# 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 des Programms und überprüft ihn nach Fehlern. Um dies umzusetzen, muss man den Programm-Code Schritt für Schritt bearbeiten.
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 oder der Speicherbereich des getracten Prozesses verändert wird.
Ziel 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 PG, 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 die grafische Umsetzung sind mehrere Optionen zur Auswahl. Das Toolkit GTK+ bietet eine GUI in einer Fensteransicht an. Die erzeugte GUI ist simpel und in Linux weit verbreitet, dabei aber leicht bedienbar. Zudem unterstützt GTK+ eine große Reihe an Programmiersprachen.
Frameworks wie Electron oder NW.js unterstützen ebenfalls Fensteransichten und implementieren in JavaScript. NW.js Applikationen können zudem auch in HTML geschrieben werden. Somit kann auf das Fenster verzichtet werden und die GUI in Browsern geöffnet werden.