USBee: Air-gap Covert-channel via Electromagnetic Emission from USB

Goals

In recent years researchers have demonstrated how attackers could use USB connectors implanted with RF transmitters to exfiltrate data from secure, and even air-gapped, computers (e.g., COTTONMOUTH in the leaked NSA ANT catalog). Such methods require a hardware modification of the USB plug or device, in which a dedicated RF transmitter is embedded. We present ‘USBee’, a software that can utilize an unmodified USB device connected to a computer as a RF transmitter.

Description

We demonstrate how a software can intentionally generate controlled electromagnetic emissions from the data bus of a USB connector. We also show that the emitted RF signals can be controlled and modulated with arbitrary binary data. We implemented a prototype of USBee, and discuss here its design and implementation details, including signal generation and modulation. We also evaluated the transmitter by building a receiver and demodulator using GNU Radio. Our evaluation shows that USBee can be used for transmitting binary data to a nearby receiver at a bandwidth of 20 to 80 BPS (bytes per second).

Researchers

Dr. Mordechai Guri
moti.guri@gmail.com

Matan Monitz
mmonitz@gmail.com

Prof. Yuval Elovici
elovici@inter.net.il

Publications

M. Guri, M. Monitz, and Y. Elovici, “USBee: Air-Gap Covert-Channel via Electromagnetic Emission from USB,” 2016. arXiv:1608.08397.

Demo Video

https://www.youtube.com/watch?v=E28V1t-k8Hk