SCREEN2AIR: Exploiting Screen Savers for Covert Long-Distance Data Exfiltration and Defense

Ye-Rim Jeong
Department of Convergence Security Engineering
Sungshin Women's University
Seoul, Korea
Email: 220254016@sungshin.ac.kr

Yeon-Jin Kim
Department of Convergence Security Engineering
Sungshin Women's University
Seoul, Korea
Email: 220246046@sungshin.ac.kr

Chea-Yeon Park
Department of Convergence Security Engineering
Sungshin Women's University
Seoul, Korea
Email: 220254013@sungshin.ac.kr

Il-Gu Lee
Department of Convergence Security Engineering
Sungshin Women's University
Seoul, Korea
Email: iglee@sungshin.ac.kr

***Abstract*—An air-gapped network is used as a representative protection mechanism to strengthen cybersecurity by physically separating systems. However, to enhance the security of such environments practically, in-depth research on air-gap attack techniques should first be conducted. This study proposes SCREEN2AIR, a novel air-gap attack technique that utilizes screen savers and a high-dimensional modulation technique to encode large amounts of information. Screen savers generally do not cause user suspicion because they are automatically executed when the user is absent and exhibit excellent detection evasion. The experimental results demonstrated that a stable extraction success rate, up to 13 times higher than that of the conventional QR code-based method, can be maintained when the number of cells is small. In addition, we propose a technique to intentionally lower screen saver image quality to defend against decoding, and we experimentally demonstrate that the attack success rate can be reduced by up to 95% compared to using normal high-quality images.**

Keywords-Air-Gap; Data Leak; Screen Saver; Cybersecurity.

I. INTRODUCTION

In recent years, as our reliance on the Internet has grown, cyberattacks have manifested in diverse forms, such as viruses, worms, and ransomware [1]. These attacks can cause significant damage, such as data breaches and network paralysis, at both the individual and national levels. The establishment of air-gapped networks is recommended to mitigate the impact of such threats and protect critical national and industrial information [2]. An air-gapped network is a security system that physically and completely isolates an internal network from external networks, thereby minimizing the risk of external intrusion and internal data leakage [3]. Air gaps are used in environments that require high security, such as national infrastructures and military systems [4].

However, in recent years, security threats targeting air-gapped networks have become a reality; specifically, attacks that exfiltrate data from internal networks to the outside using electromagnetic signals, optical signals, and vibrations generated by the operation of computer components and Internet of Things (IoT) devices are being actively studied [5]. For instance, in 2010, the Stuxnet malware targeted an Iranian nuclear facility [6]. Additionally, in 2024, the Korea Hydro & Nuclear Power Research Institute was hacked, and in 2016, the Ministry of National Defense of the Republic of Korea also suffered a cyberattack [7]. These incidents demonstrate that cyberattacks against air-gapped systems have been reported in multiple countries. Such covert channel-based attacks are challenging to detect using traditional network-based security solutions, such as Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and firewalls [8]. Therefore, a systematic analysis of potential attack vectors is essential to enhance the security of air-gapped environments.

Conventional air-gap attacks using various physical channels, including electromagnetic, optical, and vibration, have certain limitations. They are easy for users to recognize owing to their high visibility and narrow transmission range [9]. To address these limitations, this study proposes a novel information leakage technique based on a screen saver and a high-dimensional modulation method for encoding large volumes of data. The proposed technique divides the screen saver into cells of a fixed size and assigns binary data to each cell, generating a movement pattern that covertly transmits information that is recognizable only to the attacker. Because screen savers are standard system functions that are typically activated when the user is away, the attack does not raise suspicion and offers strong detection evasion. Furthermore, as the data transmission range scales with the screen size, this technique is advantageous for long-distance exfiltration.

The contributions of this paper are as follows:

- We propose a novel data leakage mechanism and a corresponding defense technique for air-gapped networks utilizing screen savers.
- We experimentally demonstrate the feasibility and effectiveness of the proposed attack with respect to the cell size and number of cells on the screen saver.

• We present a defense strategy tailored to screen-saver-based air-gap attacks and experimentally validate its practicality and performance.

The remainder of this paper is organized as follows. Section II reviews the related work. Section III introduces the proposed information leakage and defense techniques based on screen savers. Section IV presents the results of the performance evaluation. Finally, Section V concludes the study.

