Seminararbeit

Lennart Hein, Kaywan Katibeh, Maurice Happe

7. November 2018

1 Exposé

Ein Debugger ist ein wichtiges Werkzeug für jeden Software-Entwickler. Er beobachtet jeden Befehl und lässt den Benutzer Fehler in ihrem Code erkennen. Um dies umzusetzen, muss man den Programm-Code Schritt für Schritt bearbeiten können.
Auf Linux Systemen wird der System Call sys_ptrace benötigt, um einen Debugger umzusetzen. Ptrace ermöglicht es einen Prozess einen anderen laufenden Prozess aktiv zu beeinflussen, indem break points gesetzt werden oder der Speicherbereich des getracten Prozesses verändert wird.
Ziel dieser Arbeit ist es einen Debugger zu schreiben, und diesen über eine GUI (graphical user interface) für den Benutzer zugänglich zu machen. Darauf aufbauend ist in der Arbeit [CreateRemoteThread in 32 Bit Linux] von [Name] ein Funktion für Linux vorgestellt, die die Windows Bibliotheksfunktion CreateRemoteThread für 32-Bit Architektur ermöglicht. Da die Architektur veraltet ist, ist es ebenfalls Ziel dieser Arbeit,mit Hilfe des erstellten Debuggers die Funktion für 64-Bit Architektur zu implementieren.
Der Debugger soll in C geschrieben werden, das Hauptwerkzeug wird ptrace sein. Das Zielprogramm wird vom Debugger getract werden, und kann dann jederzeit pausiert oder gestoppt werden. Somit ist serielle Abarbeitung möglich. Für bessere Bedienung des Debuggers ist eine GUI über einen Browser zugänglich. Diese ist mit dem Framework NW.js in javascript geschrieben. Die GUI ist auch in einem Desktop-Fenster realisierbar, aber es wurde sich bewusst für eine GUI im Browser entschieden, da der Nutzer dann den Browser seiner Wahl benutzen kann.