BRIGHTNESS: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness

Mordechai Guri*, Dima Bykhovsky*‡, Yuval Elovici
*Department of Software and Information Systems Engineering, Ben-Gurion University of the Negev, Israel
Email: gurim@post.bgu.ac.il
‡Department of Electrical and Electronics Engineering, Shamoon College of Engineering, Israel
demo video: https://cyber.bgu.ac.il/advanced-cyber/airgap

***Abstract*—Air-gapped computers are systems that are kept isolated from the Internet since they store or process sensitive information. In this paper, we introduce an optical covert channel in which an attacker can leak (or, exfiltlrate) sensitive information from air-gapped computers through manipulations on the screen brightness. This covert channel is invisible and it works even *while* the user is working on the computer. Malware on a compromised computer can obtain sensitive data (e.g., files, images, encryption keys and passwords), and modulate it within the screen brightness, invisible to users. The small changes in the brightness are invisible to humans but can be recovered from video streams taken by cameras such as a local security camera, smartphone camera or a webcam. We present related work and discuss the technical and scientific background of this covert channel. We examined the channel's boundaries under various parameters, with different types of computer and TV screens, and at several distances. We also tested different types of camera receivers to demonstrate the covert channel. Lastly, we present relevant countermeasures to this type of attack.**

I. Introduction

Despite the existence of security measures such as intrusion detection systems (IDS), firewalls and AV programs - attackers are finding new vulnerabilities and ways to infiltrate target networks. Even networks that are completely disconnected from the Internet can be compromised by motivated adversaries using complex attack vectors. While breaching such systems has been shown to be feasible in recent years, exfiltration of data from systems without networking or physical access is still considered a challenging task. Electromagnetic, acoustic and thermal covert exfiltration channels have been examined in the last twenty years. Optical exfiltration techniques have been studied as well [1]. However, most of these methods are visible (e.g., not covert) and assume the *absence* of people in the environment.

In this paper, we propose an optical covert channel which relies on the limitations of human vision. Technically speaking, visible light represents a limited range of electromagnetic radiation, which is sensed and perceived by the human visual system. Intentional leakage of sensitive data through the visible light via a standard LCD screen is futile, since by definition it may be detected by humans who see the display. Our covert channel exploits the limits of human visual brightness perception in order to conceal sensitive data, invisible to the naked eye, on the LCD screen.

II. Related Work

Leaking data from air-gapped systems via covert communication methods has been explored in the last twenty years. The covert channels studied are electromagnetic, magnetic, electric, acoustic, thermal, and optical. Back in 1998 [2] researchers discuss the concept of software based TEMPEST attack, which employs electromagnetic emanation from LCD screen. AirHopper [3] is an attack aimed at exfiltrating data from isolated networks via radio frequencies in the FM broadcasting bands (87.5 - 108.0 MHz). The signal are received by FM radio chip in a standard smartphone. Electromagnetic covert channels are discussed in [4]–[9] and newer magnetic convert channels discussed in [10], [11]. Hanspach and Goetz [12] present a method for near-ultrasonic covert networking using speakers and microphones. Fansmitter and Diskfiltration [13], [14] are another methods of acoustic data exfiltration from computers without loudspeakers. BitWhisper [15] demonstrates a covert communication channel between adjacent air-gapped computers by using their heat emissions and built-in thermal sensors. In 2018, Guri et al presented PowerHammer [16], a method to exfiltrate data from air-gapped computers through power lines. Other types of air-gap covert channels based on acoustic [17]–[20], optical [21]–[28] and thermal [29] emissions have also been investigated.

In 2002 researcher [1] discuss the threat of data leakage through optical emanations from LEDs. They manipulates the keyboard LEDs to modulate data which was received by a camera. Using the keyboard LEDs for covert channel discussed was explored in 2019 with modern keyboard and smartphones [30]. Recently researchers discuss the threat of modulating information via the routers and LAN switches LEDs [31]. Brasspup [32] demonstrated how to hide images in a modified LCD screen but his method requires hardware modification. The term 'shoulder surfing' refers to a malicious insider or visitor looking at the screen or carrying a camera. Another threat is an exploited surveillance camera. The visitors or cameras are obtaining private data such as credit card (CC) numbers, passwords and PIN codes. With our method, the presence or absence of the user is not required, since the attacker may leak the sensitive information at any time in a stealth way.

