

PrinterLeak: Leaking Sensitive Data by Exploiting Printer Display Panels

Mordechai Guri(✉)

Department of Software and Information Systems Engineering,
Cyber-Security Research Center, Ben-Gurion University of the Negev,
Be'er Sheva, Israel
gurim@post.bgu.ac.il
http://www.covertchannels.com

Abstract. Sensitive networks hold and process confidential information and, therefore, are kept separate from the Internet. This defensive measure is known as an 'air gap.'

In this paper, we show that attackers can exploit networked printers to exfiltrate data from air-gapped networks. We show that malware in the network can control the printer display screen and status LEDs and modulate sensitive information over them using documented and undocumented firmware and software level commands. Local or remote adversaries can intercept and decode these signals from a few meters to hundreds of meters away. For reception, they can use a smartphone, a local surveillance camera, or camera mounted on a drone. The display panels of printers are currently not monitored or protected by any security measures, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS), which makes this attack highly evasive. We provide technical details, discuss the attack model, and present related work. We evaluate this new type of attack and discuss the necessary countermeasures, both defensive and preventive.

Keywords: air-gap · networks · exfiltration · covert channel · optical · printer · LCD display

1 Introduction

Organizations protect their IT networks with many tiers of defensive measures. Among these are firewalls, security appliances, and intrusion prevention systems at the network level, as well as antivirus software, anti-exploitation, and storage encryption at the host level. However, regardless of the level of security used, local networks are exposed to a wide range of cyber threats from the Internet. When sensitive or confidential information is maintained, the organization may keep the network in a physical 'air gap.' With this setup, the local network is isolated, with no direct connection between the intranet and the Internet. The air-gap policy may be used in defense and military systems, infrastructures,

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2023
O. Gervasi et al. (Eds.): ICCSA 2023 Workshops, LNCS 14106, pp. 202–217, 2023.
https://doi.org/10.1007/978-3-031-37111-0_15

public sectors, businesses, and other industries [2]. An example of an air-gapped network is the Joint Worldwide Intelligence Communications System (JWICS), a classified network operated by the US Defense Intelligence Agency.

1.1 Air-Gap Infection

Although air-gapped networks are considered safer, it has been shown that they are not entirely immune to breaches. ESET researchers found more than 20 malicious frameworks appear to target air-gapped networks [8]. In the past, several air-gap breach incidents involve compromising air-gapped networks. In the case of Agent.btz, a classified network of the United States military was infected with an APT worm [1]. Other air-gap hacking cases reported in the past include Stuxnet [25], USBFerry [3], and ProjectSauron [8].

To breach the air-gap isolation, attackers may use sophisticated techniques, such as supply chain attacks, software contamination (E.g., SolarWinds supply chain attack [31]), and insider personnel. With these methods, attackers can evade prevention and detection systems and gain their foothold in the network.

1.2 Air-Gap Exfiltration

Although breaching air-gapped networks has been demonstrated to be feasible, the exfiltration of information from disconnected networks to the Internet is a more challenging problem. This is because there is no network connectivity, wired or wireless, that the attacker can use to leak data outwards. The research domain of special covert communication techniques that work from isolated, air-gapped networks is known as air-gapped covert channels. By employing these techniques, the attacker can modulate information and transfer it. The use of electromagnetic mediums to leak data has been studied for many years. In this approach, malicious code uses electromagnetic leakage from laptops, PC, and servers for data exfiltration. Other techniques include the use of acoustic waves, magnetic fields, thermal emissions, and even vibrations for data exfiltration. The optical medium has also been explored in the context of covert communication channels. Different techniques, such as modulating information over the keyboard and hard drive LEDs, brightness levels, [12], and Infrared, were studied over the years.

1.3 Contribution

This paper introduces a novel optical covert channel to exfiltrate sensitive information from air-gapped networks. We use networked printer(s) connected to the local network and exploit their display panel LEDs and LCD panels to exfiltrate data. The main advantage over the existing air-gap exfiltration method is that the covert channel is maintained by an external device that existing security solutions, such as AVs, IDS, and IPS, do not protect. In addition, the attack is highly relevant to modern IT environments since many environments have one

or multiple printers in their local area networks. Figure 1 shows examples of the display panels that can be used for the covert channels presented in this paper on three leading printer OEMs. We show that attackers can exploit and control the printer display panels and modulate or encode textual and binary data over them in various ways. We also show that video receivers (local or remote) with line-of-sight to the device can record the display panels and deliver the leaked information to the attacker for decoding.



