David Loosli

Graduate Candidate	David Loosli
Examiner	Prof. Dr. Andreas Steffen
Co-Examiner	Dr. Ralf Hauser, PrivaSphere AG, Zürich 32 Zustellung, ZH
Subject Area	Security

Muen on ARM

Muen on ARM

Introduction: The Muen Separation Kernel (SK) is a specialised microkernel developed as a platform for high-security systems at the University of Applied Sciences Rapperswil (HSR). Muen ensures a strict and reliable isolation of components and separates security critical functions against unreliable software running on the same physical system. The programming language SPARK 2014 is used to achieve a particularly high degree of trustworthiness. The Muen SK was developed specifically for the Intel x86/64 architecture and uses the Intel VT-x and VT-d technology to separate the components.

Objective: This bachelor thesis implements the main building blocks of a separation kernel for the ARMv8-A architecture, leveraging in particular the recently introduced AArch64 Virtualization Extensions. This practical study builds on the findings of the student research feasibility study also written by the author of this paper that investigated the theoretical and practical aspects of porting the Muen SK to the ARMv8-A architecture. The target hardware platform chosen for this study is the NXP LS1012A FRDM Board.

Result: Using a Segger J-Link hardware debug probe device, the on-chip debugger software OpenOCD and the AdaCore toolchain including their integrated development environment, essential parts of a separation kernel have been implemented in Ada in the course of the project. With this basic SK prototype and its two differently configured subjects, it could be demonstrated that all requirements with respect to the porting of the Muen SK to the ARMv8-A architecture can be met applying the already examined ARMv8-A architecture design principles.