Homework Exercise 2

ENGR 201, 2017

Dylan Chong - 300373593

Topic: Available methods for finding security issues in software

Palanivel and Kanmani [6] proposed a security testing process that adds the STRIDE threat modelling approach used by Microsoft to an existing risk analysis approach in order to select the highest priority tests from a generated test suite. This reduces the amount of time required to execute the test suite [6].

It can be broken down into four phases: State Representation, Threat Modelling, Risk Analysis, Test Case Selection. The State Representation phase involves the identification of states and transitions (i.e. dependencies between states) through the creation of an Extended Finite Machine diagram of the system. The Threat Modelling phase involves using a state diagram to create a data flow diagram, which is used with the STRIDE model to identify security threats are possible in each state of the system. (STRIDE is an acronym for six different type of threats - spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege.) The results from this phase are used and the Risk Analysis phase, where a risk value is calculated for each threat (using metrics such as risk impact - the number of (dependent) states the threat could affect). Finally, the tests that involve a high number of high risk states are selected from a generated set of test cases [6].

In comparison with the existing process, which did not use the STRIDE approach for threat modelling and used different metrics in the Risk Analysis phase, the proposed process yielded a three times greater total risk value; this implies that it identified a greater number of risks / identified a greater impact for the risks. The proposed process was successfully able to reduce the generated test suite size by 13-21% [6].

Bibliography (NOTE: Not formatted using IEEE)

[6] Risk-driven security testing using risk analysis with threat modelling approach, <https://springerplus.springeropen.com/articles/10.1186/2193-1801-3-754>

Question: When doing the summary, do you have to put the source ([6]) at the end of every sentence, or is at the end of every paragraph okay?