Critique on
Bergeron, Jean, Mourad Debbabi, Jules Desharnais, Mourad M. Erhioui, Yvan Lavoie, and Nadia Tawbi. "Static detection of malicious code in executable programs."

Astha Sharma
asharma6@uno.edu

SUMMARY

The author of this paper presented an approach to detect malicious code in executable program which was based on semantic analysis of behaviour. The analysis was done on binary code and not the source code.The static analysis helps to predict the properties of the program behaviour without having to run them. The analysis is made in three major steps

The static analysis of a binary executable is achieved in three major steps: generation of intermediate representation, analyzing the data and control flow that captures security-oriented program behaviour, and finally, the static verification where the security policies are compared against the output of analysis phase.

STRENGTHS:

- Determines the properties of dynamic execution of the program without executing them.
- There's no runtime overload.
- This is a very interesting and useful paper for those working on static analysis of the executable programs for malicious code detection.

WEAKNESSES:

- The security policies are manual and not automated. And as a result, it can be time consuming and there are possibilities for error.
- There can be issues with scalability as the system is almost 20 years old and may not support large scale programs that exists today.
- The authors have not designed and defined a specific format of the inputting security policies.
- Not suitable for varying platforms.