Critique on

Edward J. Schwartz, Thanassis Avgerinos, David Brumley. 2010. All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask)

Astha Sharma
asharma6@uno.edu

SUMMARY

According to the authors of this paper, the dynamic taint analysis and forward symbol execution are the most popular security analysis techniques among all the persisting ones. However, despite of their popularity, there are no significant efforts to define these method and report critical issues associated with their implementation. Therefore, the paper puts forward a language for demonstrating some of the critical aspects associated with dynamic taint analysis and forward symbolic execution. The authors here, have defined some operational semantics for the developed language with regards to the security analysis techniques under consideration. The challenges, techniques and tradeoffs encountered during the experiment are highlighted in the paper.

STRENGTH

1. The paper formally defines the algorithms and summarizes the critical issues associated with two most common dynamic analysis techniques in security research, wiz, dynamic taint analysis and forward symbolic execution.
2. The introduced solution could change the formal english descriptions into an algorithm - operational semantics.
3. The authors have put light on the associated challenges, techniques and tradeoffs.
4. The paper presents a very good description of the major topics of dynamic taint analysis and forward execution which is relevant to the research topic.

WEAKNESSES

- The authors have suggested to use heuristics as a solution to the control dependent taint, but didn't mention how to use it to solve the issue. No real world scenario is explained.
- They also did not mention about how they would address undertainted and overtainted inputs.
- Selection of the best execution path is still unclear.