Provably Secure Separation Kernel

Henrik Karlsson (henrik10@kth.se)
Supervisor: Mads Dam
Co-Supervisor: Roberto Guanciale

Abstract

A typical operating system consists of thousands of complex components that interact in unpredictable ways. The result is bugs and security holes, some of which allow adversaries to gain complete control of a remote system. These vulnerabilities are unacceptable for safety- and security-critical applications where lives can be at stake, and for this reason, we use separation kernels.

A separation kernel partitions a system into isolated domains that can only communicate through designated channels. The separation kernel simplifies the system, letting us isolate faults and analyze the components in isolation. However, properly building a separation kernel is hard, and for this, we need rigorous techniques known as formal methods.

In this project, we are developing a new family of separation kernels for RISC-V and new efficient methods for their verification.