Fig. 1. Example of display panels on three commercial OEMs.

We discuss the adversarial attack model in Sect. 2, and examine the display panels' modulation and encoding techniques in Sect. 3. We evaluate the optical covert channel in Sect. 4. We examine the related work in Sect. 5, present countermeasures in Sect. 6, and conclude in Sect. 7.

2 Adversarial Attack Model

Exfiltration is one of the main stages in the cyber kill chain in Advanced Persistent Threat (APT) [29]. At the attack's foremost step, the adversary must compromise the target network.

A highly secured or air-gapped network can be attacked via supply chain attacks, social engineering, or insider attacks. Note that breaches of secured or air-gapped facilities are a type of attack that has been exhibited in recent years in various security breaches and APTs, such as USBCulprit [11], Agent.Btz [1], Stuxnet [25], and Ramsay [5] attacks.

2.1 Network Mapping

At the initial phase of the attack, the malware scans the network for printers to target. It works by sending packets of data to a network and then analyzing the responses received from all hosts and devices on that network. This allows it to build a network map, which can be used to identify hosts, open ports,

and running services. For example, the attacker may use the Nmap ("Network Mapper") tool, which includes a wide range of features and options, including the ability to scan specific hosts or IP ranges, use different scan types (such as TCP, UDP, or ICMP), and specify different output formats for the scan results. In the case of printers, the Nmap command would be `nmap -p 9100 --open -sV <network>`. This command scans the network for open port 9100, which is commonly used by printers for printing over TCP/IP.

2.2 Data Exfiltration

After breaching the air-gapped network and mapping the printers, the APT collects data from the compromised network and its storage. The data can be textual or binary (e.g., encryption keys and biometric information). For the exfiltration, the APT scans the network and identifies printers in the LAN. Textual or binary information is encoded on the display panels, stealthily and covertly, using various exploitation techniques detailed in Sect. 3.

2.3 Data Reception

The attacker receives optical signals via cameras with a line of sight to the compromised printers. Several types of equipment can be used in this attack model. It includes video surveillance, closed-circuit television, IP cameras, or hidden cameras that have a line of sight to the transmitting device. In this threat model, attackers can also use a malicious insider carrying a recording device (e.g., smartphone) that can position themselves to have a line of sight with the transmitting device. These video cameras record the display panels of network printers. The attacker then decodes the signals and retrieves the encoded data. The list of potential receivers and the corresponding attack vectors is presented in Table 1.

Table 1. The list of potential receivers and the corresponding attack vectors

Receiver	Attack vector
Security cameras	Remote exploitation; Wi-Fi
Hidden local cameras	Supply chain attacks; malicious insiders
Drone-carried cameras	Outsider attack
Recording cameras; smartphones	Malicious insiders/employees/visitors

Figure 2 shows the adversarial attack model. An APT collects sensitive information and encodes it on the printer display panel. The data is recorded by different cameras and transmitted to the attacker across the Internet.

3 Data Transmission and Reception

This section provides information regarding LCD control panels in the context of the covert optical channel and the corresponding attack vectors. It also discusses



Fig. 2. Adversarial attack model. An APT collects sensitive information and encodes it on the printer display panel. The data is recorded by different cameras and transmitted to the attacker across the Internet.

various data modulation and information encoding techniques. Note that the general topic of optical communication, such as screen to camera and LED to the camera, has been widely studied in the context of communication. The relevant papers discuss the types of receivers, bandwidth boundaries, as well as distances [23]. This paper limits the discussion to printer display panels and their relevance to the adversarial attack model.

3.1 Control and Display Panels

Modern printers are equipped with control panels. A typical panel contains buttons, LEDs, and a display screen, also known as a display panel. These panels help to maintain the printer and display printing preferences. The most common buttons are the 'Power,' 'Home,' 'Wireless,' 'Home,' and 'Back' buttons, usually having a corresponding LED.

