Chapter 10

Summary

Personal computers have become extensions of our brains. This symbiosis is only going to strengthen in the years to come, and not just metaphorically! The author believes it should be paramount for humankind to ensure we can trust our personal computers. Unfortunately the industry does not seem to share this opinion. Not only do we not see much effort to create secure and trustworthy hardware and Operating Systems, but we also witness the introduction of technologies, such as Intel ME, that could undermine our trust in computers, (especially personal computers) more than anytime before.

The strict separation of state-carrying (trusted) element from the rest of the hardware, proposed in this paper, is an attempt to change this game in favour of the user. While this solution might appeal to many as simple and elegant, care should be exercised in understanding various implementation-specific subtleties, many of which, hopefully, have been discussed in this paper.

The author thinks this clean separation of state might be beneficial not just for Intel x86 systems, but also for other architectures of our future personal computers.