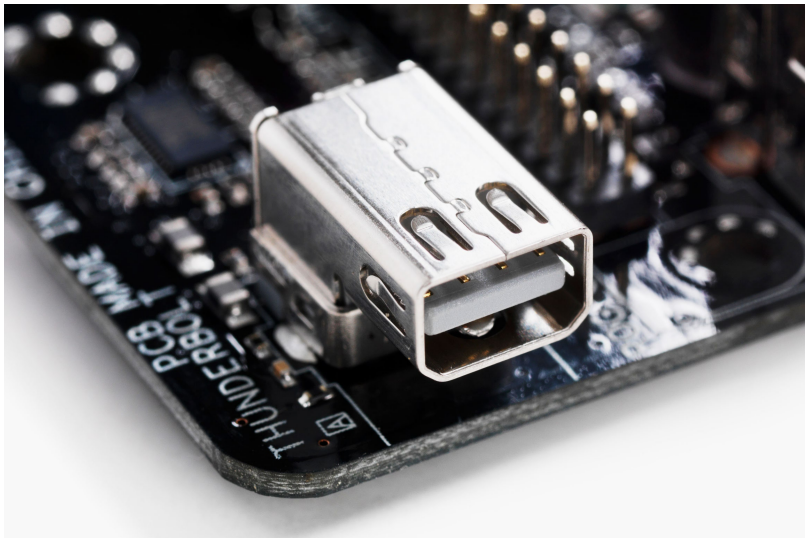
Written by Alice Marshall
13 May 2020

Dutch researcher Björn Ruytenberg reveals the common Thunderbolt port has a serious flaw--"Thunderspy," a means for hackers to bypass the login screen of a sleeping or locked PC in order to gain full access of the data within.



The flaw resides in essentially all Thunderbolt-enabled Windows or Linux PCs manufactured before 2019, and allows for what the security industry dubs an "evil maid attack." This involves the potential attacker being alone with the PC (for example, in a hotel room), and simply requires opening the case of the target laptop with a screwdriver. Once the machine is open, the attacker simply needs to momentarily attach a device, reprogram the firmware and reattach the backplate for full access to the laptop. The operation, Ruytenberg says, takes all of 5 minutes.

Worst of all, while Thunderbolt features "security levels" disallowing access to untrusted devices or even turning the input into a simple USB/display port, the Thunderspy technique bypasses such settings. It alters the firmware of the chip taking care of the Thunderbolt port and changes the security settings, allowing access to any device. In addition, it leaves no evidence the Thunderbolt firmware was modified in the OS of the PC in question.

So far, the one issue with the Thunderspy attack is the fact the attack requires an SPI programmer device and an SOP8 clip, a piece of hardware able to attach to the pins of the Thunderbolt controller. However, Ruytenberg says a well-funded hacker (or any number of three-letter agencies) should be able to create a single small device for the operation. In addition, the flaw is in the hardware, and as such cannot be patched on the software level.

In turn, Intel says it knows about the issue, and has fixed it through what it calls Kernel Direct Memory Access (DMA) protection. However OEMs are still to universally apply the fix, and in any case it will only be found in new machines. As such, customers need to be careful where they leave their machines, or upgrade to a model with Kernel DMA in place.

Go Thunderspy

https://thunderspy.io/