Chapter 1

Introduction

Modern Intel x86-based endpoint systems, such as laptops, are plagued by a number of security-related problems. Additionally, with the recent introduction of Intel Management Engine (ME) microcontroller into *all* new Intel processors, the trustworthiness of the Intel platform has been seriously questioned.

In a recently published paper [10] the author has presented an in-depth survey of these topics. In this paper the author proposes what she believes might be a reasonable, practical and relatively simple solution to most of the problems.

The main principle introduced below is the requirement for the laptop hardware to be *stateless*, i.e. lacking any persistent storage. This includes it having no firmware-carrying flash memory chips. All the state is to be kept on an external, trusted device. This trusted device is envisioned to be of a small USB stick or SD card form factor.

This clean separation of state-carrying vs. stateless silicon is, however, only one of the requirements, itself not enough to address many of the problems discussed in the article referenced above. There are a number of additional requirements: for the endpoint (laptop) hardware, for the trusted "stick", and for the host OS. We discuss them in this paper.

The author thinks the solution proposed here is not limited to solving the Intel-specific challenges and might be useful for other future platforms also.

Those readers who can't help but think that the (Intel) x86 is an already a lost battle, and that we should be moving to other architectures, are advised to have a look at the end of the paper where such alternatives are quickly discussed, and then... potentially jump back here to continue reading.