The display screen of printers is shipped in various types and sizes. The LCD module is an embedded LCD screen, usually a Thin-film-transistor liquid-crystal display module. The older printers have a monochrome passive color display, while the modern printers are commonly shipped with a larger colored LCD screen with larger sizes, e.g., 4.3", 5.7", 7", and 10.1". The display modules are hosted (integrated) in the printer as a system-on-chip and managed by an embedded controller.

In the context of this work, there are three techniques to maintain optical covert channels via the control and display panels (Fig. 3).

- **LEDs modulation.** In this technique, the control panel LEDs are used for data modulation. The behavior of the LEDs and their colors may differ from system to system.
- **LCD screen content.** In this technique, the display screen is used for data exfiltration. The data can be exfiltration directly via the context presented on the screen (e.g., via text or QR code). Another option is to use other data modulation techniques, such as frequency shift keying (FSK), via objects projected on the screen.



Fig. 3. The three techniques to maintain optical covert channels via the control and display panels.

– **LCD screen brightness.** In this technique, the control screen is used for data exfiltration. However, the screen's content is not modified; only the background color is used to modulate and encode the information.

Table 2 Summarized the three techniques for the optical covert channel. LED modulation is available in all printers and is highly stealthy. The LCD screen content modulation is relevant to all modern printers but is less stealthy since the user may notice the screen content changes. In such a scenario, the attacker is usually absent during an overnight attack. In today's printers, LCD screen brightness is available, so the user may not notice any changes to the screen content if the brightness is close enough. Note that previous work showed that close brightness levels are considered covert in terms of user awareness but can be detected with standard video cameras [12].

Table 2. The three techniques of the optical covert channel from the printer control panel

#	Method	Modulation	Stealth	Availability
1	LEDs modulation	Blinking frequency	High	All printers
2	LCD screen content	Content information	Low	All modern printers
3	LCD screen brightness	Brightness modulation	High	All modern printers

3.2 Attacking the Printer

We present three methods malware can use to infiltrate the printer control/display panel.

Firmware Attack. The attacker updates the printer firmware with malicious firmware that controls the panel and buttons' LEDs and the display screen content. Within the firmware, changing the LED state requires access to low-level registers or GPIOs, depending on the specific system. After compromising the firmware with the screen and LED control, the attacker can maintain C&C with

the printer via standard protocols such as HTTP requests, Telnet, SMB, etc. Note that this method enables the highest degree of control over display panels but is hardware-specific and mostly undocumented. As shown in previous work, many printers are vulnerable to firmware attacks. Many printer OEMs use print job mechanisms for firmware updates. Firmware modification attacks against network printers have been demonstrated by Stolfo et al. for HP printers [7], by Jordan for Canon printers, and by Weidenbach and Ernst for Xerox printers [4].

Remote Configuration Attack. In this method, no firmware modification is required. Instead, the attacker uses documented and undocumented *configuration* commands to modify the LEDs and screen content. In many network printers, the Printer Job Language (PJL), originally developed by Hewlett-Packard, can be used to modify the screen content on the fly. The PJL can control jobs, perform language switching, job separation, status readback, and issue file system commands. For example, the PJL command `[%-12345X@PJL RDYMSG DISPLAY= "SECRET PASSWORD" [%-12345X` cause the current display message to be changed to the `SECRET PASSWORD`. In addition, in modern printers, various configuration commands can also be delivered via standard HTTP requests processed by the printer's internal HTTP server. The configuration attack that can be used in this method includes modifying the display panel content, setting icons, and changing the date and time, status icons, text messages, etc. Figure 4 shows the remote configuration attack viewed by the Wireshark network protocol analyzer. In this case, the malware used the Printer Job Language command to exfiltrate a secret password by displaying it on the printer screen for a limited time.

