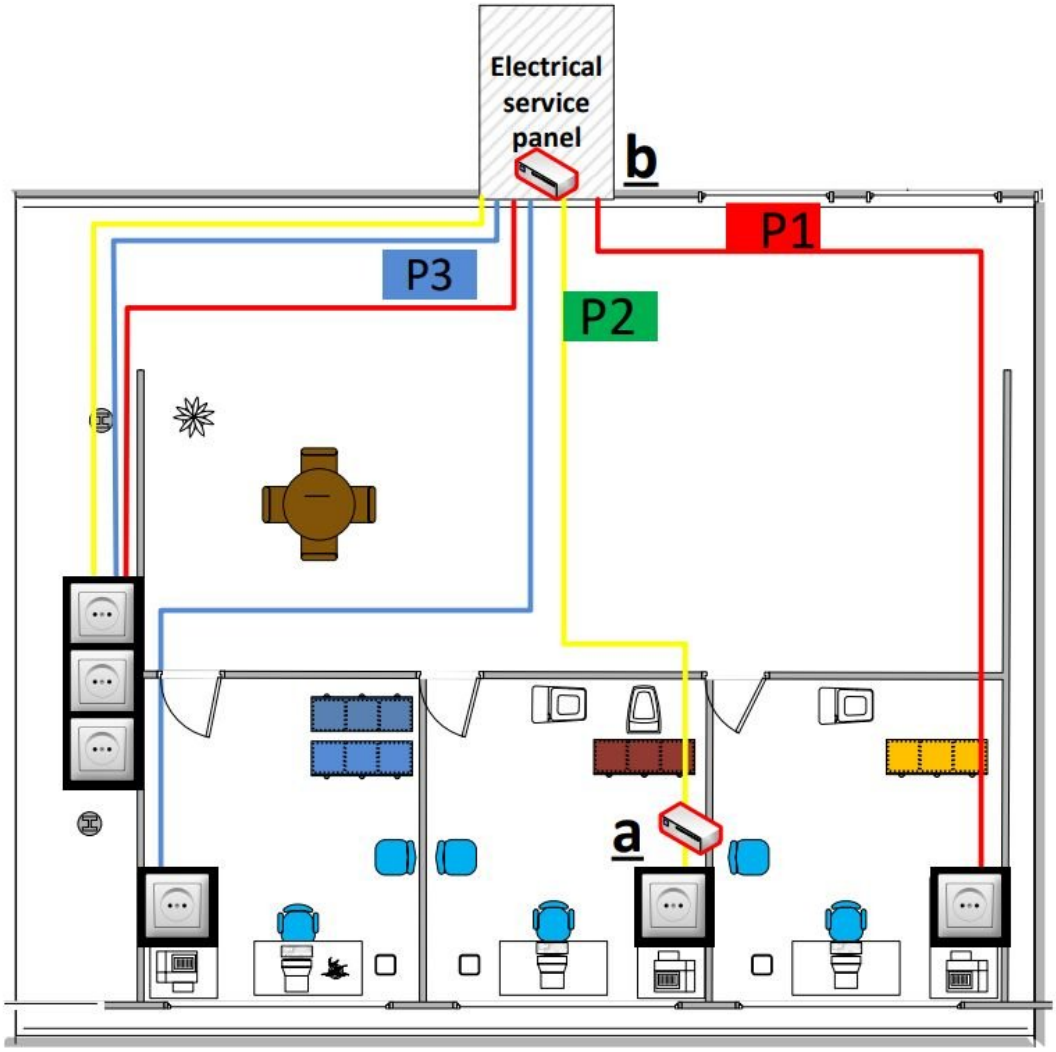
PowerHammer is wake-up call to data-stealing through power lines

April 18 2018, by Nancy Owano



The receiver implantation: (a) on the power line feeding the computer, and (b) on the power line in the main electrical service panel. Credit: arXiv:1804.04014 [cs.CR]

Can security sleuths ever complain there's nothing left to do? The answer is obvious, and one more path to mischief has been recognized in the form of power supplies serving as a data exfiltration tool. It appears that malware using power lines could exfiltrate data from air-gapped computers.

