Other discrete elements

Occasionally there might be additional discrete devices on the laptop, such as a discrete GPU. Such devices will likely come with their own internal flash memory, thus breaking the stateless principle. In most cases these discrete devices would also be bus-mastering devices (capable of issuing DMA to host memory), which means they could not only be used as a secret storage, but also interfere with the platform boot process if it is not properly secured against DMA from devices.[8]

It's thus best to ensure no discrete devices are present on the laptop, especially no discrete GPUs. We talk more about the discrete wireless cards, such as WiFi and cellular modem, below.[9]

Other modifications to the laptop

In addition to removing persistent state-carrying elements from the laptop, there are also a few other minor, yet important, modifications that are needed to assure the laptop is not harmful to the user. We discuss these below.

The wireless devices

All the wireless devices (WiFi, BT, 3G/LTE modems, etc.) deserve special consideration (even if they do not have their own flash memory) because they provide a very convenient way for the malware that runs on the platform (e.g. in the ME or SMM, or even on the host OS) to leak information using a wireless channel (so, a channel very difficult to block or notice). This could happen irrespectively of whether the user decided to consciously enable and use the actual device or not (e.g. turned on WiFi in the host OS and connected to a WiFi network).

Additionally any wireless device could be used to gather information about the user surroundings, such as e.g. the list of active WiFi networks (SSIDs) or BT devices MAC addresses.

[8] The author is not aware of any BIOS implementation that would actively try to protect itself against potential DMA attacks originating from devices during boot, especially early boot.

[9] One of the reviewers also pointed to battery as a potential element containing embedded microcontroller with its own flash memory. Needless to say such "smart batteries" should be avoided and all the charging/monitoring logic implemented by the EC, or using "dumb" electronics without persistent state storage.