III. Attack Model

At the first stage of the attack, the target network is infected with a malware. Infiltration of air-gapped network can be done in a case of motivated and capable adversaries [**?**], [33]. At the second stage, the malware collects sensitive information from the computer (e.g., documents). It then encodes it as a stream of bytes and modulates it on the screen, using small changes in the screen brightness that is invisible to humans. The third stage of the attack involves a camera which takes video recordings of the compromised computer's display. Attackers then access the recorded video stream and reconstruct the sensitive information by using image processing techniques. There are two attack scenarios which are relevant for this optical covert channel. The 'malicious insider' attack [34] (also known as 'evil maid' attack [35]) in which a person with a camera can be within the compromised computer's line of sight but does not necessarily have network access. A compromised local camera (e.g., surveillance camera) that the attacker has access to. A sample attack scenario is depicted in Fig. 1. In this scenario sensitive data (e.g., encryption key) is covertly modulated onto the computer screen brightness. It then projected on the screen either when the user is absent or while the user is working on the computer. The modulated data is then reconstructed from the video stream of a local security camera using video processing techniques.

Notably, threat models in which the attacker must be in close proximity of the emanating device are common in a variety of covert channels [1], [5], [36], [37].

IV. Technical Background

Display-to-camera (D2C) communication is a subject of significant recent interest. In this communication, a camera is used for both accessing scene elements and capturing imperceptible machine-interpretable data. The main application of D2C is to provide legitimate covert channels for multimedia services [38]–[43]. An illustration of D2C is presented in Fig. 2.

Fig. 1: Sensitive data is exfiltrated from the computer, modulated within the screen brightness, invisible and unbeknownst to the user. The video stream is recorded by a local security camera.

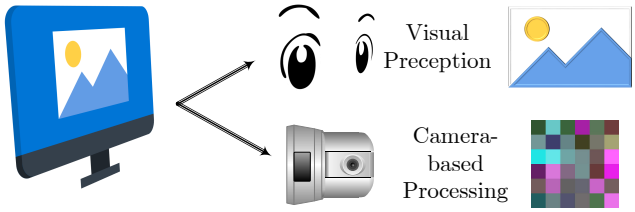

Fig. 2: Illustration of covert D2C principle: the same frame on the screen has both high-quality visually perceptible image data and imperceptible covert message.

Numerous techniques were proposed for D2C. In [38], it was proposed to apply the Laplacian Pyramid method based watermark technique that embeds data in an image frame. Wang et al [39] used complementary image frames with data blocks added to the original images, while preserving them to be imperceptible to the human eye. Li et al [40] used alpha channel manipulations. In [41], [42], a frequency domain communication method inspired by orthogonal frequency-division multiplexing (OFDM) modulation was applied. In [43], pixels or blocks of pixels are modulated by a spatial visual modulation scheme.

A. Challenges

The implementation of covert D2C communication requires minimum changes of the displayed information such that it appears unchanged to the human eye. On the other hand, the communication scheme must be immune to the effects of camera geometry, such as the scale, angle rotation and optical distortion. For example, the required inverse affine transformation of the captured image is illustrated in Fig. 3. While, in general, all mentioned effects may be effectively mitigated by sufficient image processing, they have an inevitable influence on communication performance and the required computation complexity, thus making it challenging to provide a robust communication scheme with an acceptable bit-rate and bit-error rate.

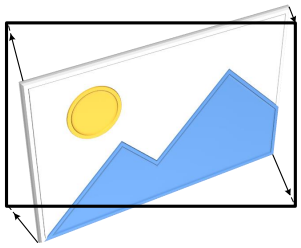

Fig. 3: Illustration of inverse affine transformation that is required for correct processing of communication data.

B. Performance

The main parameter that influences communication performance is the received optical power and the resulting SNR. The power, in turn, depends on: distance to the display,

misalignment between the camera and the display, affine transformation of the displayed image (also termed perspective distortion), optical zoom of the camera, display contrast ratio and brightness.

