Report

The purpose of this report is to explain the heuristic used in the implementation of the "sb" (squash bug) command. The command allows users to detect and track malwares by starting from a suspected process ID and displaying the parent, grandparent, and other ancestors of the process. The "-suggest" flag provides additional functionality that detects the root of all trouble based on a heuristic.

The Heuristic that we have chosen for the K part in this assignment is the follows ==>

(Total % CPU time of all children + the process / Number of children) * 0.01 > total CPU time of the Process.

- We have chosen such a Heuristic as we know that the Malware will have children and the average CPU usage of all the children is exceedingly high
- Also, we know that the CPU usage of the malware parent program is relatively very less compared to the average of all its children

Thus, we can represent both parts of this in our Heuristic; in addition, we know that the malware is the first process in the chain to show this behavior, thus we break after the first encounter of such a process.

In conclusion, the heuristic used in implementing the "sb" (squash bug) command is based on the assumption that malwares often consume more system resources and spawn more child processes than normal processes. The heuristic involves checking the time spent by each process and the number of child processes that a process has spawned to determine the root of all trouble. This heuristic can help users detect and track malwares in their systems.