Chapter 9

Alternative solutions?

Many people voice concerns that perhaps a much better strategy is to ditch the (Intel) x86 platform, and look for an alternative architecture as a foundation for secure and trustworthy personal computers... In this chapter we quickly review what options we might have, in practice, here.

ARM-based platforms?

The ARM architecture [17] seems like a natural candidate to replace x86 for desktop computers, including laptops. Indeed it has already dominated the smartphone and tablet markets, and it doesn't seem like the gap in performance is that great between these devices. This indeed might seem like a plausible direction at first sight, but there are at least two problems here:

First, there is no such thing as an "ARM processor" – rather ARM releases only a set of specifications and other IP, which are then licensed by various vendors, such as NVIDIA, Samsung, Texas Instruments, and so forth. These vendors then combine the licensed ARM IP with their own, creating unique final products: the actual processors, customary called System-on-Chips (SoCs).

This large diversity of "ARM processors", while undoubtedly beneficial in some aspects, is also problematic – e.g. it presents multiple research targets for security researchers, as well as for system architects and developers. E.g. some of the SoCs would implement IOMMU functionality adhering to the ARM-published specification, while others would use a completely different technology, invented by the OEM that makes the SoC [4].