Software Reversing Lab 2 – State Machines

You are asked to apply one of the state machine learning to a program of your choice. This can be a piece of code one of you developed, an open source project, the RERS problems, a network protocol, a user-interface (for instance a webpage or android app). You should recreate one of the experiments performed in a paper/report such as:

De Ruiter, Joeri, and Erik Poll. "Protocol State Fuzzing of TLS Implementations." *USENIX Security*. Vol. 15. 2015.

Smetsers, Rick, et al. "Complementing Model Learning with Mutation-Based Fuzzing." *arXiv preprint arXiv:1611.02429* (2016).

Mobile Application Security: An assessment of bunq's financial app - http://repository.tudelft.nl/islandora/object/uuid:37e87645-09a3-4ace-b9b2-dad897292ac9?collection=education

You may select your own experiment to recreate from a paper/report/video/blog-post, or even do your own study, but you should confirm with Sicco Verwer that the topic is sufficiently challenging (message on Slack).

When deciding on an application, please keep in mind that one of the difficult steps in state machine learning is the definition of the alphabet (the mapping from symbolic inputs to concrete values such as packets and back again). Try to find an application for which this mapping already exists (e.g. from a paper), of is easy to develop. For instance for web pages it is very straightforward to create an alphabet using the Alex tool: http://learnlib.github.io/alex/.

You have to create a video of your application, clearly demonstrating how to implement the required steps, what results are obtained, and their meaning. Optionally, you may include a short description of the required tools that need to be downloaded and how to set them up, preferably in an md file format, similar to the hand-on sessions during the lectures.

Your video will be evaluated on the following criteria:

- Clarity of presentation
- Reproducibility of performed study
- Quality of performed study
- Difficulty of performed study
- Meaning of obtained results
- Extra credit for work added to existing study

You can get extra credit by for instance combining fuzzing and learning in new ways, integrating learning and model-based testing tools, or by applying it to difficult cases such as android/iOS applications or embedded devices.