Student Assistant for the Artificial Intelligence-assisted Hardware Fuzzing

Fuzz testing is a technique that involves overwhelming target device with a large number of test cases to identify problems like memory crashes or other invalid or undefined behaviors. Building on the principles of software fuzzing, hardware fuzzing has gained traction as a method for identifying vulnerabilities in hardware and processors with minimal human involvement. Recent research shows strong capabilities of hardware fuzzing in testing across multiple processor cores. Its ability to identify vulnerabilities efficiently has made it a valuable tool in ensuring hardware security in increasingly complex computing environments.

Despite the advantages mentioned above, hardware fuzzing faces several challenges. For instance, **complexity of input semantics** is commonly overlooked by the hardware fuzzer. Existing approaches neglect these crucial aspects, focusing on basic instruction mutations. Besides, existing fuzzers receive **limited feedback** from hardware. This limited feedback causes hardware coverage to plateau quickly. Finally, hardware fuzzing is **inefficient**. The existing fuzzers require a large number of test cases to detect specific vulnerabilities. Considering the substantial overhead involved in hardware simulation and execution of test cases and the time constraints typically imposed during security evaluations, the vulnerability detection capability of the hardware fuzzing becomes limited. We aim to apply Artificial Intelligence in augmenting the performance of hardware fuzzing regarding the test case generation, hardware simulations, and bug detections.

We seek excellent student assistants motivated to be part of ongoing research in these areas and investigate the application of Artificial Intelligence (AI)-assisted hardware fuzzing. As a student assistant, you will gain hands-on experience with machine learning and hardware fuzzing, providing valuable skills in AI-driven hardware-level security.

Your tasks include:

- Developing novel AI-assisted hardware fuzzer.
- Conducting experiments on different hardware cores to validate its effectiveness.

Prerequisites

- Strong understanding of deep learning and generative AI.
- Prior experience with Deep Learning frameworks such as Pytorch or Tensorflow
- Prior knowledge with computer architecture and low-level hardware language (recommended)
- 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 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