SPECTER: A Lab Attack That Leaks Offline Computer Secrets by Flipping USB Power Settings

Kabui, Charles

2026-11-09

Read at ToKnow.ai



SPECTER is a lab attack that lets malware on an offline computer send a short secret, such as a password, through a USB port. It matters to teams guarding air-gapped computers, machines kept off every network. Once malware with administrator rights is on the machine,

it turns the secret into bits (1s and 0s) and flips a USB device's power setting on for each 1 and off for each 0, like flicking a lamp in Morse code. A phone charging from that computer is the lamp: it starts and stops charging as the setting flips, and an attacker's Android app (or a person watching an iPhone's icon) reads "charging" as 1 and "not charging" as 0. The authors' October 2026 paper reports 0.2 to 0.25 bits a second, so a 16-character password's 128 bits take about 8.5 to 11 minutes.

The authors say tools that watch network traffic and USB data transfers do not directly watch power changes. A mouse works as the lamp too. Its light goes dark when switched off, and a person or camera reads the pattern. At the authors' 1 bit a second, the same 128 bits take about 2 minutes. An antenna touching the USB cable also picked up radio bursts. The authors suggest logging repeated on-off switching of one USB device and keeping personal phones away from sensitive computers. Of five non-phone USB devices tried, three gave a readable signal on a Windows 10 laptop and none on an Ubuntu 22.04 desktop.

Read More: RAMBO, a lab attack that makes an offline computer's memory chips send data by radio

Sources:

- SPECTER: Covert Data Exfiltration from Air-Gapped Systems via USB Power Modulation (arXiv abstract and submission dates)
- SPECTER full text with the tests and defences (arXiv)
- SPECTER attack leaks air-gapped data through USB power controls (CyberInsider)
- SPECTER: Leaking Data from Air-Gapped Computers by Toggling USB Power States (RTL-SDR.com)

Disclaimer: *For information only. Accuracy or completeness not guaranteed. Illegal use prohibited. Not professional advice or solicitation.* ***Read more:*** */terms-of-service*