Design and implementation of a secure hypervisor with Rust

Mathieu Bacou  Olivier Levillain  Gaël Thomas
François Trahay

2020-2021

Despite our current knowledge on safe programming languages, most modern operating systems are still written using unsafe languages such as C or C++. One reason is that safe languages are usually not deemed fit for real-world use-cases, especially when efficiency is considered important.

However, the Rust programming language, developed by Mozilla since 2010, seems to open new horizons in the domain. Rust is indeed a safe language which allows very efficient programming (because of a very efficient and smart compiler on one hand, and because it allows for safe and mostly zero-copy parallelism) and which can be easily integrated with other languages such as C and C++. For example, Mozilla has been reimplementing parts of its browser in Rust for several years now, which helped improve the overall security.

Redox is an open-source operating system written in Rust, aiming at providing a partial POSIX implementation in a secure manner. The goal of this project is to design and implement a tiny hypervisor in Rust to assess its feasibility and to evaluate the security gains one might imagine with a safe language. For the parts that will have to be written outside Rust guarantees (in so-called unsafe blocks), it will be important to understand and express the assumptions that needs to be verified for the overall software to be safe.

Milestones

Here are important milestones that should be met during the project:

- learn the Rust programming language;
- compile Redox and have it run in qemu;
- (ideally) contribute to Redox a simple feature or a bugfix;
- write a minimalist OS/hypervisor in Rust and have it run in qemu;
- provide a reproducible and sharable development environment for this software;
- add features to aim towards a real hypervisor.
Prerequisites

To work on this project, the following skills are required:

- basic knowledge of operating systems;
- fluency in a programming language (ideally Rust, C or C++);
- notions in software engineering.

Logistics

The project will take place in Télécom SudParis labs in Palaiseau.
Applications should be directed at ???@telecom-sudparis.eu.

Bibliography

References
