Linux Processes' Memory Visualization

Tsvetkov, Vasilen

Linux processes’ memory visualization (MemVis) is a project which aims to facilitate the users who want easily to observe the memory of a currently running process and moreover to analyze it. Using this instrument the user can easily survey different errors related to the memory management and to simulate software attacks, for example, buffer overflows. At the time, alter- native utilities, allowing similar functionality are few, they do not provide graphical user interfaces and require deep technical competence of the user in debugging and low-level technical knowledge. Due to those circumstances, they are inaccessible to a beginner user who does not have the necessary skills to simulate that class of attacks and does not understand their impact. MemVis resolves this problem by providing a graphical instrument, for visualizing the memory of the chosen process, which does not depend on gdb or other such tools. After selecting the process, by writing its Process ID, the user will be dis- played information about its memory (e.g. the addresses of the stack, heap, etc.) and will be allowed to analyze ranges of memory. By building an inter- face and extending its functionality the procedure becomes more accessible for the common user. Furthermore, the user interface helps us to visualize the memory allocation step by step which could be crucial in a situation of understanding the impact of memory vulnerability. Using this tool, the user can gain insight in and debug memory-related issues with much more clarity and ease than current alternatives. For the implementation of the project, we used Python and python-ptrace for the back end and wxWidgets and wxPython for the front end.

Awards Won: