CPRE 491 Weekly Report #1

Team sdmay22-41

Project Title: RISC-V SoC Hardware Vulnerability Detection Toolset

Date: 9/28/2021

Members:

- Mason Korkowski -

- Micah Mundy -

- Gerald Edeh -

- Kolton Keller -

- Eva Kohl -

- Savva Zeglin -

- Magnus Anderson -

What we've accomplished in the past week/what we've been researching

- Mason Korkowski - Started researching System Verilog parsers that currently exist. Attempted to download and simulate the Pulpissimo RTL without much luck.

- Micah Mundy - Attempting to simulate the Pulpissimo RTL. Attempted to install dependencies on Ubuntu WSL, but a license is required for a core simulation tool called Questasim. To prevent team members and the client from acquiring licenses, I have requested and received a VM from ETG.

- Gerald Edeh - Researched bug 24 and found information about GPIO inputs. Rewatched HACK@DAC video to continue to gain understanding of project.

- Kolton Keller - Located bug 8. Researched the rules of the HACK@DAC competition. Classified bugs in the Bug_info.xlsx sheet.

-Eva Kohl - Researched bug 9 in the git repo. Located helpful information on git documentation for future bug categorization.

- Savva Zeglin - Classified bugs in the Bug_info.xlsx sheet

- Magnus Anderson - Tried installing Pulpissimo on a non-Ubuntu linux machine, didn't work well. Took a look at bug 12 and researched the debug unit.

What we're planning to do in the coming week

- Mason Korkowski - Continue looking for an open source System Verilog parser, and or create a basic prototype parser that pulls key functions out of System Verilog, and allows for adding classifications to the different parts.

- Micah Mundy - Continuing to install the testing environment for the Pulpissimo SoC. Working with ETG to install Questasim on the VM. Will meet with Dr. Duwe to see how he would prefer to manage the licenses with the toolkit. After the Pulpissimo SoC can be simulated, the Hack@DAC SoC will be downloaded and simulated.

- Gerald Edeh - Continue to research the bug and see if I can locate it. If not, try to find another bug to locate, and continue to gain understanding of the project.

- Kolton Keller - Revise/get feedback on the bug classifications, and fill out columns for info needed and how we intend to find bugs.

-Eva Kohl - Continue to understand and research bugs in the example git project and categorize them based on potential solutions for finding them.

- Savva Zeglin - For the bugs that we have a solid understanding of, look into tools/methods of finding said bugs. This will most likely be static analysis (i.e. using a script to parse HDL files and discover bugs like memory space overlap of peripherals, enable signals stuck on high, etc.).

- Magnus Anderson - Emulate the SoC to run programs, try to exploit one of the vulnerabilities in the SoC on the emulated machine. Take a look at Hack@Dac21 materials.

Issues we had in the previous week

- Mason Korkowski - Files seem to be missing in the Pulpissimo Repo. More research is needed to understand if this is simply an error of not looking in the right place, or if some files are assumed to be included.

- Micah Mundy - Simulating the RTL requires closed-source software with a license as a requirement called Questasim. Iowa State doesn't provide these licenses.

- Gerald Edeh - Some of the files the spreadsheet told me to look for were not present. I expanded all of the folders and would search for the file, but it was not present.

- Kolton Keller - Some of the files that are referenced in the Bug_info.xlsx sheet could not be found in the git repository.

-Eva Kohl - Actually finding the bugs in the code was challenging.

- Savva Zeglin - Some .sv files seem to be generated, so they don’t initially appear after cloning the git repository. Assuming they are generated during the build process, we will need to build the project before being able to look at the source code where some bugs exist

- Magnus Anderson - Getting the environment setup in order to run the 2018 hack@dac SoC has not been as easy as it feels like it should be, probably because I should have been on an Ubuntu VM the whole time.