Chapter 3

The Stateless Laptop

In this chapter a vision for the stateless laptop is described. The author believes the clean separation of state introduced by these modification would be attractive not just on current x86-based platforms, but also on any future platforms, be they based on ARM or any other processor architectures.

Also discussed are additional modifications needed to make the laptop more trustworthy, or to state it in a more direct way: much less of a threat to its user.

State-carrying elements on modern laptops

We start by identifying the state-carrying (persistence-carrying) elements on a modern x86 laptop. These are:

1. The SPI flash chip carrying the BIOS, ME, and other firmware.
2. The Embedded Controller (EC), which is an OEM-specific microcontroller (uC), and which requires its own flash memory, which might be either implemented inside the uC itself or as a discrete chip on the board (potentially shared with the SPI flash chip mentioned in the previous point).
3. Additional discrete devices, such as e.g. the WiFi or BT modules. Typically they would contain their own flash memories to hold their own firmware.
4. Finally, there is the hard disk.[1]

[1]The disk should not be confused with the SATA controller, which is part of the processor package on the latest Intel models.