# Bibliography: The Myth of the Air Gap

## Primary Academic Sources

### Peer-Reviewed Journal Articles


Carrara, B., & Adams, C. (2023). "A Survey on Air-Gap Attacks: Fundamentals, Transport Means, Attack Scenarios and Challenges." *Sensors*, 23(6), 3215. MDPI. https://www.mdpi.com/1424-8220/23/6/3215

Guri, M. (2024). "RAMBO: Leaking Secrets from Air-Gap Computers by Spelling Covert Radio Signals from Computer RAM." *arXiv preprint* arXiv:2409.02292. https://arxiv.org/abs/2409.02292

Guri, M. (2024). "SmartAttack: Air-Gap Attack via Smartwatches." *arXiv preprint* arXiv:2506.08866. https://arxiv.org/abs/2506.08866

Guri, M. (2023). "Air-Gap Electromagnetic Covert Channel." *IEEE Transactions on Dependable and Secure Computing*, 20(5), 4199-4213. https://ieeexplore.ieee.org/document/10197447/

Guri, M. (2022). "SATAn: Air-Gap Exfiltration Attack via Radio Signals From SATA Cables." *arXiv preprint* arXiv:2207.07413. https://arxiv.org/abs/2207.07413

Guri, M. (2021). "Exfiltrating data from air-gapped computers via ViBrAtIoNs." *Future Generation Computer Systems*, 122, 69-81. https://www.sciencedirect.com/science/article/abs/pii/S0167739X21001151

Guri, M. (2020). "AIR-FI: Generating Covert Wi-Fi Signals from Air-Gapped Computers." *arXiv preprint* arXiv:2012.06884. https://arxiv.org/abs/2012.06884

Guri, M. (2020). "Fansmitter: Acoustic data exfiltration from air-Gapped computers via fans noise." *Computers & Security*, 91, 101736. https://www.sciencedirect.com/science/article/abs/pii/S0167404820300080

Guri, M. (2019). "Optical air-gap exfiltration attack via invisible images." *Journal of Information Security and Applications*, 46, 222-230. https://www.sciencedirect.com/science/article/abs/pii/S2214212618304381

Guri, M. (2018). "PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines." *arXiv preprint* arXiv:1804.04014. https://arxiv.org/abs/1804.04014

Guri, M. (2018). "Bridgeware: The Air-Gap Malware." *Communications of the ACM*, 61(4), 74-82. https://m-cacm.acm.org/magazines/2018/4/226377-bridgeware/fulltext

Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., & Elovici, Y. (2014). "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies." *2014 9th International*

*Conference on Malicious and Unwanted Software*, 58-67. IEEE. https://ieeexplore.ieee.org/document/6999418/

Henríquez Santiago, F.J., Lyshyn, A., et al. (2024). "Deep-TEMPEST: Using Deep Learning to Eavesdrop on HDMI from its Unintended Electromagnetic Emanations." *arXiv preprint* arXiv:2407.09717. https://arxiv.org/abs/2407.09717

Li, L., & Wang, X. (2024). "PowerBridge: Covert Air-Gap Exfiltration/Infiltration via Smart Plug." *Applied Sciences*, 14(14), 6321. MDPI. https://www.mdpi.com/2076-3417/14/14/6321

Rodríguez, S., et al. (2025). "Securing air-gapped systems-review of covert techniques for data ex-filtration and a new clause proposal for ISO 27001." *International Journal of Information Security*, 24(1). Springer. https://link.springer.com/article/10.1007/s10207-025-01103-2

Singh, H., et al. (2024). "Protecting Data at Risk of Unintentional Electromagnetic Emanation: TEMPEST Profiling." ResearchGate. https://www.researchgate.net/publication/381132118

Zou, Y., & Wang, G. (2018). "MOSQUITO Attack Allows Air-Gapped Computers to Covertly Exchange Data." *2018 IEEE Symposium on Security and Privacy*. IEEE.

## Historical Case Studies and Incident Reports

### Stuxnet

Kaspersky Lab. (2024). "Stuxnet Definition & Explanation." Kaspersky Resource Center. https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet

Kushner, D. (2013). "The Real Story of Stuxnet." *IEEE Spectrum*. https://spectrum.ieee.org/the-real-story-of-stuxnet

Langner, R. (2011). "Stuxnet: Dissecting a Cyberwarfare Weapon." *IEEE Security & Privacy*, 9(3), 49-51.

Malwarebytes. (2024). "Stuxnet | What is Stuxnet?" https://www.malwarebytes.com/stuxnet

Zetter, K. (2019). "Stuxnet explained: The first known cyberweapon." *CSO Online*. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

### Agent.BTZ

Kaspersky Lab. (2014). "Agent.btz: a Source of Inspiration?" Securelist. https://securelist.com/agent-btz-a-source-of-inspiration/58551/

Kaspersky Lab. (2014). "How Turla and 'worst breach of U.S. military computers in history' are connected." https://www.kaspersky.com/about/press-releases/how-turla-and-worst-breach-of-u-s-military-computers-in-history-are-connected

Nakashima, E. (2010). "Defense official discloses cyberattack." *The Washington Post*.