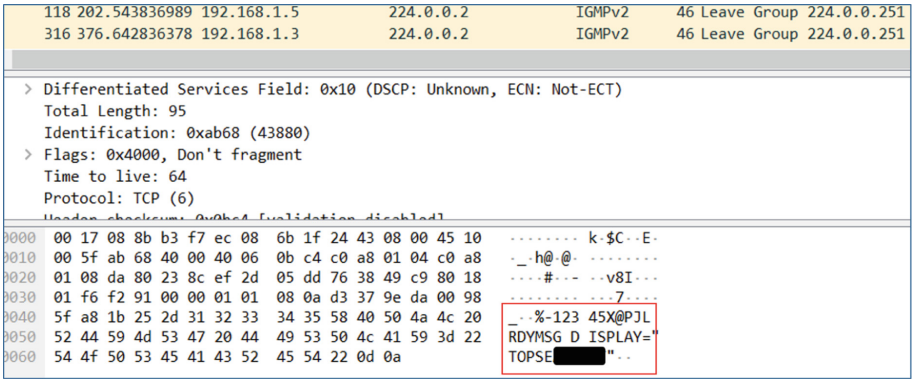

Fig. 4. Remote configuration attack as viewed by the Wireshark network protocol analyzer. In this case the malware used Printer Job Language (PJL) undocumented command to exfiltrate a secret password in the printer display screen.

Remote Operation Attack. In this method, the attackers used *control* commands to modify the LEDs and screen content. This is done via known protocols such as Printer Control Language (PCL), Printer Job Language (PJL), Internet Printing Protocol (IPP), SMB, and others. Communication is done via HTTP commands or dedicated ports such as 9100 (AppSocket), 515 (Line Printer Daemon), and 631 (Internet Printing Protocol). The commands can include setting job names, adding printing jobs to the queue and cancelling it. They can also include setting warning messages, resetting the printer, setting queue status, etc.

Table 3 presents the three attack methods, their relevance, and the corresponding attack vectors.

Table 3. The three attack methods, their relevancy to LED and LCD attack, and the corresponding attack vectors

#	Technique	LEDs	LCD	Attack vectors
1	Firmware attack	Yes	Yes	Firmware updates, local or via FTP, Telnet, and HTTPS
2	Remote configuration attack	Partial	Yes	Printer Command Language (PCL), Printer Job Language (PJL), printer HTTPS POST command
3	Printer commands attack	Partial	Yes	Spooler commands, Printer Command Language (PCL), Printer Job Language (PJL), printer POST commands

3.3 Data Modulation and Encoding

Using the signal generation techniques described above, we implemented three different types of data modulation; (1) frequency shift keying (FSK), (2) content modulation, and (3) brightness modulation.

Frequency Shift Keying (FSK). This modulation can be used for both LED control and screen control. The lack of a signal for a specific time duration encodes a zero (‘0’), while its presence for a time duration encodes a one (‘1’). In our case, the LED blinks at specific frequencies to encode ‘1’ and ‘0’. Note the generally modulating information over LED control is discussed in [18,26,27]. The FSK can also be used to modulate information over the LCD screen. In this case, a visual symbol (e.g., a black rectangle) modulates the binary information with the FSK.

Content Modulation. This encoding uses the LCD screen to exfiltration the information. The textual and binary information can be encoded in plain text, such as showing the text or image on the screen for a certain time. Another method is to use more complex encoding schemes, such as QR codes, which can be used to transfer binary and encrypted information. Modulating information over visual content is discussed in [13,30].

Brightness Modulation. The brightness modulation scheme uses different brightness levels to modulate the information. This can be seen as a form of frequency modulation at the carrier level since different colors have different

wavelengths from the optical perspective. In most simple cases, the current background encodes '0', and the darker or brighter background encodes '1'. We separate two sequential bits by setting the background to the current level for time interval T_d. Modulating information over screen brightness is discussed in [12].

4 Evaluation and Analysis

In this section, we evaluate the optical covert channel. We assume a line of sight between the printer and the recording camera (e.g., a surveillance camera or a smartphone).

4.1 Effective Distance

The number of camera frames per second (FPS) is one of the main factors important for successful reception. Three frames per bit is an optimal setting to decode the LED or LCD modulations. It means that even devices with relatively low frame rates, such as security cameras, can be used for data recording. Table 4 shows the effective distances with different types of receivers. We include a surveillance camera, a DSLR camera, a high-resolution camera, a webcam, a smartphone camera, and a telescope camera. It is known that telescopes and special focus lenses can extend the range of reception to hundred meters [23].

