/CprE/SE 491 WEEKLY REPORT 8

10/31/2024 – 11/7/2024

Group Number: ***27***

Project title: ***Open-Sourced Radio Microcontroller***

Client &/Advisor: ***Dr. Henry Duwe***

Team Members/Role:
Noah: *Team Organization*
Will: *Project Management*
Ibram: *Analog Design Lead*
Nathan: *Digital Peripheral Lead*
Nolan: *CPU/Memory Architecture Lead*
Ethan: *Software Lead*

- **Weekly Summary**

  This week the team focused on security research and on basic implementation for digital and analog components. Implementation work was done on a phase detector circuit for the PLL on the analog side and for a Wishbone Crossbar on the digital side. The Wishbone Crossbar will be run through hardening to attempt to gauge resource utilization to see if it is a viable option for connecting the memory-mapped components of the design, or if another option needs to be explored.

- **Past week accomplishments**
  - **Noah**
    - Reviewed PLL available from the Efabless market
    - Researched N divider design for the PLL
  - **Nolan**
    - Got the seven-segment controller project working with both of the seven-segment units. This project has been sent to December 2024 Senior Design Team 12 to include in the tape-out they are doing of various projects to go on a Caravel chip. Got the VexRISCV project running and generated a few RISCV processor hardware descriptions.

- **Nathan**
  - Began work on Wishbone Crossbar, have a baseline implementation that appears to work in simulation
- **Will**
  - Continued security analysis of microcontroller. Focused on encryption, key distribution, and side channels.
- **Ibram**
  - Looked at multiple phase frequency detector circuit topologies and ended up designing the schematics for a DFF based PFD.
  - Investigated the operating frequencies for ZigBee 3.0 in the United States.
- **Ethan**
  - Security analysis on control manipulation attack vectors for microcontrollers. Both hardware and software countermeasures for control flow manipulation attacks as well.
- **All Team Members:**

- **Pending issues**
  - **Nathan**
    - None
  - **Noah**
  - **Nolan**
    - VexRISCV regression tests fail.
  - **Ibram**
    - Simulation of XCHEM schematics are not referencing the DFF libraries in the 130nm process standard cell libraries.

- **Individual contributions**

NAME	Individual Contributions *(Quick list of contributions. This should be short.)*	Hours this week	HOURS cumulative
Noah	Researched Efabless 8x PLL and N divider for PLL	6	39
Will	Continued Security Analysis	6	33
Ethan	Security Analysis research, Caravel & ChipForge work	6	31
Ibram	Designed a PFD schematic and investigated Zigbee operating frequencies in the United States.	6	33

Nathan	Work on Wishbone Crossbar	7.5	41.5
Nolan	Finished seven- seg controller, generated RISCV cores using VexRISCV	6.8	45.8

- **Plans for the upcoming week**
  - **Will**
    - Make a more formal document of security analysis
  - **Nathan**
    - Continue work on Wishbone Crossbar, try and get utilization numbers and figure out how to check new design files into Git
  - **Ibram**
    - Fix the XSCHEM error for the PFD and start investigating the voltage-controlled oscillator circuit topologies.
  - **Nolan**
    - Continue to investigate VexRISCV to see how we can interface to it in the user area of the Caravel harness. Ideally, it would be good to have it in the user area and be able to execute some instructions even if they are manually provided to the processor over the wishbone bus instead of being put in SRAM.
  - **Ethan**
    - Continue writing the security analysis report. Focus on vulnerabilities on RF after microcontrollers.
  - **Noah**
    - Create proposal for N divider design for PLL

- **Summary of weekly advisor meeting**

  We started the meeting discussing how the PFD (Phase Frequency Detector) works and fits into our overall design. We discussed a way to implement the PFD with Flip-Flops with Duwe as well as the advantages and disadvantages that come with it. Our next topic was ZigBee regional operating channel frequencies. There are a couple different methods we can use, ZigBee documentation has 25 channels that are spaced 1 MHz apart, but we also found an example of a microcontroller that only uses 10 channels that are 2 MHz apart. Our final topic was the start of our security analysis. We discussed why we want to use AES encryption as well as some possible vulnerabilities in possible control flow manipulation or side channel attacks.