Optical channel gain analysis is based on the geometric parameters outlined in Fig. 4. The distance between the display and the camera is d, the axial misalignment of the display is ϕ and the axial misalignment of the camera is θ. The relation between power emitted from display element dS towards camera element dA is given by [44]

$$dh = \int_{screen} \int_{\substack{camera \\ objective}} \frac{1}{\pi d^2} \cos(\phi) \cos(\theta) dA dS. \quad (1)$$

This rigorous expression requires integration over the display area and the camera objective area of the channel gain above. This expression stresses the dependence of the gain on distance, $\sim d^{-2}$, and axial misalignment, $\sim \cos(\cdot)$.

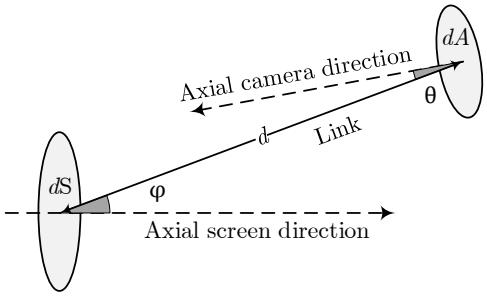

Fig. 4: D2C link geometry that includes axial misalignment of both a display and a camera.

The main image processing aspect is related to the affine transformation of the image. The reverse affine transformation (Fig. 3) is not only computationally intensive, but also produces inevitable image quality degradation, thus degrading communication performance [41].

The optical zoom of the camera physically defines the number of detector pixels that are used for the imaging of display information. Obviously, higher zoom results in better communication performance and enables a higher bit-rate and/or BER. Note that the display contrast ratio and brightness are directly related to the transmitted optical power of the communication signal. Higher brightness thresholds yield higher quality of the communication channel.

V. Data Communication

In LCD screens each pixel presents a combination of RGB colors which produce the required compound color. An illustration of the RGB principle is presented in Fig. 5(a).

In the proposed modulation, the RGB color component of each pixel is slightly changed. These changes are invisible, since they are relatively small and occur fast, up to the screen refresh rate. Moreover, the overall color change of the image in the screen is invisible to the user. The modulation process is outlined in Fig. 5(b).

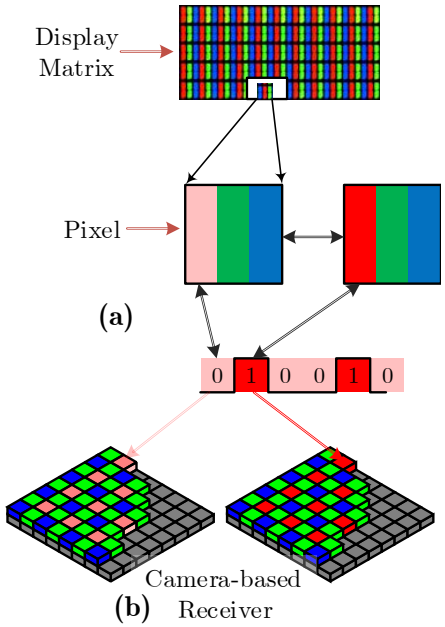

Fig. 5: (a) The signal is modulated by imperceptible changes of one of the RGB components. In this figure, small R(ed) color changes are used for modulation. (b) Camera-based receiver is used for signal detection.

In the general case we use M-level amplitude-shift keying (M-ASK). In this modulation, different lighting levels are used to represent a *symbol* that includes $\lfloor \log_2(M) \rfloor$ bits. Typically, the value of M is chosen to be a power of two. Each symbol has the same duration, T, such that the resulting bit-rate is given by $R = \lfloor \log_2(n) \rfloor T$ bit/sec. The special case of $M = 2$ is termed on-off keying (OOK).

An example of the signal modulated by 3% changes in the red color component is presented in Fig. 6. It shows the ASK modulation in two frames from the video stream. The '1' and '0' values are modulated in the brightness of the top and bottom screens, respectively. The analysis of the stream is presented in Fig. 7. In this case a bit sequence of '1010101010101010' was exfiltrated from a 19" screen at a bitrate of 5 bit/sec. It was captured by a local camera located at a distance of 6 meter from the screen.

The malware architecture is presented in Fig. 8. The image brightness encoder is a device driver which intercepts the screen buffer. It modulates the data in ASK by modifying the brightness of the bitmap according to the current bit ('1' or '0'). It changes the RGB component of every pixel by a given amount and forwards it to the video card.

