Cellphones can steal data from 'air-gapped computers'

28 July 2015

Credit: Peter Griffin/Public Domain

Researchers at the Ben-Gurion University of the Negev (BGU) Cyber Security Research Center have discovered that virtually any cellphone infected with a malicious code can use GSM phone frequencies to steal critical information from infected "air-gapped" computers.

Air-gapped computers are isolated—separated both logically and physically from public networks—ostensibly so that they cannot be hacked over the Internet or within company networks.

Led by BGU Ph.D. student Mordechai Guri, the research team discovered how to turn an ordinary air-gapped computer into a cellular transmitting antenna using software that modifies the CPU firmware. GSMem malicious software uses the electromagnetic waves from phones to receive and exfiltrate small bits of data, such as security keys and passwords.

"GSMem takes the air out of the gap and will force the world to rethink air-gap security," says Dudu Mimran, chief technology officer of BGU's Cyber Security Research Center. "Our GSMem malicious software on Windows and Linux has a tiny computational footprint, which makes it very hard to detect. Furthermore, with a dedicated receiver, we were successful exfiltrating data as far as 90 ft. (30 meters) in distance from the computer."

According to Guri, "Many companies already restrict the use of cell phones or limit the capabilities (no camera, video or Wi-Fi on cell phones) around air-gapped computers. However, phones are often otherwise allowed in the vicinity of air-gapped computers thought to be secure. Since modern computers emit some electromagnetic radiation (EMR) at various wavelengths and strengths, and cellular phones easily receive them, this creates an opportunity for attackers."

The researchers recommend that countermeasures to mitigate the issue use the "Zone" approach: defined areas or zones around these computers where mobile phones and simple devices are prohibited. Insulation of partition walls may help to mitigate signal reception distance growth if a dedicated hardware receiver is used. Additionally, anomaly detection and behavioral dynamic analysis may help.

This is the third threat the BGU cyber team has uncovered related to what are supposed to be secure, air-gapped computers. Last year, the researchers created a method called Air-Hopper, which utilizes FM waves for data exfiltration. Another research initiative, BitWhisper, demonstrated a covert bi-directional communication channel between two close-by air-gapped computers using heat to communicate.

In addition to lead researcher Mordechai Guri, the other BGU researchers include Assaf Kachlon, Ofer Hasson, Gabi Kedma, Yisroel Mirsky, and Prof. Yuval Elovici, director of the BGU Cyber Security Research Center, member of Ben-Gurion University's Department of Information Systems Engineering and director of Deutsche Telekom

Laboratories.

Guri will present the findings next month at the USENIX Security '15 Conference on August 14 at 2:00 p.m. at the Hyatt Regency Capitol Hill, 400 New Jersey Ave. NW, Washington, D.C.

Provided by American Associates, Ben-Gurion University of the Negev