# Critical Thunderbolt flaw enables five-minute stealth attack

May 11 2020, by Peter Grad

Credit: CC0 Public Domain

A new attack method affecting Thunderbolt-equipped computers can bypass locks, password-protection and encryption on ports produced before 2019.

The attack, called Thunderspy, requires physical access to a targeted computer but can be done in less than five minutes and leave no evidence of physical or digital tampering.

Dutch security researcher Björn Ruytenberg, who discovered the vulnerability and reported his results on Sunday, says there are no easy software patches. He recommends disabling all Thunderbolt ports.

All Windows and Linux PC machines with Thunderbolt ports are vulnerable, but Apple computers are not affected, Ruytenberg says.

The Thunderbolt interface has long been viewed as a potential security threat. Its primary feature—faster data speeds, up to 40Gbps—is its weak link. Thunderbolt achieves greater speeds in part by allowing more direct access to computer memory than other types of ports. It is that increased exposure to system resources that establishes a greater security threat.

Last year, security experts discovered a series of flaws collectively called "Thunderclap" that they said permitted the planting of a malicious component that could bypass security measures. They recommended the employment of Thunderbolt security levels that guarded system access at the price of limiting some Thunderbolt features.

But Thunderspy can bypass those security measures, Ruytenberg says.

"Even if you follow best security practices by locking or suspending your computer when leaving briefly, and if your system administrator has set up the device with Secure Boot, strong BIOS and operating system account passwords, and enabled full disk encryption, all the attacker needs is five minutes alone with the computer, a screwdriver, and some easily portable hardware" Ruytenberg warns.

Intel recently distributed a Thunderbolt security system called Kernel Direct Memory Access Protection that could block a Thunderspy attack. But it is available only for computers made in 2019 or later. And not all computer models made in 2019 can take advantage of it, including those by Dell, HP and Lenovo.

Ruytenberg explained that Thunderspy falls into the category of "the evil maid." This is a type of security breach that is exploited by hackers gaining unauthorized access to a computer left unattended, as in hotels where maids use master keys to gain access to guest rooms.

"All the evil maid needs to do is unscrew the backplate, attach a device momentarily, reprogram the firmware, reattach the backplate, and the evil maid gets full access to the laptop," says Ruytenberg.

He estimated that a hacker would require about $400 worth of equipment, including a programming tool and Thunderbolt peripheral.

Ruytenberg recommends the following steps for those with Thunderbolt-eqipped systems:

- Connect only your own Thunderbolt peripherals. Never lend them to anybody.
- Avoid leaving your system unattended while powered on, even when screenlocked.
- Avoid leaving your Thunderbolt peripherals unattended.
- Ensure appropriate physical security when storing your system and any Thunderbolt devices, including Thunderbolt-powered displays.
- Consider using hibernation (Suspend-to-Disk) or powering off the system completely. Specifically, avoid using sleep mode (Suspend-to-RAM).

Although millions of users own Thunderbolt-equipped computers and are thus all vulnerable, this type of assault is generally undertaken by malicious parties targeting users known to have highly sensitive or valuable information, a realm dominated by international spies. In a nod to that reality, Ruytenberg noted that tools required to launch a Thunderspy attack will eventually be reduced in size for easier application. "Three-letter agencies would have no problem miniaturizing this," he said.

**More information:** thunderspy.io/