Project 5 : Fuzzer of your choice

March 15, 2017

In the last project we want you to be creative and work on a fuzzing approach of your own choice. You will choose an accessible domain and subjects that are easy to test and does not require a large tool chain, come up with a plan for applying fuzzing techniques, try to implement the proposed techniques and evaluate their effectiveness.

Hints

As a hint to help you with your search for domains and subjects you might want to look for open source projects that offer a version history and a bug tracker. You can use older versions with known bug, in order to prove that you would have been able to find them.

1 Proposal

Before you commit to an approach of your choice we want you to write a proposal of up to one A4 page that specifies the domain and subjects you want to apply your technique to. This proposal must also contain a multi-step strategy for applying fuzzing to this domain and a plan to implement and evaluate this strategy. The deadline for this proposal is on 20.03.2017 at 12:00 (noon). The submissions must be made as PDF file by email to `security-testing-2017-staff@lists.st.cs.uni-saarland.de`.

Example for a project idea

As an example you could decide to fuzz HTTP servers like Apache. As a multi step strategy we could consider to try three techniques, where the first one is the most complicated and systematic way to generate tests and the subsequent approaches are increasingly generic but might therefore be not as effective but easier to implement. This allows you to fall back to a simpler strategy if the more complicated previous strategy did not work.

- **Plan A:** Grammar based generation of HTTP requests using a grammar/specification
- **Plan B:** Random mutation of a set of provided valid HTTP requests
- **Plan C:** Generate random strings

2 Implementation and Evaluation

After you have submitted your proposal and received positive feedback on the following day, you will follow your plan to implement and evaluate your fuzzing approach. You will document this process together with evaluation results and a conclusion on the effectiveness of your fuzzing strategy in a final report of 2 to 4 A4 pages. The deadline for this report is on 31.03.2017 at 23:59. The submissions must be made as PDF file by email to `security-testing-2017-staff@lists.st.cs.uni-saarland.de`.