Alternatively this might have been done by the Intel FSP blob.[1].

The author believe such a move would be extremely risky for a vendor like Intel. Again, we should remember that such malware insertion (by either the processor or FSP blob) could not be conditioned on any persistent state, and so would be subject to reply "attack". In other words, once the processor or the FSP got caught while pulling this off, it should be possible for the user to reproduce and demonstrate this malicious behaviour arbitrary number of times subsequently.

Of course, Intel ME, or a malicious SMM, instead of injecting malware into the host memory, might chose a more subtle approach and instead only expose a privilege escalation backdoor which could then be used by some malware to undermine security isolation offered by the host OS.[2]

Again, by using a largely open source BIOS implementation we can practically rule out such a backdoor in an SMM[3]. This leaves us with the possibility of the Intel ME providing this hidden escalation trap. That, however, is something that a processor vendor might always do *trivially*, without introducing technology such as Intel ME, as discussed e.g. in [9]. In that case, again, our only hope is that Intel would not risk being caught red-handed, given the hypothetical backdoor would need to be *stateless*.

We thus see that, while we cannot fully eliminate the problem of subversion of the host OS security by potentially malicious processor, the construction of the stateless laptop allows us to force the adversary into a very dangerous territory, requiring them to take high risk and also making the attack very complex.

It's worth nothing, however, how we have silently started assuming that we need to have a largely open source BIOS (so largely trustworthy), even on our stateless laptop. Needless to say, the coreboot project [14] is a natural candidate for such a BIOS, and we are very lucky there is such a project in the wild already.

[1] Here we assume a mostly open source BIOS has been used. Such a BIOS will still likely need to execute the Intel FSP blob, and this blob would be the only place which might inject the malware

[2] E.g. the backdoor might allow to escape a virtual machine, allowing some more-or-less standard malware which came through some standard channels, such as an email attachment, and which would otherwise be contained to some untrusted VM, to now spread over the whole system.

[3] Indeed, it's hardly imaginable for the FSP blob to bring such a backdoor into the SMM.