Master Thesis – Guided Fuzzing in K8s

Background
In the last few years fuzzing has gained traction as a useful tool to find bugs and improve security.

Guided fuzzing is a way to control the fuzzing in a way that improves the efficiency by choosing a valid scope in the given context.

Thesis Description
Are there methods and tools available that make this feasible on a microservice level in cloud environments?

One example of a tool is “American Fuzzy Lop” (https://en.wikipedia.org/wiki/American_fuzzy_lop_(fuzzer))

The following steps are envisioned as part of the thesis work:

- Investigate how guided fuzzing could be used for some selected interfaces in a 5G RAN system
- Investigate and compare tools available to enable guided fuzzing

The thesis will be concluded with a result presentation for the Ericsson team.

Qualifications
This project aims at students in electrical engineering, computer science, computer engineering or similar. Background in wireless communication is preferred.

Extent
1-2 students, 30hp each

Location
Ericsson AB Mjärdevi, Linköping

Preferred Starting Date
Spring 2022

Contact Persons
Christer Lindell
+46 730 43 55 33
crister.lindell@ericsson.com

Johan Wibeck
+46 730 43 65 22
johan.wibeck@ericsson.com