VI. Evaluation

We evaluate the covert communication channel as a function of different distances and bitrates.

A. Experimental setup

For the transmission we used two display screens; (1) Dell 24" PC Monitor (P2417H), and (2) Samsung 40" LED TV

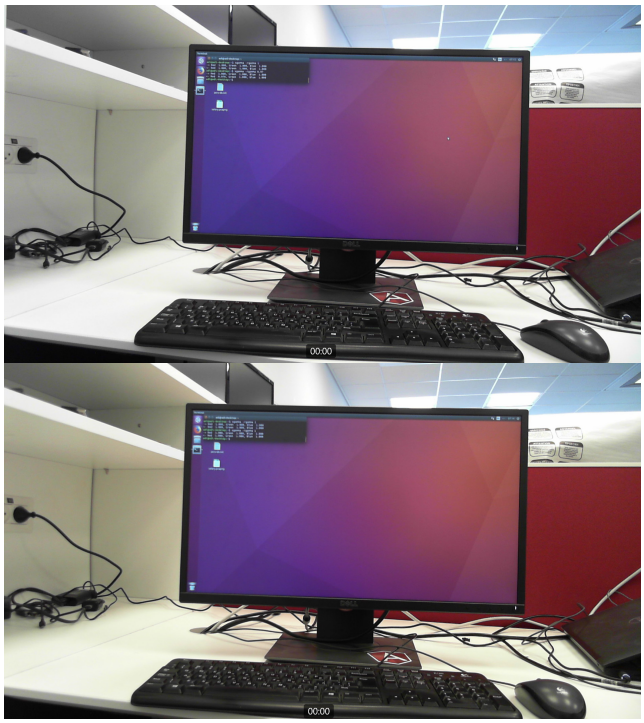

Fig. 6: The ASK modulation in a video stream. The '1' and '0' are modulated in the brightness of the top and bottom screens, respectively.

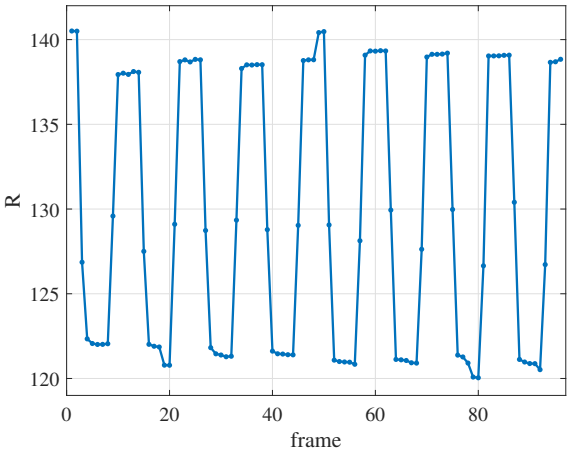

Fig. 7: Signal '1010101010101010' modulated by color change as acquired by a security camera.

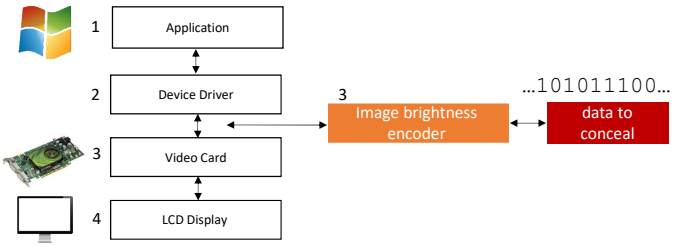

Fig. 8: The malware architecture

(UA40B6000). For the reception we tested three types of cameras: (1) a professional security camera, (2) a webcam, and (3) a smartphone camera. The camera models and the other details are summarized in Table I. For decoding the videos we used OpenCV, which is open-source computer vision library that focuses on real-time video processing for academic and commercial use. We developed a C program that receives the video as an input and calculates the frame brightness and illumination amplitudes to an output file for further MATLAB processing.

Our experiments show that the best communication performance was for adapting the red color component. In this modulation, we changed the red color of each pixel by a maximum threshold of 3%. The changes are invisible to humans but can be reconstructed from a recorded video stream. For the security camera and the webcam we could reach bit-rates of 10 bps and a maximal communication distance of 9 meters. The resulting bit-error rate (BER) was 0% for all experiments.

