Breaching Air-Gapped Systems

Raine Johnson
CSSE, School of STEM
University of Washington
Bothell, WA
rainej1@uw.edu

Erica Au
CSSE, School of STEM
University of Washington
Bothell, WA
auerical@uw.edu

Daniil Marozau
CSSE, School of STEM
University of Washington
Bothell, WA
raspie@uw.edu

***Abstract*—This paper explores the feasibility, attack methodologies, and mitigation strategies for breaching air-gapped devices, analyzing real-world attack scenarios and their implications for cybersecurity. Additionally, it discusses countermeasures such as signal shielding, anomaly detection, and hardware-based security enhancements to protect against covert exfiltration techniques.**

***Index Terms*—Air-gapped security, side-channel attacks, covert channels, electromagnetic emissions, acoustic data leakage, optical data transmission, thermal radiation attacks**

I. Introduction

Air-gapped systems, commonly known as isolated networks, protect sensitive information by keeping them physically separate from the internet and other untrusted networks. These systems are extensively utilized in high-security environments, such as military installations, financial organizations, and critical infrastructure. This separation significantly reduces the risk of external cyber threats; however, it also introduces specific cybersecurity challenges, such as difficulties in patch management, the risk of insider threats, and the possibility of data extraction and compromisation through covert methods. As cyber threats continue to evolve, it is essential to understand the vulnerabilities and protective measures for air-gapped systems to ensure their integrity and confidentiality. This paper will examine the cybersecurity challenges unique to air-gapped environments, case studies we analyzed, and strategies we propose to address these risks.

II. Understanding Air-Gapped Systems

A. Purpose

As air-gapped systems are designed to be isolated from the web and other networks, the communication of such systems with any outside source happens manually to keep connections secure. Such measures prevent the most common and well-known vector attacks that can occur such as remote exploitation of vulnerabilities or direct malware distribution. The structure of air-gapped systems often involves a layered approach to security, with multiple redundant defenses in place to further isolate and protect the network. Each layer typically involves specialized security protocols, such as the use of hardware-based firewalls, intrusion detection systems, and encryption mechanisms, to secure both physical and digital access.

B. Use Cases

Such enhanced and complex security is essential for core and most sensitive systems in the world, which will bring nation-level troubles if compromised. Some examples would be military use, government databases, and confidential corporate databases. However, even such systems are prone to vulnerabilities.

C. Limitations

Due to complete isolation from the outside network, such systems are assumed to be attack-prone and secured. The limitations of air-gapped security lie in the inability to fully prevent all forms of data exfiltration or intrusion that can occur through physical proximity or indirect communication channels. As a result, while air-gapping provides a significant layer of security, it is not a foolproof defense and requires other layers of security and practices to ensure the integrity of the system.

III. Attack Vectors Against Air-Gapped Systems

This section aims to explain possible attack vectors that can compromise the integrity of the air-gapped system. It also shows case studies of such attacks.

A. Physical Access Attacks

Case study: As a part of the operation ”Olympic Games”, malware Stuxnet worm infected an air-gapped network of computers inside Iran’s nuclear facilities and halted approximately 1,000 of the 5,000 centrifuges. We will not go into details about the purpose of the attack, focusing on physical vulnerability since the system was infected by a simple USB source plugged into one of the computers.

Analysis: Physical access to the system allows attackers to infect it and compromise it using various techniques, including worm malware and data leaks. If attackers can gain access to the system through an insider threat or by exploiting weak physical security, they can easily bypass the isolation air-gapping provides.

B. Electromagnetic Radiation from RAM

Case study: Ben-Gurion University scientists, led by Mordechai Guri, devised a means of stealing data from air-gapped computers by intercepting electromagnetic emanations

from the RAM modules of computers. Based on the intercepted emanations, intruders could reconstruct confidential information without any physical interface.

Technical details: RAM operates by switching the electrical charges to store the data and such activity causes electromagnetic emissions, which can be detected and analyzed using specialized equipment. The electromagnetic leakage is particularly pronounced in DDR RAM modules due to their high-speed operation. During the Guri's research, they stayed several meters away from the air-gapped computer with an antenna and SDR captured the EM waves. As a result of the conducted research they were able to reconstruct binary data by analyzing the modulated EM signals including sensitive data such as passwords and authentication keys.

Analysis: This is a research example of a possible electromagnetic attack. The finding was that a simple SDR (Software-defined radio) receiver can intercept sensitive data from air-gapped systems. The range required for interception varies starting from 1 and over 10 meters. Of course, due to sensitivity to EM waves the closer the distance the better, but this still shows that if the attacker has physical access to the air-gapped system or a room where it is located, it is possible to extract sensitive information.

