David
Loosli

Student	David Loosli
Examiners	Prof. Dr. Andreas Steffen, Adrian-Ken Rüegsegger
Subject Area	Security

Muen on ARM - an Evaluation

Portability of the Muen Separation Kernel to the ARMv8-A Architecture

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 protects critical security 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 feasibility study investigates the ARMv8-A architecture and in particular the AArch64 Virtualization Extensions introduced with the latest ARM architecture and evaluates how this technology could be used for porting the Muen SK to ARM. In order to be able to achieve this, the mechanisms used by Muen SK are first examined in detail. Based on this investigation, the requirements for a target processor architecture are derived and compared with the features provided by the ARMv8-A architecture. Since the target hardware platform for this study is the Raspberry Pi 3, the requirements declared as "implementation defined" by the ARM documentation are finally assessed with respect to this System on Chip designed by the Raspberry Pi Foundation.

Result: While the ARMv8 architecture and the ARMv8 Virtualization Extension principally can be considered suitable for porting the Muen SK, the risk for choosing the Raspberry Pi 3 as the target platform seems too high, especially without any further investigations. The main reasons against the Raspberry Pi 3 are the absence of a documentation on the AArch64 execution state as well as the missing implementation of the Generic Interrupt Controller and the System Memory Management Unit interfaces specified by ARM.