Note, the communication distances in both communication schemes were limited by the available indoor environment. Large distances are possible, as discussed in the following section.

B. Distance Analysis

An example of the signal decrease for a red color modulated signal as a function of distance is presented in Fig. 9. It shows the red component as extracted from the video stream of modulated '1' and '0' values at three distances.

Theoretically, the received signal is inversely proportional to the squared distance [44]:

$$\text{signal} \sim \frac{1}{d^2}. \tag{2}$$

In order to verify this dependence, the experiment of brightness-modulated communication was repeated for different distances and the results were analyzed. The analysis of signal variability is presented in Fig. 10 and clearly shows that the theoretical dependency (Eq. (2)) holds for the experimental

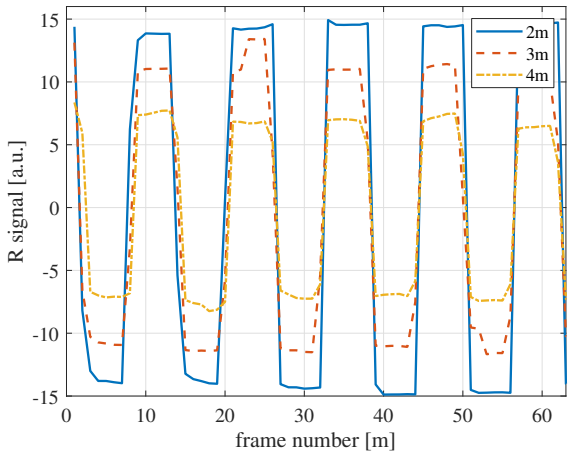

Fig. 9: Received signal examples from different distances.

TABLE I: Evaluation of brightness based covert channel with different receivers

#	Name	Model	Distance (m)	Bit-rate (bps)
1	Security camera	Sony SNC-DH120 IPELA Minidome 720P HD	1-9	5-10
2	Webcam	Microsoft Lifecam Studio	1-9	5-10
3	Smartphone	Samsung Galaxy S7	0.3-1.5	1

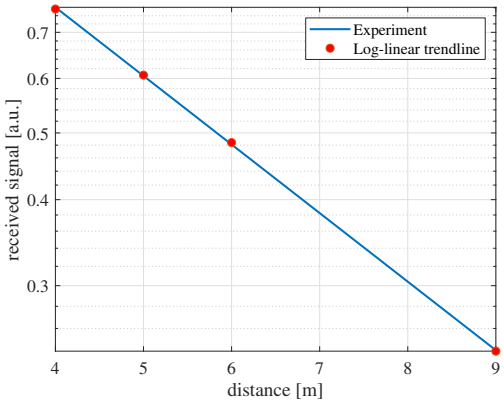

Fig. 10: Received signal is inversely proportional to the squared distance.

results. Note, the y-axis of the figure has a logarithmic scale, so the resulting linear trend-line demonstrates squared distance dependency.

VII. BER Analysis

The bit error rate (BER) of the communication channel be evaluated as

$$p_e = p(0)p(1|0) + p(1)p(0|1), \tag{3}$$

where $p(0)$ and $p(1)$ are the probabilities of transmitted '0' or '1' respectively and $p(1|0)$ and $p(0|1)$ are correspondent conditional error probabilities [45]. Using central limit theorem approximation, the received signals may be modeled by $s_0 \sim N(\mu_0, \sigma_0^2)$ and $s_0 \sim N(\mu_1, \sigma_1^2)$ with the corresponding conditional probabilities

$$p(1|0) = Q\left(\frac{thr - \mu_0}{\sigma_0}\right) \tag{4a}$$

$$p(0|1) = Q\left(\frac{\mu_1 - thr}{\sigma_1}\right), \tag{4b}$$

where $\gtrless \mathrm{thr}$ is the decision threshold for the received signal and $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{x^2}{2}\right)$. For simplifying conditions of $p(0) = p(1) = 1/2, \sigma_0 = \sigma_1 = \sigma$ and applying the optimal $thr = (\mu_1 - \mu_0)/2$ value, the resulting BER expression is given by

$$p_e = Q\left(\frac{\mu_1 - \mu_0}{2\sigma}\right). \tag{5}$$

While σ value may be considered as constant, the difference $\mu_1 - \mu_0$ reduces with distance as outlined in the evaluation.

