

Projekt/Bachelor-/Masterarbeit

Entwicklung einer Tracing-Visualisierung

Für die Security-Analyse von Soft- und Firmware-Binaries ist es häufig nützlich die Programmausführung als Folge von Basic Blocks zu betrachten. So kann z.B. analysiert werden, welche Programm-Teile durch einen Test zur Ausführung gebracht wurden und welche nicht. Ein Basic Block ist eine Sequenz von Assembler-Instruktionen, welche nicht durch Sprünge unterbrochen wird. Die Finale Instruktion eines Basic Blocks ist i.d.R. ein Sprungbefehl zum nächsten Basic Block.

Da die Sprünge abhängig vom Programmzustand unterschiedliche Basic Blocks als Ziel haben können (z.B. bei einer If-Anweisung), kann die Folge Basic Blocks auch als Graph (sog. Control-Flow-Graph, CFG) dargestellt werden. Ziel dieser Arbeit ist die Entwicklung einer graphischen Visualisierung für CFGs aus Programm-Ausführungs-Mitschnitten (Execution Traces).

Inhalte

- Linux
- Grafische Software-Entwicklung (evtl. als Web-Anwendung)
- Statische und dynamische Binary-Analyse
- Reverse-Engineering

Ansprechpartner

Lukas Senger  lukas.senger@tha.de

Prof. Dr. Lothar Braun |  lothar.braun@tha.de

THA_innos

Das Institut für innovative Sicherheit (THA_innos) bietet eine Vielzahl von Abschluss- und Projektarbeiten im Themenfeld der Cyber Security an. Unser Team unterstützt Studierende dabei mit Know-How und Praxiserfahrung und ist zudem offen für eigene Themenvorschläge. Durch die enge Zusammenarbeit mit der Forschungsgruppe vor Ort im MRM-Gebäude lernen Studierende sowohl das Institutsleben, als auch die aktuelle Forschung von THA_innos kennen.

Weitere Informationen auch unter <https://innos.tha.de>