It's worth stressing that modern computer architectures make it very hard, sometimes impossible, for the user to inspect what firmware has really been programmed into the flash memory on the platform[2]. This is especially true for any so called tamper-proof chips. The use of such "secure" chips on endpoint computing devices should be avoided at all cost (see also discussion at the end of the paper). Any tamper-proof electronics on client systems should be considered harmful to the user as they jeopardize any form of transparency or verification.

[2]Indeed, by merely asking a flash-hosting device, such as the SPI flash chip, or some other u-controller such as one used on a NIC, to tell us what firmware it has inside, we can only get as trustworthy a response as is the device itself, or worse even: as is the current firmware that is used to serve our request... A classic chicken and egg problem.