makes lots of physical attacks difficult, or simply not feasible. This applies to the "classic" Evil Maid attacks, as well as various attacks targeting the firmware.

Still, in order to somehow address (or increase the cost significantly) of the full laptop-replacing Evil Maid attacks, one can think of several solutions which include traditional physical-based protection applied to the laptop, when it is being left unattended by the user. These are things such as custom, personalized stickers, which make it more difficult to bring an identically looking laptop, as well as more classic means in a form of a vault or strong box, or a monitoring camera.

An inquisitive reader might wonder why would we need all this hassle with stateless laptops, if the user was expected to implement the physical protection, anyway? As already mentioned several times in this paper, there are many more problems with x86 platform, and which we try to resolve with the stateless laptop, than just the physical attacks. Such other problems include: software attacks on firmware, malicious firmware (backdoored by the vendor, or somewhere during the shipment), software attacks against secure boot mechanisms. A reader is, again, directed to the [10] for a more complete discussion.

The physical protections mentioned above do not, however, resolve the problem of the attackers subverting the laptop hardware at manufacturing or shipment stages. This includes, naturally, a potentially conspiring laptop vendor.

In order to address this latter problem we – the industry – need to come up with reliable and simple methods for comparing PCBs with each other. A tool analogical to 'diff', only working for PCBs rather than on files. Such a tool, implemented as a software, could e.g. take two (sets of) photos taken by the user of the two boards to compare. The photos might be taken with an ordinary camera, or, in a more sophisticated setup, using X-ray imaging to reveal also the internal layer wiring. This inititive has already been proposed by other researchers recently (e.g. [3]), so it is not unreasonable to expect some progress in this area in the near future.

Admittedly such an approach would not be able to detect sophisticated attacks which replace the original laptop board with identically looking one (connection- and chip-geometry-wise), yet with different chips. The author thinks that such attacks might be very difficult to pull off in practice, probably extremely pricey due to the need of manufacturing small series of custom integrated circuits.