CHAIR OF CYBER-PHYSICAL SYSTEMS IN PRODUCTION ENGINEERING

System Monitoring via GDB Protocol

Point of Contact: Alex Züpke
alex.zuepke@tum.de

Type: Bachelor or Master

Description:

Design a monitoring software for an embedded operating system kernel or hypervisor. The monitoring software runs on the development host system (i.e. x86 Linux) and uses a *memory read primitive* provided by a hardware debugger or by a debugger software component running on the embedded system to read and display status information from a live system (like "ps" in Linux). To infer the addresses of data of interest, the monitoring software shall use the debug information which is provided in the ELF binaries of the software running on the embedded system.

The goal for a bachelor thesis would be to develop a prototype application that reads and displays the task activities of an RTOS kernel running on QEMU using the builtin GDB-stub of QEMU.

For a master thesis, the goal is to design a software architecture that allows to apply the technique recursively to monitor the different layers in a hypervisor platform, e.g. display the internal state of an application on top of Linux on top of the Jailhouse hypervisor. This requires address translation mechanisms, i.e. scanning of page tables.

Requirements: Linux, Socket Programming, C/C++, Python/Ruby/Java/...

Chair of Cyber-Physical Systems in Production Engineering,
Technical University of Munich (TUM),
Boltzmannstr. 15, 85748 Garching b. München

https://rtsl.cps.mw.tum.de/theses