C. Acoustic Data Exfiltration

One of the most intriguing and effective covert exfiltration techniques involves acoustic data transmission, where attackers leverage sound waves—both audible and inaudible—to covertly transmit information from an air-gapped system to an external receiver. This method exploits the fact that nearly all computing devices, even those without built-in speakers, generate some form of acoustic emissions that can be modulated and encoded for data leakage.

Among the pioneering studies in this field, DiskFiltration (Guri et al., 2018) demonstrated how a speakerless air-gapped computer can be exploited to transmit data through controlled variations in hard drive noises. By manipulating the movement of the hard drive's read/write head, attackers can generate specific acoustic signals that can be picked up by nearby microphones. This technique proves that even passive components can become active vectors for data exfiltration, challenging the assumption that the absence of traditional speakers negates the risk of audio-based attacks.

Moving beyond mechanical noise, researchers have explored the deliberate use of high-frequency inaudible sound waves for data transmission. Many modern computers and electronic devices include ultrasonic-capable speakers—whether as part of a laptop's built-in hardware or peripheral devices such as monitors. This allows attackers to encode information in frequencies beyond human perception and transmit it to a compromised device equipped with a microphone (Yirka, 2024). Such techniques are particularly dangerous because they do not require user interaction; malware can silently modulate acoustic signals to leak data while remaining undetected by conventional security tools.

D. Thermal and Optical Attacks

Thermal attacks, in particular, exploit residual heat signatures left on input devices such as keyboards. Guri et al. (2016) illustrate how attackers can use thermal imaging cameras to analyze heat dissipation patterns and reconstruct keystrokes with alarming accuracy. The feasibility of such an attack is heightened by the fact that different materials retain heat differently, allowing attackers to estimate the sequence of key presses based on the decay rate of thermal residues. As this technique requires no direct electronic interaction with the target system, it poses a significant risk in environments where physical security alone is assumed to be a sufficient defense mechanism.

Optical side-channel attacks operate on a similarly covert principle, exploiting unintended light emissions from system components. Nassi et al. (2021) highlight how minor fluctuations in LED indicators, which are often dismissed as innocuous, can serve as an information leakage vector. Through high-resolution optical sensors or even consumer-grade cameras, attackers can capture these subtle fluctuations and extract meaningful data. Moreover, reflections from computer screens on nearby objects, such as eyeglasses or walls, further expand the attack surface, as demonstrated by Glowworm (Nassi et al., 2021).

E. Covert Networking Techniques

The assumption that air-gapped systems are impervious to external communication has been repeatedly challenged by research into covert networking techniques. While traditional security models rely on the idea that a lack of direct network connectivity isolates critical systems from external threats, various studies have demonstrated that attackers can exploit unintended transmission channels to establish clandestine communication pathways. These covert networking techniques leverage electromagnetic emissions, power fluctuations, and even acoustic signals to bridge the gap between an air-gapped machine and an external receiver.

One of the most striking examples of covert networking is USBee, introduced by Guri et al. (2016), which transforms USB devices into radio frequency (RF) transmitters. By modulating electromagnetic emissions from USB data buses, attackers can encode and transmit data at short distances without requiring any modification to the USB hardware itself. This technique underscores a fundamental flaw in the assumption that air-gapped systems cannot "talk" to external devices without a physical link. Similarly, POWER-SUPPLaY, another method developed by Guri (2020), demonstrates how fluctuations in power consumption can be manipulated to transmit data through power lines, effectively turning an air-gapped system's electrical activity into a communication channel.

IV. Case Study of Air-Gap Breaches

One of the most well-known cases is the Stuxnet attack, which targeted Iran's Natanz nuclear facility. Stuxnet, first discovered in 2010, was a highly sophisticated worm designed

to sabotage industrial control systems by altering the speed of centrifuges used for uranium enrichment. Despite the facility being air-gapped, Stuxnet infiltrated the system via infected USB drives, which were likely introduced by unwitting employees or supply chain contamination (Yirka, 2024). This attack proved that physical isolation is not sufficient when human factors and removable media can serve as vectors for malware introduction.

V. Mitigation Strategies and Defenses

Despite the increasing sophistication of attacks on air-gapped systems, defensive strategies continue to evolve to counteract emerging threats. Given that traditional network security measures are ineffective in fully isolated environments, mitigation efforts must focus on preventing unauthorized data infiltration, detecting covert exfiltration channels, and minimizing exploitable emissions. Air-gapping alone is no longer enough—effective security requires a multi-layered approach that accounts for physical, electromagnetic, optical, and acoustic vulnerabilities.

The first line of defense for any air-gapped system is to prevent unauthorized data entry. One of the most well-documented breaches, Stuxnet, was introduced through infected USB drives, demonstrating how supply chain security and physical access control remain critical (Yirka, 2024). To combat this, organizations must enforce strict removable media policies, including hardware-enforced USB blocking, digital signing of all external media, and isolated scanning stations for verifying files before introduction. Additionally, data diodes—unidirectional data transfer mechanisms—can help prevent unauthorized bidirectional communication while allowing necessary updates in a controlled manner.