II. RELATED WORK

Morderchai Guri [10] proposed an air-gap attack that embeds a Quick Response (QR) code into a monitor display exploiting the limitations of the human visual system in rapidly perceiving blinking images and subtle grayscale patterns. In this study, 40 participants were tested for their ability to recognize Aurmented Reality (AR) codes visually, and the detection range was evaluated using both DSLR and smartphone cameras. However, the method achieved only a 75% success rate in data extraction at a distance of 1m when using a Digital Single-Lens Reflex (DSLR) camera with a 35mm lens, and the maximum recognition range using a smartphone camera was limited to 1.5 meters. Moreover, due to individual differences in visual sensitivity, there exists a risk that an embedded attack pattern may be noticeable to some users.

Anindya Maiti et al. [11] proposed an air-gap attack that leverages the infrared (IR) functionality of smart lighting systems. They encoded the binary data by dividing the brightness levels of smart lights into discrete steps and assigning bit values to each level. A TSOP48 IR sensor connected to an Arduino board was used to detect changes in infrared intensity. Additionally, an 80mm telescope with 45-255x magnification was employed to collect infrared signals and enhance the decoding performance. However, this technique is constrained by its reliance on smart lights equipped with infrared capabilities, which limits its applicability to specific environments.

Morderchai Guri [12] proposed an air gap attack technique that finely adjusts the brightness of the monitor screen, focusing on the fact that it is difficult for the human visual system to recognize the rapidly changing minute brightness difference. In this paper, the monitor screen was photographed using a security camera, webcam, and smartphone camera. OpenCV, an open-source library, was used to process the photographed image in real-time, and a C program that performs additional MATLAB processing by calculating frame brightness was developed and used for decoding. However, this technique has limitations in that the maximum transmission distance is only 1.5m when photographed with a smartphone camera, so the transmission range is limited, and the transmission speed is slow to 1 bit/s.

Previous studies have proposed attack scenarios that exfiltrate data using computer components or IoT devices located in air-gapped environments. While these studies introduced novel attack vectors that are challenging to detect using conventional network-based security solutions, they are limited by the restricted range of usable devices, short transmission distances, and high visibility of attack patterns, which hinder their practical applicability, To address these limitations, this paper proposes a new air-gap attack technique that exploits the screen saver of a computer monitor. The proposed method enables long-distance data exfiltration while remaining inconspicuous to users. Furthermore, we enhance transmission speed by applying a high-dimensional modulation technique and supporting large-volume data leakage.

III. INFORMATION LEAKAGE ATTACK USING SCREEN SAVER AND ITS DEFENSE TECHNIQUE

A. Information Leakage Attack Using Screen Saver

Figure 1 illustrates the operation of the proposed method, SCREEN2AIR. First, after collecting the information to infect and leak malware into a PC inside the airgap, it was converted into a binary number. Subsequently, the screen saver screen was divided into cells of a certain size, and binary bits of data were assigned to each area. When an attack begins, bubbles of a specific color among the bubbles of the screen saver are moved to the corresponding cell according to the information converted to a binary number and repeatedly stopped for a certain period. At this time, since the bubbles used in the attack operate mixed with ordinary bubbles, it poses a challenge for the user to discern this as an anomalous symptom. An attacker outside the airgap photographs the screen saver with a camera and then decrypts the information by analyzing the movement of the bubbles.

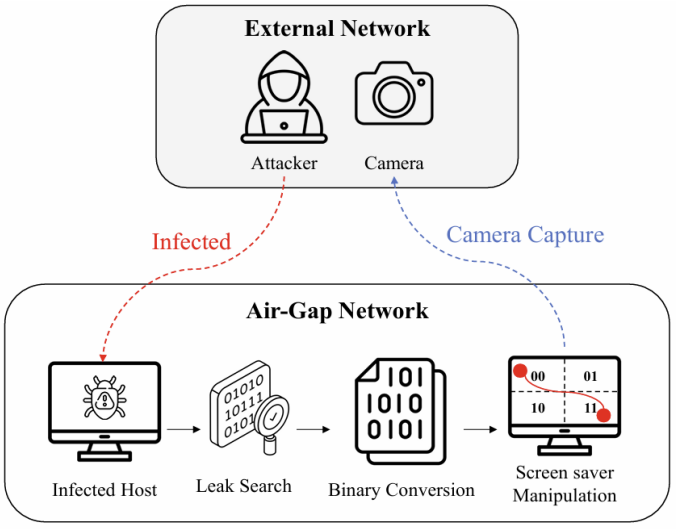

Figure 1. Method of attack using a screen saver

1) Data Encoder

In an environment where the screen saver is divided into 2^n cells, the pseudocode for transmitting information is presented in Algorithm 1. First, the information to be leaked outside the air-gap network is converted into binary data, and

