Using Hypervisor-Technology for Safe and Secure IoT Devices

Name Mehmet Özer

Abstract text

Hypervisor technology as an IT solution is a broadly accepted and a wide spread technology. The main driver for using a hypervisor is the ability to consolidate multiple systems on one hardware platform and to optimize the usage of the available computing power by balancing out the resource requirements of each running subsystem. The idea of virtualization has been developed by IBM in the early 70th of the last decade and has now manifold implementations beginning from binary translation, para-virtualization and hardware-virtualization. The Virtualization platform can be on operating system running on the hardware (type-1 hypervisor) or run as an application on a COTS operating system (type-2 hypervisor).

Hypervisor technology in the Internet of Things market place is a proven technology for safety and security critical applications requiring safety and security certification. The avionics industry has adopted this technology for their Integrated Modular Avionics (IMA) based safety systems since nearly two decades. The automotive sector uses hypervisor technology for ECU consolidation automated drivers assistance systems (ADAS) and Railway Technology benefits from the mixed criticality capabilities of a hypervisor to consolidate applications of different criticality on one hardware platform. In the security domain hypervisor technology is used to design security critical devices (such as smart meter gateways), which must adhere to the strict requirements of the IEC 15408 (Common Criteria).

The big advantage of a hypervisor over all markets is the ability to be perfectly suited for safety and security requirements. The safety and security of a hypervisor relies on the concepts of temporal and spatial separation, but specifically for safety applications the real-time behavior and determinism of the hypervisor is evident. In order to bring a system into a safe state, the operating system has to react in a guaranteed time without any compromises. Most popular type-2 hypervisor implementations like VirtualBox, VmWare etc. provide an execution environment to run a commodity operating system like Windows or Linux on top of another Windows or Linux OS that is usually called host-OS. These hypervisors depend on the functionality and assurance of that host-OS. These implementations have been developed for performance-oriented virtualization. Thus, safety and security aspects as well as assurance needed for certification have been not considered.

A separation kernel based type-1 hypervisor follows a highly modular approach with least-privilege and minimal trusted-code base principles. It consists of a microkernel, which ensures the basic resource management. Such a hypervisor focuses on separation, i.e. controlled information flow and separation of criticalities, with a possibility for full isolation. The modular design of a separation kernel hypervisor enables treating safety critical requirements for hard-real-time and worst-case execution at the hypervisor design level.

Thus, safety and security requirements and assurance can be coherently answered and created in one single product. This paper will explain the general concept of hypervisor technology and dive into deeper aspects of separation kernel based hypervisor. We will elaborate on the aspects how hypervisor technology addresses safety and security requirements of IoT devices.