High Assurance Security Products on COTS Platforms

Rolf Blom, Senior Researcher in the Security Lab at SICS Swedish ICT
Oliver Schwarz, Researcher in the Security Lab at SICS Swedish ICT

With commodity operating systems failing to establish unbreakable isolation of processes, there is a need for stronger separation mechanisms. A recently launched open source project aims at applying virtualization to achieve such isolation on the widespread embedded ARM architectures. Strong assurance is established by formal verification and common criteria certification. Coexisting guest systems are able to run unmodified on the multicore platform, in a resource and cost efficient manner. The solution is rounded anchored in a secure boot process.

Today we see that governments, big organizations and authorities are increasingly starting to require independent verification (certification) of claimed security properties of deployed products and systems. For IT-solutions a well-established method is to use the Common Criteria (CC) (ISO 15408) framework and certify products according to defined and internationally recognized security requirements and assurance levels. The CC addresses protection of assets against unauthorized disclosure, modification, and loss of use.

The High Assurance Security Products on COTS (commercial of the shelf) Platforms project (HASPOC) is targeting a security solution for use in embedded systems, i.e. a trusted, cost and resource efficient virtualized commercial-off-the-shelf platform, which should have proven and Common Criteria certified security properties. The project is led by SICS Swedish ICT and carried out together with a consortium including Ericsson Research and KTH, the Royal Institute of Technology. The key feature offered by the platform is guaranteed isolation between different users and services running on it and their associated information. The isolation is provided by a formally security verified boot and hypervisor solution. Background on the design of a hypervisor for isolation can be found in [1].

The COTS platform selected for HASPOC is an ARMv8-A based multicore system on a chip of the form indicated in Figure 1. The HASPOC developed hypervisor takes advantage of the available hardware virtualization support (MMU, S-MMU, etc.) and is in principle a bare metal solution running essentially unmodified guests. The hypervisor will support Linux as guest OS. The solution will be released as open source; the boot solution under a GNU GPL v.2 license and the hypervisor code under an Apache v.2 license.

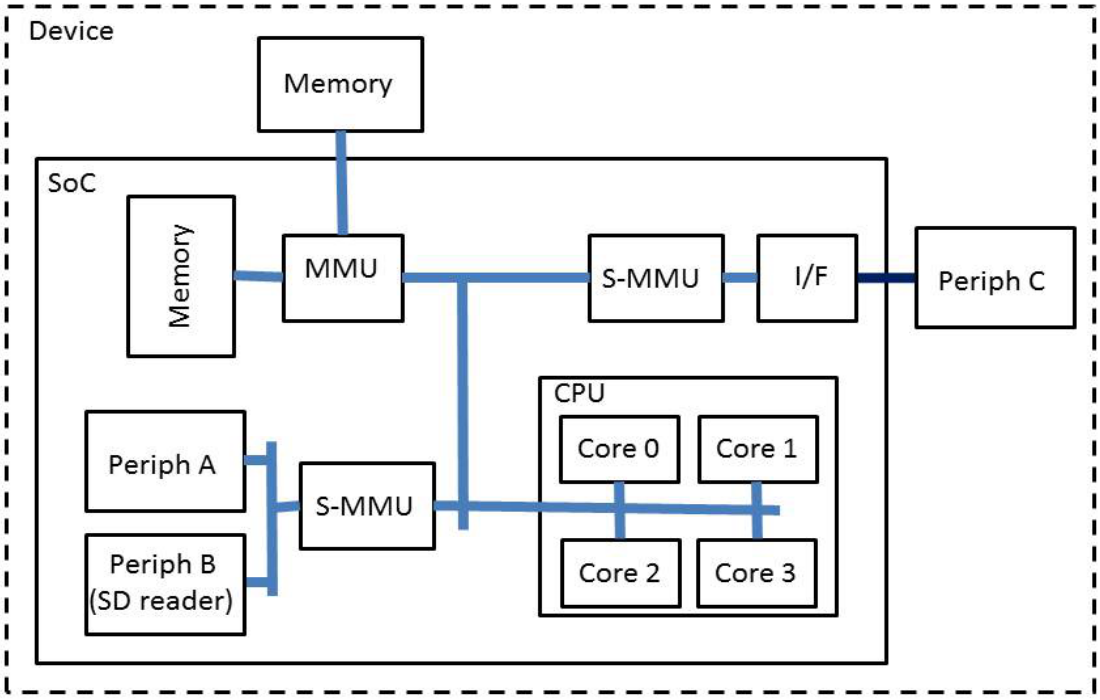

Figure 1: High level view of HASPOC compliant system on a chip.

The platform security solution is supported by trust anchoring and boot solutions developed by project partner T2 Data. The hypervisor builds on the SICS Thin Hypervisor (STH) for ARMv7, which in a joint KTH-SICS project PROSPER has been studied regarding the formal verification of its security claims (isolation properties). These existing solutions will be enhanced and modified to cover the new technology offered by the ARMv8 platform, product requirements and requirements for achieving high assurance level (EAL 5/6) Common Criteria evaluations.

The project will also produce baseline documents needed for a formal CC evaluation at EAL 6, i.e. a Security Target and supporting documentation needed in the evaluation process. The idea is that these baselines documents can be used as a starting point when a product based on the HASPOC platform should be CC certified. The project itself will not perform a formal CC evaluation as it will not develop a specific product.

In the formal verification process we create a mathematical and machine checkable proof that guests executing in coexistence on the HASPOC platform behave in the same way as if each guest runs on its own machine. This guarantees isolation relaxed by desired and controlled inter-guest communication. With hardware taking over more and more virtualization tasks, the formal verification of separation platforms departs from a pure software verification towards an integrated verification of hardware architectures, their isolation mechanisms and their interaction with software. The principles behind the formal verification work are described in [2].

Demonstrators in the secure communications area (encryption solutions with strict red/black separation) will be built within the project framework to test and demonstrate the efficiency and usability of the platform solution. This is an excellent test area as its security requirements are strict and high, while at the same time there is an increasing demand for new generations of High Assurance security products with increased functionality resulting in a corresponding need to find tools to enable agile product revisions. By the introduction of trusted components like the HASPOC platform in product development, a decrease in lead time from user requirement to developed, evaluated and deployed solution can be realized.

The developed technology will, in addition to specific security products like crypto equipment, secure mobile phones and firewalls, be applicable in a wide range of areas like SCADA systems, mobile communication networks, vehicular, avionics and medical systems, and also for devices in the Internet of Things (IoT). Particularly interesting areas in the industrial sector are issues around mixing personal and enterprise information in the same user device (e.g. a laptop), cloud computing (allowing tenants to share pooled resources) etc.

References:

[1] Affordable Separation on Embedded Platforms: Soft Reboot Enabled Virtualization on a Dual Mode System, *Oliver Schwarz, Christian Gehrmann and Viktor Do.* Proceedings of Trust and Trustworthy Computing (TRUST) 2014.

[2] Formal Verification of Information Flow Security for a Simple ARM-Based Separation Kernel *Mads Dam, Roberto Guanciale, Narges Khakpour, Hamed Nemati and Oliver Schwarz* Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (CCS'13).

Links:

The HASPOC project:	https://haspoc.sics.se/
The PROSPER project:	http://prosper.sics.se
ARM Architecture	http://www.arm.com/products/processors/instruction-set-architectures/index.php
CC; Common Criteria	https://www.commoncriteriaportal.org/

Please contact:

Rolf Blom, SICS Swedish ICT
tel: +46 70 3251906
e-mail: rolfb@sics.se