Master’s thesis: Fuzz Testing System for Contiki-NG

Overview
Contiki-NG is an open-source operating system for Internet of Things devices developed partly by RISE Research Institutes of Sweden [1]. To make sure that Contiki-NG maintains a good quality over time, it is tested using a regression test framework. An important aspect not covered with the existing tests is security. In recent years, fuzz testing has been used increasingly to find vulnerabilities by mutating inputs to trigger crashes or hangs. Hence, as part of an effort to improve the security of Contiki-NG, this thesis project extends the Contiki-NG tests with fuzzing.

Description
There are three main parts of the thesis project:

- Design and implement a fuzz testing framework that will be to integrate with the existing test framework for Contiki-NG. The fuzz testing should cover various protocol implementations in the network stack primarily, but can also be extended to other software modules. At least two existing fuzz testing tools should be supported.

- Develop a web UI that presents fuzz testing statistics for different Contiki-NG versions. The UI will track fuzzing results over different versions of Contiki-NG.

- Evaluate the achieved code coverage of the fuzz testing, and compare it with the code coverage of the existing Contiki-NG tests.

The expected outcome of the implementation is a fuzz testing tool that can be applied before each Contiki-NG release to discover bugs and possible security vulnerabilities.

Time plan
The following table shows an estimate of the required time for each task of the project. The thesis writing should preferably be spread out over the project.

<table>
<thead>
<tr>
<th>Activity</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background study of Contiki-NG and fuzz testing</td>
<td>4 weeks</td>
</tr>
<tr>
<td>Design &amp; implementation of fuzz testing system</td>
<td>6 weeks</td>
</tr>
<tr>
<td>Development of test statistics UI</td>
<td>3 weeks</td>
</tr>
<tr>
<td>Evaluation</td>
<td>2 weeks</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Thesis writing</td>
<td>5 weeks</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>20 weeks</strong></td>
</tr>
</tbody>
</table>

**Competence**
We are looking for a bright M.Sc. student with who has fulfilled the course requirements. Good programming skills are required, preferably with embedded software experience, as is good spoken and written English.

**Application**
Applications should include a brief personal letter, a CV, and a grade transcript. Candidates are encouraged to submit their application as soon as possible. Suitable applicants will be interviewed as applications are received.

**Start time**
As soon as possible.

**Location**
RISE SICS in the Electrum building in Kista.

**References**

**Contact**
Dr. Nicolas Tsiftes <nicolas.tsiftes@ri.se>