

BitWhisper turns up heat on air-gap security

March 24 2015, by Nancy Owano



Ben Gurion University reported Monday that researcher Mordechai Guri, assisted by Matan Munitz and guided by Prof. Yuval Elovici, uncovered a way to breach air-gapped systems—that's quite something considering that air-gapped systems, said the *Daily Mail*, are among the most secure computers on the planet, used in high security settings such as classified military networks, payment networks processing credit and debit card transactions for retailers, and industrial control systems for critical infrastructure.

The research initiative was given the name BitWhisper, part of research

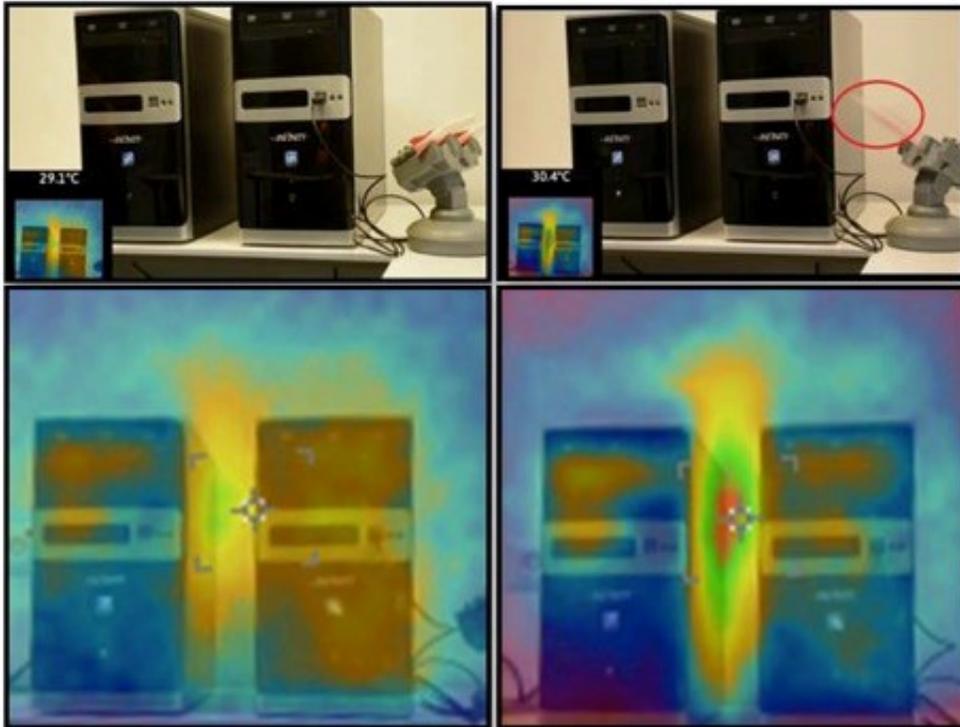
on the topic of air-gap [security](#) at the Cyber Security Research Center at Ben-Gurion University. Dudu Mimran, the CTO of Cyber Security Labs, blogged on Monday, "BitWhisper is a demonstration for a covert bi-directional communication channel between two close by air-gapped [computers](#) communicating via [heat](#). The method allows bridging the air-gap between the two physically adjacent and compromised computers using their heat emissions and built-in thermal sensors to communicate."

Two physically adjacent and compromised computers used heat emissions and built-in thermal sensors to communicate. According to the university's account, a scenario with two adjacent computers is prevalent in many organizations in which two computers are situated on a single desk, one connected to the internal network and the other connected to the Internet. The method that was demonstrated can serve for data leakage for low data packages and for command and control. The *Daily Mail* on Monday said the team planned to present their findings at a security conference in Tel Aviv next week and to [release](#) a paper describing their work.

Kim Zetter in *Wired* said, "The technique works a bit like Morse code, with the transmitting system using controlled increases of heat to communicate with the receiving system, which uses its built-in [thermal sensors](#) to then detect the temperature changes and [translate](#) them into a binary '1' or '0.'" Zetter also made the observation that, depending on how much processing they are doing, computers produce varying levels of heat. "In addition to the CPU, the graphics-processing unit and other motherboard components produce significant heat as well. A system that is simultaneously streaming video, downloading files and surfing the internet will consume a lot of power and generate heat," she added.

Air-gap security is a focus area at the Cyber Security Research Center and the lab practices applied cyber security research. Last year, Prof. Elovici, who heads BGU's Cyber Security Lab, and team made news

when they demonstrated that by using an "AirHopper" method one could leak data from an isolated computer to a [mobile phone](#) without the presence of a network. The main idea behind their research was to use radio frequencies to transmit secret data from the computer to the [mobile](#) phone.



Two air-gapped PCs positioned in the parallel layout. Using BGU's BitWhisper, the left computer transmits a command that instructs the right computer to calibrate and fire a USB game rocket.

"The common policy in such secure organizations is to leave your mobile phone in some locker when you enter the facility and then pick it up when you go out. We at the [cyber security](#) labs challenged this assumption and found a way to leak data from a computer inside the organization to a mobile phone without using Wifi or Bluetooth."

They said this was the first time that a mobile phone was considered in an attack model as the intended receiver of maliciously crafted radio signals emitted from the screen of the isolated computer. AirHopper demonstrated how textual and binary data can be exfiltrated from [computer](#) to mobile phones at a distance of 1 to 7 meters, with effective bandwidth of 13-60 Bps (Bytes per second).

More information: BitWhisper: The Heat is on the Air-Gap, cyber.bgu.ac.il/blog/bitwhisper-heat-air-gap

BitWhisper: Putting the Heat on Air-Gapped Computers: aabgu.org/bitwhisper-putting-t...ir-gapped-computers/

© 2015 Tech Xplore

Citation: BitWhisper turns up heat on air-gap security (2015, March 24) retrieved 20 September 2024 from <https://techxplore.com/news/2015-03-bitwhisper-air-gap.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.