Student Assistant for the Vulnerability Detection on High Performance RISC-V processor with Hardware Fuzzing

There are multiple high performance open-source RISC-V processors coning out recently that is designed to be competitive with the industry. This project (current job position) focuses on enhancing the security of these processors by detecting vulnerabilities through hardware fuzzing techniques. Hardware fuzzing involves generating random or semi-random test inputs to trigger and expose potential security flaws in the processor's architecture, design, and implementation. By applying fuzzing strategies, this project aims to uncover weaknesses that could lead to security exploits, thus contributing to the development of secure hardware systems.

We seek excellent student assistants motivated to be part of ongoing research in these areas and contribute to cutting-edge research in processor security. As a student assistant, you will gain hands-on experience in applying fuzzing techniques to detect real-world vulnerabilities. You will be supervised with a dynamic team of hardware security experts, making a tangible impact on the future of secure RISC-V processors.

Your tasks include:

- Design and implement hardware fuzzing techniques tailored to RISC-V processors architecture.
- Develop fuzzing harnesses and testing frameworks to automate vulnerability detection.
- Analyze the results of fuzzing campaigns to identify, categorize, and document potential security vulnerabilities.

Prerequisites

- Interest in hardware security, vulnerability research, and secure processor design.
- Solid understanding of computer architecture, particularly RISC-V architecture.
- Proficiency in hardware description languages (HDL), such as Verilog or VHDL
- Experience with fuzzing tools and techniques.
- Experience with artificial intelligence (AI) or generative AI is a plus.
- Ability to work independently and strong motivation
- Ability to collaborate effectively in a team

Contact

If you are intrigued by this cutting-edge subject, please get in touch with Dr. Lichao Wu, Dr. Huimin Li, and Mr. Mohamadreza Rostami at *info@trust.tu-darmstadt.de* to obtain further information. To facilitate the process, kindly include **a summary of your academic background** and a copy of your **transcripts**.

Technische Universität Darmstadt
FB Informatik – System Security Lab
S2|20 (CYSEC Gebäude)
Pankratiusstraße 2
64289 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

September 2024