Deploying Unikernels in Unsecure Environments (AISEC)

Driven by smart manufacturing there is a growing trend towards new tooling machines. Machines are not sold but rather provided to the customer, with the manufacturer retaining ownership. To manufacture parts, the customer is allowed to program the machines with their own parameters or control algorithms. As the parameters or control algorithms may contain the customer’s intellectual property, it is in their interest that the machine manufacturer does not have access to them. In this topic, we want to evaluate whether unikernels can be used to securely deploy control algorithms. Unikernels have been introduced as a new paradigm for virtualization in the cloud environment, as they offer fast execution and a reduced trusted code base. Thus, in turn, increasing the security by reducing the attack surface.

Prerequisites

Task Description
Your task will be to gain and understanding of unikernels (especially unikernels based on Unikraft) and explore how they can be utilized within the scenario described above. In particular, you will be looking into securely deploying, booting, or executing unikernels. Based on this evaluation, ideas and proposals can be implemented. Requirements
- Basic knowledge of IT security
- Basic knowledge of virtualization, embedded systems and programming
- Interest in learning manufacturing engineering topics
- Structured thinking and ability to work self-directed and systematically

Contact

Product Protection and Industrial Security
Mail: chi.hieu.ta@aisec.fraunhofer.de
Phone: +49 89 322 9986-1049
Mail: nikolai.puch@aisec.fraunhofer.de
Phone: +49 89 322 9986-142

Fraunhofer Institute for Applied and Integrated Security (AISEC)
Lichtenbergstr. 11, 85748 Garching near Munich

Publication Date: 11.03.2024

Advisors

Georg Sigl
Chi Hieu, (Herr/Mr.) TA + Nikolai Puch (Fraunhofer AISEC)