Paper Summary Of Protocol state fuzzing of TLS implementations

Song Li(sol315)

October 21, 2015

1 Main Idea

This paper mainly uses LearnLib, SUT and many other methods such as improved W-method to test different TLS implementations. They use the state machine to judge if a implementation is in normal work status. They also do many detailed works to make their method can work for all nine implementations. Finally they found some security issues of 3 implementations.

2 Strengths

Different from the simple test cases and output analysis, they use state machine learning to analysis implementations. In order to finish their design, they used LearnLib. What's more, they improve the W-method to make it more useful to their works. The main strengths I think is they changed many exist tools and make these tools fit their works better.

3 Improvement

For a test on a specific aspect of TLS implementations, I think they have done a decent job. Maybe for those implementations which they can't detect any security issues, they can make the method they used like "W-method" become more difficult to pass. I mean, the stantard for different implementations should be different.

4 Future work

Using state machine learning and LearnLib is a good way to analysis a implementation. We can use this way to help many other areas such as web test and software test. Some tools like LearnLib should be developed in many other test areas.