Google Summer of Code

Overview

by Anton Kochkov (xvilka)

What is GSoC?

- Radare (and Cutter) participates in Google Summer of Code since 2014
- A program by Google for a summer internship to work on open source projects
- Full time, requires a lot of dedication from students and mentors
- We also also run our own Radare Summer of Code when appropriate
- A lot of improvements and new features done by the students

Contributions

- Improved Windows platform support and file formats
- Remote GDB debugging support
- Function arguments detection
- Types inference
- Various console interface improvements
- FLIRT and Yara signatures support
- Loading DWARF and PDB debug symbols
- Objective C metadata parsing
- Radeco decompiler (abandoned)

This year

- https://rada.re/gsoc/2020

- 5 proposals, 4 successfully finished.
- 2 radare2 projects, 1 cutter, 1 r2ghidra

Radare2 Projects

- Loading types information from DWARF and PDB
- Debugging and reversible debugging improvements

DWARF and PDB were parsed even before but only basics, the type information extracted wasn’t integrated into the analysis

Reversible debugging was implemented a few years ago but wasn’t complete and didn’t support non-native backends

Cutter Projects

- Decompiler widget

  Basic decompilation output as text was available before but without easy navigation, context menu and integration with the rest of Cutter. This work focused on making the r2dec, r2ghidra, retdec output in Cutter nice looking and better integrated.

R2Ghidra Projects

- SLEIGH disassembler backend

  Will allow to integrate existing Ghidra modules and tools that operate on SLEIGH architecture description level into the radare2 and Cutter.

R2Ghidra Projects

We really hope there will be students willing to work on:

- Improving exploitation capabilities
- Diffing features in both radare2 and Cutter
- Heap viewer in both radare2 and Cutter
- Parallelism
- Better integration with other tools

THANK YOU