Hiwi, IDP, Research Internship

Hypervisor-based Virtualization for ARM Embedded Devices

The NXP i.MX8 based embedded systems are widely used for various applications in automotive and industry. The underlying ARM Cortex-A 64-bit processor architecture includes hardware extensions for virtualization support, which can be utilized to run multiple operating systems on one device in a secure and efficient manner.

Task Description

The goal of this project is practical implementation and evaluation of novel security concepts based on hardware-assisted virtualization technologies for ARM 64-bit powered high-end embedded devices, such as NXP i.MX8. Virtualization technologies can be utilized to isolate critical components and build a foundation for runtime integrity verification and anomaly detection by means of virtual machine introspection.

The particular tasks include the following:

- Literature and current state of research review with regard to the utilization of hypervisors for embedded devices.
- Setup and evaluation of various hypervisor solutions on ARM64 based embedded platforms.
- Design and implementation of security architectures and concepts based on virtualization.

Prerequisites

- High motivation and ability to work independently
- Experience in embedded software development, e.g., Yocto toolchain
- Very good system programming skills in C/C++
- Experience or at least theoretical knowledge in hypervisor technologies

Contact

Monika Huber
Telefon: +49 89 322-9986-148
E-Mail: monika.huber@aisec.fraunhofer.de

Mykolai Protsenko, Dr.-Ing.
Telefon: +49 89 322-9986-192
E-Mail: mykolai.protsenko@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Secure Operating Systems
Lichtenbergstraße 11, 85748 Garching (near Munich), Germany
https://www.aisec.fraunhofer.de

Date of publication: December 21, 2020