While malware introduction is a primary concern, the covert exfiltration of data is an even greater threat. Attacks such as USBee (Guri et al., 2016) and POWER-SUPPLaY (Guri, 2020) exploit electromagnetic emissions and power fluctuations to transmit data outside of the air-gapped system. To counteract this, security teams must implement TEMPEST shielding, which involves physical and electronic barriers that contain electromagnetic leakage. Additionally, randomized power consumption patterns and intelligent anomaly detection systems can help identify suspicious fluctuations that may indicate covert exfiltration attempts.

Physical emissions, such as sound and light, present another significant avenue for attacks. Techniques like DiskFiltration (Guri et al., 2018) use hard drive noises to transmit data, while Glowworm (Nassi et al., 2021) can reconstruct audio by analyzing LED fluctuations. To mitigate these risks, organizations must employ acoustic dampening measures, such as white noise generators, and disable unused speakers or microphones in secured areas. Optical countermeasures, including LED shielding and randomized flickering of indicator lights, can disrupt visual exfiltration channels.

A more proactive approach involves continuous monitoring for anomalous emissions in electromagnetic, acoustic, and optical spectrums. By deploying intrusion detection systems (IDS) specifically designed for non-traditional attack vectors, security teams can establish a baseline of normal emissions and detect deviations that may indicate an active side-channel attack. Physical security measures, such as Faraday cages and ultrasonic jammers, add another layer of defense by actively interfering with unauthorized transmission methods.

A. Air-Gap Integrity Testing

After vulnerabilities are detected through air-gap integrity testing, organizations must implement defensive measures and revalidate their effectiveness. We propose these countermeasures:

- Shielding hardware against electromagnetic leakage using TEMPEST-rated enclosures
- Deploying noise generators and randomized LED flickering to disrupt covert optical and acoustic transmissions
- Restricting removable media access and ensuring strict file integrity monitoring
- Implementing anomaly detection systems that continuously monitor power consumption, sound emissions, and unexpected hardware behavior

Following the deployment of these countermeasures, a secondary round of penetration testing and emissions analysis should be conducted to confirm that mitigation efforts have successfully blocked all previously detected leaks.

VI. Future Scope and Evolving Techniques

Machine learning and artificial intelligence (AI) are revolutionizing cyberattack methodologies, enabling automated reconnaissance, side-channel analysis, and adaptive evasion techniques. AI-driven attacks can analyze power consumption fluctuations, acoustic signals, and subtle variations in LED brightness more efficiently than human adversaries. Automated pattern recognition in electromagnetic and optical emissions could make existing air-gap exfiltration techniques significantly more precise and difficult to detect. Deep-learning-powered malware could autonomously identify weaknesses in air-gapped environments and refine exfiltration strategies in real-time (Yirka, 2024).

While quantum computing primarily threatens cryptographic security, it also introduces new risks for air-gapped systems. Quantum techniques may enhance side-channel attacks, allowing adversaries to model and reconstruct cryptographic keys by analyzing power fluctuations, electromagnetic emissions, or CPU timing patterns at a level of detail previously unattainable (Guri, 2020). Moreover, the potential for quantum-assisted signal decoding could improve covert exfiltration techniques that leverage acoustic or optical signals.

Modern industrial and military environments increasingly incorporate the Internet of Things (IoT) and cyber-physical systems (CPS) that interface with air-gapped networks. These systems often include wireless-capable sensors, embedded processors, and machine-learning algorithms that create new attack vectors. Compromised IoT devices within proximity of an air-gapped system could serve as bridge points for electromagnetic, power-based, or acoustic covert channels.

Furthermore, AI-powered CPS systems could be tricked into manipulating actuators, sensors, or physical processes in ways that leak sensitive information or cause operational disruptions.

Other emerging countermeasures signal a shift from passive air-gapping to proactive defense strategies. Security measures must adapt dynamically as attacks evolve, integrating AI-driven detection, quantum-resistant shielding, active jamming, and enhanced physical isolation. The future of air-gap security will not rely solely on isolation but on continuous, adaptive, and intelligent defense mechanisms designed to disrupt any potential attack vector before it can be exploited.

A. Related Work

The security of critical infrastructures should expand to defend against more subtle and sophisticated attacks. Related works and other areas of research including resilience and recovery strategies, secure data transfer methods, and insider threats are well worth considering for society's essential systems.

