Fansmitter: Acoustic Data Exfiltration from (Speakerless) Air-gapped Computers

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, "Fansmitter: Acoustic Data Exfiltration from [Speakerless] Air-Gapped Computers," 2016. arXiv:1606.05915.

Demo video

https://www.youtube.com/watch?v=v2_sZIfZkDQ

Goals

Because computers may contain or interact with sensitive information, they are often air-gapped and thus kept isolated and disconnected from the Internet. In recent years the ability of malware to communicate over an air-gap by transmitting sonic and ultrasonic signals from a computer speaker to a nearby receiver has been demonstrated. In order to eliminate such acoustic channels, current best practice recommends the elimination of speakers (internal or external) in secure computers, thereby creating a so-called 'audio-gap.' In this paper, we present 'Fansmitter,' a malware that can acoustically exfiltrate data from air-gapped computers, even when audio hardware and speakers are not present.

Description

The 'Fansmitter' method utilizes the noise emitted from the CPU and chassis fans, which are present in virtually every computer. We show that a software can regulate the internal fans' speed in order to control the acoustic waveform emitted from the computer. Binary data can be modulated and transmitted over these audio signals to a remote microphone (e.g., on a nearby mobile phone). We present Fansmitter's design considerations, including acoustic signature analysis, data modulation, and data transmission. We also evaluate the acoustic channel, present our results, and discuss countermeasures.

Using our method we successfully transmitted data from an air-gapped computer without audio hardware to a smartphone receiver in the same room. We demonstrated the effective transmission of encryption keys and passwords from a distance of zero to eight meters, with bit rate of up to 900 bits/hour. We also demonstrated that our method can be used to leak data from different types of IT equipment, embedded systems, and IoT devices that have no audio hardware, but contain fans of various types and sizes.