Information theft via manipulating screen brightness in air-gapped computers

February 8 2020, by Nancy Cohen

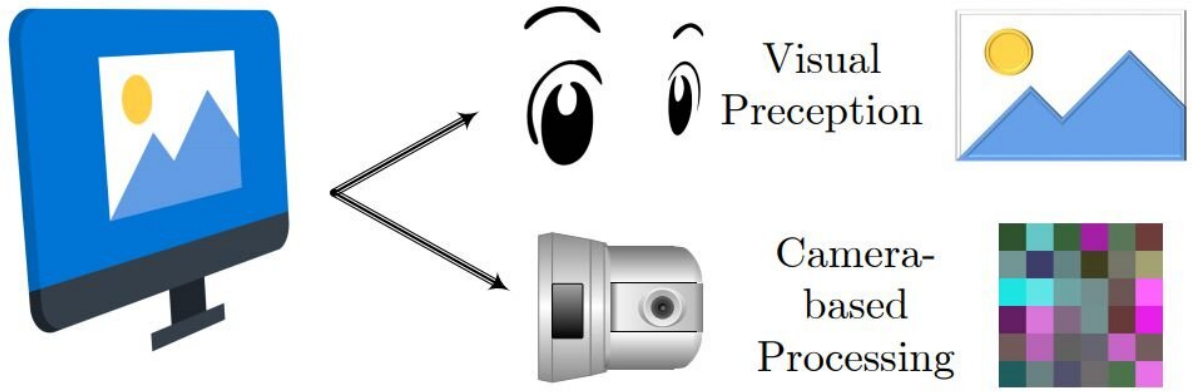

Illustration of covert D2C principle: the same frame on the screen has both high-quality visually perceptible image data and imperceptible covert message. Credit: arXiv:2002.01078 [cs.CR]

Data can be stolen from an air gapped personal computer just by using variations in screen brightness. Researchers at Ben-Gurion University wrote a paper on it.

As the team defines them, "Air-gapped computers are systems that are kept isolated from the Internet since they store or process sensitive information."

That they have come up with yet another discovery on how to wrest sensitive data from a computer came as no shock to Naked Security, which recognized that "Researchers at Ben-Gurion University of the Negev have made a name for themselves figuring out how to get data out of air-gapped computers. They've dreamed up ways to communicate using speakers, blinking LEDs in PCs, infrared lights in surveillance cameras, and even computer fans."

Graham Cluley writing in *Tripwire* reckoned, ok, "It may not be the most efficient way to steal data from an organisation, let alone the most practical, but researchers at Ben-Gurion University in Israel have once again detailed an imaginative way to exfiltrate information from an air-gapped computer."

Mordechai Guri, head of cybersecurity research center at Ben-Gurion University in Israel," talked about the process, Shane McGlaun in HotHardware had some details. The hack was possible via something called a "covert optical channel." It allowed data theft from air-gapped computers "without needing network connectivity or physically contacting the devices."

How so? Geek.com's Jordan Minor: "By infecting the target PC with the right malware, the monitor then subtly shifts the brightness of the LCD monitor."

The thief is recording the information communicated through those changes in brightness and can steal whatever sensitive data desired.

Mohit Kumar in *The Hacker News* referred to the fundamental idea behind encoding and decoding of data, where malware encodes the collected information as a stream of bytes and then modulate it as '1' and '0' signal. In this attack instance, the thief uses small changes in the LCD screen brightness to modulate binary information in patterns.

Matthew Humphries in PCMag also explained what the process was all about:

"Stealing data from the infected machine is achieved by encoding the information and transmitting it using the screen brightness changes in a sequential pattern, which is very similar to how Morse code works. The only other requirement for this to work is a camera pointed at the display which can either record or stream the pattern being transmitted. Once the pattern is received, it can be converted back into meaningful data."

The computer display in turn serves as a key tool.

The attacker can collect the data stream, said Kumar, "using video recording of the compromised computer's display, taken by a local surveillance camera, smartphone camera, or a webcam and can then reconstruct exfiltrated information using image processing techniques."

The researchers' paper is titled "BRIGHTNESS: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness," and the authors are Mordechai Guri, Dima Bykhovsky and Yuval Elovici. The paper is up on arXiv.

In their paper, they noted the optical covert channel was invisible— and could even work while the user was working on the computer. The ball is in the hacker's court. "The small changes in the brightness are invisible to humans but can be recovered from video streams taken by cameras such as a local security camera, smartphone camera or a webcam," they stated.

Yes, there are countermeasures and the authors proposed several.

Included in their countermeasure ideas were "organizational policies aimed to restrict the accessibility of sensitive computers" by placing

them in secured areas, and where only authorized staff were allowed to access them.

Any sort of cameras, said another, would be prohibited within the perimeter of certain restricted areas.

Another countermeasure took the form of a polarized film covering the screen. Although the user got a clear view, "humans and cameras at a distance" would view a darkened display.

Cyber Security Labs at Ben-Gurion University posted a video demo on Feb. 4. In this demo, the screen secretly exfiltrated the text of "Winnie-the-Pooh" by A.A. Milne.

The video sparked comments, such as, Why put all this out there?

"You are doing nothing but hurting others by making this information available," said one comment....You are doing a disservice to the security community and the public by posting content openly like this."

However, another comment pointed out that this was not a manufacturer issue, and "really isn't something that can just be patched. This is using a normal function, screen brightness. Locking down any application's ability to adjust the screen brightness would do more harm than good."

Another comment came to the research team's defense. "It's important to bring this things up and make them public, so we can come up with counter measures."

Meanwhile, how worrisome is this computer issue?

Minor shared his perspective over the research findings: "This is more of an exercise in what's possible rather than what's viable," he wrote. Minor

said such a hack needs "so much prior setup that no scammer is going to just randomly do it to you out of nowhere." Minor noted that "you still have to get the malware on there somehow like through a conscious physical USB drive."

Cluley made a similar comment. "It feels like an awful lot of effort to go to, and far beyond the desire of the typical cybercriminal. My feeling is that in many cases if you really wanted to get your paws on the data on that computer there might be easier ways to get it than this."

Mohit Kumar in *The Hacker News* weighed in. The techniques may sound "theoretical and useless to many," he wrote, but when it comes to high-value targets, these "could play an important role in exfiltrating sensitive data from an infected but air-gapped computer."

Actually, it was Cluley who posed thoughts about how attackers might operate, no matter how impractical the scheme sounded. "Imagine, for instance, malware planted on a USB stick known to be used by staff who use the computer, or the opportunities for meddling that might have made themselves available in the supply chain, or if an employee of the targeted organisation was secretly working for the attackers."

Nonetheless, Cluley's verdict was still this: "In short, full marks for creativity—but this isn't a threat I'm going to lose any sleep over."

Looks like *Naked Security* would not argue. "Ultimately, this is interesting academic research, with the emphasis on 'academic'."

More information: Mordechai Guri et al. Brightness: Leaking Sensitive Data from Air-Gapped Workstations via Screen Brightness, *2019 12th CMI Conference on Cybersecurity and Privacy (CMI)* (2020). DOI: 10.1109/CMI48017.2019.8962137 . On Arxiv: arxiv.org/abs/2002.01078

cyber.bgu.ac.il/advanced-cyber/airgap