Chapter 4

The Trusted Stick

The Trusted Stick, a small device of a "USB stick" or an SD card form factor, is an element that the user always carries with themselves and which contains all the "state" for the platform. This includes the (encrypted) user files and platform configuration. It also is expected to carry all the software and – what is unique as of today – firmware for the platform, and also enforce read-only'iness of these.[1]

As the name suggests, it is assumed the device is to be *trusted*. In other words, should this device malfunction (due to a bug in its own firmware), or get compromised by the attacker somehow, the security of the user data is in jeopardy.

It is thus expected this device should be as simple as possible to assure it's reasonably secure, and also to make it possible for various vendors, ideally by users themselves, to be able to build it. It goes without saying the device should be an open-source, open-hardware device. The author believes there is no excuse for entrusting proprietary products with such important things as ones digital life.

We are now considering what functionality should the Trusted Stick implement.

Firmware Storage

First of all it should provide read-only (from the host perspective at least) storage for all the platform firmware. This includes the Intel ME, the BIOS (including any blobs it might depend on, such as the FSP, ACMs, etc.), any of the standard

[1] A mechanism for updating the software and firmware on the stick should be explicitly under the control of the user. One can easily imagine this to be implemented using a physical switch on the stick, i.e. something that software could not be able to interfere with.