Diaphora

Support for r2

What have we learned? (not gonna explain again)

- Not much. jk

- Why it matters to support r2?
- How to use (demo)
- Internals
    - Refactored code
    - IDA api
    - Sqlite format
- Visualization
    - GUI required?
- Future

Who we are?

Joxean Koret (matalaz)

- Blablabla
- He presented himself already

Sergi Àlvarez (pancake)

- me
- Author of radare and other stuff
- Mobile Security Analyst at NowSecure
- Published and maintains many open-source tools like acr, valabind, .. but everything always ends up collapsing into r2

Why support r2?

- Because science
- Headless batch analysis
- Fully Open Source solution
- Helpful to compare results and features with IDA
- Useful to define a wrapper layer for the IDA api
- Experiment with different diffing tools and algorithms
- Show how easy is to use r2pipe

Use cases

- Malware indexing
  - MalTindex. An open source project that aims to help doing attribution in malware.
- Identify changes between versions of specific libraries or programs
- Patch analysis
- Others??

How to use?

Generate a database with the analysis information of the target program

- Python diaphora_r2.py target
- Sqlite output.sqlite

Diffing two databases

- Python diaphora.py a.sqlite b.sqlite

Visualizing the results

- Use your brain

Installation

As everything in r2land, it’s available via r2pm

- r2pm -i diaphora

After this we should have the diaphora command in the r2 PATH.

- r2pm -r diaphora-r2 /bin/ls

Calling it from r2

As long as the integration is done with r2pipe it is possible to use diaphora by spawning a new instance of r2 or just calling it from the current session.

So, in case for relocatable binaries we can rebase the bin if we compare with a database generated from a debugging session for example.

- r2 -i diaphora_r2.py /bin/ls

Or from the shell

- . diaphora_r2.py

Internals

- Refactored code
  - Remove all gui dependant code
  - Added separated functions that call r2 to get info
  - Add prompt for overwriting databases
- Ida api
  - Originally diaphora was written on top of the IDA api
  - Some python objects needed to be faked
  - At some point will be done in a separate module
  - Help to identify differences between r2 and IDA
- Sqlite format
  - Tables of interest
  - Benefits

Visualizing the results

How to take the diffed database and print it in a human friendly way?

- TODO: write a tool that runs a webserver to render the data

Visualizing analysis information is useful to identify bugs in the process. As well as allowing to compare between different tools, analysis commands or configurations will help us to make the r2 analysis better

Future

This is just an initial implementation, it’s far from perfect and needs

- Performance
- User Interface with options
- Better visualizations
- Integrate with r2’s hud or visual mode
- Create a community around it,
- Add a testsuite
- Create server database
- Port to other backends. (pyew?)

Q&A

--pancake+matalaz @ r2con2017