ReOxide

Building Infrastructure for Rust Decompilation (and more!)

cluosh

February 2, 2025

Decompilation

- Compiled program back to source
  - **Or:** compiled program to understandable representation

Decompilation

- Compiled program back to source
  - **Or:** compiled program to understandable representation
- Decompilers usually produce pseudo-C code as output
  - **Implicit assumption:** Code was generated with a C compiler

Decompilation

- Compiled program back to source
  - **Or:** compiled program to understandable representation
- Decompilers usually produce pseudo-C code as output
  - **Implicit assumption:** Code was generated with a C compiler
- Works okay for understanding assembly
  - Maybe not so much for understanding **the program**

Rust and Friends

- Modern compiled languages don't map nicely to C

Rust and Friends

- Modern compiled languages don't map nicely to C
- Generics, macros blow up code size

Rust and Friends

- Modern compiled languages don't map nicely to C
- Generics, macros blow up code size
- Different control-flow (e.g. Iterators)

Rust and Friends

- Modern compiled languages don't map nicely to C
- Generics, macros blow up code size
- Different control-flow (e.g. Iterators)
- Better optimizations than C

Rust Stack Optimization

```
local_40 = i32>::fmt;
local_30 = i32>::fmt;
/* ... */
std::io::stdio::_print(&local_78);
/* ... */
local_40 = (code *)0x4;
local_30 = (code *)0x3;
std::io::stdio::_print(&local_48);
```

ReOxide

- Take existing decompiler and extend it
  - Most “production”-grade, open source decompiler is **Ghidra**

ReOxide

- Take existing decompiler and extend it
  - Most “production”-grade, open source decompiler is **Ghidra**
- Ghidra has Java plugin system for frontend
  - But no access to intermediate decompiler information
  - **ReOxide** tries to provide that

ReOxide

- Take existing decompiler and extend it
  - Most “production”-grade, open source decompiler is **Ghidra**
- Ghidra has Java plugin system for frontend
  - But no access to intermediate decompiler information
  - **ReOxide** tries to provide that
- Funded through NGI Zero Entrust
  - Currently very rough prototype
  - Next milestone: Write Plugins in other languages than C++

Ideas, Wishes, Contributions?

- Let's chat!
- ReOxide
  - https://reoxide.eu/
  - https://codeberg.org/ReOxide
- Contact me
  - contact@cluo.sh
  - @cluosh@chaos.social
  - Slides: https://cluo.sh/talks/