System Security
Constructor University
Dr. Jürgen Schönwälder

Module: MCSSE-CYB-02
Date: 2025-04-04
Due: 2025-05-02

Problem Sheet #6

Problem 6.1: *trace file open calls using ebpf* (2+2+2+2+2 = 10 points)

The goal of this problem is to trace file open calls by installing an eBPF program into the Linux kernel. You are expected to use the Aya eBPF library for the Rust programming language, following the example discussed in class. The task can be broken down into the following steps:

a) Setup Rust and Aya and the aya-tool as described in the Aya documentation.

b) Create a project using `cargo generate https://github.com/aya-rs/aya-template` that hooks on the `file_open` LSM hook.

c) Using the `aya-tool`, generate a Rust interface for the `file` data structure used by the Linux kernel.

d) Extend the eBPF code to display the names of the files opened by the kernel. Helper functions like `bpf_probe_read_kernel_str_bytes()` may be useful for the conversion of C strings to Rust strings.

e) Document which files are opened when you execute the shell commands `id` and `date`.