DiskFiltration: Data Exfiltration from Speakerless Air-gapped Computers via Covert Hard Drive Noise

Goals

Air-gapped computers are disconnected from the Internet physically and logically. This measure is taken in order to prevent the leakage of sensitive data from secured networks. It has been shown that malware can exfiltrate data from air-gapped computers by transmitting ultrasonic signals via the computer's speakers. However, such acoustic communication relies on the availability of speakers on a computer.

We present 'DiskFiltration,' a covert channel which facilitates the leakage of data from an air-gapped compute via acoustic signals emitted from its hard disk drive (HDD).

Description

Our 'DiskFiltration' method is unique in that, unlike other acoustic covert channels, it doesn't require the presence of speakers or audio hardware in the air-gapped computer. A malware installed on a compromised machine can generate acoustic emissions at specific audio frequencies by controlling the movements of the HDD's actuator arm. Digital information can be modulated over the acoustic signals and then be picked up by a nearby receiver (e.g., smartphone, smartwatch, laptop, etc.). We examine the HDD anatomy and analyze its acoustical characteristics. We also present signal generation and detection, and data modulation and demodulation algorithms. Based on our proposed method, we developed a transmitter on a personal computer and a receiver on a smartphone. We also evaluated our covert channel on various types of internal and external HDDs in different computer chassis and at various distances. With 'DiskFiltration' we were able to covertly transmit data (e.g., passwords, encryption keys, and keylogging data) between air-gapped computers to a smartphone at an effective bit rate of 180 bits/minute (10,800 bits/hour) and a distance of up to two meters (six feet).

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Dr. Yosef Solewicz
yosef.solewicz@gmail.com

Andrey Daidakulov
daidakul@post.bgu.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M, Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise," 2016. arXiv:1608.03431.

Demo Video

https://www.youtube.com/watch?v=H7lQXmSLiP8