Table 4. The effective distance with different receivers

Receiver	Type	Distance
Surveillance camera	Sony SNCEB 30fps	30 m
DSLR camera	Nikon	50 m
high resolution camera	GoPro	50 m
Webcam	Microsoft LifeCam	30 m
Smartphone camera	Samsung Galaxy	30 m
Telescope	Various	100 m

4.2 Data Transmission

Table 5 show the time it takes to exfiltrate various types of information with each method. Note that the exact time may change from printer to printer depending on the display panel type and size. A 128 bits password (16 bytes) can be exfiltrated in less than a minute or real-time, depending on the exfiltration method. Bitcoin private key and pin codes can be exfiltrated in less than a minute with all methods. An RSA encryption key of 4096 bits takes between 5 min to 30 min, depending on the method used. For keystrokes, each keystroke can be leaked in almost real-time. Small images and QR codes are relevant only for LCD screen content modulation and can be exfiltrated in real time.

Table 5. The exfiltration of various types of information with each method

]Information	Size	Display Panel LEDs	LCD screen content	LCD screen brightness
Passwords	128 bits	0.5 min	realtime	1 min
Bitcoin private key	256 bits	1 min	realtime	2 min
PIN codes	64 bits	0.25 min	realtime	0.5 min
RSA encryption keys	4096 bits	20 min	5 min	30 min
Keylogging	8 bits per key	realtime	realtime	realtime
Small image	64×64	N/A	realtime	N/A
QR code	21×21	N/A	realtime	N/A

4.3 Visual Detection

With the cameras specified in Table 4, we achieved about 100% detection rates of the panel LEDs, which maintained 20 bps per LED. The cameras were able to accurately detect the LED's in various lighting conditions and at a wide range of distances. The results were reliable, consistent and showed no signs of deterioration over time. As a result, these cameras provide a dependable and accurate solution to detecting panel LEDs. This is regardless of lighting conditions or distance in our attack model. Our algorithm performs the following steps for each video frame.

1. Convert the image to grayscale.
2. Apply a Gaussian blur to reduce noise in the image.
3. Apply a threshold to the image to create a binary image, where the LED(s) should be brighter than the background.
4. Apply morphological operations (erosion and dilation), to remove small objects and fill gaps in the binary image.
5. Find contours in the binary image.
6. For each contour, calculate its area and centroid.
7. Apply a circularity test to each contour to filter out non-circular shapes that are not likely to be LEDs.
8. Apply color filtering to further isolate the LEDs in the image (if they have a specific color).
9. Marks the detected LEDs using their centroids and radii.

4.4 Distance Analysis

We presented the covert channel distance given specific transmitters and receivers. An optical communication formula can calculate the effective distance in the general case.

$$P_r = P_t \frac{A_r}{d^2} \tag{1}$$

where P_r is the received power, P_t is the transmitted power, A_r is the effective area of the receiver, and d is the distance between the transmitter and receiver.

In this formula, P_r is the power the receiver receives, which is the LED receiving the signal. P_t is the power transmitted by the transmitter, which is the LED sending the signal. The effective area of the receiver A_r is the area of the receiver that can capture the signal. d is the distance between the transmitter and receiver. The formula states that the received power, P_r, is equal to the transmitted power P_t, multiplied by the ratio of the effective area of the receiver A_r, to the square of the distance between the transmitter and receiver d^2. This relationship is known as the inverse square law, which states that radiation intensity decreases as the square of the distance from the source increases. Consequentially, as the distance between the transmitter (the printer display panel) and receiver (the receiving camera) increases, the received power decreases because the signal spreads over a larger area. Similarly, if the receiving camera effective area is larger, more of the optical signals will be captured, and the received power will increase.

Bit Error Rates (BER). There are a number of factors that affect the bit error rate in our covert communication channel, including the threshold voltage, the noise standard deviation, and the signal-to-noise ratio of the received signal. This formula can be expressed as follows.

$$\text{BER} = \frac{1}{2}\text{erfc}\left(\sqrt{\frac{I \cdot h \cdot d}{2qAN_0}}\right) \tag{2}$$

This is a special function that represents the probability that a Gaussian random variable will exceed a given threshold. Using erfc as the complementary error function, the LED current is I, h is the photodetector's sensitivity, d is the distance between the light source, q is the elementary charge, A is the photodetector's area, and N_0 is the noise power spectral density. Note that an in-depth analysis of optical channel characteristics is beyond the scope of this paper and is given in relevant literature on optical communication [32].