Researchers from the Ben-Gurion University of the Negev discovered malware that nabs data through power lines.

"PowerHammer works by infecting an air-gapped computer with malware that intentionally alters CPU utilization levels to make the victim's computer consume more or less electrical power," said Catalin Cimpanu, *BleepingComputer*. Wait, air-gapped computers?

Mordechai Guri, Boris Zadov, Dima Bykhovsky, Yuval Elovici, in a paper about their work, pointed out that "even airgapped networks are not immune to breaches. In the past decade, it has been shown that attackers can successfully penetrate air-gapped networks by using complex attack vectors."

Their paper, "PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines" is on arXiv. They call the malware PowerHammer, and they described its behavior. "Data is modulated, encoded, and transmitted on top of the current flow fluctuations, and then it is conducted and propagated through the power lines." They said this was phenomena known as a conducted emission.

Swati Khandelwal in *The Hacker News* said it was specially designed malware creating fluctuations in the current flow "in morse-code-like pattern to transfer data hints in binary form (i.e., 0 and 1)."

The authors wrote, "We implemented a malicious code that controls the power consumption of a computer by regulating the momentary utilization of the CPU cores."

Writing in *SecurityWeek*, Eduard Kovacs explained that "A computer's CPU is a significant power consumer and its workload has a direct impact on power consumption and implicitly the flow of current in the device's power cable. By overloading the CPU with calculations and stopping and starting the workload, it's possible to generate a signal over the power lines at a specified frequency."

Richard Chirgwin, *The Register*, said, "The PowerHammer malware spikes the CPU utilisation by choosing cores that aren't currently in use by user operations (to make it less noticeable)." He remarked that "it's pretty simple, because all the attacker needs is to decide where to put the receiver current clamp: near the target machine if you can get away with it, behind the switchboard if you have to."

That brings one to how they tested. The team used two approaches. One was line-level: Compromising the power lines inside the building that connects the computer. The other was phase-level: playing with the building' outside electrical service panel.

Chirgwin explained that "Depending on the attacker's approach, data could be exfiltrated at between 10 and 1,000 bits-per-second. The higher speed would work if attackers can get at the cable connected to the computer's power supply. The slower speed works if attackers can only access a building's electrical services panel."

Discussing their experiment, the authors said they evaluated the covert channel in different scenarios with three types of computers: a desktop PC, a server and a low power IoT device.

Results? The authors wrote that "The results show that data can be exfiltrated from air-gapped computers through the power lines at bit rates of 1000 bit/sec for line level powerhammering, and 10 bit/sec for phase level power-hammering."

Countermeasures? There are several discussed in the paper: monitoring the currency flow on the power lines; attaching filters to power lines; jamming; host-based intrusion detection systems.

More information: PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines, arXiv:1804.04014 [cs.CR] arxiv.org/abs/1804.04014

Abstract

In this paper we provide an implementation, evaluation, and analysis of PowerHammer, a malware (bridgeware) that uses power lines to exfiltrate data from air-gapped computers. In this case, a malicious code running on a compromised computer can control the power consumption of the system by intentionally regulating the CPU utilization. Data is modulated, encoded, and transmitted on top of the current flow fluctuations, and then it is conducted and propagated through the power lines. This phenomena is known as a 'conducted emission'. We present two versions of the attack. Line level powerhammering: In this attack, the attacker taps the in-home power lines1 that are directly attached to the electrical outlet. Phase level power-hammering: In this attack, the attacker taps the power lines at the phase level, in the main electrical service panel. In both versions of the attack, the attacker measures the emission conducted and then decodes the exfiltrated data. We describe the adversarial attack model and present modulations and encoding schemes along with a transmission protocol. We evaluate the covert channel in different scenarios and discuss signal-to-noise (SNR), signal processing, and forms of interference. We also present a set of defensive countermeasures. Our results show that binary data can be covertly

exfiltrated from air-gapped computers through the power lines at bit rates of 1000 bit/sec for the line level power-hammering attack and 10 bit/sec for the phase level power-hammering attack.