VisiSploit: An Optical Covert-channel to Leak Data through an Air-gap

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Ofer Hasson
hassonofer@gmail.com

Gabi Kedma
gabikedma@hotmail.com

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "VisiSploit: An Optical Covert-Channel to Leak Data through an Air-Gap," 2016. arXiv:1607.03946.

Goals

In recent years, various out-of-band covert channels have been proposed that demonstrate the feasibility of leaking data out of computers without the need for network connectivity. The methods proposed have been based on different type of electromagnetic, acoustic, and thermal emissions. However, optical channels have largely been considered less covert: Because they are visible to the human eye and hence can be detected, they have received less attention from researchers.

We introduce VisiSploit, a new type of optical covert channel which, unlike other optical methods, is also stealthy.

Description

Our method exploits the limitations of human visual perception in order to unobtrusively leak data through a standard computer LCD display. Our experiments show that very low contrast or fast flickering images (which are invisible to human subjects) can be recovered from photos taken by a camera. Consequentially, we show that malicious code on a compromised computer can obtain sensitive data (e.g., images, encryption keys, passwords) and project it onto a computer LCD screen, invisible and unbeknownst to users, allowing an attacker to reconstruct the data using a photo taken by a nearby (possibly hidden) camera. In order to demonstrate the feasibility of this type of attack and evaluate the channel's stealth, we conducted a battery of tests with 40 human subjects. We also examined the channel's boundaries under various parameters, with different types of encoded objects, at several distances, and using several kinds of cameras. Our results show that binary data can be leaked via our covert channel. Further research and discussion may widen the scope of this field beyond its current boundaries, yielding novel attack paradigms that exploit the subtle mechanisms of human visual perception.