TECHNICAL PAPER

ULTRASONIC DATA TRANSFER: Covert Communication Channels Across Air-Gapped Networks

How audio peripherals can be exploited to transfer data between isolated systems—and how hardware-based protection can prevent it.

HighSecLabs
Highest Security Solutions

HLT40008 Rev 1.0

TABLE OF CONTACTS

Introduction 3

How Ultrasonic Data Transfer Works 4

Ultrasonic Communication as a Cybersecurity Threat 5

Practical Demonstration 7
- Ultrasonic Data Transfer Demonstrator: 7

Preventing Ultrasonic Data Leakage with HSL Secure Media Diodes 8
- Low-Pass Filtering 8
- Unidirectional Audio Flow 9

Conclusion 10

References 11

INTRODUCTION

Air-gapped networks are designed to protect sensitive information by physically isolating computers from external networks and communication channels. However, physical network isolation does not necessarily guarantee complete information isolation.

Research has demonstrated that computers equipped with speakers and microphones can exchange information through acoustic signals, including frequencies that are difficult or impossible for humans to hear. By exploiting these audio peripherals, attackers can establish covert communication channels between otherwise disconnected devices.

This technique, known as **ultrasonic data transmission**, creates a potential bridge across air-gapped environments, allowing sensitive information to be transferred without conventional network connectivity.

HOW ULTRASONIC DATA TRANSFER WORKS

Digital information is fundamentally represented as binary data: sequences of zeros and ones. These sequences can be converted into acoustic signals by encoding binary values into specific audio frequencies.

A transmitting device uses its speaker to generate sound waves representing the encoded data. A receiving device captures these signals through its microphone and processes them to reconstruct the original binary information.

One possible encoding technique is Frequency-Shift Keying (FSK), in which two different frequencies represent binary 0 and 1. The receiver identifies the transmitted frequencies and converts them back into digital data.

When frequencies above or near the upper limit of human hearing are used, the communication can take place without producing sounds that are readily noticeable to people nearby.

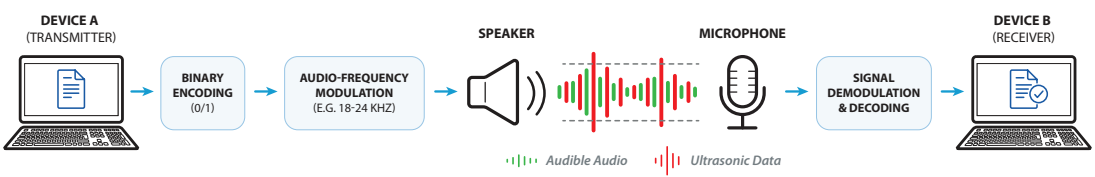

Figure 1. Ultrasonic data transmission

The feasibility of this technique has been demonstrated in academic research. In particular, the MOSQUITO research by Guri et al. demonstrated speaker-to-speaker communication between air-gapped computers, including scenarios where dedicated microphones were unavailable. The researchers investigated near-ultrasonic frequencies in the 18–24 kHz range.

ULTRASONIC COMMUNICATION AS A CYBERSECURITY THREAT

The same technology that enables legitimate data exchange can be exploited to bypass conventional network isolation.

An attacker who successfully compromises an air-gapped computer may be able to use its audio hardware to transmit sensitive information through high-frequency acoustic signals. A nearby device equipped with a microphone can receive and decode these signals, potentially transferring the recovered information to an external network.

Importantly, this attack does not require a physical network connection between the transmitting and receiving computers. The acoustic channel effectively creates an alternative communication path through the surrounding environment.

The potential attack scenario involves:

- **Compromised source:** Malware gains access to sensitive information on an isolated computer.
- **Data encoding:** The information is converted into binary sequences and modulated into high-frequency audio signals.
- **Acoustic transmission:** The computer's speaker broadcasts the encoded information.
- **Signal reception:** A nearby microphone captures the acoustic transmission.
- **Data extraction:** The receiving device decodes the signal and reconstructs the transmitted information.

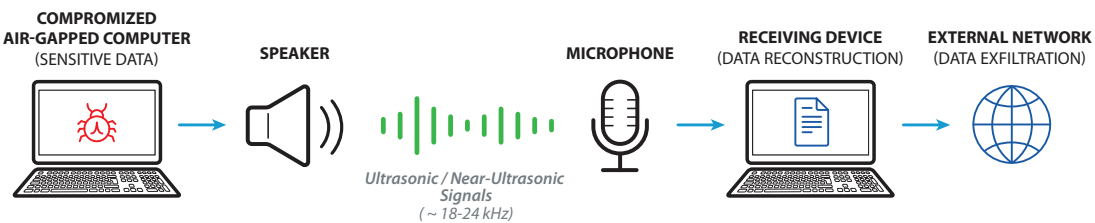

Figure 2. Acoustic data exfiltration from an air-gapped computer

The implications extend beyond conventional speaker-to-microphone communication. Research has also demonstrated that, under certain hardware and audio-chip conditions, passive speakers and headphones can be repurposed as input devices, effectively allowing two computers to communicate using speakers alone.