We Are The Mighty. (2024). "The worst cyber attack in DoD history came from a USB drive found in a parking lot." https://www.wearethemighty.com/mighty-history/worst-cyber-attack-usb/

Wikipedia. (2024). "2008 malware infection of the United States Department of Defense." https://en.wikipedia.org/wiki/2008_malware_infection_of_the_United_States_Department_of_Defense

### ProjectSauron

Kaspersky Lab. (2016). "ProjectSauron: Top Level Espionage Platform Covertly Extracts Encrypted Government Comms." https://www.kaspersky.com/about/press-releases/projectsauron-top-level-espionage-platform-covertly-extracts-encrypted-government-comms

### Other Nation-State Operations

ESET Research. (2021). "Jumping the air gap: 15 years of nation-state effort." We Live Security. https://www.welivesecurity.com/2021/12/01/jumping-air-gap-15-years-nation-state-effort/

Volexity. (2024). "The Nearest Neighbor Attack: How A Russian APT Weaponized Nearby Wi-Fi Networks for Covert Access." https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/

## Industry Reports and Analysis

### Security Vendor Reports

Darktrace. (2024). "Securing OT Systems: The Limits of the Air Gap Approach." https://www.darktrace.com/blog/why-the-air-gap-is-not-enough

DataCore. (2024). "The Role of Air Gaps in Cyber Resilience." DataCore Software. https://www.datacore.com/blog/the-role-of-air-gaps-in-cyber-resilience/

F5 Networks. (2024). "Attacking Air-Gap-Segregated Computers." F5 Labs. https://www.f5.com/labs/articles/cisotociso/attacking-air-gap-segregated-computers

IBM. (2024). "What is an Air Gap?" IBM Think. https://www.ibm.com/think/topics/air-gap

IBM. (2024). "83% of organizations reported insider attacks in 2024." https://www.ibm.com/think/insights/83-percent-organizations-reported-insider-threats-2024

Microsoft Security. (2017). "Mind the air gap: Network separation's cost, productivity, and security drawbacks." Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/2017/05/01/mind-the-air-gap-network-separations-cost-productivity-and-security-drawbacks/

Silverfort. (2024). "What is an Air-Gapped Network?" Silverfort Glossary. https://www.silverfort.com/glossary/an-air-gapped-network/

### Industry Standards and Best Practices

Cloudflare. (2024). "Zero Trust security | What is a Zero Trust network?" https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/

Cloudflare. (2024). "What is defense in depth? | Layered security." https://www.cloudflare.com/learning/security/glossary/what-is-defense-in-depth/

ISA Global Cybersecurity Alliance. (2024). "The Air Gap: Myth and Reality." https://gca.isa.org/blog/the-air-gap-myth-and-reality

ISA Global Cybersecurity Alliance. (2024). "Common ICS Cybersecurity Myth #1: The Air Gap." https://gca.isa.org/blog/common-ics-cybersecurity-myth-1-the-air-gap

Open Access Government. (2018). "Securing industrial control systems by closing the air gap security loophole." https://www.openaccessgovernment.org/securing-industrial-control-systems/55043/

Veridify Security. (2024). "Zero Trust - A Virtual Air Gap for OT Security." https://www.veridify.com/zero-trust-a-virtual-air-gap-for-ot-security/

## Trade Publications and News Sources

CSO Online. (2024). "How to bridge and secure air gap networks." https://www.csoonline.com/article/550036/how-to-bridge-and-secure-air-gap-networks.html

Dark Reading. (2024). "Fancy Bear 'Nearest Neighbor' Attack Uses Nearby Wi-Fi Network." https://www.darkreading.com/cyberattacks-data-breaches/fancy-bear-nearest-neighbor-attack-wi-fi

Dark Reading. (2024). "USB Devices the Common Denominator in All Attacks on Air-Gapped Systems." https://www.darkreading.com/cyberattacks-data-breaches/usb-devices-common-denominator-in-all-attacks-on-air-gapped-systemsd

Energy Central. (2024). "Beating the Air-Gap: How Attackers Can Gain Access to Supposedly Isolated Systems." https://energycentral.com/c/iu/beating-air-gap-how-attackers-can-gain-access-supposedly-isolated-systems

Hackaday. (2020). "GPU Turned Into Radio Transmitter To Defeat Air-Gapped PC." https://hackaday.com/2020/04/24/gpu-turned-into-radio-transmitter-to-defeat-air-gapped-pc/

MixMode. (2024). "Air-Gapped Systems Breached: A Deep Dive into the Attack and Prevention." https://mixmode.ai/blog/air-gapped-systems-breached-a-deep-dive-into-the-attack-and-prevention/

PortSwigger. (2020). "'Air-Fi' attack renders air-gapped computers open to data exfiltration through WiFi signals." The Daily Swig. https://portswigger.net/daily-swig/air-fi-attack-renders-air-gapped-computers-open-to-data-exfiltration-through-wifi-signals

