## Scenario 0: An air-gapped system (no network)

Contrary to what it might seem at first sight, the mere fact that we are keeping the laptop not connected to any network does not automatically make it a truly air-gapped system! If there is malware on the laptop it can still establish communication with the outside world through a number of channels: it might use the existing WiFi or BT, or LTE/3G devices to send packets to other attacker-controlled devices[1], ostensibly without connecting to any network. It might even use more exotic means of establishing covert channels, such as the audio spectrum using the built-in speakers, as mentioned previously in this document.

Also, even if the system is not yet compromised (i.e. no malware or backdoors running on it yet), it might get compromised when devices such as WiFi or BT are exposed to the environment and are processing the (untrusted) input "from the air" around the laptop.[2]

Thus to keep the laptop truly air-gapped one must ensure access to all these devices is forbidden, and not just to the host OS, but also to any of the hardware on the platform, including the processor. The physical kill switches seem to be a reliable way for guaranteeing this, as discussed previously. Obviously, assuming such kill switches have been fitted (and set to the "off" positions), and assuming that the stateless laptop is indeed lacking any persistent memory, and that even if the ME (or any other rootkit) managed to steal any of the user data, it would not be able to leak them anyway.[3]

A truly world-disconnected computer is of very limited use, however. In practice we would like to transfer some files from/to such an air-gapped system. One popular approach is to use a USB storage device (stick) for that purpose. Such an approach, however, exposes the air-gapped computer to potential infections when its host OS is processing the device, volume, and filesystem metadata brought by this device. Additionally, and more importantly, a potential backdoor, e.g. in the ME, might now dump all the previously stolen data onto the stick (and these blobs might now not be easy discoverable by the user, thanks to e.g. the wear levelling mechanisms used on the stick, or potentially backdoored firmware on the said USB device).

A better approach is to use physically read-only media, such as DVD-R. While such a medium can still bring infection to the air-gapped system, it wouldn't be

[1] Which might be the user phone or Smart TV, for example.

[2] This is especially true if the host OS does not explicitly try to sandbox the devices, drivers, and corresponding stacks, which is often the case.

[3] One reviewer pointed the malware might try to e.g. modulate CPU usage, thus indirectly trying to leaking the data via electro-magnetic field...