PRACTICAL DEMONSTRATION

The following web application demonstrates how digital information can be transferred acoustically using ultrasonic signals:

ULTRASONIC DATA TRANSFER DEMONSTRATOR:

https://veto-place-54839978.figma.site/](https://veto-place-54839978.figma.site/

The demonstration illustrates the underlying principle: converting digital information into acoustic signals, transmitting them through audio hardware, and reconstructing the original information at the receiving end.

It highlights how an alternative communication channel can exist between devices even when conventional network connectivity is unavailable.

PREVENTING ULTRASONIC DATA LEAKAGE WITH HSL SECURE MEDIA DIODES

Preventing acoustic data leakage requires controlling the physical signal paths between computers and their connected media peripherals.

High Sec Labs (HSL) Secure Media Diodes provide a hardware-based security barrier between host computers and audio peripherals, including speakers, headphones, and microphones.

Two key mechanisms help mitigate the threat:

LOW-PASS FILTERING

All audio signals passing through HSL Media Diodes are processed by an integrated low-pass filter. The filter restricts the audio frequency range to frequencies compatible with human hearing, attenuating high-frequency signals used for ultrasonic data transmission.

By preventing high-frequency data signals from passing through the audio connection to the speaker, the Media Diode mitigates the use of connected audio peripherals as a covert data-exfiltration channel.

UNIDIRECTIONAL AUDIO FLOW

HSL Media Diodes also enforce unidirectional audio flow from the host computer to the connected media device. This prevents reverse audio transmission from the peripheral back to the host, mitigating attacks that exploit speakers or headphones as makeshift microphones.

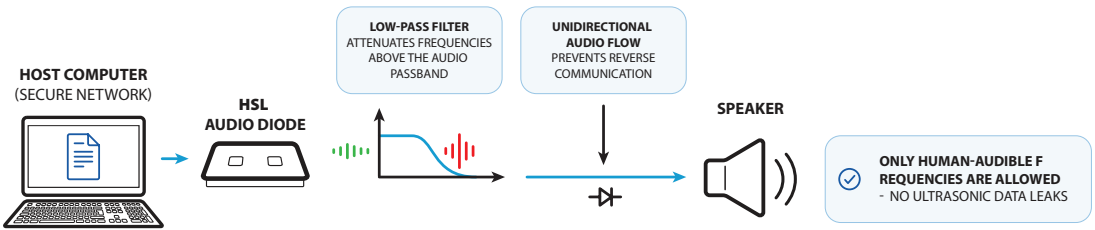

Figure 3. HSL Secure Media Diode protection

Together, these hardware-enforced mechanisms address both high-frequency acoustic transmission and the exploitation of audio peripherals as input devices.

CONCLUSION

Ultrasonic data transmission demonstrates that physical network isolation alone may not be sufficient to prevent information leakage. By exploiting audio peripherals and high-frequency acoustic signals, compromised computers can potentially communicate across air-gapped environments without conventional network connections.

HSL Secure Media Diodes address this overlooked attack vector by enforcing physical control over audio signal paths. Their integrated low-pass filtering attenuates high-frequency transmissions, while unidirectional audio flow prevents reverse communication through connected peripherals.

Because securing isolated networks requires more than disconnecting network cables. It requires controlling every potential communication path.

REFERENCES

[1] Guri, M., Solewicz, Y., & Elovici, Y. (2020). *Speaker-to-speaker covert ultrasonic communication*. Journal of Information Security and Applications, 51, 102458. https://doi.org/10.1016/j.jisa.2020.102458

[2] Guri, M., Solewicz, Y., Daidakulov, A., & Elovici, Y. (2018). *MOSQUITO: Covert Ultrasonic Transmissions between Two Air-Gapped Computers Using Speaker-to-Speaker Communication*. IEEE Conference on Dependable and Secure Computing. https://doi.org/10.1109/DESEC.2018.8625124

[3] Hanspach, M., & Goetz, M. (2013). *On Covert Acoustical Mesh Networks in Air*. Journal of Communications, 8(11), 758–767. https://doi.org/10.12720/jcm.8.11.758-767

[4] High Sec Labs. *The World's Most Secure Media Diodes: Prevent Data Leaks Through Media Peripherals

www.highseclabs.com

High Sec Labs (HSL) develops high-quality cyber-defense solutions in the field of network and peripheral isolation for protecting national assets and infrastructure.

The company, headquartered in Or Akiva, Israel, was founded in 2008 and has a second manufacturing site in the United States.

High Sec Lab's roots are deeply embedded in the defense and commercial industries developing cyber protection solutions. Among its customers are some of the world's leading governments and defense organizations as well as commercial companies such as banks, healthcare providers, and national infrastructure companies.

HighSecLabs
Highest Security Solutions

© 2026 HighSecLabs Ltd. All rights reserved. All trade names are trademarks or registered trademarks of respective manufacturers listed.
Specifications are subjected to change without prior notice. Patents: www.highseclabs.com/patents/. HLT40008 Rev 1.0