Using Intel Processor Tracing (for Runtime Monitoring)

Modern Intel CPUs write trace data to their RAM for the purpose of debugging. This trace data can be used to monitor the program running on the CPU without interfering with the program. This thesis is about exploring this technology and how it can be used runtime monitoring of Intel CPUs.

Non-invasive Runtime Monitoring Classical monitoring and testing techniques all involve some kind of instrumentation. This is needed to gather information about the running program, but certain bugs are hard to find if you modify the source code. So called Heisenbugs are characterized by the fact that they disappear if you add debug statements to the source code in order to find them. To overcome these problems we are developing non-invasive monitoring of CPUs by using CPU debugging facilities, which allow monitoring without code instrumentation.

Intel equips all modern CPUs with a new debugging facility that writes trace data to the RAM at runtime: "Intel Processor Trace is a low-overhead execution tracing feature that [captures] information about software execution on each hardware thread using dedicated hardware facilities so that after execution completes software can do processing of the captured trace data and reconstruct the exact program flow."
[1]

This trace data can be extracted using the Intel Processor Trace decoder library available on GitHub[1].

Problem Statement This thesis is about exploring this new technology and evaluating how it can be used for runtime monitoring of CPUs. Questions to address are:

– How to use Intel Processor Tracing at all?

– How to retrieve the logged trace data with the Intel Processor Tracing decoder library?
– How to trigger Inter Processor Tracing recording? What can be used as trigger?

This proposal can lead to a bachelor or master thesis. In a master thesis additional the following questions should be addressed:

– How to use Intel Processor Tracing for online monitoring?
– How to pass the data generated by Intel Processor Tracing to an FPGA used for monitoring via PCI Express?
– How to decode the data generated by Intel Processor Tracing on an external FPGA at runtime?

Requirements You are

– able to program in C,
– interested in low level processor architecture and
– capable of making things work in real-world applications.

COEMS The COEMS project is a European project with international academic and industrial partners from Norway, Romania, Austria and Germany. This thesis can be done in combination with an ERASMUS stay in Norway.

Literature

[1] James R., Processor Tracing, September 18, 2013, https://software.intel.com/en-us/blogs/2013/09/18/processor-tracing

---

[1] https://github.com/01org/processor-trace