Master's thesis: Fuzz Testing an IoT Operating System using Hardware Emulation

We are looking for a dedicated Master's student to join us in the Connected Intelligence Unit at RISE.

The Connected Intelligence Unit is part of RISE Computer Science in Stockholm. The current research focus is on the Internet of Things. Among the group's key technologies are the Contiki-NG operating system, uIP stack, ContikiRPL, SICSLoWPAN, and the COOJA network simulator. The unit conducts projects together with industry and academic partners from Sweden and across the world.

Thesis Description

Fuzz testing has emerged as an efficient method to find bugs and vulnerabilities in software. In recent years, fuzz testing has been applied on IoT operating systems with several successful fuzz testing campaigns to find a variety of vulnerabilities in communication stacks. A limitation of the fuzz testing has been that the test target; I.e., the IoT operating system, has been executed in native mode, meaning that it executes as a regular application in a host operating system. Hence, several hardware-dependent parts of the operating system, such as protocols at lower layers in the network stack and device drivers, have not been tested to the same extent.

In this project, you will be fuzz testing an IoT operating system executing in the Renode emulator by Antmicro. Renode can emulate IoT devices that are supported by IoT operating systems such as Contiki-NG, RIOT OS, and Zephyr OS. The base functionality for fuzz testing with Renode has been recently implemented and will be the starting point for the project. The three main tasks of the thesis project are the following:

Task 1: Implement functionality to fuzz test different parts of an IoT OS that are not easy to fuzz test using regular fuzzing on the native platform, e.g., including communication with SoC peripherals. This work involves setting up a fuzz testing harness in the IoT OS and customizing the fuzz testing scripts for the Renode emulator.

Task 2: Run fuzz testing experiments using the functionality from Task 1, and investigate whether bugs can be found in different software modules.

Task 3: Evaluate the code coverage and potential optimizations of fuzz testing using the hardware emulator. Optimizations may include techniques such as analysis of stateful vs stateless workflows, pre-setting of the simulation state and others.

Terms:

- Start Time: January 2024
- Scope: 30 hp
- Location: RISE Computer Science, Kista, Stockholm

Who are you?

We expect you to have a good knowledge of C programming and embedded systems. It is also a merit if you have worked with software testing.

Welcome with your application!

If this sounds interesting and you would like to know more, please contact Nicolas Tsiftes, phone +46 707349247 or Joakim Eriksson, phone +46 102284364.

You can apply for the position at https://www.ri.se/en/work-with-us/open-job-positions/masters-thesis-fuzz-testing-an-iot-operating-system-using-hardware

Applications should include (1) a brief personal letter, (2) a CV, and (3) a recent grade transcript. Candidates are encouraged to send in their application as soon as possible, but at the latest by December 1, 2023. Suitable applicants will be interviewed as applications are received.

Master's thesis, Contiki-NG, Fuzz Testing, Embedded systems, Emulation, Renode, Internet of Things, RISE, Stockholm