A fork is an easy-to-find nonstandard USB device

devblogs.microsoft.com/oldnewthing/20061129-48

November 29, 2006

Raymond Chen

Remember the Ten Immutable Laws of Security. Today, we're going to talk about number three: If a bad guy has unrestricted physical access to your computer, it's not your computer any more. There was a bug which floated past my field of vision many months ago that went something like this: "I found a critical security bug in the USB stack. If somebody plugs in a USB device which emits a specific type of malformed packet during a specific step in the protocol, then the USB driver crashes. This is a denial of service that should be accorded critical security status." Now, it's indeed the case that the driver should not crash when handed a malformed USB packet, and the bug should certainly be fixed. (That said, I'm sure some people will manage to interpret this article as advocating not fixing the bug.) But let's look at the prerequisites for this bug to manifest itself: The attacker needs to build a USB device that is intentionally out of specification in one particular way and plug that device into a vulnerable machine. While that's certainly possible, it's a lot of work for your typical hacker to burn a custom EEPROM with USB firmware that manages to hit the precise conditions necessary to trigger the driver bug. It's much easier just to grab a fork. You see, since this attack requires physical access to a USB port, you may as well attack the machine in a much more direct manner that doesn't require you to spend hours with a soldering gun and a circuit board: Just grab a fork and jam it into the USB port. I haven't tried it, but I suspect that will crash the machine pretty effectively, too. If you can't get the fork to work, pouring a glass of water into the USB port will probably seal the deal. Doron tells me that some companies address this problem by removing physical access: They fill the USB ports on all their machines with epoxy.

Update: Randy Aull tells me that the USB 2.0 specification anticipated the fork attack and requires that all transceivers be able to withstand short circuits "of D+ and/or D- to VBUS, GND, other data lines, or the cable shield at the connector, for a minimum of 24 hours." (Though I'm not sure if that also covers shorting VBUS to GND.) I wonder if they also have a paragraph specifying that USB devices must also withstand water immersion… Of course, you could still use that fork to push the power button or jam it into an outlet on the same circuit as the computer you want to take down in order to blow a fuse.

Raymond Chen

Follow