BitWhisper: Covert Signaling Channel Between Air-gapped Computers Using Thermal Manipulations

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Matan Monitz
mmonitz@gmail.com

Yisroel Mirsky
yisroel@post.bgu.ac.il

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "BitWhisper: Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations," 2015. arXiv:1503.07919.

Demo video

https://www.youtube.com/watch?v=EWRk51oB-1Y&t=15s

Goals

It has been assumed that the physical separation (air-gap) of computers provides a reliable level of security, such that should two adjacent computers become compromised, the covert exchange of data between them would be impossible. In this paper, we demonstrate BitWhisper, a method of bridging the air-gap between adjacent compromised computers by using their heat emissions and built-in thermal sensors to create a covert communication channel.

Description

The BitWhisper method is unique in two respects: it supports bidirectional communication, and it requires no additional dedicated peripheral hardware. We provide experimental results based on implementation of a BitWhisper prototype, and examine the channel properties and limitations. Our experiments included different layouts, with computers positioned at varying distances from one another, and several sensor types and CPU configurations (e.g., virtual machines). Our discussion of signal modulation and communication protocols demonstrates how BitWhisper can be used for the exchange of data between two computers in a close proximity (at distance of 0-40 cm) at an effective rate of 1-8 bits per hour, a rate which makes it possible to infiltrate brief commands and exfiltrate small amount of data (e.g., passwords) over the covert channel.