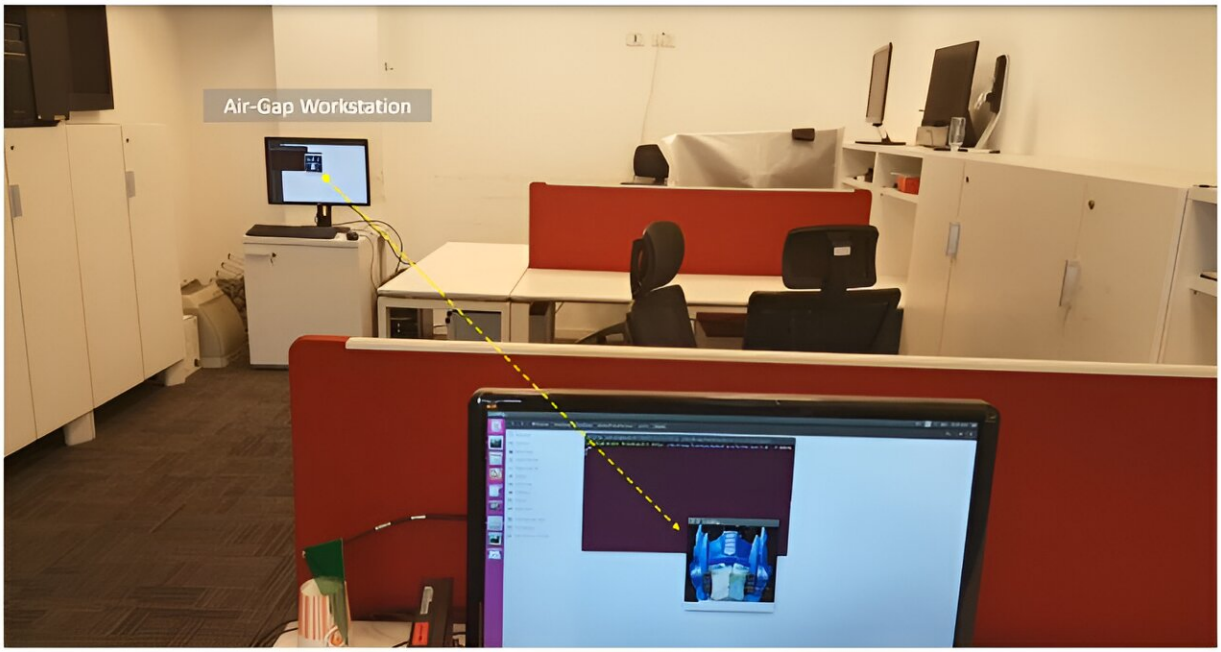
Usable data hacked from air-gapped computer

September 10 2024, by Bob Yirka



Attack demonstration. An air-gap workstation processes a secret image (Optimus Prime). The RAMBO covert channel attack transmits the image via electromagnetic waves. A remote attacker intercepts the information and recovers the secret image. Credit: *arXiv* (2024). DOI: 10.48550/arxiv.2409.02292

A team of software and information systems engineers at Ben-Gurion University of the Negev, in Israel, has demonstrated an ability to extract useful data from an air-gapped computer. The group has posted a paper

to the *arXiv* preprint server describing their experiments and results.

Over the past several years, hackers have made headlines by sneaking their way onto computer systems used for public services, such as monitoring water treatment equipment. Others have conducted denial-of-service attacks on larger systems, or more brazenly, ransomware attacks on hospitals or other critical service systems.

One thing they all have in common is their connection to the Internet, leading some to wonder why such user sites connect to the Internet if it makes them so vulnerable. In this new effort, the research team in Israel has found that even computers not connected to the Internet can be vulnerable to attack.

Computers that are not connected to another network, or the Internet, are said to be air-gapped—there is nothing but empty air between them and any other computer. Such systems would seem to be impervious to attack, especially since floppy drives are no longer used. But that is not always the case as the researchers have demonstrated.

To show that it is possible to hack an air-gapped computer, the researchers developed a type of malware that manipulates the RAM on a target computer into generating very faint radio signals. The software was designed in such a way that the radio waves that were generated reflected data held on the RAM devices and were encoded in such a way as to be readable from a nearby device.

The researchers tested their idea by infecting an air-gapped computer and then by placing another device close enough to listen to the radio waves emitted from the test computer. The signals were then decoded and the messages they held were revealed by software running on the second computer. Under such an arrangement, the team found that they could capture passwords, keystrokes, and other types of data and, in

some cases, even small images.

The research team acknowledges that hacking a computer in such a way in the real world would be challenging, but they also note that it would not be impossible.

More information: Mordechai Guri, RAMBO: Leaking Secrets from Air-Gap Computers by Spelling Covert Radio Signals from Computer RAM, *arXiv* (2024). DOI: 10.48550/arxiv.2409.02292

Citation: Usable data hacked from air-gapped computer (2024, September 10) retrieved 10 September 2024 from https://techxplore.com/news/2024-09-usable-hacked-air-gapped.html