# Chapter 2

# State(-carrying) considered harmful

There are several fundamental reasons why endpoint computing devices, such as laptops, without clearly defined separation of state-carrying elements are problematic:

1. The presence of persistent storage intermixed with the hardware makes it possible for the attacker to persist malware on the platform, without the user to have any simple way of learning about it, nor removing it (e.g. via OS re-installation).

2. This also allows dishonest vendors, such as the OEMs or shipping agents, to deliver already infected hardware without the user being able to easily find out. This also includes Evil Maid attacks, which might be executed by other actors than vendors.

3. The malware, once installed on the platform somehow, is given places where to store stolen secrets from the user. This is especially worrisome in the context of disk encryption keys, which could be exfiltrated this way even on air-gapped machines.[1]

4. Finally, these state-carrying elements make it possible to identify platforms and ultimately their users, due to various personally identifiable information, such as MAC addresses for WiFi or BT, which make the hardware unique.

[1] In such cases the leaked keys would become readily available to whoever has seized the laptop and has the keys to decrypt the backdoor-created data with the keys inside.