Admittedly though, most such exfiltration channels would require the attacker to be physically close to the user's laptop, so for some of the users this might not be a realistic threat[10]. Notably with one exception – if the malware managed to interpose on legitimate traffic generated by the user, e.g. by finding and modifying network buffers in the host memory, it might then easily leak the stolen secrets at least to the user's ISP, or with some luck, to whatever server on the Internet the user chose to establish connection with. We discuss this problem as well as potential countermeasures later in this paper.

Similarly not every user would be concerned about their physical location being leaked (through the information sniffed by the wireless devices). But for those who care, a mechanism is needed to prevent this from happening.

The easiest way to address all the above mentioned problems is to fit a physical kill switch for each (or all) of the wireless devices. Care should be taken for the switch(es) to control the actual power supply wires to the devices, rather than merely asking the devices to disable themselves, a request which a malicious device (or one with an infected firmware) might simply ignore.

Of course physical kill switches are not an elegant solution, as in most cases the user would like to have some form of wireless connectivity. After all there is a reason we want to have these networking devices in the first place... As mentioned we will consider this problem in more details later in this paper. For now suffice to say that it would be beneficial to either: 1) not have any internal WiFi or BT card, or 2) a simple networking proxy implemented on an external (trusted) uC, not directly connected to the host processor.

It should be pointed out for completeness, that a GPS receiver (if fitted to the laptop), while a one-way radio device, should also be fitted with a kill switch, for the reasons discussed above.

The audio and camera devices

The audio and video (camera) devices can compromise user's privacy similarly to the above discussed wireless devices. In addition to the obvious threats posed by these devices, it's perhaps worth mentioning a possibility of using the mic and the camera not only to sniff the conversations in the room where the laptop is kept, but also to allow the attacker to sniff the user's disk and login password. Also, it seems possible, in theory at least, for the malware to use the speakers to

[10] Although the adversary might use e.g. the user's phone as a relaying device