There are two ways how to solve the above problems:

1. Get rid of the hard disk, and rely on external storage only (perhaps also implemented on the Trusted Stick) connected e.g. through USB or SD protocols. Of course this solution is neither elegant nor convenient. Also an internal disk will always excel in terms of speed and capacity for a given cost.

2. Use an internal disk with *trusted* firmware satisfying the requirements discussed in the next section.

The trusted internal hard disk requirements

The first requirement for using an internal disk would be for it be flash-less, of course. The disk uC would need to obtain its firmware from the trusted stick, just like the EC described above is expected to do that.

Additionally, the firmware that would power the disk would need to be *trusted* (this is in contrast to e.g. the ME firmware which we do not assume to be trusted!). Trusted, to do a few things:

1. Implement reliable read-only protection for select partitions on the disk (e.g. those containing the /boot and root filesystems),

2. Implement reliable transparent encryption for anything that is ever written to the disk. In other words make it impossible (e.g. for the malware in the ME or on the host) to store anything on the disk that would not be encrypted with a *user* controllable key. This requirement has an added advantage that wiping of all the user data on the disk can be implemented by simply throwing away the encryption key, something that could be done very quickly and easily.

The above requirements demand, in practice, the disk hardware to be of open-hardware design, running open-firmware. Fortunately it appears significant work has already been made in this area [15], which should be a good starting point.

It should be reiterated here the requirement for the trusted internal disk is an optional one, and it is envisioned that meanwhile an external disk could used, ideally integrated into the Trusted Stick.