Resilience and recovery strategies ensure the continuity of operations in critical sectors, not only limited to sectors that rely on air-gapped security, but grow to include society's core sectors like energy, healthcare, and even transportation. These sectors need to be resistant to attacks and be capable of recovering quickly after disruptions. As air-gapped devices are isolated from external networks, they could be prone to slow recovery. Usual methods of recovery stem from cloud-based support, which is off-limits because external access is restricted. Air-gapped systems need a more robust remote recovery system to prevent significant downtime. Because of this, air-gapped systems must be self-sufficient. Research into resilience and recovery strategies would supplement air-gapped recovery so that backup systems, disaster recovery plans, and system reboots can be executed within the isolated environment without relying on external resources.

Research into secure data transfer methods has also been highlighted in our work, but much research has yet to be done to improve one-way data transfer mechanisms. One-directional flow of data is a core part of air-gapped security as it allows information to be securely transferred into these systems without the risk of malware introduction or unauthorized data exfiltration of sensitive data. Other recent studies on quantum-resistant encryption and encrypted USB drives have emerged as a central focus on protecting static data as well as data in transit to prevent interceptions. Researchers have also proposed a method into blockchain-based solutions which are quickly gaining attention as a method to ensure data integrity by verifying data records.

However, research is not the only way to protect air-gapped systems. Active training on insider threats is often an overlooked risk that could prevent individuals with legitimate access from exploiting their privileges to intentionally sabotage system operations. Behavioral anomaly detection could spot suspicious activity deviations early on to identify risks. Additionally, techniques such as least-privilege access and multi-factor authentication have been emphasized as effective measures for limiting the scope of insider threats by restricting unnecessary access.

These approaches are particularly important in air-gapped environments and proactive measures are the key to insulate our most critical systems from external cyber-attacks.

VII. Conclusion

Air-gapped systems offer a golden standard of security by keeping critical infrastructure away from direct network threats, but they are not completely foolproof. We have explored and studied both real-world attacks and research cases of air-gapped security being breached. Attacks using electromagnetic and acoustic emissions show how physical separation is not enough to guarantee total security. Even considering the high cost of preparation and execution of such attacks, air-gapped systems usually protect highly confidential information and must be protected from all possible exploits. To effectively defend against these threats, we emphasise the need for a multi-layered strategy that includes strong physical security, electromagnetic shielding, anomaly detection, and controlled data transfer methods. As cyber threats keep evolving, it highlights how crucial it is to stay ahead with ongoing research, proactive security measures, and thorough testing of air-gap integrity to keep these systems resilient against new attack techniques.

Acknowledgment

The authors would like to express gratitude for those who supported the success of this project.

First and foremost, we would like to thank our professor, Dr. Geetha Thamilarasu for their expertise and feedback throughout our project. Their insights inspired our work and served as the core for our understanding of emerging topics in cybersecurity.

We would also like to acknowledge the support of the Computer Science and Software Engineering Department at the University of Washington Bothell, for providing us with the resources and environment necessary for completing this project.

And lastly, a special thanks to our peers and fellow students in the CSSE program for their collaboration, discussions, and shared knowledge.

Thank you all for your contributions to this project.

References

[1] Liu, X., Zhang, S. (2022). A novel neural network-based method for power system state estimation. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9808153

[2] Wang, Y., Zhang, X. (2018). A deep learning approach to power system fault detection. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8282701

[3] Guri, et al. "USBee: A Covert Channel from Electromagnetic Emissions of USB Devices." arxiv.org, 2016, https://arxiv.org/pdf/1608.08397

[4] Zhang, Y., He, H. (2021). Optimization of smart grid operation using machine learning techniques. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/9311995

[5] Wu, J., Zhang, Q. (2023). An adaptive algorithm for real-time control in power distribution systems. IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/10580382

[6] Guri, Mordechai. ”POWER-SUPPLaY: A New Power-Based Side-Channel Attack on Cryptographic Devices.” eprint.iacr.org, 2020, https://eprint.iacr.org/2020/516.pdf

[7] Yirka, B. (2024, September 10). Usable data hacked from air-gapped computer. TechXplore. https://techxplore.com/news/2024-09-usable-hacked-air-gapped.html

[8] Nassi et .al. ”Glowworm: Recovering Sound from Optical Emanations of Power Indicator LEDs.” eprint.iacr.org, 2021, https://eprint.iacr.org/2021/1064.pdf b9 Guri, et al. ”DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise.” databorder.com, 2018, https://arxiv.org/pdf/1608.03431

[9] Detection of cyber-attacks on smart grids using improved VGG19 deep neural network architecture and Aquila optimizer algorithm Ahmed Mhmood, Özgür Ergül, Javad Rahebi Signal, Image and Video Processing https://doi.org/10.1007/s11760-023-02813-7

[10] M. Guri, ”Air-Gap Electromagnetic Covert Channel,” in IEEE Transactions on Dependable and Secure Computing, vol. 21, no. 4, pp. 2127-2144, July-Aug. 2024, doi: 10.1109/TDSC.2023.3300035. https://ieeexplore.ieee.org/document/10197447