CPRE 491 Weekly Report #3

Team sdmay22-14

Project Title: RISC-V SoC Hardware Vulnerability Detection Toolset

Date: 10/17/2021

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 Simulation of the 2021 new Design. Continued looking at Verilog Linters and Verilog Hierarchy Model creation.

- Micah Mundy - Demonstrated the process of compiling a C program and running it on the SoC design for this year's Hack@DAC challenge.

- Gerald Edeh - Understanding the design document process and how to use the lotus blossom technique.

- Kolton Keller - Finding out what security / other requirements we should aim for. Most likely to come from Hack@Dac 2018 info.

-Eva Kohl - Worked on the design document and worked on understanding the emulation on the VM.

- Savva Zeglin - Worked on design document, also further researched listing properties violated by bugs

- Magnus Anderson - Worked on design document, didn't get much done in terms of the emulator though unfortunately.

What we're planning to do in the coming week

- Mason Korkowski - Have a prototype for the hierarchy model creation tool done. Additionally continue work on the Linter research.

- Micah Mundy - Simulate a C program running on the SoC from Hack@DAC 2018. Attempt to parse simulation output from the SoC for this year's challenge. Establish a development environment that is conducive to testing the SoC in Java and Python.

- Gerald Edeh -Start working on testing assignment and ask questions about older bugs and their meanings.

- Kolton Keller - Make requirements and previously identified properties meet in the middle to form a list of solid properties that should not be violated by the SoC.

-Eva Kohl - Research previous requirements from other Hack@Dac competitions and continue to work on the weekly assignments given.

- Savva Zeglin - Use our working simulation of the Hack@Dac SoC to try to find/exploit known bugs

- Magnus Anderson - Find a bug in the 2021 CTF competition or look at automatically running inputs to the simulated SoC

Issues we had in the previous week

- Mason Korkowski - The motherboard in my computer that had the VM died, I lost a lot of time waiting on replacement parts. It is back up and running so I can continue working on the simulation portions of the design.

- Micah Mundy - Hack@DAC provided a Ubuntu VM that contains all software and RTL design files to compile C programs and execute them on the simulated RTL. I had no success running the VM in VirtualBox and had to resort to VMWare Workstation. Simulation also takes a very long time. (For example, 1 `printf` statement takes about 10 minutes to simulate).

- Gerald Edeh - Was confused on some aspects of the project, will ask questions with professor and teammates during future meetings.

- Kolton Keller - Finding the security requirements for Hack@Dac 2018 is challenging. So far no definitive documentation like what we have for 2021 has been found.

-Eva Kohl - I don't have a history of working with SoC chips. I took a computer science emphasis in software engineering and I'm taking a bit longer to understand some hardware things.

- Savva Zeglin - Need to do more research (i.e. find/exploit bugs on SoC) to fully understand properties violated by SoC bugs. So my understanding is still lacking in that area

- Magnus Anderson - I had 3 midterms this week and an essay due which burnt me out and didn't give me much time to focus on the project