n bit grouping is performed to map it to cells in the screen saver. The height and width of the monitor on which the screen saver was executed was assessed, and the color of the bubbles to be used for data leakage were selected. The screen was divided into 2^n cells based on its height and width and assigned n bits of binary data to each cell. According to the information converted into binary data, the selected bubbles moved to the corresponding coordinates within the cell and stopped at that position for a certain period while normal bubbles maintained their normal movement. For all n bit groups, the corresponding operation process was repeated, and the binary data were leaked to the outside through the position movement pattern of the bubbles.

Algorithm 1 Data Encoder Algorithm (Quadrant-based Transmitter)

```
function TransmitInformation(info)
    binaryData ← ConvertToBinary(info)
    bitPairs ← GroupIntoBitPairs(binaryData)
    screenSize ← GetScreenSize()
    width, height ← screenSize.width, screenSize.height
    targetBubbles ← SelectSpecialColoredBubbles(minCount = 2)
    for each bitPair in bitPairs do
        if bitPair = "00" then
            cx ← random value in range [width/2, width]
            cy ← random value in range [0, height/2)
        else if bitPair = "01" then
            cx ← random value in range [0, width/2)
            cy ← random value in range [0, height/2)
        else if bitPair = "10" then
            cx ← random value in range [0, width/2)
            cy ← random value in range [height/2, height]
        else                                          ▷ bitPair = "11"
            cx ← random value in range [width/2, width]
            cy ← random value in range [height/2, height]
        end if
        MoveBubblesTo(targetBubbles, (cx, cy))
        PauseAtQuadrant(targetBubbles, duration = FIXED_DURATION)
        UpdateNormalBubbles()
        Wait(TIME_INTERVAL)
    end for
end function
```

Algorithm 1. Data encoder pseudocode.

2) Data Decoder

The pseudocode for decrypting information in an environment where the screen saver is divided into 2^n cells is presented in Algorithm 2. First, the image captured by the screen saver is inserted into the decoder. The decoder analyzes the height and width of the image and converts it into an HSV color space. Subsequently, the image is analyzed to identify the location of the mark. Because the bubbles on the screen saver have translucent characteristics, two HSV (Hue, Saturation, Value) coordinates were set by adjusting the brightness and saturation according to the color of the mark. To distinguish colors accurately, the image was masked using Gaussian blur, and the color was recognized in the image according to the HSV coordinates. The area of each cell was classified according to the height and width of the analyzed image, and the binary data allocated according to the area where the recognized color was located was output.

Algorithm 2 Data Decoder Algorithm (Quadrant-based Reception)

```
Load the image from file
Convert image to RGB color space
Get image height and width
Convert image to HSV color space
Define two HSV ranges for detecting red
for each red HSV range do
    Create a mask for the current HSV range
    Print the number of non-zero pixels in the mask
    Apply Gaussian blur to the mask
    Find contours in the mask
    for each contour do
        if area of contour > 30 then
            Calculate the center point (cx, cy)
            if cx >= width/2 and cy < height/2 then
                bit ← "00"
            else if cx < width/2 and cy < height/2 then
                bit ← "01"
            else if cx < width/2 and cy >= height/2 then
                bit ← "10"
            else
                bit ← "11"
            end if
            Save bit value
            break inner loop
        end if
    end for
    if result is found then
        break outer loop
    end if
end for
if result is found then
    Print bit value
else
    Print "No red region detected"
end if
```

Algorithm 2. Data decoder pseudocode.

B. Defense Techniques for Information Leakage Attack Using Screen saver

Screen savers are automatically activated when a computer remains idle for a certain period, thereby preventing screen burn-in, preserving user privacy, and conserving power. Although they were originally developed to prevent burn-in in older display technologies such as Cathode-Ray Tube (CRT) and Plasma Display Panel (PDP), their necessity has diminished with the widespread adoption of Liquid Crystal Display (LCD) and Light-Emitting Diode (LED) displays. Nevertheless, screen savers are still used for screen protection and privacy enhancement.

Detecting data leakage attacks that exploit screen savers in air-gapped environments using traditional security solutions can be challenging because they utilize legitimate system programs as cover channels. In this study, we propose a defense technique that intentionally degrades the image quality of screen savers to reduce the stealthiness of such attacks and lower their success rate. The proposed method decreases the resolution of the screen saver to reduce the clarity of the visual information, thereby significantly diminishing the accuracy of data decryption when the screen is captured by an external camera.

