HASPOC: Secure virtualization on ARMv8

Name Rolf Blom

Abstract text

The open-source HASPOC platform employs virtualization to provide strong isolation between guests for ARMv8 multicore systems. Guests enjoy exclusive access to cores and peripherals, as well as controlled inter-guest communication. For high assurance in a pervasive security, the solution is trust anchored by a secure boot, is prepared for Common Criteria evaluation (EAL6), and is formally verified on machine code level. The proven properties guarantee isolation equal to guests executing on physically separated platforms.

With less than 128 KB footprint the HASPOC platform is very small and efficient. The secure boot performs slightly better than the standard ARM Trusted Firmware Boot, while the included hypervisor incurs a minimal performance penalty. Different flavors of Linux guests (Debian, Ubuntu, Android) have been tested.

HASPOC is applicable in – for instance – secure mobile phones, crypto equipment, mobile networking, SCADA, vehicular, avionics and medical systems, cloud application platforms, and the IoT.