

MQP A Term Wrapup

Zachary Porter

2022-10-12

1 Problem Statement

It is currently difficult to identify the flow of "program-level"/macro logic from static or even dynamic analysis.

2 Goal Statement

I hope to use record and replay technology to allow researchers to move easily peer into a binary to find important addresses and to identify the most important instructions for "program-level" logic.

3 Minimum A-Term Deliverables

- ☒ Code capable of tracing data through a program's execution
- ☒ A plan for comparing the traces and identifying shared points between traces
- ☒ A platform for my UI that I am comfortable with
- ☒ Recording infrastructure to support scrubbing along the timeline of a program
- ☒ Tests for all code I have written (within reason)
- ☐ Documentation for all code that reasonably requires documentation
- ☐ An example use case to demonstrate value

4 Revised use case

Capturing functions from other programs.

$f(a*) \rightarrow b$

4.1 Acrobat PDF Viewer

Suppose that you have a very complicated

4.2 Zoom Get Personal Meeting Room ID

How to use: Start zoom via MQPProj Signin using auth method (username, pw) Navigate to personal page Unhide your personal meeting room id. Close.

Start MQPProj on recording that was just created. Scrub start of timeline to before signin Scrub end of timeline to seeing your personal room ID. Indicate to MQPProj the function input (username, pw) Indicate to MQPProj the output of the function (personal meeting room id) Have it generate an executable for $f(username, pw) \rightarrow personalmeetingroomid$