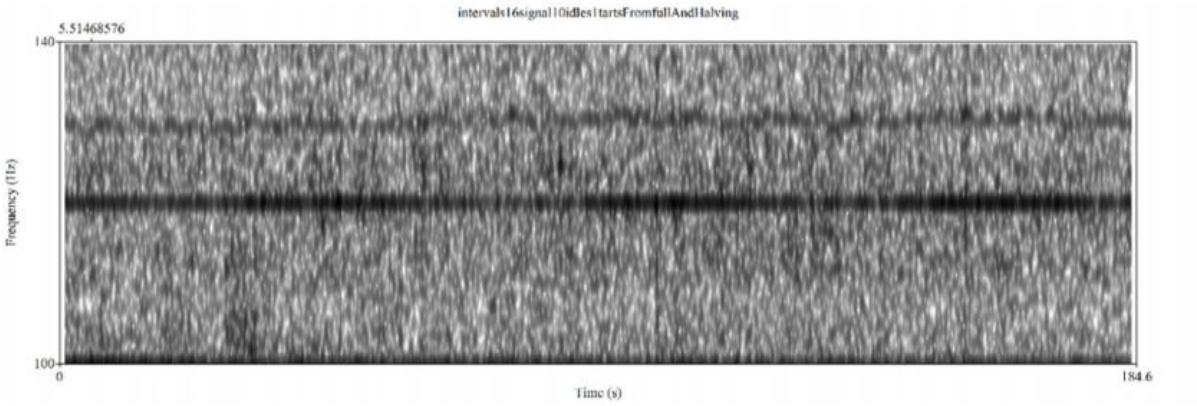
# Disk drive trick allows hackers to transmit data covertly from an air-gap computer

August 15 2016, by Bob Yirka




Spectrogram of idle acoustic noise generated by a HDD with an RPM of 7200. Credit: arXiv:1608.03431 [cs.CR]

(Tech Xplore)—A small team of researchers at Ben-Gurion University in Israel has found a way to hack an air-gap computer using the sounds made by a hard drive actuator. They describe the technique and possible ways it might be used in a paper they have uploaded to the preprint server *arXiv*.

One way to keep hackers from stealing data from your computer is to unplug it from the Internet and to disable its WiFi, Bluetooth and speakers—creating an air gap between it and all other computer

devices—at least according to conventional thinking. But now the team in Israel has shown even that may not be enough because they have found a way that hackers can read information off your computer then broadcast it using the noises your computer hard drive makes as it reads and writes information.

The idea works like this; a hacker somehow manages to install a small bit of malware onto your supposedly secure computer—that code reads data from the computer, i.e. the hard drive, keystrokes as a user types in a password or information it finds in memory, etc., and then uses a special algorithm to convert that message into a sound signal by manipulating the actuator used by the hard drive to move the head to different parts of the drive below it. That sound signal can then be picked up by any smart electronic device, such as a phone, and decoded revealing the data sent from the computer. The researchers offer proof in the form of a video they have uploaded to YouTube.

The method does have its limitations, of course, the sound produced by an actuator is pretty soft, so much so that a reader would have to be no more than six feet away and it has an extremely slow transmission rate—approximately 180 bits per minute (it would take approximately 25 minutes to transmit a 4,096-bit encryption key, for example) which would make it impractical for larger files. Still the researchers suggest there are some applications where their technique would be useful—in the world of spies and government covert operations, it is assumed.

**More information:** DiskFiltration: Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard Drive Noise, arXiv:1608.03431 [cs.CR] arxiv.org/abs/1608.03431

**Abstract**
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. In the past, 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. In this paper, 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). Our 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, and we provide the design and implementation details. We also evaluate 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).