SecurityWeek. (2024). "Hackers Can Stealthily Exfiltrate Data via Power Lines." https://www.securityweek.com/hackers-can-stealthily-exfiltrate-data-power-lines/

SecurityWeek. (2024). "Ethernet LEDs Can Be Used to Exfiltrate Data From Air-Gapped Systems." https://www.securityweek.com/ethernet-leds-can-be-used-exfiltrate-data-air-gapped-systems/

TechRadar. (2024). "The threats of USB-based attacks for critical infrastructure." https://www.techradar.com/pro/the-threats-of-usb-based-attacks-for-critical-infrastructure

The Hacker News. (2022). "New Air-Gap Attack Uses MEMS Gyroscope Ultrasonic Covert Channel to Leak Data." https://thehackernews.com/2022/08/new-air-gap-attack-uses-mems-gyroscope.html

The Hacker News. (2018). "MOSQUITO Attack Allows Air-Gapped Computers to Covertly Exchange Data." https://thehackernews.com/2018/03/air-gap-computer-hacking.html

The Hacker News. (2018). "Hacker Can Steal Data from Air-Gapped Computers through Power Lines." https://thehackernews.com/2018/04/hacking-airgap-computers.html

The Intercept. (2019). "Everybody Does It: The Messy Truth About Infiltrating Computer Supply Chains." https://theintercept.com/2019/01/24/computer-supply-chain-attacks/

The Register. (2013). "Hear that? It's the sound of BadBIOS wannabe chatting over air gaps." https://www.theregister.com/2013/12/05/airgap_chatting_malware/

Threatpost. (2020). "Air-Gap Attack Turns Memory Modules into Wi-Fi Radios." https://threatpost.com/air-gap-attack-turns-memory-wifi/162358/

Tom's Hardware. (2024). "University researchers tout using smartwatches to steal data from air-gapped systems." https://www.tomshardware.com/tech-industry/cyber-security/university-researchers-tout-using-smartwatches-to-steal-data-from-air-gapped-systems-smartattack-paper-proposes-using-wearable-as-a-covert-ultrasonic-signal-receiver

## Statistical Sources and Threat Intelligence

Cyware. (2022). "New Air-Gap Attack Uses MEMS Gyroscope Ultrasonic Covert Channel to Leak Data." Cyware Alerts. https://cyware.com/news/new-air-gap-attack-uses-mems-gyroscope-ultrasonic-covert-channel-to-leak-data-675eca58/

Eftsure. (2024). "Insider Threat Statistics: Malicious Intent or Ignorance?" https://www.eftsure.com/statistics/insider-threat-statistics/

Google Cloud. (2024). "The Spies Who Loved You: Infected USB Drives to Steal Secrets." Mandiant Blog. https://cloud.google.com/blog/topics/threat-intelligence/infected-usb-steal-secrets/

Scadafence. (2024). "The Stuxnet Worm: A USB-based Attack with Major Consequences." https://blog.scadafence.com/usb-borne-threats-ot-environments

StationX. (2025). "Insider Threat Statistics: (2025's Most Shocking Trends)." https://www.stationx.net/insider-threat-statistics/

Syteca. (2025). "Insider Threat Statistics for 2025: Facts, Reports & Costs." https://www.syteca.com/en/blog/insider-threat-statistics-facts-and-figures

## Research Resources and Databases

Ben-Gurion University Cyber Security Research Center. "Air Gap Research Page." https://cyber.bgu.ac.il/air-gap/

CovertChannels.com. "Home | Air Gap Research Page." https://www.covertchannels.com

GitHub. "Best Papers in Computer Security." https://github.com/prncoprs/best-papers-in-computer-security

GitHub. "Awesome ML Security Papers." https://github.com/gnipping/Awesome-ML-SP-Papers

Google Scholar. "Mordechai Guri." https://scholar.google.com/citations?user=F8gvBUkAAAAJ&hl=en

ResearchGate. "Mordechai Guri's research works." https://www.researchgate.net/scientific-contributions/Mordechai-Guri-2055581535

## Reference Works

ScienceDirect. "Stuxnet - an overview." ScienceDirect Topics. https://www.sciencedirect.com/topics/computer-science/stuxnet

Wikipedia. "Air gap (networking)." https://en.wikipedia.org/wiki/Air_gap_(networking)

Wikipedia. "Agent.BTZ." https://en.wikipedia.org/wiki/Agent.BTZ

Wikipedia. "Stuxnet." https://en.wikipedia.org/wiki/Stuxnet

Wikipedia. "Supply chain attack." https://en.wikipedia.org/wiki/Supply_chain_attack

Wikipedia. "Tempest (codename)." https://en.wikipedia.org/wiki/Tempest_(codename)

---

*Note: All URLs were accessed and verified during the research phase of this paper (August 2025). Given the dynamic nature of web content, some links may change or become unavailable over time.*