Cyberattack can steal data via cooling fan vibrations

April 24 2020, by Peter Grad

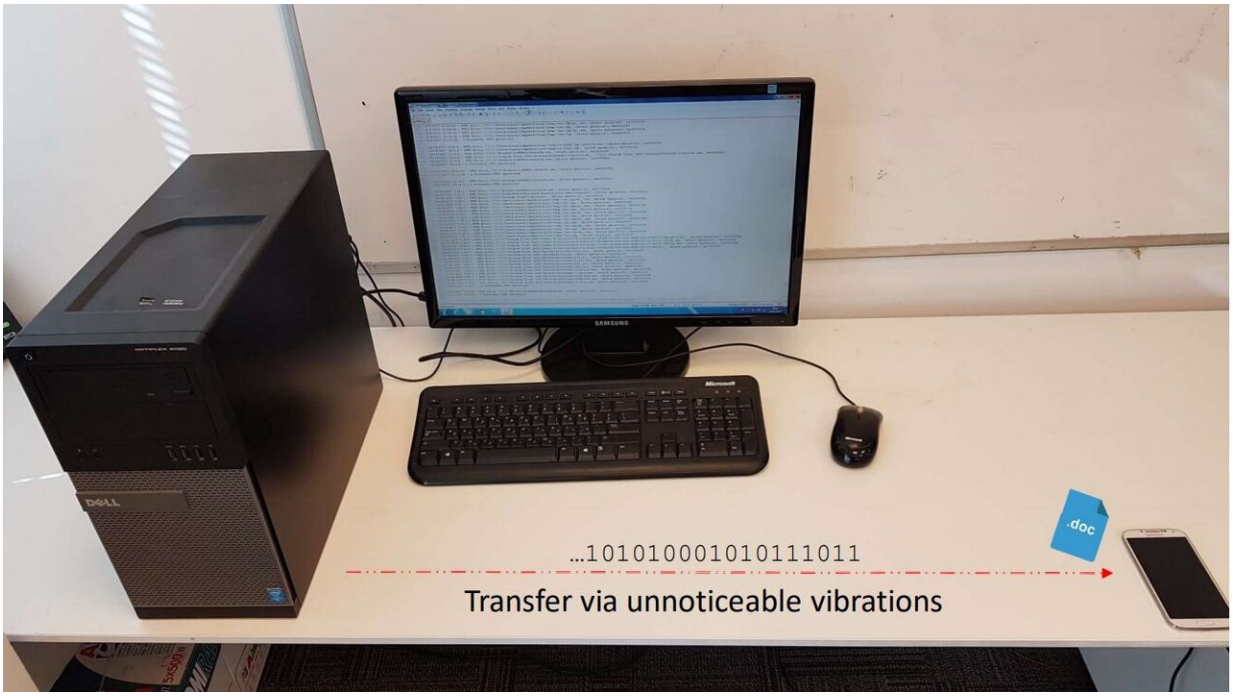

Illustration of the cover channel. The malware in the compromised computer transmits signals to the environment via vibrations induced on the table. A nearby infected smartphone detects the transmission, demodulates and decodes the data, and transfers it to the attacker via the Internet. Credit: arXiv:2004.06195 [cs.CR]

Israeli researchers uncovered a novel way that hackers could steal sensitive data from a highly secured computer: by tapping into the

vibrations from a cooling system fan.

Lead cyber-security researcher Mordechai Guri at Ben-Gurion University of the Negev said data encoded by hackers into fan vibrations could be transmitted to a smartphone placed in the vicinity of the targeted computer.

"We observe that computers vibrate at a frequency correlated to the rotation speed of their internal fans," Guri said. Malware can control computer vibrations by manipulating internal fan speeds, he explained. "These inaudible vibrations affect the entire structure on which the computer is placed."

The covertly transmitted vibrations can be picked up by a smartphone resting on the same surface as the computer.

Since accelerometer sensors in smartphones are unsecured, they "can be accessed by any app without requiring user permissions, which make this attack highly evasive," he said.

Guri demonstrated the process, named AiR-ViBeR, with an air-gapped computer setup. Air-gapped computer systems are isolated from unsecured networks and the internet as a security measure.

The research team said three measures would help secure a computer system against such an assault. One would be to run the CPU continuously at maximum power consumption mode, which would keep it from adjusting consumption. Another would be to set fan speeds for both CPU and GPU at a single, fixed rate. The third solution would be to restrict CPUs to a single clock speed.

The Ben-Gurion University cybersecurity team specializes in what are termed side-channel attacks. Rather than exploiting software or coding

vulnerabilities, side-channel attacks zero in on the manner in which a computer accesses hardware.

"This is the very essence of a side-channel attack," Guri said of AiR-ViBer. "The malware in question doesn't exfiltrate data by cracking encryption standards or breaking through a network firewall; instead, it encodes data in vibrations and transmits it to the accelerometer of a smartphone."

AiR-ViBer relied on vibration variances sensed by an accelerometer capable of detecting motion with a resolution of 0.0023956299 meters per square second. There are other means of capturing data through side channels. They include electromagnetic, magnetic, acoustic, optical and thermal.

In 2015, for instance, Guri's team introduced BitWhisper, a thermal covert channel that allowed a nearby computer to establish two-way communication with another computer by detecting and measuring changes in temperature.

A year earlier, his team demonstrated malware that extracts data from air-gapped computers to a nearby smartphone through FM signals emitted by the screen cable. He subsequently showed that he could exfiltrate data using cellular phone frequencies generated from buses connecting a computer's RAM and CPU.

More information: AiR-ViBeR: Exfiltrating Data from Air-Gapped Computers via Covert Surface ViBrAtIoNs, arXiv:2004.06195 [cs.CR] arxiv.org/abs/2004.06195v1

Air-Gap Research Page: cyber.bgu.ac.il/advanced-cyber/airgap

© 2020 Science X Network

Citation: Cyberattack can steal data via cooling fan vibrations (2020, April 24) retrieved 24 April 2024 from https://techxplore.com/news/2020-04-cyberattack-cooling-fan-vibrations.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.