Notably the above list does not contain the processor package, which includes the actual processor (CPU), and what was previously known as "the chipset", comprising the MCH (formerly the "northbridge"), and ICH/PCH (formerly the "southbridge"). Indeed, it seems that none of the modern processors are being equipped with flash-able memory. The reason for this seems to be resulting from the limitation of the manufacturing technology as used for modern processors. If it was otherwise, we would likely not see discrete SPI flash chips for holding of the BIOS, ME, and other firmware on notebook motherboards anymore...

Although it's worth mentioning that Intel processor packages still contain a residual form of persistent state storage: so called fuses. It's unclear to the author if it's possible for the processor itself to blow its own fuses.[2] Even if that was possible, however, it seems like the usefulness of this form of state storage would be very limited to the attacker: it could potentially only be used once, and only for storing very short secrets. Notably, it doesn't seem it could be used for platform re-infection.[3]

Because we don't have any control over the processor package, i.e. we must accept it the way it is, at least if we want to build an x86 laptop today, and also because of the limitations mentioned above, we will treat the processor package as a stateless element in the rest of this paper. Nevertheless, it would be desirable if the processor vendors used such a technology for fuses implementation, as it would not be possible for the processor itself to self-blow these.

Let us now discuss what we could potentially do about all the above mentioned state-carrying elements.

## The SPI flash chip

The platform's firmware-carrying flash chip (the SPI flash as it's often called) presents the biggest challenge for us, the state-less laptop proponents. The SPI flash chip is tasked with several crucial goals on modern Intel x86 laptops:

1. It provides the firmware to the Intel ME processor. Failure to do so would, most likely, result in the platform shutdown.[4]

[2] More specifically: for either the instructions running on the host CPU, or those running on the ME processor to blow the fuses.

[3] Although it could be used to implement reply-protection for hypothetical CPU-based backdoors, as discussed in [9].

[4] While there is no clear officially statement in the Intel platform specs about this, it's considered a tribal knowledge among many experts.