. Guri, Y. Solewicz, and Y. Elovici. 2018. MOSQUITO: Covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker communication. In *Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC'18)*. 1–8.

[19] M. Guri, B. Zadov, and Y. Elovici. 2020. ODINI: Escaping sensitive data from Faraday-caged, air-gapped computers via magnetic fields. *IEEE Transactions on Information Forensics and Security* 15 (2020), 1190–1203.

[20] Mustafa Kamasak, Anand V. Deshpande, Kok Leong Thoon, Charles A. Bouman, George T.-C. Chiu, and Jan P. Allebach. 2001. Dynamic print mode control for inkjet printing. In *Proceedings of the 2001 International Conference on Digital Printing Technologies*. 78–82. https://www.ingentaconnect.com/content/ist/nipdf/2001/00002001/00000001/art00014.

[21] Kaspersky Lab. 2016. *The ProjectSauron APT*. Kaspersky Lab. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07190154/The-ProjectSauron-APT_research_KL.pdf.

[22] P. Krishnamurthy, F. Khorrami, R. Karri, D. Paul-Pena, and H. Salehghaffari. 2018. Process-aware covert channels using physical instrumentation in cyber-physical systems. *IEEE Transactions on Information Forensics and Security* 13, 11 (2018), 2761–2771.

[23] Daniel L. Lau and Gonzalo R. Arce. 2008. Introduction. In *Modern Digital Halftoning* (2nd ed.). CRC Press, Boca Raton, FL, 1–19.

[24] Je-Ho Lee and J. P. Allebach. 2005. Inkjet printer model-based halftoning. *IEEE Transactions on Image Processing* 14, 5 (2005), 674–689. https://doi.org/10.1109/TIP.2005.843787

[25] B. Nassi, A. Shamir, and Y. Elovici. 2019. Xerox day vulnerability. *IEEE Transactions on Information Forensics and Security* 14, 2 (2019), 415–430.

[26] Laxmidhar Nayak, Smita Mohanty, Sanjay Kumar Nayak, and Ananthakumar Ramadoss. 2019. A review on inkjet printing of nanoparticle inks for flexible electronics. *Journal of Materials Chemistry C* 7, 29 (2019), 8771–8795. https://doi.org/10.1039/C9TC01630A

[27] S. Rokka Chhetri, A. Barua, S. Faezi, F. Regazzoni, A. Canedo, and M. A. Al Faruque. 2021. Tool of spies: Leaking your IP by altering the 3D printer compiler. *IEEE Transactions on Dependable and Secure Computing* 18, 2 (2021), 667–678.

[28] Ignacio Sanmillan. 2020. Ramsay: A cyber-espionage toolkit tailored for air-gapped networks. Retrieved October 12, 2020 from https://www.welivesecurity.com/2020/05/13/ramsay-cyberespionage-toolkit-airgapped-networks/.

[29] Seth Schoen. 2005. Secret code in color printers lets government track you. *Electronic Frontier Foundation*. Retrieved October 10, 2020 from https://www.eff.org/press/archives/2005/10/16.

[30] C. Shen, T. Liu, J. Huang, and R. Tan. 2021. When LoRa meets EMR: Electromagnetic covert channels can be super resilient. In *Proceedings of the 2021 IEEE Symposium on Security and Privacy (SP'21)*. IEEE, Los Alamitos, CA, 1304–1317. https://doi.org/10.1109/SP40001.2021.00031

[31] Atasheh Soleimani-Gorgani. 2016. Inkjet printing. In *Printing on Polymers*, Joanna Izdebska and Sabu Thomas (Eds.). William Andrew Publishing, 231–246. https://doi.org/10.1016/B978-0-323-37468-2.00014-2

[32] Chen Song, Feng Lin, Zhongjie Ba, Kui Ren, Chi Zhou, and Wenyao Xu. 2016. My smartphone knows what you print: Exploring smartphone-based side-channel attacks against 3D printers. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS'16)*. ACM, New York, NY, 895–907. https://doi.org/10.1145/2976749.2978300

[33] The Linux Foundation. 2016. *PDF as Standard Print Job Format*. The Linux Foundation. https://wiki.linuxfoundation.org/openprinting/pdf_as_standard_print_job_format.

[34] Cihan Ulaş, Ulaş Aşik, and Cantürk Karadeniz. 2016. Analysis and reconstruction of laser printer information leakages in the media of electromagnetic radiation, power, and signal lines. *Computers & Security* 58 (2016), 250–267. https://doi.org/10.1016/j.cose.2016.02.001

[35] Faheem Ullah, Matthew Edwards, Rajiv Ramdhany, Ruzanna Chitchyan, M. Ali Babar, and Awais Rashid. 2018. Data exfiltration: A review of external attack vectors and countermeasures. *Journal of Network and Computer Applications* 101 (2018), 18–54. https://doi.org/10.1016/j.jnca.2017.10.016

[36] Matthias Wandel. n.d. Un-building an ink jet printer. Retrieved October 8, 2020 from https://woodgears.ca/tech/printer.html.

[37] Ziqi Wang, Zhe Chen, Akash Deep Singh, Luis Garcia, Jun Luo, and Mani B. Srivastava. 2020. UWHear: Through-wall extraction and separation of audio vibrations using wireless signals. In *Proceedings of the 18th Conference on Embedded Networked Sensor Systems*. 1–14.

[38] Colin Ware. 2004. Color. In *Information Visualization: Perception for Design* (Interactive Technologies) (2nd ed.). Morgan Kaufmann, San Francisco, CA, 95–141.

[39] Zhice Yang, Qianyi Huang, and Qian Zhang. 2017. NICScatter: Backscatter as a covert channel in mobile devices. In *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking (MobiCom'17)*. ACM, New York, NY, 356–367. https://doi.org/10.1145/3117811.3117814

[40] Zihao Zhan, Zhenkai Zhang, and Xenofon Koutsoukos. 2020. BitJabber: The world's fastest electromagnetic covert channel. In *Proceedings of the 2020 IEEE International Symposium on Hardware Oriented Security and Trust (HOST'20)*. 35–45. https://doi.org/10.1109/HOST45689.2020.9300268

Received October 2021; accepted January 2022