IV. EVALUATION RESULTS AND ANALYSIS

A. *Evaluation of Air-Gap Attack Experiments Based on Screen Saver*

This experiment was conducted by photographing the screen saver screen of a Samsung Galaxy Book Pro laptop with the camera of a Galaxy S25 smartphone and then processing the image to extract information. Shooting was performed by gradually increasing the distance between the screen and camera, and the data leaked from the photographed image were decrypted using an automated script. The air-gap attack technique, which converts leaked data into a QR code and inserts it into an image with lower visibility to evaluate the performance of the proposed model and compare it with existing techniques, was implemented as a conventional model.

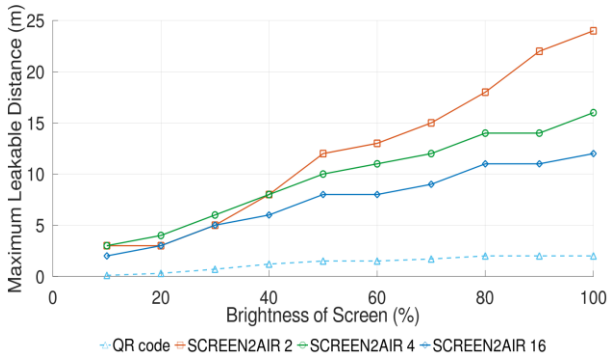

Figure 2. Maximum leakable distance depending on scree brightness.

Figure 2 illustrates the result of comparing the maximum outflow distance according to the screen's brightness. The proposed model (SCREEN2AIR 2) with two cells recorded the longest transmission distance because it can transmit information up to about 24m. On the other hand, the conventional study (QR code) was limited to a maximum of 2m. And as the number of cells increased, the transmission distance tended to decrease somewhat. Since the conventional technique relies on camera-based static image recognition, it was confirmed that the robustness against ambient illumination change is low, and due to this, there is a limit to the transmission distance.

Figure 3 illustrates the results of comparing the information leakage based on the transmission distance of the proposed model with 2, 4, and 16 cells, respectively. In this experiment, the word "hello" was attempted to be transmitted, and each character is expressed as 8 bits (ASCII code), so the maximum information leakage is 40 bits. In the proposed model with 16 cells, the outflow began to decrease from the 12m point and decreased to 3 bits at the 24m point. However, in the proposed model with 4 cells, the outflow decreased from 15m and recorded 13 bits at 24m. The proposed model with 2 cells exhibited the most stable performance, maintaining a 40-bit level even at 24m.

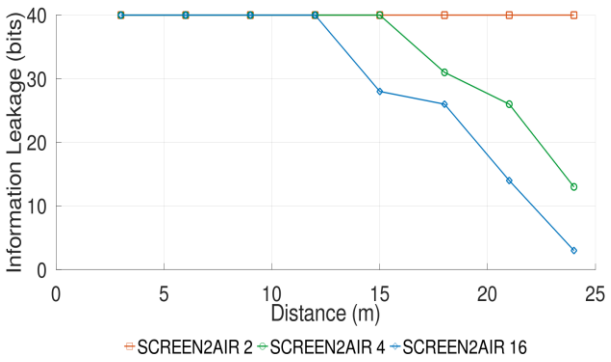

Figure 3. Information leakage by distance by cell count

This result is interpreted as follows: as the number of cells increases, the boundaries between the cells become closer to each other, and the cells where the bubbles are located are not distinguished, thereby increasing the probability of a decoding error. In particular, when the number of cells is 16, the gap between cells is very narrow; therefore, there is a high possibility of a signal hanging over the boundary or a recognition error occurring during long-distance transmission, resulting in a sharp decrease in information leakage. However, when the number of cells was as low as two, the size of the cells was large, and the boundaries were wide, enabling stable information leakage even over a long distance. However, the higher the number of cells, the higher the transmission efficiency because more binary data can be encoded in a single cell. In other words, it has the advantage of transmitting more information at once; however, reliability decreases in a long-distance environment because the gap between cells narrows. In addition, the results of this experiment show that as the screen size increases, the cell gap widens, so even if more cells are placed when using a large screen, a sufficient gap between cells is secured. Thus, a high outflow can be expected, even when long-distance transmissions are performed.