5 Related Work

The term covert channel refers to a communication channel that enables data transfer between entities where communication is forbidden. Covert channels are widely studied in the context of covert communication between processes, CPU cores, virtual machines, and computers.

To maintain covert communication while bypassing security measures, attackers may use various legitimate protocols to conceal information, including protocols such as TCP/IP, HTTP, SMTP, and DNS [28].

In the air-gap scenario, covert communication is more challenging since there is no Internet connectivity. An attacker may use out-of-band communication

techniques categorized into electromagnetic, magnetic, acoustic, thermal, and optical channels to exfiltrate data through the air gap. These special types of covert channels are also called air-gap covert channels. Electromagnetic medium is the most common subject of research in this field. The techniques involve using components that emit electromagnetic waves in computers or devices and exploiting them to modulate sensitive information.

Kuhn used radio frequencies emanating from display screens to leak information [24]. Modern attacks such as Air-Fi [9], AirHopper [15], and GSMem [14] use computer buses to modulate information in various frequency bands and deliver it to nearby malware-infected mobile phones. Similarly, magnetic covert channels have recently been proposed to exfiltrate data from air-gapped computers kept in Faraday cages [21]. Bauer et al. discussed using anti-EMI features in the CPU for communication [6]. Research from previous years also demonstrated the use of power lines to carry covert communication [19].

Sound also can be used to maintain covert communication, especially in inaudible frequency bands, mainly above 18 kHz.

Hanspach et al. showed different acoustic frequencies to maintain contact between computers [22]. However, speakers might be forbidden in air-gapped networks in a defense measure known as an 'audio gap.' Guri et al. introduced cover channels for air-gapped, audio-gapped networks in methods such as Fansmitter [17], Diskfiltration, and PowerSupplay [10]. With these techniques, malware can produce sound waves without standard audio hardware. Thermal-based covert channels between computers were also demonstrated. BitWhisper is an attack that exploits heat emission and heat sensors in computers to maintain data transmission overheat [16].

5.1 Optical

Loughry presented the threats of covert communication with optical emanations via network and keyboard row of LEDs [26,27]. Guri et al. introduced the modern adversarial attack model by encoding signals sent from USB keyboard LEDs at various speeds [18]. They also exploited hard disk drives (HDD) status LEDs and network devices LEDs [20]. Two attacks relevant to LCD screens are Brightness [12], and VisiSploit [13], which use LCD display screens to conceal information. With these methods, invisible images or brightness levels are used to encode sensitive information. Remote cameras receive and decode data. Other works proposed to project invisible images on screens to secure air-gapped infrastructures [30]. Note that all previous works used the standard LCD screen of computers and hence can be monitored by AV, IDS, and IPS systems. Networked printer display panels currently lack protection and defense measures.

This work presents the usage of networked printer display panels to retrieve data from air-gapped networks. The network printer display screen used for malicious purposes has not been studied before, theoretically or technically. We examined this covert channel technique's characteristics, opportunities, and limitations. We discuss attack vectors at the firmware to software level, transmission methods, and various receivers.

6 Countermeasures

The main protective countermeasures for optical attacks include the restriction of cameras and video recorders in areas of networked printer devices. However, surveillance cameras cannot be banned since, in many cases, they monitor sensitive areas. Host-based filtering is another way of mitigating the optical threat presented in this paper. In this approach, a network filter component is installed on the computer, usually as a driver in the kernel. This driver filters all network traffic at the lowest level before transferring data to the network card. The driver monitors all network protocols - Ethernet, IP, TCP, UDP, and performs deep packet inspection to detect attacks. Figure 5 shows the architecture of such a firewall implementation on Windows OS. The Network Driver Interface Specification (NDIS) filter driver filters printer traffic at different ports (e.g., 9100 and 80), and if an attack is detected, the traffic is blocked. An external firewall is another solution that may be deployed as a detection and prevention system on a local LAN firewall (Fig. 6, A). In this case, a stateful inspection paradigm is used to inspect each printer's traffic separately, identify suspicious traffic, and block it. Such a hardware solution can be deployed as a dedicated hardware firewall where each printer has a small device filtering its LAN incoming traffic (Fig. 6, B). An external monitoring solution includes a local video camera that records the networked printer to detect anomalies in its optical activities at the control panel. A practical implementation of external monitoring would be complex because the printer screen content may be related to a specific vendor. It is challenging to define anomalies in their content. In addition, this type of detection would likely have high rates of false positives due to the legitimate dynamic content on the printer display screen. This is due to warning and error messages, notifications and alerts, etc.



