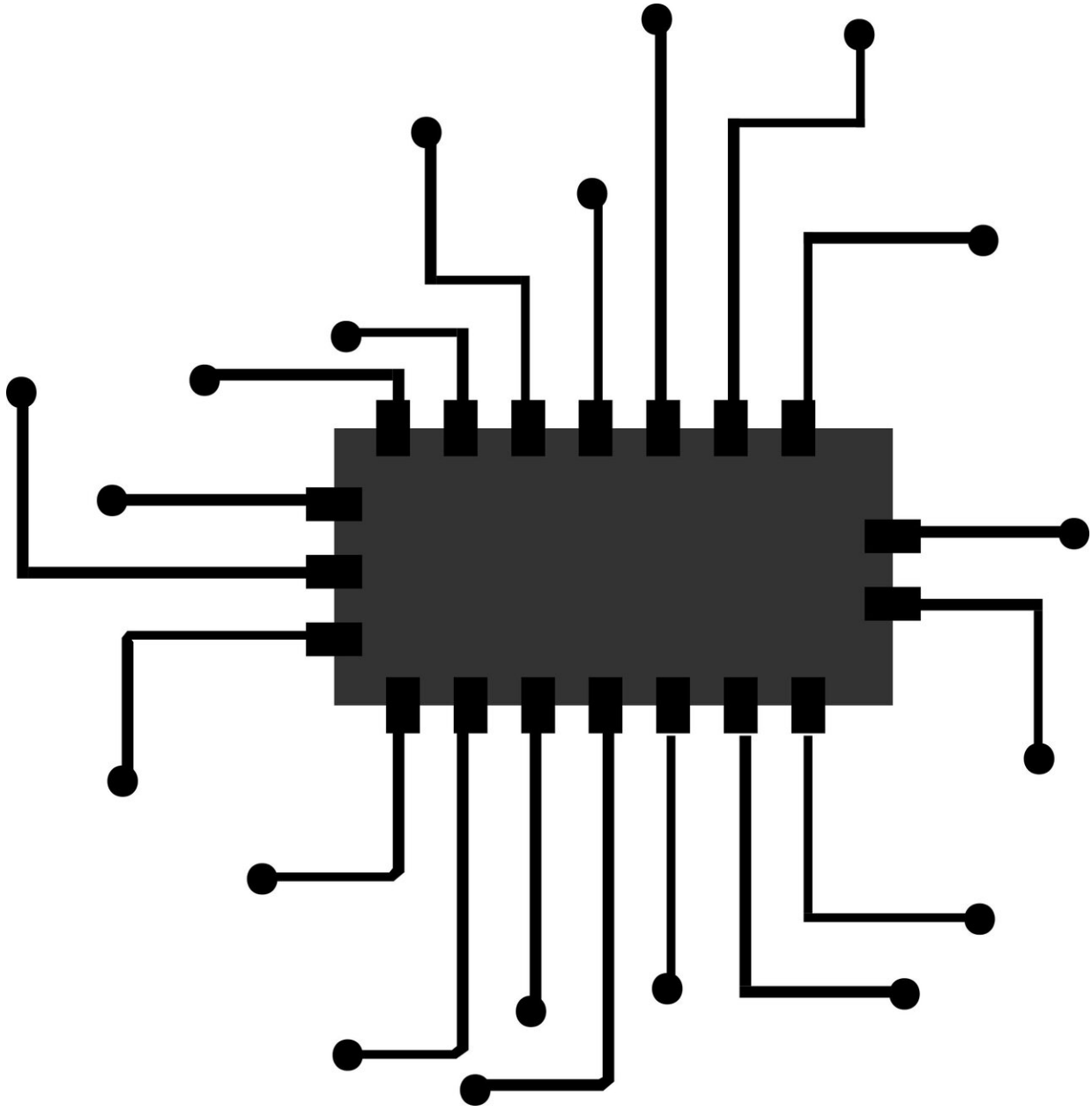
Unfixable security flaw found in Intel chipset

March 8 2020, by Peter Grad



Credit: CC0 Public Domain

The bad news: A security research firm has found that Intel chipsets used in computers over the past five years have a major flaw that allows hackers to bypass encryption codes and quietly install malware such as keyloggers.

The worse news: There is no complete fix for the problem.

The security firm Positive Technologies announced late last week that the vulnerability, hard-coded in the boot ROM, exposes millions of devices using Intel architecture to industrial espionage and leaks of sensitive information that cannot be detected as they happen. Because the flaw occurs at the hardware level, it cannot be patched.

The firm said that a hacker would need direct access to a local network or machine, thus somewhat limiting the possibility of attack. They also noted that one barrier to attack is an encrypted chipset key inside the one-time programmable (OTP) memory, although the unit that initiates such encryption is itself open to attack.

Researchers made it clear the threat is a serious one.

"Since the ROM vulnerability allows seizing control of code execution before the hardware key generation mechanism … is locked, and the ROM vulnerability cannot be fixed, we believe that extracting this [encryption] key is only a matter of time," Positive Technologies researchers said.

"When this happens, utter chaos will reign."

They warned of forged hardware IDs, extracted digital content and decryption of data on hard drives.

Intel's most recent line of chips,10th Gen processors, are not vulnerable to this threat.

Intel, which acknowledged it was aware of the problem last fall, issued a patch last Thursday that partially addresses the problem. A spokesman for the company explained that while they cannot secure hardcoded ROM in existing computers, they are trying to devise patches that will quarantine all potential system attack targets.

The flaw is located in Intel's Converged Security Management Engine (CSME), which handles security for firmware on all Intel-powered machines. In recent years, Intel has confronted a few serious security flaws such as the Meltdown and Spectre processor vulnerabilities and the CacheOut attack.

The latest crisis comes at a time of increasing fierce competition with AMD, developer of the popular Ryzen chip.

But perhaps the most serious blow is to Intel's longstanding reputation of excellence. The latest flaw, according to Mark Ermolov, lead specialist of OS and hardware security at Positive Technologies, strikes at the heart of Intel's most vital asset: trust.

"The scenario that Intel system architects, engineers, and security specialists perhaps feared most is now a reality," Ermolov said. "This vulnerability jeopardizes everything Intel has done to build the root of trust and lay a solid security foundation on the company's platforms."

More details of Intel's efforts to address the vulnerability can be found on the company's support page: intel .com/content/www/us/en/support/articles/000033416/technologies.html" target="_blank">www.intel.com/content/ … 16/technologies.html