Additionally, increasing the resolution and quality of an image can potentially improve the success rate of information extraction. The pre-image optimization process must be performed since images with low or high resolution are likely to cause errors or missing information during the data extraction process. Therefore, in this paper, image quality processing was performed using "upscale.media [13]", and Artificial Intelligence (AI)-based image upscaling service. "upscale.media" uses an AI super-resolution algorithm to improve low-resolution images up to 8 times to preserve details and textures as much as possible. Rather than simply enlarging the image, the neural network improves the clarity without deteriorating the quality of the original image by analyzing the patterns and boundaries of the image and naturally restoring the missing pixels.

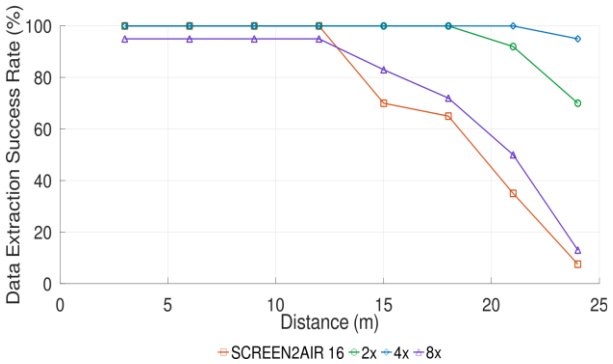

Figure 4. Success rate of information extraction according to distance by Scaling Factor when there are 16 cells

Figure 4 compares the performances of the same scaling factors when the number of cells is 16. The 4x scaling factor maintained a stable data extraction success rate of 100% up to 21m and slightly decreased to 95% at 24m. The 2x scaling factor maintained 100% performance up to 18m and then gradually decreased to 70% at 24m. The 8x scaling factor showed a 95% success rate up to 12m and then decreased to 13% at 24m. Consequently, when an appropriate scaling factor was applied, the information extraction success rate was improved in a long-distance transmission environment. In particular, when a 4x scaling factor was applied to a system with 16 cells, a high information extraction success rate of 95% was recorded at a distance of 24m; this shows that the scaling factor significantly impacts the information extraction performance when the scaling factor is not used, compared to 7.5%. These findings show that proper image scaling more clearly distinguishes inter-cell boundaries and amplifies the detailed features of the mark to effectively offset the effect of noise generated during long-distance transmission; this also suggests that excessive scaling can cause noise amplification or artifact generation, which can degrade leakage data-decoding performance.

Through experiments, it was confirmed that the optimization of the scaling factor plays an important role in increasing the effectiveness and reliability of information leakage. Therefore, it is expected that effective information extraction will be possible through the selection and optimization of the scaling factor in long-distance data leakage scenarios within an air-gap network in the future.

B. Experimental Evaluation of Defense Techniques for Attack Techniques Based on Screen Savers

Figure 5 shows the change in the information extraction success rate according to the attack distance. The information extraction performance was compared with that of normal screen savers with 2 and 4 cells, respectively, and screen savers with deteriorated image quality by applying a defense technique. Normal screen savers maintain a 100% data-extraction success rate up to a distance of 24m. However, in the case of screen savers with deteriorated image quality, the data extraction success rate decreased sharply when the distance was over 9m. As such, screen savers with deteriorated image quality decreased by 95% compared with normal screen savers at a distance of 24m and decreased by approximately 29.5% on average. This suggests that by lowering the image quality of the screen savers, the quality of the visual information decreases, which significantly decreases the decoding accuracy of the attack side. According to the experimental results, the deterioration in the image quality of screen savers can effectively reduce the reliability of an attack as the physical distance increases. This demonstrates that screen saver quality control can be used as a security enhancement technique in an air-gap environment.

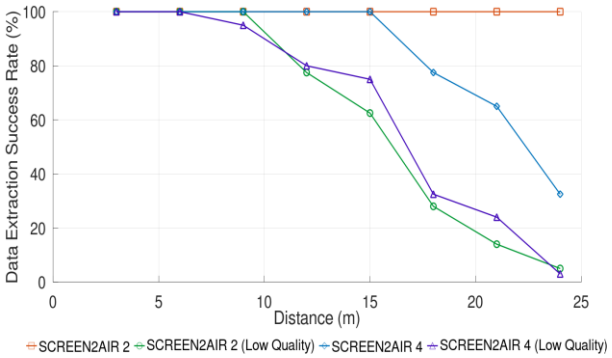

Figure 5. Success rate of information extraction according to distance by image quality

V. CONCLUSION

Building an air-gapped network is recommended to mitigate the impact of cyberattacks and protect critical national and industrial information. However, data leakage attacks that exploit various types of signals within air-gapped systems have been actively studied. Because covert channel-based attacks are difficult to detect using traditional network-based security solutions, proactive re-search on air-gap attack techniques is essential for enhancing the security of such environments.