VIII. Scientific discussion

In this section we present the scientific background regarding human visual perception limitations which facilitate the success our optical covert channel. The ability of humans to resolve blinking images and brightness perception are discussed in [46]–[49]. Physiological aspects of human color vision are discussed further by Gouras [50]. Coren et al also provide a general discussion of the human visual system [51], along with details regarding the perception of brightness and darkness [51], [52], lightness constancy [51] [53], and temporal properties of the visual system [51], [54].

A. Brightness and darkness perception

The level of ambient (environmental) light is known to affect visual perception, including the perception of brightness [51], [52]. In fact, the human visual system consists of photopic or daylight vision, which includes the perception of color, and scotopic or twilight vision. In the human retina, two separate types of cells (cones and rods) are responsible for daylight and twilight vision: cones are associated with photopic vision, while rods are associated with scotopic vision. The sensitivity of the visual system gradually adapts as one move to a darker or brighter environment. Consequently, our experiments are performed under a controlled level of ambient light. Also, subjects are given some time to adapt to the laboratorys level of ambient light. It is also believed that human perception of relative brightness and darkness involves two separate systems [51], [52].

Concerning the duration of the blinking image, particularly with low levels of illumination, increasing the duration can increase the likelihood that the stimulus will be detected, a phenomenon known as Bloch's law [51], [52]. Concerning perception of flickering light, the retinal receptors in the human eye can resolve up to several hundred cycles per second (cps). However, the sensitivity of neurons in the primary visual cortex to flickers is much lower [51], [54]. The critical fusion frequency (CFF) is used to measure subjects' discrimination between steady and flickering light. This measure varies between 10 cps and 60 cps (exposure time between 50 ms and 8.3 ms, respectively). The CFF varies based on several factors, including the current level of light/dark adaptation, the intensity of the light, the distance from the fovea, and the wavelength composition of the light. Consequently, our experiments are performed under controlled values for those factors. In the human retina, separate ganglion cells are responsible for sustained (steady) light and transient (flickering) light (see

also [51]). Interestingly, it has been demonstrated [51], [54] that low contrast flashes and equiluminant chromatic (color) flashes activate different pathways. In this research, we are particularly interested in low contrast flashes of gray tones.

IX. Countermeasures

The countermeasures for this optical attack can be categorized to prevention and detection. Preventive countermeasures include organizational policies aimed to restrict the accessibility of sensitive computers by placing them in secured areas ('zones') where only authorized staff may access them. In addition any sort of cameras (including smartphone and wearable cameras) may be prohibited within the perimeter of certain restricted areas. Note that the surveillance camera itself may be infected with a malware. Another technological countermeasure consists of a polarized film which covers the screen. The user gets a clear view while humans and cameras at a distance would view a darkened display. Detection countermeasures may include monitoring of the sensitive computer for the presence of suspicious display anomalies at runtime. However, detection mechanisms within the operating systems are considered untrusted since they can be evaded by malware (e.g., rootkits) at the user and kernel levels. A trusted monitoring can be achieved by taking videos of the computers display and searching for hidden brightness change patterns. The detection can be done by a camera-based receiver. Since camera sensors are based on RGB optical filter arrays, the signal can be detected by one of the sensor components. However, practical implementation of camera based monitoring seems nontrivial in the wide scale due to the resources and maintenance it requires.

X. Conclusion

In this paper we present an optical covert channel in which data is concealed on the LCD screen brightness, but is invisible to users. We presented a malware scheme that can exfiltrate sensitive data from isolated (air-gapped) computers. The attack model consists of (a) contaminating the target network, a task which has been demonstrated to be within the capabilities of a modern advanced persistent threat (APT), and (b) using a camera to take videos of the computers display, a task that can be performed by a malicious insider or visitor, or by exploiting a surveillance camera. We exploit the limitations of bare human vision, concerning brightness perception, using sufficiently low values of contrast between the brightness levels. Consequently, the current results demonstrate the feasibility of our covert channel, while outlining its boundaries. Notably, this kind of covert channel is not monitored by existing data leakage prevention systems.

