Security researcher finds hack vulnerability in Mac battery chips

July 26 2011, by Bob Yirka

(PhysOrg.com) -- Research consultant Charlie Miller, currently with Accuvant Labs, has made it known that he intends to demonstrate a security hole in certain Mac laptops at next month's Black Hat security conference. In an interview with Forbes, he says the chip that controls the battery can be hacked because Apple uses only two passwords for the firmware for all of their laptops, which he says he's been able to figure out, which of course means, others with less noble purpose could do it as well.

Miller claims to have figured out the security breach by examining a firmware upgrade Apple sent out in 2009. Being able to breach the firmware in the chip means he can alter settings such as those that monitor the battery and the interface between it and the operating system. Miller says he’s “bricked” or killed the batteries in seven laptops, presumably to prove that it wasn’t a fluke, and believes if he wanted to, he could cause the batteries to ignite or even blow up, though that is still debatable as the batteries themselves come with a fuse to prevent such an occurrence.

Miller says he’s found he can hack into MacBooks, MacBook Pros and MacBook Airs, and says he’s notified both Apple and chip maker Texas Instruments of his findings, but says he hasn’t heard anything back from them. He also says that he believes this vulnerability is particularly insidious because if a hacker did manage to breach the battery firmware and implant malware, the user of the computer, upon discovering something wrong, wouldn’t be able to eradicate it unless he or she thought to remove the battery, not something most would think of right off the bat. It should be noted here that just because a hacker gets into the battery chip, that doesn’t mean they’ve got a clear shot to the operating system and the rest of the computer. Chipmakers do add additional security measures to their chips so a hacker would have to be able to hack that part as well in order to embed malware that could do other things besides just mess with the battery.

Miller also says he’s developed a "fix" for the problem, a patch that will change the password on the firmware to a random number, though users who apply it will no longer be able to get firmware upgrades from Apple.

While this discovery by Miller does indeed highlight a serious vulnerability, it’s not like it’s one that is confined to just Mac laptops or even laptops in general. Most computers have several chips in them with programmable firmware, protected only by simple passwords, and their vulnerabilities are well documented. What’s truly interesting is that more hackers aren’t trying to sneak in via this approach; though no doubt Miller’s presentation will serve as a reminder to those with nefarious intent who may have forgotten about such vulnerabilities or simply haven't been paying attention.

Citation: Security researcher finds hack vulnerability in Mac battery chips (2011, July 26) retrieved 25 April 2024 from https://phys.org/news/2011-07-hack-vulnerability-mac-battery-chips.html