Conventional air-gap attacks that utilize physical channels, such as electromagnetic and optical signals, are limited by their high visibility, which makes them easily detectable by users, and their short transmission range. To address these limitations, we propose a novel air-gap attack technique that leverages a screen saver combined with a high-dimensional modulation scheme to encode high-capacity information. The proposed method divides the screen saver into cells of fixed size and assigns binary data to each cell to generate a movement pattern for covert data transmission.

The experimental results revealed that a stable extraction success rate of up to 13 times higher can be achieved at long distances when the number of cells is small. Furthermore, applying an appropriate scaling factor improves the success

rate of information extraction by up to 7.6 times, even in long-distance scenarios, confirming the feasibility of effective data leakage over extended ranges.

In addition, we evaluate a defense technique that intentionally degrades the image quality of a screen saver to reduce the reliability of the attack. The experimental results showed that, while the data extraction success rate was maintained almost completely up to 24 m under normal image quality, it dropped sharply to a maximum of 5% at the same distance when the image quality was reduced. These findings experimentally demonstrate that lowering screen-saver image quality is an effective and practical defense technique.

In future work, we plan to compare and analyze additional defense strategies against information leakage attacks using screen savers. These strategies include inserting invisible watermarks into screen content and applying privacy-protection films on the monitor.

ACKNOWLEDGMENT

This study was supported by the Industrial Innovation Human Resources Growth Support Project (RS-2024-00415520), the Information Protection Core Source Technology Development Project (RS-2024-00437252) of the Ministry of Trade, Industry and Energy, and the Korea Institute of Industrial Technology Promotion in 2024.

REFERENCES

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments," Energy Reports, vol. 7, 2021, pp. 8176–8186..

[2] P. Vähäkainu, M. Lehto, and A. Kariluoto, "Cyberattacks against critical infrastructure facilities and corresponding countermeasures," in Cyber Security: Critical Infrastructure Protection, Springer, Cham, 2022, pp. 255–292.

[3] M. R. Na and K. B. Sundharakumar, "A study on air-gap networks," in *Proc. 2024 5th Int. Conf. Innovative Trends in Information Technology (ICITIIT)*, IEEE, 2024, pp. 1–6.

[4] J. Park *et al.*, "A survey on air-gap attacks: Fundamentals, transport means, attack scenarios and challenges," *Sensors*, vol. 23, no. 6, 2023, p. 3215.

[5] Y.-J. Kim, N.-E. Park, and I.-G. Lee, "Air-Fuzz: Feasibility analysis of fuzzing-based side-channel information leakage attack in air-gapped networks," in *Proc. Int. Conf. Information Security Applications*, Springer Nature, Singapore, 2024, pp. 231–242.

[6] S. Q. Abbas and H. Fatima, "Cyber security threats to Iran and its countermeasures: Defensive and offensive cyber strategies," *Journal of Research in Social Sciences*, vol. 12, no. 2, 2024, pp. 1–21.

[7] J. Lee *et al.*, "Optical air-gap attacks: Analysis and IoT threat implications," *IEEE Network*, vol. 38, no. 6, 2024, pp. 342–352.

[8] M. Guri, "Air-gap electromagnetic covert channel," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, 2023, pp. 2127–2144.

[9] M. T. Naz and A. M. Zeki, "A review of various attack methods on air-gapped systems," in *Proc. 2020 Int. Conf. Innovation and Intelligence for Informatics, Computing and Technologies (3ICT)*, IEEE, 2020, pp. 1–6.

[10] M. Guri, "Optical air-gap exfiltration attack via invisible images," *Journal of Information Security and Applications*, vol. 46, 2019, pp. 222–230.

[11] A. Maiti and M. Jadliwala, "Light ears: Information leakage via smart lights," *Proc. ACM Interactive, Mobile, Wearable and Ubiquitous Technologies*, vol. 3, no. 3, 2019, pp. 1–27.

[12] M. Guri, D. Bykhovsky, and Y. Elovici, "Brightness: Leaking sensitive data from air-gapped workstations via screen brightness," in *Proc. 2019 12th CMI Conf. Cybersecurity and Privacy (CMI)*, IEEE, 2019, pp. 1–6..

[13] upscale.media, https://www.upscale.media, [retrieved: June, 2025]