Fig. 5. The architecture of the printer firewall on Windows OS as an NDIS filter driver.

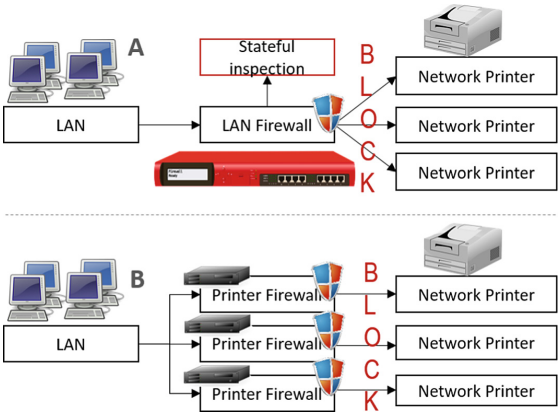

Fig. 6. The two types of firewall architecture used to detect and block the attacks; are (A) a stateful module on the network and (B) a printer firewall device for each networked printer.

7 Conclusion

This paper explores a new type of covert channel that enables attackers to leak data from air-gap networks. Our attack exploits networked printers' display screens and status LEDs to encode sensitive data. To that end, the attack uses documented and undocumented commands at a user process or firmware level. Information such as keystrokes, texts, credentials, passwords, and encryption keys can be encoded and modulated over these signals. These signals can be intercepted and decoded by an adversary with line-of-sight to the printer. For example, using a drone, local surveillance camera, and smartphone camera. We presented related work, discussed the various attack techniques, and proposed hardware and software defensive countermeasures for this attack.

References

1. Agent.btz - Wikipedia. https://en.wikipedia.org/wiki/Agent.BTZ. Accessed 01 Jan 2023
2. Air gapped networks: a false sense of security? - sentinelone. https://www.sentinelone.com/blog/air-gapped-networks-a-false-sense-of-security/. Accessed 13 Nov 2022
3. Hackers target the air-gapped networks of the Taiwanese and Philippine military — zdnet. https://www.zdnet.com/article/hackers-target-the-air-gapped-networks-of-the-taiwanese-and-philippine-military/. Accessed 01 Jan 2023
4. hacking printers. https://hacking-printers.net/wiki/index.php/Firmware_updates#cite_note-jordon2014wrestling-4. Accessed 10 Nov 2022
5. New ramsay malware can steal sensitive documents from air-gapped networks— zdnet. https://www.zdnet.com/article/new-ramsay-malware-can-steal-sensitive-documents-from-air-gapped-networks/. Accessed 01 Jan 2023