References

[1] J. Loughry and D. A. Umphress, "Information leakage from optical emanations," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 3, pp. 262–289, 2002.

[2] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations." in *Information hiding*, vol. 1525. Springer, 1998, pp. 124–142.

[3] M. Guri, M. Monitz, and Y. Elovici, "Bridging the air gap between isolated networks and mobile phones in a practical cyber-attack," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 8, no. 4, p. 50, 2017.

[4] ——, "USBee: Air-gap covert-channel via electromagnetic emission from USB," in *14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 264–268.

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

[6] C. Kasmi, J. Lopes Esteves, and P. Valembois, "Air-gap limitations and bypass techniques: command and control using smart electromagnetic interferences," *The Journal on Cybercrime & Digital Investigations*, vol. 1, no. 1, Dec. 2016, Botconf 2015, Paris.

[7] Z. Yang, Q. Huang, and Q. Zhang, "Nicscatter: Backscatter as a covert channel in mobile devices," in *Proceedings of the 23rd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '17. New York, NY, USA: ACM, 2017, pp. 356–367.

[8] Z. Zhou, W. Zhang, and N. Yu, "Data Exfiltration via Multipurpose RFID Cards and Countermeasures," *arXiv e-prints*, p. arXiv:1902.00676, Feb. 2019.

[9] M. Guri and M. Monitz, "Lcd tempest air-gap attack reloaded," in *2018 IEEE International Conference on the Science of Electrical Engineering in Israel (ICSEE)*. IEEE, 2018, pp. 1–5.

[10] M. Guri, B. Zadov, and Y. Elovici, "Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," *IEEE Transactions on Information Forensics and Security*, 2019.

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

[12] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *Journal of Communications*, vol. 8, no. 11, pp. 758–767, Nov. 2013.

[13] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers," *arXiv preprint arXiv:1606.05915*, 2016.

[14] ——, "Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise (diskfiltration)," in *European Symposium on Research in Computer Security*. Springer, 2017, pp. 98–115.

[15] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *Proc. 9th Int. Conf. Malicious and Unwanted Software: The Americas (MALWARE)*, Oct. 2014, pp. 58–67.

[16] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines," *ArXiv e-prints*, Apr. 2018.

[17] L. Deshotels, "Inaudible sound as a covert channel in mobile devices." in *WOOT*, 2014.

[18] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *arXiv preprint arXiv:1406.1213*, 2014.

[19] B. Carrara and C. Adams, "On acoustic covert channels between air-gapped systems," in *International Symposium on Foundations and Practice of Security*. Springer, 2014, pp. 3–16.

[20] P. Krishnamurthy, F. Khorrami, R. Karri, D. Paul-Pena, and H. Salehghaffari, "Process-aware covert channels using physical instrumentation in cyber-physical systems," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 11, pp. 2761–2771, Nov. 2018.

[21] M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "VisiSploit: An optical covert-channel to leak data through an air-gap," in *14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 2016, pp. 642–649.

[22] J. Loughry and D. A. Umphress, "Information leakage from optical emanations," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 3, pp. 262–289, 2002.

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

[24] M. Guri, B. Zadov, and Y. Elovici, *LED-it-GO: Leaking (a lot of) Data from Air-Gapped Computers via the (small) Hard Drive LED*. Cham: Springer International Publishing, 2017, pp. 161–184.

[25] J. Loughry, "Optical TEMPEST," in *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*. IEEE, Aug. 2018.

[26] D. Bak, P. Mazurek, and D. Oszutowska–Mazurek, "Optimization of demodulation for air–gap data transmission based on backlight modulation of screen," in *Lecture Notes in Computer Science*. Springer International Publishing, 2019, pp. 71–80.

[27] Z. Zhou, W. Zhang, S. Li, and N. Yu, "Potential risk of IoT device supporting IR remote control," *Computer Networks*, vol. 148, pp. 307–317, Jan. 2019.

[28] M. Guri and D. Bykhovsky, "aIR-jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (IR)," *Computers & Security*, vol. 82, pp. 15–29, may 2019.

[29] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations," in *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*. IEEE, 2015, pp. 276–289.

