communicate with other devices (such as the user's phone or even an internet-connected TV) in order to exfiltrate some low-bandwidth information (e.g. the disk decryption key stolen from the host DRAM page or registers).

For this reason it seems only reasonably to put all the audio and video devices behind physical kill switches, just like it was recommended for all the wireless ones. Again it should be stressed the physical switches should be cutting the actual power or signal lines to the devices, accounting for potentially misbehaving ones.

Volatile memory quick wiping

Finally, one additional aspect of building a stateless laptop is to account for all the state accumulated in the *volatile* memory, specifically DRAM and the processor internal SRAM used by the ME. Even though we're talking about volatile memory, it's a well know fact that residual information might remain there for a surprisingly long time [6]. Additionally, the ME internal memory (SRAM) is believed to remain to be sustained despite platform normal shutdown state, as the ME is still in operation, albeit it might be in sleep mode (again, the platform does not need to be in e.g. S3 for this).

Thus a mechanism is needed to ensure, upon user's request, a reliable and quick clearing of all the volatile memories fitted on the platform. This might be the default behaviour every time the platform is going to be shutdown for hibernation. One of the reviewers suggested short-circuiting Vcc with GND pins might do the trick for the processor and DRAM.