6. Bauer, J., Schinzel, S., Freiling, F., Dewald, A.: Information leakage behind the curtain: abusing anti-EMI features for covert communication. In: 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp. 130–134. IEEE (2016)
7. Cui, A., Costello, M., Stolfo, S.: A case study of embedded exploitation, When firmware modifications attack (2013)
8. Dorais-Joncas, A., Munõz, F.: Jumping the air gap (2021)
9. Guri, M.: Power-supplay: leaking sensitive data from air-gapped, audio-gapped systems by turning the power supplies into speakers. IEEE Trans. Dependabl. Secur. Comput. 1 (2021)
10. Guri, M.: Power-supplay: leaking sensitive data from air-gapped, audio-gapped systems by turning the power supplies into speakers. IEEE Trans. Dependabl. Secur. Comput. (2021)
11. Guri, M.: USBculprit: USB-borne air-gap malware. In: European Interdisciplinary Cybersecurity Conference, pp. 7–13 (2021)
12. Guri, M., Bykhovsky, D., Elovici, Y.: Brightness: leaking sensitive data from air-gapped workstations via screen brightness. In: 2019 12th CMI Conference on Cybersecurity and Privacy (CMI), pp. 1–6. IEEE (2019)
13. Guri, M., Hasson, O., Kedma, G., Elovici, Y.: An optical covert-channel to leak data through an air-gap. In: 2016 14th Annual Conference on Privacy, Security and Trust (PST), pp. 642–649. IEEE (2016)
14. Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., Elovici, Y.: GSMEM: data exfiltration from air-gapped computers over GSM frequencies. In USENIX Security Symposium, pp. 849–864 (2015)
15. Guri, M., Kedma, G., Kachlon, A., Elovici, Y.: Airhopper: bridging the air-gap between isolated networks and mobile phones using radio frequencies. In: 2014 9th International Conference on Malicious and Unwanted Software: The Americas (MALWARE), pp. 58–67. IEEE (2014)
16. Guri, M., Monitz, M., Mirski, Y., Elovici, Y.: Bitwhisper: covert signaling channel between air-gapped computers using thermal manipulations. In: 2015 IEEE 28th Computer Security Foundations Symposium (CSF), pp. 276–289. IEEE (2015)
17. Guri, M., Solewicz, Y., Elovici, Y.: Fansmitter: acoustic data exfiltration from air-gapped computers via fans noise. Comput. Secur. 101721 (2020)
18. Guri, M., Zadov, B., Bykhovsky, D., Elovici, Y. 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, pp. 801–810. IEEE (2019)
19. Guri, M., Zadov, B., Bykhovsky, D., Elovici, Y.: PowerHammer: exfiltrating data from air-gapped computers through power lines. IEEE Trans. Inf. Forens. Secur. (2019)
20. Guri, M., Zadov, B., Elovici, Y.: LED-it-GO: leaking (A Lot of) data from air-gapped computers via the (small) hard drive LED. In: Polychronakis, M., Meier, M. (eds.) DIMVA 2017. LNCS, vol. 10327, pp. 161–184. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60876-1_8
21. Guri, M., Zadov, B., Elovici, Y.: Odini: escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields. IEEE Trans. Inf. Forensics Secur. **15**, 1190–1203 (2019)
22. Hanspach, M., Goetz, M.: On covert acoustical mesh networks in air. J. Commun. **8**(11), 758–767 (2013)
23. Jovicic, A., Li, J., Richardson, T.: Visible light communication: opportunities, challenges and the path to market. IEEE Commun. Mag. **51**(12), 26–32 (2013)

24. Kuhn, M.G., Anderson, R.J.: Soft tempest: hidden data transmission using electromagnetic emanations. In: Aucsmith, D. (ed.) IH 1998. LNCS, vol. 1525, pp. 124–142. Springer, Heidelberg (1998). https://doi.org/10.1007/3-540-49380-8_10
25. Kushner, D.: The real story of Stuxnet. IEEE Spectrum. **3**(50), 48–53 (2013)
26. Loughry, J.: Optical tempest. In: 2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE), pp. 172–177. IEEE (2018)
27. Loughry, J., Umphress, D.A.: Information leakage from optical emanations. ACM Trans. Inf. Syst. Secur. (TISSEC). **5**(3), 262–289 (2002)
28. Mazurczyk, W., Wendzel, S., Zander, S., Houmansadr, A., Szczypiorski, K.: Information Hiding in Communication Networks: Fundamentals, Mechanisms, Applications, and Countermeasures. John Wiley & Sons (2016)
29. Virvilis, N., Gritzalis, D.: The big four-what we did wrong in advanced persistent threat detection? In: 2013 International Conference on Availability, Reliability and Security, pp. 248–254. IEEE (2013)
30. Weise, M.: A QR-Code Optical Covert Channel in an Air-Gapped Secure Data Infrastructure. Ph.D. thesis, Wien (2022)
31. Wolff, E.D., Growley, K.M., Gruden, M.G., et al.: Navigating the Solarwinds supply chain attack. Procure. Lawyer. **56**(2) (2021)
32. Yariv, A., Yeh, P.: Photonics: Optical Electronics in Modern Communications. Oxford University Press (2007)