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

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

[32] G. Sarah. (2013, May) How to make a computer screen invisible. dailymail. [Online]. Available: http://www.dailymail.co.uk/sciencetech/article-2480089/How-make-screen-INVISIBLE-Scientist-shows-make-monitor-blank-using-3D-glasses.html

[33] E. Osnos, D. Remnick, and J. Yaffa, "Trump, Putin, and the new Cold War," The New Yorker, Mar. 2017, [Online; accessed 26 August 2018]. [Online]. Available: https://www.newyorker.com/magazine/2017/03/06/trump-putin-and-the-new-cold-war

[34] I. Khimji. (2015, May) The malicious insider. [Online]. Available: http://www.tripwire.com/state-of-security/security-awareness/the-malicious-insider/

[35] M. Rouse. evil maid attack. [Online]. Available: http://searchsecurity.techtarget.com/definition/evil-maid-attack

[36] A. H. Lashkari, S. Farmand, D. O. B. Zakaria, and D. R. Saleh, "Shoulder surfing attack in graphical password authentication," *International Journal of Computer Science and Information Security*, vol. 6, no. 2, pp. 145–154, Nov. 2009.

[37] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography." in *ISSA*, 2005, pp. 1–11. [Online]. Available: http://martinolivier.com/open/stegoverview.pdf

[38] W. Yuan, K. Dana, A. Ashok, M. Gruteser, and N. Mandayam, "Dynamic and invisible messaging for visual MIMO," in *Proc. IEEE Workshop the Applications of Computer Vision (WACV)*, Jan. 2012, pp. 345–352.

[39] A. Wang, C. Peng, O. Zhang, G. Shen, and B. Zeng, "Inframe: Multiflexing full-frame visible communication channel for humans and devices," in *Proceedings of the 13th ACM Workshop on Hot Topics in Networks*, ser. HotNets-XIII. New York, NY, USA: ACM, 2014, pp. 23:1–23:7.

[40] T. Li, C. An, X. Xiao, A. T. Campbell, and X. Zhou, "Real-time screen-camera communication behind any scene," in *Proceedings of the 13th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '15. New York, NY, USA: ACM, 2015, pp. 197–211. [Online]. Available: http://doi.acm.org/10.1145/2742647.2742667

[41] B. W. Kim, H. C. Kim, and S. Y. Jung, "Display field communication: Fundamental design and performance analysis," *Journal of Lightwave Technology*, vol. 33, no. 24, pp. 5269–5277, Dec. 2015.

[42] S.-Y. Jung, H.-C. Kim, and B. W. Kim, "Implementation of two-dimensional display field communications for enhancing the achievable data rate in smart-contents transmission," *Displays*, jul 2018.

[43] J. Wang, W. Huang, and Z. Xu, "Demonstration of a covert camera-screen communication system," in *Proc. 13th Int. Wireless Communications and Mobile Computing Conf. (IWCMC)*, Jun. 2017, pp. 910–915.

[44] B. E. Saleh and M. C. Teich, *Fundamentals of Photonics*, 2nd ed. Wiley, 2007.

[45] J. Proakis and M. Salehi, *Digital Communications*, 5th ed. McGraw-Hill, 2008.

[46] J. Liu, S.-M. Morgens, R. C. Sumner, L. Buschmann, Y. Zhang, and J. Davis, "When does the hidden butterfly not flicker?" in *SIGGRAPH Asia 2014 Technical Briefs*. ACM, 2014, p. 3. [Online]. Available: https://graphics.soe.ucsc.edu/papers/flicker/

[47] *Proceedings of the National Academy of Sciences of the United Stated of America*.

[48] H. Yamamoto, S. Farhan, S. Motoki, and S. S., "Development of 480-fps led display by use of spatiotemporal mapping," 2012.

[49] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," vol. 90, p. 727752, 2010.

[50] P. Gouras, *Color vision*. Elsevier, 1991, pp. 467–479.

[51] S. Coren, L. M. Ward, and J. T. Enns, "The visual system," in *Sensation and perception, 5th edition*. Harcourt, 1999.

[52] ——, "Brightness and spatial frequency," in *Sensation and Perception, 5th edition*. Harcourt, 1999.

[53] ——, "The constancies," in *Sensation and perception, 5th edition*. Harcourt, 1999.

[54] ——, "Time," in *Sensation and perception*. Harcourt, 1999.