Compromise a laptop with 5 minutes of physical access

When going for conferences outside my home country, especially security conferences, I usually do not bring my laptop. Why? One of the reasons is the threat of "evil maid" attacks.

For those who do not know, an "evil maid" attack is an attack on an information asset (usually a laptop). The term "evil maid" comes from the idea of a cleaning staff that has a brief access to your computer who does something to the computing device.

Early in July 2018, Mickey Shkatov of the firm Eclypsium demonstrated that an attacker could "flash" the firmware of a laptop with a malicious version in under 5 minutes. Code for the creation of such exploits can be found online – a SMM (System Management Mode) backdoor for UEFI based platforms is available on Github as a proof of concept.

So what can we do?

The "best" method which I have been using is to not bring the laptop at all. This is the approach that I have been using. I have found that I can perform the necessary work (that needs to be done within the duration of the conference) using my mobile phone.

Sometimes, there are times which we need to bring a laptop to an insecure place as we are there for an extended period of time. In such cases, we can perform the following:

(1) Minimize time when we are not physically close to the laptop.
(2) Encrypt the entire hard disk using full disk encryption
(3) Restrict physical access to the laptop when we are not with the laptop. Sometimes, it's the hotel safe.
(4) Detect unauthorized access to that restricted space. For example, using a motion detector camera and/or a phone with the application "Haven" (which detects movement)
(5) Update the laptop's firmware, operating system and software to the latest patches and secure settings (including "Secure boot")

References:

- https://security.stackexchange.com/questions/159173/what-exactly-is-an-evil-maid-attack
- https://motherboard.vice.com/en_us/article/a3q374/hacker-bios-firmware-backdoor-evil-maid-attack-laptop-5-minutes
- https://theintercept.com/2017/12/22/snowdens-new-app-uses-your-smartphone-to-physically-guard-your-laptop/
- https://github.com/cr4sh/smmbackdoor